DATA-THEFT Incident Response Playbook

Redback Operations

Version	Modified By	Approver	Date	Changes made
0.1	Devika Sivakumar		13 April 2024	First draft
1.0	Devika Sivakumar	Joel Daniel	29 April 2024	Approved for publishing.

Contents

1. Introduction

An organization's reputation may be harmed, confidential data may be compromised, and financial losses may ensue from data theft occurrences. To minimise the effects of data theft events and protect organisational assets, this playbook offers methods and principles for doing so.

1.1 Overview

A structured approach for identifying, containing, mitigating, and recovering from data theft events is described in the data theft incident response playbook. To enable a well-coordinated and efficient response effort, it sets roles, duties, and protocols.

1.2 Purpose

This playbook's goals are to:

- Establish a uniform framework for handling situations involving data theft.
- Make sure that data breaches are promptly detected and contained.
- Reduce the negative effects that data theft events have on the stakeholders, the organization's operations, and its reputation.
- Encourage response teams and stakeholders to collaborate, coordinate, and communicate with one another.

1.3 Attack Definition

Unauthorised access to, exfiltration of, or exposure of confidential company information is referred to as data theft. This can contain financial information, confidential information, intellectual property, and personally identifiable information (PII). Incidents of data theft can be caused by several techniques, including as malware, social engineering, phishing, external assaults, and insider threats.

1.4 Scope

Any incidences of data theft affecting the systems, apps, networks, and data assets of the company are covered by this playbook. It includes events that have an impact on both internal and external stakeholders, such as partners, customers, staff members, and outside vendors. Regardless of the origin or mode of attack, instances involving both purposeful and accidental data theft are included in the scope.

2. Attack Types

The different types of Data-Theft attacks include:

2.1 Insider Threat

An insider threat is when someone steals data from an organisation by using contractors, business partners, or employees.

Signs of Insider Threat:

- Abnormal access patterns: Workers accessing private data after hours or on the weekends, in addition to their regular duties.
- Illegal data access: Workers gaining access to systems or files for which they are not normally authorised.
- Unauthorised information sharing: Workers disclosing private information to outside parties or persons they are not authorised to.
- Behavioural or performance changes: Workers displaying abrupt behavioural shifts, such heightened confidentiality or attempts to avoid discovery.
- Employee discontent or unhappiness: When staff members voice their unhappiness with their jobs or the company, it may spark aggressive behaviour.

2.2 External Attack

Data theft carried out by external parties, such as nation-state enemies, hackers, or cybercriminals, is referred to as an external attack.

Signs of External Attack:

- Illegal entry attempts: Brute force attacks or suspicious login attempts directed at the networks or systems of the company.
- Unusual patterns of network traffic: Distinctive communication patterns or massive amounts of data being moved to other sites are examples of anomalies in network traffic.
- Malicious software or malware presence: Finding malware problems, including ransomware, trojans, or keyloggers, on the company's networks or systems.
- Phishing attempts: Getting shady emails or communications that try to fool staff members into disclosing private information or installing malicious software.
- Exploitation of applications or system vulnerabilities: Identification of attempted or accomplished exploitation of known weaknesses in the infrastructure of the company, such as improperly configured systems or unpatched software.

2.3 Data Breaches

Data breaches happen when unapproved parties obtain entry to confidential data that is kept on file by a company.

Signs of Data Breaches:

- Unexpected modifications to a user's rights or access authorisation.
- Unauthorised access attempts indicated by anomalies in system logs.
- Abnormal network activity patterns, such massive data transfers to other addresses.
- Conditions in user behaviour, including accessing private information after hours.

2.4 Phishing Attacks

Phishing attacks include sending people false emails or messages with the intention of fooling them into disclosing private information, including login passwords or bank account information.

Signs of Phishing Attacks:

- Getting faked or unknown sender emails that raise red flags.
- Email or message requests for private information, including account numbers or passwords.
- Links in emails that take recipients to phoney websites intended to steal login information.
- Sent with bad grammar or poor writing quality.

2.5 Ransomware Attacks

Ransomware attacks entail the introduction of software into a victim's computer or network, encrypting files and requesting payment for the key to unlock them.

