

Business Email Compromise Playbook

**Authorised by** **:**

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

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

# Table of Contents

[1. Table of Contents 2](#_Toc210207232)

[2. Document Control 3](#_Toc210207233)

[2.1 Document Revision 3](#_Toc210207234)

[3. Assumptions & Disclaimer 4](#_Toc210207235)

[3.1 Assumptions 4](#_Toc210207236)

[3.2 Disclaimer 4](#_Toc210207237)

[4. Background 5](#_Toc210207238)

[5. Objectives 7](#_Toc210207239)

[5.1 Proactive Response 7](#_Toc210207240)

[5.2 Quick Containment 7](#_Toc210207241)

[5.3 Effective Remediation 7](#_Toc210207242)

[6. Readiness 8](#_Toc210207243)

[6.1 General Readiness 8](#_Toc210207244)

[6.2 Prepare Phase Readiness 8](#_Toc210207245)

[6.3 Detect Phase Readiness 9](#_Toc210207246)

[6.4 Analyse Phase Readiness 9](#_Toc210207247)

[6.5 Contain Phase Readiness 9](#_Toc210207248)

[6.6 Eradicate Phase Readiness 9](#_Toc210207249)

[6.7 Recover Phase Readiness 10](#_Toc210207250)

[6.8 Post-Incident Handling Phase Readiness 10](#_Toc210207251)

[7. NIST Incident Handling Categories 11](#_Toc210207252)

[7.1 NIST Framework Incident Response Life Cycle 11](#_Toc210207253)

[7.2 Prepare 13](#_Toc210207254)

[7.3 Detect 15](#_Toc210207255)

[7.4 Analyse 19](#_Toc210207256)

[7.5 Contain 24](#_Toc210207257)

[7.6 Eradicate 27](#_Toc210207258)

[7.7 Recover 28](#_Toc210207259)

[7.8 Post-Incident 30](#_Toc210207260)

[8. Glossary 33](#_Toc210207261)

# 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

A Business Email Compromise (BEC) is an email-based fraud technique designed to allow an attacker to gain unauthorised access to confidential information or extract money through fraudulent requests for payment or bank transfers.

Threat actors typically:

* Target executives or employees authorised to make payments and attempt to trick them into transferring money to fraudulent accounts.
* Approach employees of companies, passing themselves off as a known vendor or client of the company. Such actors commonly take over the email accounts of the vendor or impersonate the vendor by creating a similar-looking email.
* Attempt to impersonate CEOs or senior executives to request sensitive data, often with a view to bypass security verification and authentication tools.

BEC scams do not often require advanced techniques or tooling but rely on social engineering techniques to manipulate victims. The simplicity of the fraud, as well as the potentially high financial gain, is what lends to the persistence and prevalence of BEC attacks.

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 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 handling Business Email Compromise incidents can be extremely expensive, it is particularly important for organisations to conduct a robust assessment of lessons learned after major Business Email Compromise incidents to prevent similar incidents from occurring. |

The Incident Response Plan (IRP) may contain references to the organisation-defined playbooks. The playbooks will define the steps to follow in case of a specific incident, in this current playbook (Business Email Compromise). 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

In the initial phase, organisations will perform preparatory measures to ensure 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.

A diagram of a process

AI-generated content may be incorrect.

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  IT Team  Leadership team (CISO, CIO, CTO…etc) |
| 7.2.2 | Review and maintain a timeline | Create and maintain a timeline of events | Incident Response Team |
| 7.2.3 | Determine Extended Team & Define Roles | Define teams that are involved in the incident | Incident Response Team  IT Team |
| 7.2.4 | Define Escalation Path | Determine the list of stakeholders in case of escalation and define types of escalations | 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.

A diagram of a diagram

AI-generated content may be incorrect.

