

Data Theft Playbook

**Authorised by** **:**

**Date issued or last reviewed/revised** **:**

**Date last exercised** **:**

# Table of Contents

[1. Table of Contents 2](#_Toc210225741)

[2. Document Control 3](#_Toc210225742)

[2.1 Document Revision 3](#_Toc210225743)

[3. Assumptions & Disclaimer 4](#_Toc210225744)

[3.1 Assumptions 4](#_Toc210225745)

[3.2 Disclaimer 4](#_Toc210225746)

[4. Background 5](#_Toc210225747)

[5. Objectives 7](#_Toc210225748)

[5.1 Proactive Response 7](#_Toc210225749)

[5.2 Quick Containment 7](#_Toc210225750)

[5.3 Effective Remediation 7](#_Toc210225751)

[6. Readiness 8](#_Toc210225752)

[6.1 General Readiness 8](#_Toc210225753)

[6.2 Prepare Phase Readiness 8](#_Toc210225754)

[6.3 Detect Phase Readiness 9](#_Toc210225755)

[6.4 Analyse Phase Readiness 9](#_Toc210225756)

[6.5 Contain Phase Readiness 9](#_Toc210225757)

[6.6 Eradicate Phase Readiness 9](#_Toc210225758)

[6.7 Recover Phase Readiness 10](#_Toc210225759)

[6.8 Post-Incident Handling Phase Readiness 10](#_Toc210225760)

[7. NIST Incident Handling Categories 11](#_Toc210225761)

[7.1 NIST Framework Incident Response Life Cycle 11](#_Toc210225762)

[7.2 Prepare 13](#_Toc210225763)

[7.3 Detect 15](#_Toc210225764)

[7.4 Analyse 18](#_Toc210225765)

[7.5 Contain 23](#_Toc210225766)

[7.6 Eradicate 26](#_Toc210225767)

[7.7 Recover 30](#_Toc210225768)

[7.8 Post-Incident 33](#_Toc210225769)

[8. Glossary 36](#_Toc210225770)

# Document Control

## Document Revision

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Issue Date | Changes |
| 0.1 | Name | XX/XX/2025 | Initial Draft |
| 0.2 |  | XX/XX/XXXX | Draft Review |
| 1.1 |  | XX/XX/XXXX | Final release |

# Assumptions & Disclaimer

## Assumptions

* This playbook must be followed by an experienced Incident Response Team
* This playbook is reviewed and updated as part of the post-incident review exercise at the end of each similar incident
* This playbook must be approved by the relevant stakeholders
* This playbook is accessible by the Incident Response Team
* Perform a continuous impact assessment during the incident treatment
* Additional logs collection might be required throughout the incident treatment

## Disclaimer

This playbook is to be followed by an experienced Incident Response Team. The steps defined in this document, in the different workflows available in the NIST incident handling categories section, are presumed to be validated and approved by the appropriate stakeholders in the organisation. In case of an incident falling under this playbook category, the Incident Response Team will follow the process described below and will presume that their actions are approved in applying the appropriate security control to reduce the threat identified.

Incident Response Teams must maintain their knowledge of products, processes, and systems and ensure access to systems is adequate and accessible in the event of an incident.

The organisation following this playbook must be aware of the applicable laws, regulations, and compliance obligations such as GDPR, PCI and NDB schemes etc.

# Background

Data theft is the act of stealing computer-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information. Data theft incidents are on the increase for both residential users and organisations of all sizes.

To reduce the impact of data theft, it is recommended to follow the NIST approach to facing such security incidents and apply a risk-based approach by:

* Being prepared to handle any incident
* Control the situation, minimising the impact on the business
* Efficiently manage the response across multiple departments
* Communicate effectively to ensure risk mitigation methods are applied
* Prioritise resources and activities where they matter most
* Report and tune based on response learning, reducing risk moving forward

