Project 2

Investigation of a Data Breach

Cyber Security Internship

At

Extion Infotch

Prepared by

Devesh Kapase

Sr. No.	Content	Page No.

Table of Contents

Introduction to Cybersecurity

Cybersecurity is an essential discipline in protecting sensitive information and infrastructure from malicious activities. The digital era has introduced sophisticated threats that require robust security measures to mitigate risks effectively. This report delves into the investigation and resolution of a data breach incident at ABC Secure Bank, a prominent financial institution known for its commitment to security and trust. The purpose of this document is to provide an in-depth analysis of the breach,

covering its origin, progression, and resolution, while offering actionable strategies to mitigate future risks.

The investigation focuses on uncovering the technical details of the breach, assessing its impact on stakeholders, and outlining key compliance and communication

measures.

The primary objectives of the report are:

1. Determining the root cause of the breach and identifying security vulnerabilities.
2. Analyzing the extent and scope of the compromised data.
3. Crafting efficient strategies for containment, recovery, and remediation.
4. Ensuring full compliance with relevant regulations and industry standards.
5. Recommending robust, long-term security measures to safeguard the organization.

2. Threat Landscape Overview

Scenario Overview

During a routine security audit, ABC Secure Bank, a renowned financial institution, discovered a significant data breach. Anomalies detected in database activity logs raised concerns about unauthorized access to sensitive client data, including names, account numbers, and transaction histories. This breach severely jeopardized the bank's reputation, regulatory compliance, and customer privacy.

Detailed Scenario

Breach Discovery: Suspicious patterns of database access were identified through regular monitoring, raising alarms about potential unauthorized activity.
Impact: The breach exposed millions of customer records, including transaction data and personally identifiable information (PII), to unauthorized access.
Attacker's Methods: The attackers exploited a vulnerability in an outdated software component, specifically an unpatched API endpoint.
Exfiltration Timeline: The breach persisted for over three months, allowing attackers to exfiltrate data in stages, avoiding detection through careful batch processing.

Challenges Faced

Delayed Detection: Gaps in continuous monitoring allowed the breach to remain undetected for an extended period.
Regulatory Pressures: Ensuring compliance with regulations like the CCPA and GDPR, including timely breach notification, was a critical priority.
Customer Trust: Restoring customer confidence in the wake of such an event required transparent communication and proactive support measures.

3. Investigation Process

i. Incident Response Preparation –

When ABC Secure Bank first discovered anomalies during a routine security check, the breach raised immediate concerns regarding the safety of customer data. To ensure a swift and coordinated response, the bank quickly activated its incident response plan. This initial preparation focused on effective containment, analysis, and resolution. Key actions included:

- **Multidisciplinary Incident Response Team:** A team of IT security experts, legal advisors, and communication specialists was assembled to address the breach comprehensively. Each member had defined roles to address technical, legal, and public relations concerns.
- **Initial Assessment of Critical Systems:** The incident response team quickly evaluated critical systems to understand the full extent of the breach. Systems containing sensitive customer data were prioritized to ensure no further unauthorized access could occur.
- **Isolation of Affected Systems:** The team immediately isolated the vulnerable application and any other affected systems to prevent further exploitation by the attackers. Disconnecting the affected systems from the network ensured the breach would not continue while the investigation was underway.

ii. Evidence Collection –

To build a thorough investigation and ensure data integrity, forensic analysts took detailed steps to preserve evidence related to the breach. The evidence collection process was pivotal in determining the scope of the breach and understanding the methods of attack. Key actions included:

- **System Replication and Imaging:** Forensic teams created exact copies of the compromised systems to preserve the state of critical logs, configurations, and application states.
- **Securing Database Backups:** Analysts also secured database backups that might contain additional information about the attackers' actions, including the logs showing exfiltrated data.
- **Use of Checksum Tools for Evidence Integrity:** To maintain the authenticity and integrity of the collected evidence, checksum tools were employed to ensure that no data was altered or tampered with during the investigation.
- **Log and Configuration Collection:** Analysts gathered all relevant logs,

configurations, and communication logs to trace back the source of the attack, the timeline of events, and the methods used to exploit system vulnerabilities. Analyzing Attack Vectors-

A deep and detailed investigation was carried out to understand the attack vectors used by the

perpetrators to gain unauthorized access. The analysis focused on identifying the point of entry, the attack methods employed, and the specific vulnerabilities that were exploited. Key findings included:

- **Point of Entry:** Forensic investigation determined that the attackers exploited a vulnerability in an outdated software application, which was part of the bank's infrastructure. The application had an unpatched API endpoint that was vulnerable to a known exploit, which had been publicly disclosed.
- **Attack Methods (SQL Injection):** The attackers used SQL injection techniques, a well-known attack vector, to bypass authentication and access sensitive

customer data. They executed fraudulent SQL queries that allowed them to gain unrestricted access to the bank's customer database, which contained personally identifiable information (PII) and financial data.

- **Exploitation Timeline:** The attack began with automated tools used by the attackers to scan for unpatched systems.
- **Exploit Methodology:** The attackers were able to exfiltrate customer data in batches, likely to avoid detection by security systems.

iii. Compliance and Legal Considerations-

Given the sensitive nature of the breach, it was imperative that ABC Secure Bank ensured compliance with data protection regulations and handled the legal aspects of the incident carefully. In the wake of the breach, ensuring compliance with regulatory standards was a critical priority:

- GDPR and CCPA Adherence: Notifications were sent to affected customers and relevant regulatory bodies within the mandated timeframes.
- Legal Coordination: Legal teams worked closely with law enforcement to identify the perpetrators, assess liabilities, and prepare for potential litigation.
- Documentation: Comprehensive records of the breach and all recovery actions were maintained to support audits and compliance reviews, ensuring full transparency and legal preparedness.

iv. Communication Strategies-

Clear and transparent communication was vital to maintaining trust and ensuring all stakeholders were informed:

- **Internal Communication:** Regular updates were provided to executive teams, IT staff, and legal advisors to ensure coordinated response efforts.
- **External Communication:** Customers were notified promptly about the breach and given clear instructions on how to protect their personal information, such as updating passwords and monitoring their accounts.
- **Regulatory Communication:** Reports detailing the breach, its scope, and the

remedial actions taken were submitted to relevant authorities to ensure regulatory compliance.

vi Lessons Learned and Improvement-

In the aftermath of the breach, ABC Secure Bank focused on enhancing its security posture to prevent future incidents:

- **Employee Training:** Ongoing cybersecurity training programs were initiated to raise awareness among employees about common threats like phishing and social engineering.
- **Advanced Threat Detection:** The bank deployed Security Information and Event Management (SIEM) systems to provide real-time threat intelligence and alerts, strengthening the ability to detect and mitigate future attacks.
- **Network Segmentation and Data Encryption:** Sensitive systems were isolated within segmented networks to limit access, and encryption protocols were enforced for both stored and transmitted data to reduce exposure risks.

- **Third-Party Audits:** Regular third-party security assessments were initiated to ensure that external vendors adhered to the bank's strict security standards.

4. Conclusion

The ABC Secure Bank breach underscores the necessity of proactive cybersecurity measures. Key takeaways include:

1. The importance of addressing software vulnerabilities promptly.
2. Developing robust incident response and recovery plans.
3. Emphasizing transparent communication and regulatory compliance.
4. Fostering a culture of cybersecurity awareness and continuous improvement.

By leveraging advanced threat detection tools and prioritizing data protection, organizations can mitigate risks and build resilience against future cyber threat