**Template for Creating a Major Cyber Incident Response Plan**

Table of Contents

[**Instructions for Use** 3](#_heading=h.gjdgxs)

[**1. Introduction** 3](#_heading=h.30j0zll)

[**2. Incident Response Team** 3](#_heading=h.3znysh7)

[**3. Incident Detection and Reporting** 4](#_heading=h.2et92p0)

[**4. Initial Assessment and Triage** 4](#_heading=h.tyjcwt)

[**5. Containment Strategies** 5](#_heading=h.3dy6vkm)

[**6. Eradication and Recovery** 6](#_heading=h.1t3h5sf)

[**7. Communication Plan** 7](#_heading=h.4d34og8)

[**8. Evidence Collection and Preservation** 8](#_heading=h.2s8eyo1)

[**9. Testing and Maintenance** 8](#_heading=h.17dp8vu)

[**Appendices** 9](#_heading=h.3rdcrjn)

[**A. Incident Response Checklist** 9](#_heading=h.26in1rg)

[**B. Contact Lists** 10](#_heading=h.lnxbz9)

**Instructions for Use**

This Major Incident Response Template provides a framework for developing a comprehensive cyber incident response plan. It contains sample content that should be customised to fit the organisation's specific needs, structure, and resources.

Key stakeholders should be involved in developing the plan, which should be reviewed and updated regularly.

**Template**

**1. Introduction**

**1.1 Purpose and Scope of Plan**

***Sample content:***

This Major Cyber Incident Response Plan outlines the procedures for detecting, responding to, and recovering from significant cyber security incidents that may impact [Organisation Name]'s operations, data integrity, or reputation.

The objectives of this plan are to:

* Rapidly detect, contain and eradicate cyber incidents.
* Minimise damage and data loss.
* Restore normal operations as quickly as possible.
* Preserve evidence for potential legal proceedings.

**1.2 Definition of a Major Incident**

***Sample content:***

A Major Cyber Incident is defined as any event that:

* Compromises critical systems or sensitive data.
* Disrupts business operations for more than xx hours.
* Potentially impacts more than xxxx customers or employees.
* May result in financial losses exceeding $xxxxxx.
* Could lead to regulatory non-compliance or legal issues.

**2. Incident Response Team**

**Purpose:** Define the structure and roles of the incident response team.

* List all roles (e.g., Incident Commander, Technical Lead, Communications Officer).
* Provide contact information for each team member.
* Outline the escalation procedures.

***Sample Content:***

**2.1 Incident Response Team Structure:**

* Incident Commander/Leader: [Name], [Contact Info]
  1. Oversees the entire incident response process.
  2. Makes critical decisions and approves major actions.
* Technical Lead: [Name], [Contact Info]
  1. Directs technical investigation and containment efforts.
  2. Coordinates with IT and security teams.
* Communications Officer: [Name], [Contact Info]
  1. Manages internal and external communications.
  2. Liaises with PR and legal teams.
* Legal Advisor: [Name], [Contact Info]
  1. Provides legal guidance throughout the response.
  2. Ensures compliance with relevant regulations.
* HR Representative: [Name], [Contact Info]
  1. Manages employee-related aspects of the incident.
* Business Continuity Manager: [Name], [Contact Info]
  1. Oversees business impact assessment and recovery efforts.

**2.2 Escalation Procedures:**

***Sample Content***

* Initial incident reported to Technical Lead.
* Technical Lead assesses severity and notifies Incident Commander if criteria for major incident are met.
* Incident Commander activates the full Incident Response Team if necessary.
* Team members to be on standby within 30 minutes of notification.
* Full team assembly (virtual or physical) within 2 hours for major incidents.

**3. Incident Detection and Reporting**

**Purpose:** Establish procedures for detecting and reporting incidents.

* Provide step-by-step reporting procedures for employees.
* Include reporting templates or forms if applicable.

**3.1 Incident Detection and Reporting Process:**

***Sample Content*:**

1. If you suspect a cyber security incident, do not investigate on your own.
2. Immediately report the incident to the IT Help Desk:
   * Contact Info: [Help Desk Contact Info Number]
   * Email: [Help Desk Email]
3. Provide the following information:
   * Your name and contact information.
   * Date and time the incident was discovered.
   * Brief description of the incident.
   * Any observed impact on systems or data.
4. Follow any instructions provided by the IT Help Desk.
5. Do not discuss the incident with anyone unless instructed to do so by the Incident Response Team.

**4. Initial Assessment and Triage**

**Purpose:** Guide the team in assessing and prioritising incidents.

* Define criteria for assessing incident severity (e.g., data sensitivity, system criticality).
* Outline the triage process, including initial steps and decision points.