According to NIST Special Publication 800-61 rev 2, an incident response process contains four main phases: preparation, detection and analysis, containment/eradication/recovery, and post-incident activity. Descriptions for each are included below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Prepare** | **Detect & Analyse** | **Contain, Eradicate & Recover** | **Post-Incident Handling** |
| The initial phase is where organisations will perform preparatory measures to ensure that they can respond effectively to incidents if and when they are uncovered.  This should also include regular testing of playbooks to ensure they are robust, easy to follow and incorporate any recent learnings | The second phase is where organisations should strive to detect and validate incidents rapidly because infections can spread through an organisation within a matter of minutes.  Early detection can help an organisation minimise the number of infected systems, which will lessen the magnitude of the recovery effort and the amount of damage the organisation sustains as a result of the incident. | The third phase, containment, has two major components: stopping the spread of the attack and preventing further damage to systems. It is important for an organisation to decide which methods of containment to employ early in the response. Organisations should have strategies and procedures in place for making containment-related decisions that reflect the level of risk acceptable to the organisation. | Because the handling of Data Theft incidents can be extremely expensive, it is particularly important for organisations to conduct a robust assessment of lessons learned after major Data Theft incidents to prevent similar incidents from occurring. |

The Incident Response Plan (IRP) may contain references to the organization-defined playbooks. The playbooks will define the steps to follow in case of a specific incident, in this current playbook (Data Theft). In case of an incident, it is recommended to refer to the IRP, if an incident response is covered in a playbook, the use of the playbook takes priority on the IRP.

This playbook will not cover the areas below that might already be available in the IRP.

The IRP may cover the areas below:

* Data Categories for Tracking Incidents
* Types of Incident Detection Channels
* Incident prioritisation matrix and triage process
* Incident Response Workflow
* Incident Root-cause Framework
* Incident Response Lifecycle
* Incident Response Checklist (During)
* Post-Incident checklist (After)
* Incident Response Performance Metrics
* Incident Response Process/Procedures/Playbook List
* Roles and Responsibilities
* Incident Response Team
* Incident Response Team Organisational Structures
* The communication process in case of an incident
* Checklist for Communicating with Media
* Incident Communication Memo to Employees - Template
* Sample Customer Notification Letter - Template
* Response Plan for Compromise of Personal Information - Template
* Incident evidence collection log

For any information related to the above, please refer to the Incident Response Plan.

# Objectives

## Proactive Response

A playbook helps security teams optimise their actions for efficiency and productivity. Your security team can plan and prioritise their actions in a methodical and repeatable fashion. Following a playbook, your team will have the best chance to respond and contain incidents when and where they occur.

## Quick Containment

Time and speed are crucial in assessing the environment and risk in the context of your business. Playbooks give a complete view of the necessary tasks to capture the data needed to support proper recovery and forensics. The efficiency a playbook brings to a security team allows for quick responses to finding the source of the attack, following lateral movement across the organisation, and taking the proper steps to mitigate damage.

## Effective Remediation

Playbooks facilitate security processes, mitigation plans, and smooth communication between multiple departments. By working methodically through data collection, analysis, and communications, you improve the odds for effective eradication, recovery with integrity, and forensic-quality reporting.

# Readiness

Incident Response Teams function in a state of constant readiness. A security incident can occur at any time of day or night so Incident Response Teams should always be prepared to respond.

A state of readiness involves checking their processes, procedures, tools, and access in the downtime to ensure that when an incident occurs, they are familiar with the processes and tools involved to reduce wasted time and effort.

## General Readiness

* Ensure that the organisation has an Incident Response Plan (IRP) that is up to date, reviewed, approved by the appropriate stakeholders, authorised by the appropriate executive, and communicated to the appropriate teams (Incident Response Teams, IT Support Team, IT Team).
* Ensure that the required playbooks to support the IRP exists or are being developed.
* Ensure that the playbooks and all required processes and procedures in responding to an incident are referred to in the IRP.
* Ensure that the organisation has a functioning knowledge base tool.
* Ensure that the required users have access to the organisation’s knowledge base.
* Ensure that the organisation has a training plan in place to upskill the employees in the required area that will speed up their reaction in dealing with a threat.