Signs of Ransomware Attacks:

- Unable to access folders or files because they are encrypted.
- The appearance of messages requesting money in order to unlock the ransom.
- Abnormal network behaviour as the malware propagates.
- The existence of files or processes connected to ransomware on compromised computers.

2.6 Credential Theft

Theft of login credentials, which include usernames and passwords, from people or organisations is known as credential theft. The goal is to obtain unauthorised access to accounts or systems.

Signs of Credential Theft:

- Notifications of illegal access to systems or user accounts.
- Unusual locations or a pattern of unsuccessful login attempts are examples of anomalies in login behaviour.
- Malware that is intended to intercept keystrokes or steal passwords that have been stored.
- Using credentials that have been stolen to gain access to private data or carry out unauthorised activities.

3. Stakeholders

3.1 IT Security Team

The IT security team oversees overseeing and maintaining the company's security infrastructure, keeping an eye out for any security risks, and handling instances of data theft. Among their duties and functions are:

- Examining and assessing security events to ascertain the scope of identity theft.
- Putting security measures and controls in place to stop more illegal access.
- Working together with the incident response team to control and lessen the effects of occurrences involving data theft.
- Using forensic analysis to find the source of security vulnerabilities and stop such situations in the future.
- Informing top management and other relevant parties on procedure upgrades for incident response and suggesting security enhancements.

3.2 Incident Response Team

The incident response team oversees overseeing the incident response procedure and organising the organization's reaction to occurrences involving data theft. Among their duties and functions are:

- Identifying the extent and consequences of data theft occurrences and taking the necessary remedial measures.
- Organising staff and resources to limit and lessen the impact of instances of data theft.
- Carrying out forensic investigations to ascertain the origin and scope of data theft and collect proof for prospective legal proceedings.
- Keeping customers, third-party vendors, senior management, the IT security team, and other stakeholders at all levels informed about incident response procedures and recovery activities.
- Recording best practices and lessons gained from data theft events to strengthen the company's incident response skills.

3.3 Communication Team

The communication team oversees overseeing both internal and outside communications about cases of data theft and making sure that messages are clear and consistent. Among their duties and functions are:

- Creating and carrying out communication strategies to notify stakeholders, including staff members, clients, and outside suppliers, about instances of data theft.
- Writing and distributing communication materials to respond to questions and concerns from stakeholders, including as statements, news releases, and FAQs.

- Organising public relations and media relations campaigns to safeguard the company's image and lessen the negative effects of data theft occurrences on its reputation.
- Regularly updating upper leadership and the incident response team on the state of stakeholder engagement and communication initiatives.

3.4 Customers

Customers are people or organisations that may be impacted by instances of data theft and have a stake in the goods or services offered by the company. Among their duties and functions are:

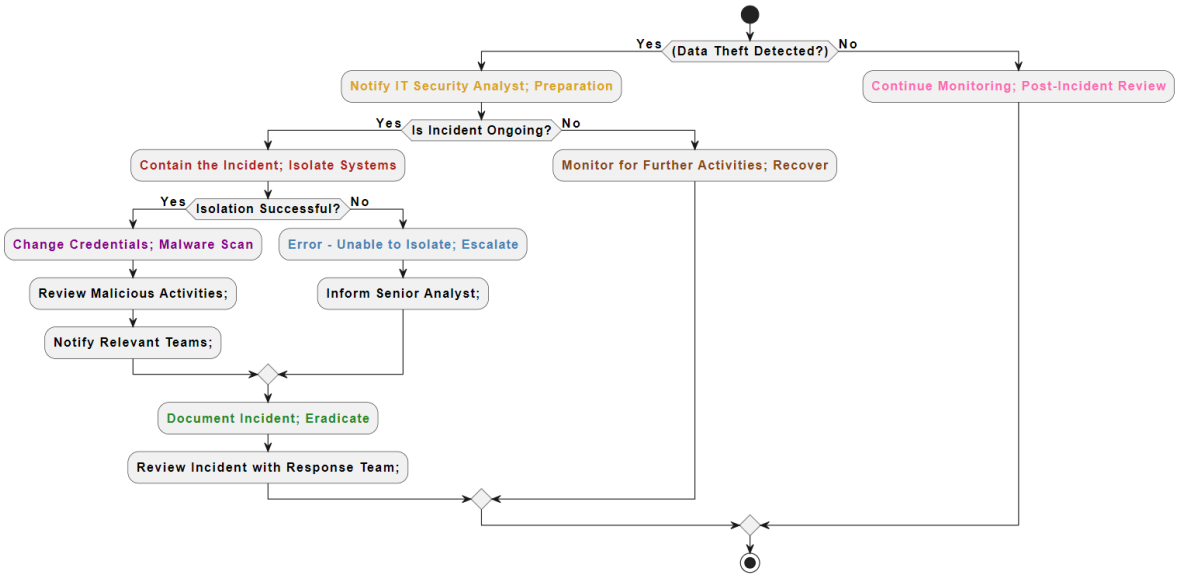
- Notifying the organisation of any unauthorised or questionable activity pertaining to their accounts or transactions.
- Participating in the investigation of data theft occurrences by offering pertinent data or proof to the organization's incident response team.
- Adhering to the organization's recommendations and instructions about how to safeguard their personal data and lessen the effects of data theft occurrences.

