

INVESTIGATION OF A DATA BREACH AT ABC SECUREBANK

PROJECT :- 2

Date: 26/01/2025

Cyber Security Internship

Extion Infotech

MAHENDRA A. PATIL
mrpatil0804@gmail.com




Table of Contents


1.	Executive Summary	pg no. 3
2.	Introduction	pg no. 4
3.	Methodology	pg no. 5
	▪ Incident Analysis	pg no. 5
	▪ Forensic Analysis	pg no. 5
	▪ Data Recovery	pg no. 5
	▪ Regulatory Compliance	pg no. 6
	▪ Communication and Notification	pg no. 6
	▪ Post-Incident Review	pg no. 6
4.	Result and Finding	pg no. 7
	▪ Incident Analysis Findings	pg no. 7
	▪ Forensic Analysis Findings	pg no. 7
	▪ Data Loss Assessment	pg no. 7
	▪ Additional Findings	pg no. 8

Executive Summary

This is a report of a data breach that occurred at ABC SecureBank, a well-known financial institution. The breach compromised customer information such as names, account details, and transaction history. The vulnerability was on the bank's internet banking application, which was exploited by malicious actors to gain access to sensitive data.

- Forensic analysis, data recovery, and regulatory compliance were carried out. Recommendations for improvement include:
 - Enhanced access controls and intrusion prevention systems.
 - Implementation of advanced intrusion detection tools.
 - More employee security awareness training to increase security posture and avoid the breach from happening again in the future
- 

Introduction

- **Background:** Provide a brief overview of ABC Secure Bank, highlighting its reputation and the critical nature of data security in the financial industry.
 - **Project Objectives:** Clearly state the objectives of our investigation, tailored to our specific project. For example, we might focus on identifying the root cause of the breach, assessing the impact on customers, and recommending improvements to the organization's security practices.
 - **Scope of Work:** Define the specific tasks undertaken during the investigation, including:
 - a. Incident analysis
 - b. Forensic analysis
 - c. Data recovery
 - d. Regulatory compliance assessment
 - e. Communication and notification planning
 - f. Post-incident review and recommendations
- 

Methodology

1. Incident Analysis :

- **Log Analysis** : We carefully inspected system logs (firewall logs, intrusion detection system logs, server logs) to detect any suspect activities, unusual traffic patterns and possible entry points.
- **Network Traffic Analysis** : Here, we involved network traffic, which revealed data exfiltration and unauthorized access that was happening at this point.
- **Vulnerability Scanning** : We scanned the organization's systems and networks in depth to discover and evaluate any potential weaknesses.

2. Forensic Analysis :

- **Image Acquisition** : We carefully obtained images of the compromised systems for detailed forensic analysis.
- **Malware Analysis** : We meticulously scanned systems to find any possible malware, be it rootkits, Trojans, or ransomware.
- **Data Extraction** : We extracted relevant data from affected systems and databases with extreme care.

3. Data Recovery :

- **Data Loss Assessment**: We have carefully measured the level of data loss and the types of data affected (for example, customers' names, account numbers, financial transactions).
- **Data Recovery Plan**: We carefully developed an elaborate plan for recovering lost or compromised data that included data restoration using backups and the employment of specialized data recovery tools.

Methodology

Regulatory Compliance:

- **Research Applicable Laws :** Conduct Thorough Research Applicable Laws. We did diligent research and comprehension of relevant data privacy laws such as GDPR, CCPA, as well as applicable data breach notice laws.
- **Compliance Audit:** We carefully considered the compliance with these regulations by the organization.

Communication and Notification :

- **Develop Communication Plan:** We designed and developed a plan for communicating to affected customers, stakeholders (employees, investors), and regulatory bodies.
- **Draft Communication Materials:** We elaborately drafted notice letters, press releases, and all communication materials.