## Prepare Phase Readiness

* Ensure access to the breached systems.
* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure that the learnings from the previous similar incident are included in the knowledge base.
* Ensure access to the RACI matrix to identify the point of escalations.
* Ensure access to escalation paths.
* Ensure access to contact details (email, phone number) of the stakeholders designated as points of escalation.
* Ensure access to contact details (email, phone number) of the appropriate contact in the legal team.
* Ensure access to contact details (email, phone number) of the appropriate contact in the Governance and Compliance Team (GRC).
* Ensure access to contact details (email, phone number) of the appropriate contact in the marketing/communication team.
* Ensure access to contact details of vendors for the tools used and authority to engage vendor support teams where applicable and escalation contact details.

## Detect Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure that the learnings from the previous similar incidents are included in the knowledge base.
* Ensure that detection tuning learnings from previous incidents have been updated in the appropriate toolsets.
* Ensure toolsets are up to date.

## Analyse Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure toolsets are up to date.

## Contain Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure good functioning of firewalls and other network devices.
* Ensure that tools such as SIEM, IDS, Scanners, and Antiviruses are updated.
* Ensure that firewall rules are documented.
* Ensure access to the organisation’s risk framework, process, and acceptance criteria.
* Ensure access (read and write) to the organisation’s asset register to update the status of the affected assets.

## Eradicate Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure that the Incident Response Team is aware of the communication plan in the event of incidents.

## Recover Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure that the learnings from the previous similar incident are included in the knowledge base.
* Ensure that tools such as SIEM, IDS, Scanners, and Antiviruses are updated.
* Ensure that cloud services and other data stores are synchronised.
* Ensure that any network changes are documented.
* Ensure any existing related risks are reviewed, reassessed, and updated.
* Create any risk items identified.

## Post-Incident Handling Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure that the learnings from the previous similar incident are included in the knowledge base.

# NIST Incident Handling Categories

## NIST Framework Incident Response Life Cycle

[[1]](#footnote-1)Lifecycle diagram from NIST Computer Incident Handling Guide SP 800-61 Revision 2

**Preparation**[[2]](#footnote-2)

Incident response methodologies typically emphasise preparation—not only establishing an incidentresponse capability so that the organisation is ready to respond to incidents, but also preventing incidentsby ensuring that systems, networks, and applications are sufficiently secure. Although the incident response team is not typically responsible for incident prevention, it is fundamental to the success of incident response programs.

**Detection & Analysis**[[3]](#footnote-3)

In the event of an incident, the Incident Response Team must detect and identify the type of incident occurring. In addition, it is necessary to collect the relevant data (logs, files, information) to be analysed. Once the above is completed, it is required to document the incident, prioritise it then communicate it to the appropriate authorities. The legal team of the organisation should be notified in the case of an event occurring that falls under the Notifiable Data Breaches (NDB) scheme.

**Containment, Eradication & Recovery**[[4]](#footnote-4)

Once the incident is identified, the Incident Response Team should be able to plan a strategy to stop the breach and reduce the risk of the threat spreading, therefore starting the recovery phase.

**Post Incident Activity**[[5]](#footnote-5)

Once an incident is resolved, the next step for the team is to go back to the beginning and prepare for the next incident; input from each new incident should help inform the preparation process, whether by adding new information about new threats or simply as a means of fine-tuning procedures that are part of the incident management process. Post-Incident Review is one of the main activities of this phase, and it includes the review and update of the incident playbook and the update of the knowledgebase.

Periodic risk assessments of systems and applications should determine what risks are posed by combinations of threats and vulnerabilities. This should include understanding the applicable threats, including organisation-specific threats. Each risk should be prioritised, and the risks can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached. Another benefit of conducting risk assessments regularly is that critical resources are identified, allowing staff to emphasise monitoring and response activities for those resources.[[6]](#footnote-6)

The objectives of using the NIST Framework are the following:

* A better understanding and management of cybersecurity risks
* A decrease in cybersecurity risks
* Prioritisation of cybersecurity activities
* Prioritisation in cybersecurity investments and maximisation of the impact of each dollar spent on cybersecurity
* Define a common language to communicate inside and outside an organisation
* Improvement of communications, awareness, and understanding between and among IT, planning, and operating units, as well as senior executives
* Defined cybersecurity posture

## Prepare

The initial phase is where organisations will perform preparatory measures to ensure that they can respond effectively to incidents if and when they are uncovered.