3.5 Third-Party Vendors

Third-party vendors are outside companies that supply the company with goods, services, or support; they may also have access to its networks, systems, or data. Among their duties and functions are:

- Working in tandem with the company's incident response team to locate and fix security flaws or breaches pertaining to their goods or services.
- Offering the company help and support as it investigates and handles data theft issues that impact its networks or systems.
- Honouring contractual commitments and legal mandates pertaining to privacy and data security, including disclosing security breaches, and assisting with incident response.

4. Flow Diagram



1. Preparation (Prep): Yellow

    - Notify IT Security Analyst: The IT security analyst is instantly contacted to begin incident response preparations upon detection of data theft.

2. Identification (Identify): Red

    - Contain the Incident; Isolate Systems: Containment procedures, such as isolating impacted systems to prevent additional unauthorised access, are put in place if the issue is continuing.

3. Notification (Notif): Violet

    - Change Credentials; Malware Scan: Changing passwords and running malware scans are two urgent steps that should be taken after a successful isolation to lessen the effect of the occurrence.
    - Review Malicious Activities; Notify Relevant Teams: Malicious activity is found through additional analysis, and teams who need to respond are alerted so that they may plan accordingly.

4. Containment (Contain): Sky Blue

    - Error - Unable to Isolate; Escalate: Senior analysts are notified to resolve the issue and the incident is escalated if the impacted systems cannot be isolated.

5. Eradication (Erad): Light Green

    - Document Incident; Eradicate: To eliminate any last hazards and return to regular operations, the occurrence is recorded, and eradication procedures are put in place.

6. Recovery (Recover): Brown

    - Monitor for Further Activities; Recover: To guarantee the organization's resilience, recovery actions are started and ongoing monitoring for additional activities is carried out.

7. Post-Incident Actions (Post): Light pink

    - Continue Monitoring; Post-Incident Review: Continuous observation persists, and a post-event assessment is carried out to appraise the efficacy of the reaction and pinpoint opportunities for enhancement.

5. Incident Response Stages

5.1 Preparation

- **Objective:** Establishing the rules, processes, and resources required to properly handle cases of data theft is the main goal of the preparation phase.
- **Activities:**
  - Forming an incident response group with clearly defined duties.
  - Creating processes and strategies for incident response that include escalation routes and communication protocols.
  - Regularly providing incident responders with training and drills to guarantee preparedness.
  - Putting security measures and monitoring systems in place to identify and stop instances of data theft.
- **Outcome:** A well-equipped company capable of reacting to instances of data theft swiftly and efficiently.

5.2 Detection

- **Objective:** Finding signs of illegal access or data theft within the organization's networks and systems is the task of the detection stage.
- **Activities:**
  - Keeping an eye out for suspicious activities, such as strange access patterns or unauthorised file transfers, by monitoring system logs and network traffic.
  - Putting in place security information and event management (SIEM) and intrusion detection system (IDS) solutions to find any attacks.
  - Examining abnormalities and alarms to differentiate between harmful and legitimate activity.
- **Outcome:** Early data theft event identification allows for quick response and mitigation actions.