**4.1 Incident Severity Assessment Criteria:**

***Sample Content:***

1. Critical (Severity 1):
   * Widespread system outages affecting critical business operations.
   * Confirmed data breach of sensitive information.
   * Active cyber attack with potential for significant damage.
2. High (Severity 2):
   * Limited system outages affecting important business operations.
   * Suspected data breach, extent unknown.
   * Signs of targeted attack or advanced persistent threat (APT).
3. Medium (Severity 3):
   * Minor system disruptions with limited operational impact.
   * Potential policy violations with security implications.
   * Unusual activities requiring investigation.
4. Low (Severity 4):
   * Isolated security events with no immediate risk.
   * Minor policy violations.
   * Routine security alerts requiring attention.

**4.2 Triage Process:**

***Sample Content:***

1. Initial report received by Technical Lead.
2. Technical Lead performs rapid assessment:
3. For Severity 1 or 2 incidents:
   * Immediately escalate to Incident Commander.
   * Activate full Incident Response Team.
4. For Severity 3 incidents:
   * Technical Lead initiates investigation.
   * Escalates to Incident Commander if the situation worsens.
5. For Severity 4 incidents:
   * Handle through normal IT support channels.
   * Monitor for potential escalation.

**5. Containment Strategies**

**Purpose:** Provide strategies to limit the damage of an incident.

* List immediate actions to take for different types of incidents.
* Include procedures for isolating affected systems.
* Outline decision-making criteria for containment actions.

**5.1 Immediate Containment Actions by Incident Type:**

***Sample Content:***

1. Malware Outbreak:
   * Disconnect infected systems from the network.
   * Disable affected user accounts.
   * Block malicious IP addresses and domains at the firewall.
2. Data Breach:
   * Revoke access credentials for compromised accounts.
   * Encrypt sensitive data that may be at risk.
   * Implement additional access controls on critical systems.
3. Denial of Service (DoS) Attack:
   * Engage with ISP to filter malicious traffic.
   * Activate Cloud-based DoS mitigation services.
   * Temporarily take down public-facing services if necessary.
4. Insider Threat:
   * Revoke all access privileges for the suspected insider.
   * Preserve system logs and user activity data.
   * Monitor for any ongoing suspicious activities.

**5.2 System Isolation Procedure:**

* Identify all affected systems and their network connections.
* Determine the potential impact of isolation on business operations.
* Obtain approval from the Incident Commander for isolation actions.
* Use network segmentation tools to isolate affected systems.
* Implement firewall rules to restrict traffic to/from isolated systems.
* Monitor isolated systems for any signs of continued malicious activity.

**6. Eradication and Recovery**

**Purpose:** Guide the process of removing the threat and restoring systems.

* Outline steps for identifying and removing the root cause of the incident.
* Provide procedures for system restoration, including testing and verification.
* Include guidelines for determining when systems can be brought back online.

**6.1 Eradication Process:**

***Sample Content:***

1. Conduct thorough malware scans on all affected systems.
2. Remove any identified malware or unauthorised software.
3. Delete or disable compromised user accounts.
4. Patch all identified vulnerabilities.
5. Reset all passwords on affected systems.
6. Remove any unauthorised system changes or backdoors.

**6.2 System Restoration Procedure:**

***Sample Content:***

1. Prepare clean installation media or verified system images.
2. Reinstall operating systems and applications from trusted sources.
3. Apply all necessary security patches and updates.
4. Restore data from clean, verified backups.
5. Reassess the system to validate and ensure systems are clean.
6. Implement additional security controls as needed.

**6.3 Testing and Verification:**

***Sample Content:***

1. Conduct vulnerability scans on restored systems.
2. Perform penetration tests to verify system integrity.
3. Monitor system and network activity for any signs of persistent threats.
4. Verify functionality of all critical business applications.

**7. Communication Plan**

**Purpose:** Establish protocols for internal and external communication during an incident.

* Develop templates for different types of communications.
* List all stakeholders who need to be informed, including legal and PR teams.
* Include guidelines for communicating with the media and customers.

**7.1 Internal Communication Protocol:**

***Sample Content:***

* Initial notification to executives and department heads within xx hour of incident confirmation.
* Regular status updates to all employees every xx hours or as significant developments occur.
* Detailed briefings to affected teams or departments as needed.
* Use secure communication channels for sensitive information.

**7.2 External Communication Stakeholders:**

***Sample Content:***

* Customers
* Partners and vendors
* Regulatory bodies
* Law enforcement agencies
* Media outlets
* General public

**7.3 Media Communication Guidelines:**

***Sample Content:***

* All media inquiries to be directed to the Communications Officer.
* Prepare holding statements for initial responses.
* Schedule regular press briefings for significant incidents.
* Focus on facts and avoid speculation.
* Emphasise actions being taken to resolve the incident and protect stakeholders.