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 two 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 – 7.3.1.9 | 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 the Incident | Define the category of the incident or order to define its priority and the escalation level | Incident Response Team |
| 7.3.4 | Request relevant logs and information | Collect the logs and relevant evidence related to the incident, including up to 90 days before, to identify its origin  Sub steps: 7.3.4.1 – 7.3.4.2 | Incident Response Team |
| 7.3.5 | Gather details on impacted recipients | Gather information on the incident, such as the list of employees impacted and any remediation steps taken to date | Incident Response Team |
| 7.3.6 | Obtain copies of recently detected phishing emails | Collect any recently detected phishing emails that may be relevant to the incident | Incident Response Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.3.1.1 | Notification of updated payment details | Identify customers that have been sent fraudulent payment details | Incident Response Team  Legal team |
| 7.3.1.2 | Work performed outside of regular business hours | Identification and investigation of the work that was performed outside of agreed business hours | Incident Response Team  IT team |
| 7.3.1.3 | 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 |
| 7.3.1.4 | 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 |
| 7.3.1.5 | Suspicious forwarding rules | Check forwarding rules using the RSS folder or forwarding emails outside of the organisation | Incident Response Team  IT team |
| 7.3.1.6 | Suspicious logins | Identify logins from unknown IP addresses or unusual country locations | Incident Response Team  IT team |
| 7.3.1.7 | Indications of brute force attempts | Check for multiple back-to-back failed login attempts | Incident Response Team  IT team |
| 7.3.1.8 | Permission Changes | Identify any accounts that have been added to administrator groups or roles, or have been given permissions to other mailboxes | Incident Response Team  IT team |
| 7.3.1.9 | Items shared with individuals outside of the organisation | Identify items being shared with individuals outside of the organisation | Incident Response Team  IT team |
| 7.3.4.1 | Unified Audit Log | Ideally, a complete extract of all categories where time allows | Incident Response Team  IT team |
| 7.3.4.2 | OAuth Grants | List all current grants for applications, including the scope | Incident Response 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:

A diagram of a process

AI-generated content may be incorrect.

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)  Incident Response Team |
| 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 – 7.4.1.10 | Risk Management Team (GRC)  Incident Response Team |
| 7.4.2 | Custom | Define custom risk factor  Sub steps: 7.4.2.1 | Risk Management Team (GRC)  Incident Response Team |
| 7.4.3 | Research IOC (Indicators of Compromise) | Collect the sender’s email address, collect sending server details, collect URLs in the body of the malicious email, collect email attachments, collect and search for hash | Incident Response Team |
| 7.4.4 | Analyse account logins | Collect successful and unsuccessful login attempts for accounts included in the incident  Sub steps: 7.4.4.1 – 7.4.4.2 | Incident Response Team |
| 7.4.5 | Analyse account activity | Collect all activity for the suspected compromised accounts and analyse any activity from unknown IP addresses  Sub steps: 7.4.5.1 – 7.4.5.3 | Incident Response Team |
| 7.4.6 | Analyse all emails sent and received | Collect all emails sent and received by the accounts and identify any suspicious emails  Sub steps: 7.4.6.1 – 7.4.6.3 | Incident Response Team |
| 7.4.7 | Go to the post-incident phase | Move to the post-incident phase if no accounts were | Incident Response Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.4.1.1 | IP is at risk of being exposed | Identify if IP has been exposed | Risk Management Team (GRC)  Incident Response Team  IT Team |
| 7.4.1.2 | PII is at risk of being exposed | Identify if PII has been exposed | Risk Management Team (GRC)  Incident Response Team  IT Team |
| 7.4.1.3 | Customers are affected by this incident | Identify customers that are affected | Risk Management Team (GRC)  Incident Response Team  IT Team |
| 7.4.1.4 | Public safety is affected | Identify if public safety is affected | Governance and Compliance team  Legal Team |
| 7.4.1.5 | Personnel safety is not affected | Check that personnel safety is not affected | Risk Management Team (GRC)  Incident Response Team  The leadership team (C level) |
| 7.4.1.6 | This act could be exploited for criminal activity | Make sure that the information exposed is not used for illegal activity | Risk Management Team (GRC)  Incident Response Team  The leadership team (C level) |
| 7.4.1.7 | This act could harm the public brand | Document the incident and communicate it to the appropriate stakeholder and define the communication and legal approach | Legal Team  Communication Team  The leadership team (C level) |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.4.1.8 | Products, goods, or services are affected by this incident | Detect and list the assets affected by the incident | 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 external knowledge of this incident | Identify the external channel aware of the incident occurring | Incident Response Team  Legal Team  Communication/PR Team |
| 7.4.2.1 | Custom Factors | Identify the risk management process in specific scenarios unique to the organisation | Risk Team |
| 7.4.4.1 | Brute force attempts | Identify any accounts that may have been brute forced by analysing all successful and unsuccessful login events | Incident Response Team  IT Team |
| 7.4.4.2 | Multi-Factor Authentication (MFA) | Identify any logon events where the user was not issued, or failed, an MFA challenge, and the number of attempts before a successful login | Incident Response Team  IT Team |
| 7.4.5.1 | IP Geolocation | Use IP geolocation to identify activity from unknown locations, noting the dates of the first and last activity, and the user agents for each | Incident Response Team  IT Team |
| 7.4.5.2 | Suspicious IPs | Where suspicious IPs are identified, analyse all traffic from the IPs to identify any other users that may have been compromised |  |
| 7.4.5.3 | Impossible Travel | Ensure the user can physically travel between locations in the duration between logged activities. VPN usage may cause false positives | Incident Response Team  IT Team |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.4.6.1 | Received Emails | Analyse all emails received by the account to identify the source of the incident. If found, investigate the entire organisation for additional accounts that received the email | Incident Response Team  IT Team |
| 7.4.6.2 | Sent Emails | Identify any emails sent by the threat actor | Incident Response Team  IT Team |
| 7.4.6.3 | Inbox and Transport Rules | Analyse all inbox and transport rules within the organisation to identify any malicious rules that may be forwarding email outside the organisation or attempting to hide email within the associated account | Incident Response Team  IT 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.