The organisation should have an Incident Response Plan (IRP) well documented, thoroughly explaining the roles and responsibilities of the employees/teams involved in the incident handling process. The plan must be tested to assure that your employees will perform as they were trained.

Additional procedures might be followed according to the organisation's systems and service structure.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.2.1 | Determine Core Ops Team & Define Roles | Define roles and responsibilities in case of an incident and define the points of escalation | Incident Response Team and IT Team and Leadership team (CISO, CIO, CTO…etc) |
| 7.2.2 | Engage the Legal Team in case of an event falling under NDB | If the incident occurring falls under the Notifiable Data Breach scheme, the incident response team must notify and engage the legal team | Incident Response Team |
| 7.2.3 | Review & Maintain Timeline | Review the timeline of an incident and maintain it for review and monitoring purposes | Incident Response Team |
| 7.2.4 | Interviews | Interview users, managers, and people in charge of the physical security and key stakeholders | Interviews held by Security Analysts from Incident Response Team |
| 7.2.5 | Request relevant logs and information | Collect the logs and relevant evidence related to the incident to identify its origin | Incident Response Team |

## Detect

The second phase is where organisations should strive to detect and validate incidents rapidly because infections can spread through an organisation within a matter of minutes. Early detection can help an organisation minimise the number of infected systems, which will lessen the magnitude of the recovery effort and the amount of damage the organisation sustains as a result of the incident.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| - | Define Threat Indicators | Decision box to illustrate the 2 paths possible (follow standard threat indicator or custom threat indicators) | Incident Response Team |
| 7.3.1 | Standard | An Indicator represents an atomic piece of information that has some intelligence value, and there is a standard threat indicator that is predefined and makes the process smoother  Sub steps: 7.3.1.1 – 7.3.1.8 | Incident Response Team |
| 7.3.2 | Custom | An Indicator represents a piece of information that has some intelligence value. There are custom threat indicators according to the type of incident or threat | Incident Response Team |
| 7.3.3 | Categorise Incident | Define the category of the incident or order to define its priority and the escalation level | Incident Response Team |
| 7.3.4 | Request Packet Capture | Request and gather packet capture to be used in the analyse phase | Incident Response Team |
| 7.3.5 | Conduct Scans | Perform scans to detect vulnerabilities in the internal and external environment of the organisation | Incident Response Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.3.1.1 | Large data dumps of databases, network shares or other computer systems | Investigate if there was a large data dump of the database, network shares or other computer systems | IT Team (Network Team)  Incident Response Team |
| 7.3.1.2 | Identification or publication of proprietary information outside the organisation | Define the intellectual property of the organisation to protect the organisation’s valuable trade property and confidential information | Legal team  Incident Response Team  IT Team |
| 7.3.1.3 | Notification of extortion to recover stolen data | In a situation of stolen data, there is a high chance to receive an extortion notification (ransom) for recovering the stolen data | Incident Response Team  Legal team |
| 7.3.1.4 | Work performed outside of normal business hours | Identification and investigation of the work that was performed outside of agreed business hours | Incident Response Team  IT team |
| 7.3.1.5 | Emails returned as Undeliverable due to size limitations | Check emails that were returned to sender due to the size of the email and attachment files | Incident Response Team  IT team |
| 7.3.1.6 | Local disk or network shares that are near full capacity | Check the capacity of the local and network shares and highlight the ones that are near to full capacity | Network team |
| 7.3.1.7 | Reporting of large emails being sent by a single user | Cross-check anomalies such as large emails being sent by a single user. This can be found in email management reports | IT Support Team |
| 7.3.1.8 | Reports of removable or mobile devices being used to copy data | Request reports of the removable or mobile device being used to copy data from the appropriate team (IT Support) | IT Support Team  IT Team |

## Analyse

Analyse the incident using a risk-based approach to define the criticality of the event and its impact on the business and therefore define the type of resolution approach to follow:



