EXTION INFOTECH PROJECT 2

INVESTIGATION OF DATA BREACH

By – Sai Raghavendra . Baswa

Application id/ registration number-SAIR200472

# Table of Contents

1) Objective

2) Scenario Overview

3) Tasks and Findings

3.a) Incident Analysis

3.b) Forensic Analysis

3.c) Data Recovery

3.d) Regulatory Compliance

3.e) Communication and Notification

3.f) Post-Incident Review

4) Conclusion

# Objective:

The objective of the given report is to investigate a data breach that recently occurred at a fictional

but highly reputable financial institution known as ABC Secure Bank. It outlines how this breach occurred, the extent of the damage, forensic examination, data recovery, recommendations to the applicable regulation, communication strategy, and after event assessment. This case assesses forensic and investigative skills in response to a data breach.

# Scenario:

There has been a data breach at a renowned website, and your task is to investigate this breach.

While the website's name is fictional, the scenario will test your investigative and forensic skills.

**Details** : ABC Secure Bank, a highly reputable financial institution.

**Breach Discovery**: The breach was discovered during a routine security audit, and it appears that

sensitive customer data may have been exposed.

**Scope of Breach**: The breach involves potential exposure of customer account information, including names, account numbers, and transaction history.

# Tasks and Findings:

**1) Incident Analysis**

*Objective*: Investigate the situation of the breach, determine the point of entry, the magnitude of the breach, and the time span of the breach.

*Findings:*

*• Point of Entry*: The breach was traced to an employee's accidental opening of a phishing email. The employee's PC became infected with malware due to a malicious link in this email.

• *Extent of Breach*: The attackers were able to gain access to the internal network(due to virus).They obtained access to the network. A database containing account information for each client was made available to them.

• *Period:* Before discovery through a scheduled security scan .The hack was active for roughly two weeks.

**2) Forensic Analysis**

*Objective*: Perform a digital forensic examination of the impacted systems to trace malware or any kind of suspicious activities. Collect all evidence and logs.

*Findings:*

• *Malware Found*: The malware that was found is a Remote Access Trojan (RAT) called "RAT-X." This RAT let the attackers to remotely gain control of the infected computer as well as into the network.

• *Logs and Evidence*: Network logs showed unusual activities coming from the compromised employee's computer, like unauthorized queries on the databases and attempts of data ex filtration.

• *Additional Tools*: The attackers used legitimate administrative tools for lateral movement within the network, making it difficult to detect.

**3) Data Recovery**

*Objective:* Determine what type and quantity of customer information may have been compromised. Outline a plan to recover data and contain the breach.

*Findings:*

*• Exposed Data*: An estimated 80,000 customer records, containing names, account numbers, and transaction history, could have been accessed.

*• Data Recovery Plan*

1) *Containment:* Isolate and remove the infected computer from the network.

2) *Backup Restoration*: Restore affected databases from backups prior to the breach.

3 ) *Network Monitoring*: Deploy enhanced network monitoring to detect any more suspicious activity.

4) **Compliance with Regulation**

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

*Findings* :

*• Regulatory Requirements*: As per data protection regulations (e.g., GDPR, CCPA), the company must inform the affected customers and regulatory bodies within a specified time frame.

*• Compliance Measures*: Notify the relevant data protection authorities within 72 hours of discovering the breach. Inform the affected customers about the breach, describing the Compromised data and steps taken to mitigate the impact. Ongoing updates to regulatory bodies as new information becomes available.

5) **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:* Hold meetings with the key stakeholders to explain the breach: its impact, and measures to correct it.

• *Regulatory Bodies*: Report the incident in detail to relevant authorities, including a timeline of the breach and the remediation steps taken.

6) **Post-Incident Review**

*Objective:* After the breach is mitigated and contained, conduct an in-depth review to determine areas of vulnerability within the security posture and provide recommendations for improving the security controls.

*Findings:*

• Security Weaknesses Identified : Lack of sufficient employee training on phishing threats. Insufficient network segmentation, allowing lateral movement. Inadequate monitoring of network activity for suspicious behavior.

• *Recommendations:*

1. *Training:* Conduct frequent cyber security training with all employees on focus on Phishing and Social Engineering.
2. *Network Segmentation* : Upgrade Network segmentation in order to limit access to sensitive data.
3. Monitoring: Increase network monitoring and deploy IDS to detect suspicious activity faster and then respond to it.
4. *More frequent auditors*: Conduct more frequent security audits and vulnerability assessments.

# Conclusion:

The investigation into the data breach of ABC Secure Bank revealed basic vulnerabilities in the company's security posture.

In implementing the steps listed which include incident analysis, forensic investigation, data recovery,

regulatory compliance, communication, and post-incident review, the company can appropriately respond to the breach and enhance its defenses against any future attacks.

This comprehensive process not only solves the immediate breach but also facilitates long-term security improvements.