**Investigation of a Data Breach in an ABC bank**

August 8, 2024

Investigated by: Sheik Abdul Basith

# Table of Contents

1. Objective
2. Scenario Overview
3. Tasks and Findings
   1. Incident Analysis
   2. Forensic Analysis
   3. Data Recovery
   4. Regulatory Compliance
   5. Communication and Notification
   6. Post-Incident Review
4. Conclusion

# Objective

This report's goal is to look into a data breach that occurred at a fictitious but very respectable financial institution called ABC Secure Bank. How the breach happened, the amount of damage, forensic analysis, data recovery, compliance with regulations, communication tactics, and post-incident evaluation are all covered by the inquiry. This case evaluates forensic and investigative abilities in managing a data breach.

# Scenario Overview

* **Company Name:** ABC Secure Bank
* **Breach Discovery:** Discovered during a routine security audit check
* **Scope of Breach:** Potential exposure of sensitive customer data, including names, account numbers, and transaction history

# Tasks and Findings

1. **Incident Analysis**

**Objective:** Examine the circumstances around the breach, identify the point of entry, the size of the breach, and the duration of the breach.

**Findings:**

* + **Point of Entry:** The compromise was linked to an employee's inadvertent opening of a phishing email. The employee's PC was infected with malware thanks to a malicious link in this email.
  + **Extent of Breach:** Attackers were able to enter the internal network thanks to the virus. They then had access to a database that held data on client accounts.
  + **Timeframe:** Before it was found during a normal security check, the hack had been operational for around two weeks.

1. **Forensic Analysis**

**Objective:** Conduct digital forensics on the affected systems to identify malware or any suspicious activities. Gather evidence and collect logs.

**Findings:**

* **Malware Identified:** The malware discovered was a Remote Access Trojan (RAT) named "RAT-X." This RAT enabled attackers to remotely control the infected computer and access the network.
* **Logs and Evidence:** Network logs revealed unusual activity originating from the compromised employee's computer, including unauthorized database queries and attempts at data exfiltration.
* **Additional Tools:** Attackers utilized legitimate administrative tools for lateral movement within the network, complicating detection efforts**.**

1. **Data Recovery**

**Objective:** Identify the type and amount of customer data that may have been exposed. Create a strategy for data recovery and incident containment.

**Findings:**

* + **Data Exposed:** Approximately 80,000 customer records, including names, account numbers, and transaction history, may have been exposed.
  + **Data Recovery Strategy:**
* **Containment:** Isolate and remove the infected computer from the network.
* **Backup Restoration:** Restore affected databases from backups taken before the breach.
* **Enhanced Monitoring:** Implement enhanced network monitoring to detect any further suspicious activity.

1. **Regulatory Compliance**

**Objective:** Take into account the legal and regulatory aspects of the data breach and ensure the company complies with all reporting requirements.

**Findings:**

* Regulatory Requirements: According to data protection regulations (e.g., GDPR, CCPA), the company must notify affected customers and regulatory bodies within a specified timeframe.
* Compliance Steps:
* Notify relevant data protection authorities within 72 hours of discovering the breach.
* Inform affected customers about the breach, detailing the compromised data and steps taken to mitigate the impact.
* Provide ongoing updates to regulatory bodies as new information becomes available.

1. **Communication and Notification**

**Objective:** Create a communication plan to notify affected customers, stakeholders, and regulatory bodies. Ensure the communication is clear and complies with privacy laws.

**Findings:**

* + **Communication Plan:**
* **Customers:** Notify affected customers via email and letter, providing details about the breach, the exposed information, and recommended actions, such as monitoring their accounts for suspicious activity.
* **Stakeholders:** Conduct meetings with key stakeholders to explain the breach, its impact, and the measures being taken to address it.
* **Regulatory Bodies:** Submit a comprehensive incident report to relevant authorities, including a timeline of the breach and the remediation steps taken.

1. **Post-Incident Review**

**Objective**: Once the breach has been contained and mitigated, perform a detailed review to identify vulnerabilities in the security posture and offer recommendations for enhancing security measures.

**Findings:**

* + **Security Weaknesses Identified:**

- Insufficient employee training on phishing threats.

- Lack of adequate network segmentation, enabling lateral movement of attackers.

- Inadequate monitoring of network activity for suspicious behavior.

* + **Recommendations:**

**- Training:** Implement regular cybersecurity training for all employees, with a focus on phishing and social engineering threats.

**- Network Segmentation:** Enhance network segmentation to restrict access to sensitive data.

**- Monitoring:** Improve network monitoring and deploy intrusion detection systems (IDS) to detect and respond to suspicious activity more rapidly.

**- Regular Audits:** Conduct more frequent security audits and vulnerability assessments.

# Conclusion

* The investigation into the data breach at ABC Secure Bank uncovered critical weaknesses in the company’s security posture. By implementing the outlined steps
* Such as incident analysis, forensic investigation, data recovery, regulatory compliance, communication, and post-incident review
* The company can effectively address the breach and bolster its defences against future attacks. This thorough approach not only resolves the immediate breach but also promotes long-term security enhancements.