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| - | Define Risk Factors | Decision box to illustrate the two paths possible (follow standard risk factors or custom risk factors) | Risk Management Team (GRC |
| 7.4.1 | Standard | Define standard risk factors according to the organisation’s risk management process and acceptance criteria that have a privacy impact, a business impact, and technical impact  Sub steps: 7.4.1.1 – 7.4.1.17 | Risk Management Team (GRC) |
| 7.4.2 | Custom | Define custom risk factor  Sub steps: 7.4.2.1 | Risk Team |
| 7.4.3 | Determine Patch Methods | Choose the patch method to apply. E.g., Deploy vendor-supplied update or change of configuration to close the vulnerability | Incident Response Team  IT Support team  IT Team |
| 7.4.4 | Log Collection | Collect the logs with a focus on the timeline of the incident recorded to identify any suspicious activity | Incident Response Team  IT Team  Support Team |
| 7.4.5 | Evidence Collection | Collect all the evidence of the incident for investigation and post-incident learning purposes | Incident Response Team  IT Team |
| 7.4.6 | Data Capture | Capture data to gather key information linked to the incident using data capture tools | Incident Response Team  IT Team  Support Team |
| 7.4.7 | Analysis | Analysis of the incident by analysing the log collection files, the data capture, and all the evidence collected as a result of this incident | Incident Response Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| . | External user PII or other protected information has been stolen | Define the level of risk for this situation and the mitigation methods | Risk Management Team (GRC)  Incident Response Team  IT Team |
| 7.4.1.2 | Internal user PII or other protected information has been stolen | Define the level of risk for this situation and the mitigation methods | Risk Management Team (GRC)  Incident Response Team  IT Team |
| 7.4.1.3 | Stolen data damaging to business operations or brand of the organisation | Define the level of risk for this situation and the mitigation methods | Risk Management Team (GRC)  Incident Response Team  IT Team |
| 7.4.1.4 | Compliance regulations have been violated | Identify the regulations and controls that have been violated | Governance and Compliance team  Legal Team |
| 7.4.1.5 | PII or other protected information has been compromised | Define the level of risk for this situation, the mitigation methods, and the level of escalation and communication of the incident | Risk Team  Incident Response Team  The leadership team (C level) |
| 7.4.1.6 | Products, goods, or services are affected by this attack | Define the level of risk for this situation, the mitigation methods, and the level of escalation and communication of the incident | Risk Team  Incident Response Team  The leadership team (C level) |
| 7.4.1.7 | Customers are affected by this incident | Define the level of risk for this situation, the mitigation methods, and the level of escalation and communication of the incident to the relevant stakeholders | Legal Team  Communication Team  The leadership team (C level) |
| 7.4.1.8 | Public or personnel safety affected | Define the level of risk for this situation and the mitigation methods | Legal Team  Governance and Compliance Team |
| 7.4.1.9 | There is internal knowledge of this incident | Define the communication plan in case of an incident and define the communication channels and the audience | Communication Team  Change management team |
| 7.4.1.10 | There is an indication of who performed data theft | Identify who performed data theft | Incident Response Team |
| 7.4.1.11 | Ability to control, record, measure, or track any significant amounts of inventory, products, cash, or revenue lost | Monitor the systems and teams that can control, record, or measure and track any significant amounts of inventory, products, cash, or revenue loss | Incident Response Team  IT Team |
| 7.4.1.12 | Identify business operations that may be affected and identify any alternate courses | Identification of point of impact of the data theft incident (which team/department?) is affected and identify the connection of the affected point to another area of the business | Incident Response Team |
| 7.4.1.13 | Identify worst-case business impact if unable to mitigate risk attack | Define simulation that will cover worst and best-case scenarios and evaluate the impact and therefore the mitigation method to reduce the risk of an attack | Risk Team  Incident Response Team |
| 7.4.1.14 | There is external knowledge of this incident | Identify the external channel aware of the incident occurring | Incident Response Team  Legal Team  Communication/PR Team |
| 7.4.1.15 | Determine the risk of the stolen data being released to the public | Define the level of risk for this situation, the mitigation methods, and the level of escalation and communication of the incident | Legal Team  Communication/PR Team |
| 7.4.1.16 | Identify technical implications of the Data Theft | List the technical implication of a data theft incident | Incident Response Team  IT Team |
| 7.4.1.17 | Identify business implications of the Data Theft | Define the implication of the data theft incident on the business | Leadership Team (C-level) |
| 7.4.2.1 | Custom Factors | Identify the risk management process in specific scenarios unique to the organisation | Risk Team |