**8. Evidence Collection and Preservation**

**Purpose:** Ensure proper handling of evidence for potential legal proceedings.

**Sample Content:**

Evidence Collection Procedure:

* Create forensic images of affected systems using write blockers.
* Collect in-memory data before powering down systems.
* Securely bag and tag all physical evidence.
* Maintain detailed logs of all evidence-collection activities.

**9. Post-Incident Analysis**

**Purpose:** Learn from the incident to improve future response and prevention.

* Conduct a root cause analysis and business impact analysis.
* Implementing lessons learned.

**Sample Content: Lessons Learned Report**

1. Executive Summary
2. Incident Overview
   * Date and duration of the incident.
   * Systems and data affected.
   * Initial detection method.
3. Incident Timeline
4. Root Cause Analysis
5. Impact Assessment
   * Technical impact.
   * Business impact.
   * Financial impact.
6. Response Effectiveness
   * What worked well.
   * Areas for improvement.
7. Recommendations
   * Short-term actions.
   * Long-term improvements.

**10. Testing and Maintenance**

**Purpose:** Keep the plan up-to-date and ensure team readiness.

* Establish a schedule for regular plan reviews and updates.
* Outline different types of exercises (e.g., tabletop, full-scale simulations).

**Sample Content:**

Plan Review and Update Schedule:

* Monthly: Review and update contact lists and technical resource inventory.
* Quarterly: Conduct tabletop exercises and update response procedures.
* Annually: Perform full-scale simulation and comprehensive plan review.

Types of Exercises:

1. Tabletop Exercises
   * Frequency: Quarterly
   * Duration: 2-4 hours
   * Participants: Incident Response Team and key stakeholders
   * Format: Facilitator-led discussion of a simulated scenario
2. Functional Exercises
   * Frequency: Semi-annually
   * Duration: 4-8 hours
   * Participants: Incident Response Team and IT staff
   * Format: Hands-on response to simulated incidents in a test environment
3. Full-Scale Simulations
   * Frequency: Annually
   * Duration: 1-2 days
   * Participants: All employees, with external observers if possible
   * Format: Organisation-wide response to a complex, evolving scenario

**Appendices**

**A. Incident Response Checklist**

Initial Response:

* Assess the situation and verify the incident.
* Notify the Incident Commander.
* Activate the Incident Response Team if necessary.
* Establish a secure communication channel for the team.
* Start the incident log.

Containment:

* Identify affected systems and isolate them if necessary.
* Disable compromised user accounts.
* Block malicious IP addresses or domains.
* Preserve volatile evidence before any system changes.

Eradication:

* Perform deep scans for malware on all affected systems.
* Remove all malicious components identified.
* Patch vulnerabilities that were exploited.
* Reset all passwords on affected systems.
* Remove any unauthorised accounts or access points.

Recovery:

* Restore systems from clean backups or rebuild from scratch.
* Apply all necessary security patches and updates.
* Reconfigure system settings according to security baselines.
* Verify system and data integrity.
* Test system functionality before bringing it back online.
* Implement additional security controls as needed.

Post-Incident:

* Conduct a thorough post-incident analysis.
* Document lessons learned.
* Update incident response plan based on findings.
* Conduct additional training if necessary.
* Prepare and deliver post-incident reports to stakeholders.

**B. Contact Lists**

1. Incident Response Team
   * Incident Commander: [Name], [Contact Info]
   * Technical Lead: [Name], [Contact Info]
   * Communications Officer: [Name], [Contact Info]
   * Legal Advisor: [Name], [Contact Info]
   * HR Representative: [Name], [Contact Info]
   * Business Continuity Manager: [Name], [Contact Info]
2. Key Internal Stakeholders
   * CEO: [Name], [Contact Info]
   * CIO: [Name], [Contact Info]
   * CISO: [Name], [Contact Info]
   * Department Heads: [List with contact details]
3. External Resources
   * Cyber Security Firm: [Company Name], [Contact Person], [Contact Info]
   * Forensic Investigators: [Company Name], [Contact Person], [Contact Info]
   * Legal Counsel: [Firm Name], [Legal Name], [Contact Info]
   * PR Firm: [Company Name], [Contact Person], [Contact Info]
4. Relevant Authorities
   * Australian Federal Police: [Department Name], [Contact Info]
   * Australian Cyber Security Centre [Name], [Contact Info]
   * Office of the Privacy Commissioner: [Name], [Contact Info]