A diagram of a computer program

AI-generated content may be incorrect.

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.5.1 | Additional Information Gathering | Identify the systems that have been affected, the data compromised, the IT services being impacted, and the ways the attack spread  Sub steps: 7.5.1.1 – 7.5.1.7 | 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 compromise the account | Investigation to find out how the account was compromised | Incident Response Team  IT Team |
| 7.5.4 | Identify lateral movement of the compromised user throughout the enterprise | Follow the spreading of the attack to identify the compromised user in the whole organisation  Sub steps: 7.5.4.1 – 7.5.4.4 | Incident Response Team |
| 7.5.5 | Block malicious URLs on Web proxy | Ensure the blocking of the malicious URLs | Incident Response Team  IT Team |
| 7.5.6 | Consider email filtering based on IOC gathering | Proceed to email filtering to ensure the rejection of the malicious emails | Incident Response Team |
| 7.5.7 | Determine the level of communication | Consider the type and level of communication according to the spread and impact of the incident in the organisation | Incident Response 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 |
| 7.5.4.1 | View Report | Generate a report on the compromised users or credentials | Incident Response Team |
| 7.5.4.2 | View Record Details | Check the details of the record | Incident Response Team |
| 7.5.4.3 | Select Records | Select records | Incident Response Team |
| 7.5.4.4 | Copy Record Details | Copy records details | Incident Response Team |

## Eradicate

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

A diagram of a computer program

AI-generated content may be incorrect.

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.6.1 | Consider password rest | Impacted users must change their corporate credentials. They should also consider changing the password to personal accounts such as social media or banking if they were associated with the email account | Incident Response Team |
| 7.6.2 | Consider full AV scan | Perform a full antivirus scan | Incident Response Team  IT Team |
| 7.6.3 | Remove malicious email from contaminated recipient’s mailbox | Eradicate the malicious emails from contaminated mailboxes if found to lead to the compromise of the account | 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;

A diagram of a company

AI-generated content may be incorrect.

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.7.1 | Consider education campaign | Promote education campaign | Incident Response Team |
| 7.7.2 | Consider organisation security awareness training | Organise security awareness training  Sub steps: 7.7.2.1 – 7.7.2.2 | 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** |
| 7.7.2.1 | Prepare security awareness training material | Define the content of security awareness training with a focus on phishing | Incident Response Team |
| 7.7.2.2 | Define security awareness training schedule | Prepare a security awareness training schedule | Incident Response Team |

## Post-Incident

Because the handling of incidents can be extremely expensive, it is particularly important for organisations to conduct a robust assessment of lessons learned after major business email compromise 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 incident | 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 organisation | 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)