## Contain

The third phase, containment, has two major components: stopping the spread of the attack and preventing further damage to systems. An organisation needs to decide which methods of containment to employ early in the response. Organisations should have strategies and procedures in place for making containment-related decisions that reflect the level of risk acceptable to the organisation.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.5.1 | Identify the system(s) that have been affected | List the systems and devices that have been corrupted  Sub steps: 7.5.1.1 – 7.5.1.6 | Incident Response Team  IT Team |
| 7.5.2 | Identify user credentials compromised or at risk | Investigate the credentials that have been compromised or at risk and define the action on these | Incident Response Team  IT Team |
| 7.5.3 | Identify the method used to steal data | Investigation to find out which data has been lost and the degree of sensitivity, confidentiality, and importance | Incident Response Team  IT Team |
| 7.5.4 | Identify system(s) used to steal data | Identify the systems that facilitated the breach and its spreading | Incident Response Team |
| 7.5.5 | Identify any source attribution collected | Identify the source of attribution to observe the exposure to the breach  Sub steps: 7.5.5.1 – 7.5.5.3 | Incident Response Team |
| 7.5.6 | Identify lateral movement or compromised user throughout the enterprise | Follow the spreading of the attack to identify the compromised user in the whole organisation  Sub steps: 7.5.6.1 – 7.5.6.4 | Incident Response Team |
| 7.5.7 | Identify the tools used to detect the attack | Each organisation have in place tools to detect, monitor and manage incidents  Sub steps: 7.5.7.1 – 7.5.7.6 | Incident Response Team  IT Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.5.1.1 | Server | Check, isolate, and list servers that have been corrupted | Incident Response Team  IT Team |
| 7.5.1.2 | Desktop | Check, isolate, and list desktops that have been corrupted | Incident Response Team  IT Team |
| 7.5.1.3 | Laptop | Check, isolate, and list laptops that have been corrupted | Incident Response Team  IT Team |
| 7.5.1.4 | Mobile | Check, isolate, and list mobiles that have been corrupted | Incident Response Team  IT Team |
| 7.5.1.5 | VM | Check, isolate, and list virtual machines that have been corrupted | Incident Response Team  IT Team |
| 7.5.1.6 | LDAP Directory | Check, isolate, and list LDAP Directory that has been corrupted | Incident Response Team  IT Team |
| 7.5.5.1 | Select Database | Choose a database for observation | Incident Response Team |
| 7.5.5.2 | Query Database | Extract data from the chosen database | Incident Response Team |
| 7.5.5.3 | Generate Report | Generate the report to identify the abnormal activity | Incident Response Team |
| 7.5.6.1 | View Report | Generate a report on the compromised users or credentials | Incident Response Team |
| 7.5.6.2 | View Record Details | Check the details of the record | Incident Response Team |
| 7.5.6.3 | Select Records | Select records | Incident Response Team |
| 7.5.6.4 | Copy Record Details | Copy records details | Incident Response Team |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.5.7.1 | SIEM | Security information and event management systems are used to provide real-time analysis of security alerts generated by applications and network hardware. This tool should be used, monitored, and owned by the organisation’s security operation centre (SOC) | Incident Response Team |
| 7.5.7.2 | IDS | Use a monitoring system such as IDS | Incident Response Team |
| 7.5.7.3 | Firewall | It is necessary to have in place a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules | Incident Response Team  IT Team |
| 7.5.7.4 | Scanners | Implemented and updated | Incident Response Team  IT Team |
| 7.5.7.5 | Antivirus | Implemented and updated | Incident Response Team  IT Team |
| 7.5.7.6 | Removable Device Monitors | Installed and functioning | Incident Response Team  IT Team  Support Team |