5.3 Analysis

- **Objective:** The investigation and comprehension of the type and extent of the data theft occurrence are the main objectives of the analysis stage.
- **Activities:**
  - Gathering information and determining the origin and scope of the data theft through forensic analysis.
  - Examining hacked networks and systems to ascertain the attack strategies and the effects on compromised data.
  - Recognising threat actors' tactics, methods, and procedures (TTPs) and indications of compromise (IOCs).

- **Outcome:** A thorough comprehension of the data theft occurrence, considering its attribution, consequences, and underlying reasons.

5.4 Containment

- **Objective:** To stop more unauthorised access or data exfiltration, the containment step entails reducing the incident's effect and spread.
- **Activities:**
  - Separating hacked networks and systems to stop attackers from moving laterally.
  - Putting in place limits and access controls to stop unwanted individuals from accessing private information.
  - Putting harmful files, programmes, or network traffic in quarantine or blocking it to stop further damage.
- **Outcome:** Successful management of the data theft event, reducing the damage it caused to the systems and data of the company.

5.5 Eradication

- **Objective:** The goal of the eradication step is to eradicate any remaining risks or vulnerabilities as well as the attackers' presence from the company's IT infrastructure and networks.
- **Activities:**
  - Deleting harmful software and data from hacked computers and returning them to a safe condition.
  - Upgrading or patching susceptible systems and software to stop further exploitation.
  - Examining and revising security rules and practices to fix any flaws or vulnerabilities found.
- **Outcome:** Eradicating all evidence of the data theft event and reducing vulnerabilities to stop such ones in the future.

5.6 Recovery

- **Objective:** Restoring impacted systems and information to regular functioning and carrying on business as usual are the objectives of the recovery stage.
- **Activities:**
  - Restoring systems and data backups that were hacked to guarantee data availability and integrity.
  - Rebuilding or reorganising networks and systems to increase security and stop such events.

- Implementing user education and awareness campaigns to stop data theft in the future.
- **Outcome:** Complete resumption of operations and services together with more robust security measures to reduce the likelihood of a repeat.

5.7 Post- Incident Review

- **Objective:** In the post-incident review phase, the organization's reaction to the data theft incident is assessed, and opportunities for improvement and lessons learned are noted.
- **Activities:**
- Carrying out a comprehensive examination of the incident response procedure, considering its advantages, disadvantages, and room for development.
- Recording best practices and lessons learned to improve incident response skills in the future.
- Adjusting incident response protocols, guidelines, and security measures considering the review's conclusions.
- **Outcome:** Constant enhancement of incident response capacities and preparedness for upcoming data theft events.

6. Terminology

- Data Theft: The illicit procurement, duplication, or elimination of private or sensitive information from a company's networks or systems.
- Insider Threat: A security risk brought on by employees of a company who may, whether on deliberately or accidentally, abuse or divulge sensitive information for nefarious or personal benefit.
- External Attack: An attempt to steal confidential information through a cyberattack carried out by people or organisations not connected to its internal network, such as hackers, cybercriminals, or nation-state enemies.
- Incident Response: A methodical strategy for dealing with and handling security events, such as data theft incidents, with the objectives of minimising harm, restarting operations, and averting such occurrences.
- Indicators of Compromise (IOCs): Observable indicators, such as strange network traffic patterns, unauthorised access attempts, or questionable file alterations, that point to the existence of malicious activity or a security breach.
- Security Controls: Procedures put in place to guard against security risks, such as instances of data theft, and to safeguard networks, systems, and data. Intrusion detection systems (IDS), encryption, access restrictions, and security awareness training are a few examples of security controls.
- Forensic Analysis: The methodical inspection of digital evidence connected to a security event, such data theft, to collect and examine data for legal or investigative needs, including figuring out the incident's cause and consequences.
- Vulnerability: Vulnerabilities or weaknesses in networks, apps, or systems that an attacker may use to get unauthorised access, steal information, or interfere with normal operations. Inadequate security measures, incorrect setups, and software defects can all lead to vulnerabilities.