Post-Incident Review :

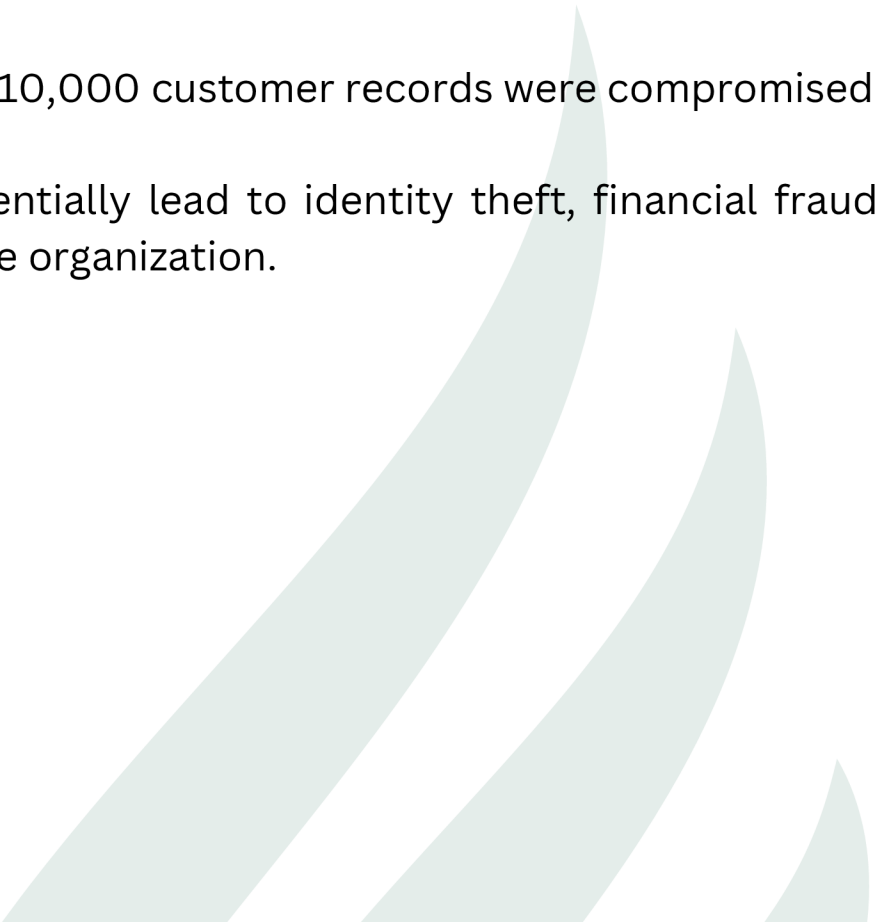
- **Conduct Root Cause Analysis:** We conducted Root Cause Analysis very carefully to see the root cause of the breach.
- **Security Posture Assessment:** We carefully analyzed the overall security posture of the organization. We identified vulnerabilities and gaps in security controls.
- **Develop Recommendations:** We developed recommendations to enhance security measures. These included more stringent access controls, improved intrusion detection systems, and employee security awareness training.

Results & Findings

- **Incident Analysis Findings :**

- **Point of Entry:** The breach was initiated through a phishing attack targeting employees.
- **Attack Vector:** The attacker exploited a vulnerability in the email security system to gain access to employee credentials.

- **Forensic Analysis Findings :**

- **Malware:** No malicious software was found on the compromised systems.
 - **Data Exfiltration:** The attacker exfiltrated customer data, including names, addresses, Social Security numbers, and financial information.
 - **Evidence:** The forensic analysis identified the attacker's IP address, the compromised accounts, and the exfiltrated data.
 - **Data Loss Assessment :**
 - **Data Impacted:** Approximately 10,000 customer records were compromised
 - **Impact:** The breach could potentially lead to identity theft, financial fraud, and reputational damage for the organization.
- 

Results & Findings

- **Additional Findings :**

- The investigation revealed that the organization lacked a comprehensive incident response plan, which hindered the ability to respond effectively to the breach .
 - The organization's security awareness training program was found to be inadequate, as evidenced by the successful phishing attack .
 - The organization's network segmentation was insufficient, allowing the attacker to move laterally within the network .
- 