## Eradicate

Eradicate the risk of spreading the incident after the containment of the incident.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.6.1 | Triage & Confirm Incident Report | Triage is the first post-detection incident response step. It is recommended to always pass through the triage step to detect false positives  Sub steps: 7.6.1.1 – 7.6.1.3 | Incident Response Team |
| 7.6.2 | Communications | Check if the communication channels have been corrupted then communicate the identification of the incident using the right channels of communication and targeting the right audience (escalation point)  Sub steps: 7.6.2.1 – 7.6.2.6 | Incident Response Team  IT Team |
| 7.6.3 | Eradicate Malware | Remove corrupted items and ensure the regular scanning of systems  Sub steps: 7.6.3.1 – 7.6.3.3 | Incident Response Team  IT Team |
| 7.6.4 | Monitor Network Traffic for Ongoing Theft | Constant monitoring of network traffic  Sub steps: 7.6.4.1 – 7.6.4.3 | Incident Response Team  IT Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.6.1.1 | Request System Patch | Request a system patch if a vulnerability is detected to fix the bug and improve the system functionality | Incident Response Team  IT Team |
| 7.6.1.2 | Test Code | Review and test code to detect any malicious code that could be injected for malicious intents | Incident Response Team  IT Team  Dev Team |
| 7.6.1.3 | Contain Malicious Code Sample | Process of containment is required if malicious code has been found | Incident Response Team  SOC Team  IT Team |
| 7.6.2.1 | Conference Call | Check if this communication channel is corrupted and if not, this channel can be used as Business as Usual. Inform the selected audience about the breach via conference call | Incident Response Team  IT Team |
| 7.6.2.2 | Intranet Meeting | Check if this communication channel is corrupted and if not, this channel can be used as Business as Usual. Inform the selected audience about the breach via Intranet Meeting | Incident Response Team  IT Team |
| 7.6.2.3 | Internet Meeting | Check if this communication channel is corrupted and if not, this channel can be used as Business as Usual. Inform the selected audience about the breach via Internet Meeting | Incident Response Team  IT Team |
| 7.6.2.4 | Direct Phone Call | Check if this communication channel is corrupted and if not, this channel can be used as Business as Usual. Inform the selected audience about the breach via direct phone call | Incident Response Team  IT Team |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.6.2.5 | In-Person Meeting | Check if this communication channel is corrupted and if not, this channel can be used as Business as Usual. Inform the selected audience about the breach in-person meeting | Incident Response Team  IT Team |
| 7.6.2.6 | Mobile Messaging | Check if this communication channel is corrupted and if not, this channel can be used as Business as Usual. Inform the selected audience about the breach via mobile messaging | Incident Response Team  IT Team |
| 7.6.3.1 | Add, change, or remove the affected system, site, or network | Action what is required | Incident Response Team |
| 7.6.3.2 | Platform data forensics | Search, preserve and analyse information on the platform to find potential evidence | Incident Response Team  IT Team |
| 7.6.3.3 | Determine the method of removing data from the organisation’s enterprise network | Incident response team to action | Incident Response Team  IT Team |
| 7.6.4.1 | Create an alert signature for suspected data exfiltration | Incident response team to action | Incident Response Team |
| 7.6.4.2 | Prepare to temporarily scan or block all outbound data more than MB in size | Incident response team to action | Incident Response Team |
| 7.6.4.3 | Implement device control monitoring and control systems | Select and implement a tool to control and monitor systems | Incident Response Team  IT Team |

## Recover

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact of a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements;



