Case Study

Ransomware Attack

Company/Affected parties:
Bank of America &
Infosys McCamish Systems

Attack Category: Ransomware Attack

Ransomware is a type of malware that encrypts a victim’s data or systems, demanding a ransom for decryption. Attackers may also threaten to leak the data if the ransom isn’t paid.

Statistic:
In 2023, there were a reported 2,814 ransomware incidents globally, leading to the breach of 8,214,886,660 records. This statistic underscores the alarming frequency and scale of ransomware attacks, highlighting the significant threat they pose to organizations across industries, including the financial sector.

Example:
For Bank of America and Infosys McCamish Systems, the ransomware attack resulted in the compromise of sensitive data, including nonqualified deferred compensation plans, highlighting the severe consequences such attacks can have on financial institutions and their customers.

Sources:
The Cyber Express
Fintech Futures
TechRadar
Times of India

Company Description and Breach Summary

Company Descriptions:

- **Bank of America:** A leading financial institution offering banking, investment management, and other financial and risk management products and services.
- **Infosys McCamish Systems:** A provider of platform-based insurance process management solutions and services to the life insurance industry.

Security Incident Summary:

- **Data Breach Source:** The breach originated from a cyberattack on Infosys McCamish Systems, affecting Bank of America customers.
- **Data Compromised:** Personal information including names, Social Security numbers, and financial account details were accessed without authorization.
- **Impact:** 57,028 individuals were affected by the breach.
- **Response:** Infosys McCamish Systems engaged a third-party forensic firm for investigation and recovery, and Bank of America notified the impacted customers.

This incident underscores the importance of robust cybersecurity measures and the potential risks associated with third-party service providers. It also highlights the need for timely communication and response to protect customer data and maintain trust.

Timeline

This sequence of events outlines the progression of the breach and the response from both Infosys McCamish Systems and Bank of America. It highlights the importance of timely detection, communication, and response in managing cybersecurity incidents.

1. **October 29, 2023**:
   The data breach occurred.

2. **October 30, 2023**:
   The cybersecurity event was first detected.

3. **November 3, 2023**:
   Infosys McCamish Systems became aware of the cyberattack, leading to certain applications and systems becoming inaccessible.

4. **November 24, 2023**:
   Infosys McCamish Systems notified Bank of America about the potential impact on their customers' data.

5. **February 6, 2024**:
   Bank of America began contacting affected customers by sending notification letters regarding the data breach.

6. **February 15, 2024**:
   Bank of America filed a notice of the data breach with the Attorney General of Texas.

Vulnerabilities

The data breach at Infosys McCamish Systems, which impacted Bank of America, involved unauthorized access to sensitive customer information, including names, Social Security numbers, and financial account details. Over 57,000 individuals were affected. The breach was a result of a cyberattack on Infosys McCamish Systems, highlighting the risks associated with third-party service providers. The incident underscores the need for enhanced security measures, better risk management with third-party vendors, and faster breach detection and response protocols to protect sensitive customer information.

Third-party Service Provider Risk:

The breach occurred through Infosys McCamish Systems, indicating a risk associated with third-party vendors managing sensitive data.

Inadequate Security Measures:

The attackers were able to exploit vulnerabilities in the systems managed by Infosys McCamish Systems, suggesting that the security measures in place were insufficient.

Delayed Detection and Response:

There was a delay in detecting the breach and responding to it, which allowed the attackers more time to exploit the accessed data.

Lack of Robust Encryption and Monitoring:

The breach could indicate that the data was not encrypted robustly enough, and there was inadequate monitoring to detect unusual activities promptly.

Costs and Prevention

Costs

- Remediation, restoration, and communication efforts incurred costs around $30 million.
- Additional costs for indemnities or damages/claims are indeterminable currently.

Prevention

- Engage a third-party forensic firm for recovery and system rebuilding.
- Correct malicious activity and enhance response capabilities.
- Offer complimentary identity theft protection services to affected customers.
- Implement system changes to prevent the disclosure of sensitive data.
- Regularly monitor credit reports and account statements for signs of fraud.
- Change passwords and security questions for online accounts to bolster security.