INVESTIGATION OF A DATA BREACH ON ABC SECUREBANK

CHANDAN KUMAR

Aim : Investigation of a Data Breach on ABC SecureBank

- Incident Analysis
- Forensic Analysis
- Data Recovery
- Regulatory Compliance
- Communication and Notification
- Post-Incident Review

WHAT IS DATA BREACH

- Data Breach means accessing someone's data without knowing them or without any authorization. Data Breach also called data leaking or information leaking. Data can be of any type it may be health-related data, can be business-related data, or any other sensitive data. Someone may be done intentionally or unintentionally and can use it to harm you personally or financially. Data breach now becomes a very popular attack in the field of hacking. Many growing hackers try these types of attacks to enhance their skills

  A data breach can affect anyone in different ways of damage to down the company or someone's reputation, and it can also affect the client of the companies

➢ Incident Analysis

•**Description of the Breach:**

Date of breach: 09 February 2024

Number of affected customers: Approximately 7.6 million

Types of data compromised: Personal identification information, account details, and financial data.

•**How the Breach Occurred:**

The bank was targeted by a LockBit ransomware attack, which initially went unrecognized and was misdiagnosed as a hardware issue.

Point of Entry:

The breach was caused by unauthorized parties breaching into the bank's network. The breach was likely caused by a cyber attack.

➢ Forensic Analysis & Data Recovery

Initial Misdiagnosis : One of the biggest challenges in the breach was that the initial symptoms of the cyberattack were misinterpreted as hardware issues. This could have stemmed from the initial absence of clear signs of malicious activity, common in sophisticated cyberattacks. Such incidents often begin subtly, with disruptions that mimic hardware or software failures, leading IT teams to look for technical faults rather than security breaches.

Due to the latency in proper identification, the ransomware had time to spread unfettered, increasing the attack's impact. Without appropriate early detection, the organization could not take mitigating steps, leading to widespread data compromise. Even without early detection, proactive steps to prevent such data loss would have also significantly mitigated this breach.

Response & Mitigation : This attack compromised the personal information of approximately 7.6 million individuals, including names, Social Security numbers, bank account numbers, and contact information.
After realizing that the disruptions at the bank were not due to hardware issues but a ransomware attack, the bank took swift action to mitigate the damage. Immediate steps included shutting down affected systems to contain the spread of the ransomware and initiating a comprehensive investigation with the help of cybersecurity experts. In the long term, the bank implemented enhanced security protocols to fortify its defenses against future attacks.

➢ Regulatory Compliance

ABC SecureBank has confirmed in a filing with the local Attorney General that 7,640,112 individuals were affected in a data breach it experienced in February.

In its notice of data breach letter, the bank wrote that it identified systems that were not operating correctly and assumed it to be hardware failure, only to discover the presence of unauthorized activity.

After initiating incident response processes, the bank launched an investigation with third-party experts to determine the nature and scope of the breach. The financial services company reports that the threat actors did not access any customer funds; however, they were able to access and download customer information from the company's database, as well as a file share.

➢ Communication & Notification

The bank sent online notice to all customers affected by the breach. To support customers whose personal information had been compromised, the bank offered credit monitoring and identity protection services, providing some reassurance in the wake of the breach.

Notification and Protection Services

•Type of Notification: **Electronic**
•Date(s) of consumer notification: **July 08, 2024**
•Were identity theft protection services offered: **Yes**

➢ Post-Incident Review

Prior to the incident, ABC SecureBank had a significant number of cybersecurity measures in place. Since becoming aware of the incident, the bank has taken steps to further strengthen its security response protocols, policies and procedures, and its ability to detect and respond to suspected incidents.

Recommendations

•Enhance Cybersecurity Measures:

- Implement multi-factor authentication for all employee accounts.
- Regularly update and patch security systems to address vulnerabilities.

•Employee Training:

- Conduct regular training sessions on recognizing phishing attempts and other cyber threats.

•Incident Response Plan:

- Develop a comprehensive incident response plan to quickly address future breaches.

Conclusion

The data breach at ABC SecureBank highlights the critical need for robust cybersecurity practices in the banking sector. By implementing the recommendations outlined in this report, the bank can enhance its security posture and better protect its customers' sensitive information.

References

https://votiro.com/blog/the-evolve-bank-breach-and-the-rising-ransomware-tide/#:~:text=Understanding%20the%20Financial%20Data%20Breach,misdiagnosed%20as%20a%20hardware%20issue.

https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a2e61e38-f78d-403d-9abb-3810771bb5d2.html

https://www.maine.gov/cgi-bin/agviewerad/ret?loc=697