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.7.1 | Recover Systems | Recover systems that have been touched by the incident by making sure to have a backup process defined, a disaster recovery process and a backup policy  Sub steps: 7.7.1.1 – 7.7.1.3 | IT Team |
| 7.7.2 | Incident Remediation | Addressing a breach in the most effective way possible to limit the amount of damage that can potentially be done to the organisation  Sub steps: 7.7.2.1 – 7.7.2.5 | Incident Response Team |
| 7.7.3 | Validation & Assurance | The following assurance considerations should be considered during the recovery phase:   * Perform a baseline vulnerability scan * Perform penetration testing * Ensure configuration adheres to best practice * Perform a code review if relevant * Document the findings gathered from the assessment above * Update the risk and issue registers with the findings and prioritised them | Incident Response Team  IT Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.7.1.1 | Reimage | Perform a reimage to replace corrupted files and keep data intact | IT Team  IT Support |
| 7.7.1.2 | IDS/IPS & firewall updates | Update the organisation’s monitoring and control systems and keep these up to date | Incident Response Team  IT Team IT Support |
| 7.7.1.3 | Identify ways to mitigate further removal of data | Define methods to reduce the risk of removal and loss of data | Incident Response Team  IT Team |
| 7.7.2.1 | Wipe & baseline system | Wipe the damaged systems or devices to get new and fresh devices clean of any malicious or corrupted files | IT Support |
| 7.7.2.2 | Scan host with updated signature | Performing scanning of a host with an updated signature to identify any vulnerabilities | Incident Response Team  IT Support |
| 7.7.2.3 | Scan file share with updated signature | Performing scanning on a file share with an updated signature to identify malware | Incident Response Team  IT Support |
| 7.7.2.4 | Manage vulnerabilities | Review vulnerabilities in the vulnerability assessment report and treat them by order of criticality | Incident Response Team  IT Support |
| 7.7.2.5 | Coordinate AV updates from AV vendor | It is recommended to drive this activity to make sure that the updates are deployed effectively and promptly | Incident Response Team  IT Support |

## Post-Incident

Because the handling of data theft incidents can be extremely expensive, it is particularly important

for organisations to conduct a robust assessment of lessons learned after major data theft incidents to prevent similar incidents from occurring.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.8.1 | Incident review | It is necessary to include an incident review in the Incident management process | Incident Response Team (IRP) |
| 7.8.2 | Lessons uncovered | Identify the items that require improvements such as policy updates, new controls to implement, new standards or frameworks to implement, etc.  Sub steps: 7.8.2.1 – 7.8.2.4 | Incident Response Team |
| 7.8.3 | Lessons applied | Determine what worked well in the organisation’s incident response plan and opportunities for improvement. Lessons learned from both mock and real events will help strengthen systems against future attacks.  Sub steps: 7.8.3.1 – 7.8.3.3 | Incident Response Team |
| 7.8.4 | Response workflow updated | Check that the new configurations are in place via the performance of internal audits and following a continuous improvement process | IT Team  Incident Response Team |
| 7.8.5 | Update of the knowledgebase | Add the new processes or procedures used in this incident to the organisation’s knowledgebase | IT Team  Incident Response Team |
| 7.8.6 | Update Risk Register | Update the risk register to define the new level of the risk and define its new status | Incident Response Team  GRC Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.8.2.1 | Discovery meeting | Once the investigation is complete, hold an after-action meeting with all Incident Response Team members and discuss what was learned from the data breach | Incident Response Team |
| 7.8.2.2 | Policy updates defined | Define the uplift required to improve the organisation’s security policies by embedding them in the organization | Incident Response Team  IT Team  Governance & Compliance Team  Leadership Team (C-Level) |
| 7.8.2.3 | Process updates | Update processes to ensure the inclusion of the new steps identified as missing to ensure an improved security posture | All organisation |
| 7.8.2.4 | Configuration updates defined | Implement the configuration updates as required to strengthen systems against future attacks | Incident Response Team  IT Team |
| 7.8.3.1 | Policies implemented | Once policies are updated, these have to be implemented and communicated within the organisation. Owners should be defined for each policy, and the review date should be determined | Policy Owners |
| 7.8.3.2 | Process changes implemented | Implementation of the uplifted or updated processes | Policy Owners  Organisational Change management Team  The project team in charge of the process update project |
| 7.8.3.3 | Configurations applied | Check that the updated configurations are in place and following a continuous improvement process | IT Team |

# Glossary

CIO: Chief Information Officer

CISO: Chief Information Security Officer

CTO: Chief Technology Officer

GRC: Governance Risk & Compliance

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

IR Team: Incident Response Team

IRP: Incident Response Plan

IT: Information Technology

LDAP: Lightweight Directory Access Protocol

Malware: Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network

MB: Megabyte

NDB: Notifiable Data Breach

Procedure: A document written to support a specific process

Process: A series of actions or steps taken to achieve a particular end state

SIEM: Security Information and Event Management

SOC: Security Operation Centre

VM: Virtual Machine

1. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-1)
2. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-2)
3. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-3)
4. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-4)
5. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-5)
6. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-6)