**Ransomware Incident Response Playbook**

### **Purpose**

This playbook provides a tactical, step-by-step guide for preparing, detecting, analysing, containing, and recovering from ransomware incidents. It is intended for use by Managed SOC providers, customer IT/Security teams, and other stakeholders involved in cybersecurity incident response.

###

### **Structure**

The playbook aligns with the eight-phase incident response lifecycle

1. Prepare
2. Identification
3. Triage
4. Analysis
5. Containment
6. Eradication
7. Recovery
8. Review

Each phase outlines actions, responsibilities, triggers, and documentation requirements.

**Approval:** This document template is made publicly available by Talanos Cybersecurity for use within your own organisation, where it can be customised, approved and then marked CONFIDENTIAL.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Author** | **Version** | **Changes** |
| 1 July 2025 | Talanos Cybersecurity | 1.0 | Initial version – Base Template |
|  |  |  |  |

Contents

[**Purpose** 1](#_Toc206490597)

[**Structure** 1](#_Toc206490598)

[**1. Prepare** 4](#_Toc206490599)

[**2. Identification** 7](#_Toc206490600)

[**3. Triage** 7](#_Toc206490601)

[**4. Analysis** 8](#_Toc206490602)

[**5. Containment** 8](#_Toc206490603)

[**Escalation decision matrix (post-containment)** 9](#_Toc206490604)

[**Roles & Responsibilities** 10](#_Toc206490605)

[**6. Eradication** 10](#_Toc206490606)

[**7. Recovery** 11](#_Toc206490607)

[**8. Review** 11](#_Toc206490608)

[**Appendix A – Incident Log Template** 12](#_Toc206490609)

[**Appendix B – Ransomware Incident Questions** 12](#_Toc206490610)

###

### **1. Prepare**

**Objective:** Establish policies, tools, and training to minimise ransomware risk and enable a rapid, coordinated response. The risk of ransomware attacks can be drastically reduced if the correct controls are implemented extensively.

Key Actions:

**1. Governance & Planning**

* Define and approve a Ransomware Response Policy that sets clear authority, escalation paths, and decision-making powers.
* Maintain an Incident Response Team (IRT) roster with 24/7 contact details for internal leads, SOC, vendors, cyber insurer, law enforcement, and regulators.
* Ensure legal counsel is engaged in advance for potential breach notifications.
* Well documented infrastructure including business and application owners, reduce the response time during an attack.

**2. Asset Management & Criticality Mapping**

* + Maintain an up-to-date inventory of all IT assets, including servers, endpoints, network devices, SaaS apps, and OT systems.
	+ Classify systems and data based on business criticality and sensitivity (e.g., AD, ERP, customer PII).

**3. Backup & Recovery Readiness**

* + Implement 3-2-1 backup strategy (3 copies, 2 media types, 1 offline/offsite).
	+ Regularly test backup restoration for integrity and recovery speed.
	+ Ensure offline backups are immutable or protected from ransomware encryption.
	+ Protect backup network devices shares, avoid anonymous and everyone access.

**4. Security Controls**

* + Deploy and maintain EDR/XDR on all endpoints and servers.
	+ Enforce multi-factor authentication (MFA) for all privileged and remote access.
	+ Disable unnecessary services (e.g., RDP if not required).
	+ Patch operating systems and 3rd party software within defined SLAs.
	+ Review network shares and avoid unprotected shares that everyone has access to.
	+ Enable advanced threat protection on email systems to prevent email-based attacks.
	+ Regularly review access to privileged accounts.
	+ Disable SMB v1, this outdated protocol is a common target
	+ Restrict external access to SMB ports (445, 137, 138, 139)
	+ Review RDP (3389) access from external 3rd parties, avoid options that enable file transfer e.g. copy from clipboard allowed
	+ Actively monitor logs and develop a good knowledge of the environment’s normal operation

**5. Network Architecture & Segmentation**

* + Segment critical business systems from general user and Wi-Fi networks.
	+ Limit administrative privileges and use just-in-time (JIT) access.
	+ Implement egress filtering to block malicious C2 traffic.
	+ Review the Firewall rules at least quarterly and ensure a default “block any” rule is implemented.

**6. Detection & Monitoring**

* + Configure SIEM/SOC to detect:
* Unusual file modification spikes.
* Mass encryption activity.
* New/unknown executable execution.
	+ Establish alert severity and escalation criteria.
	+ Review and test detection rules that are implemented for the detection of ransomware

**7. Training & Awareness**

* + Run phishing simulation campaigns at least quarterly.
	+ Conduct ransomware tabletop exercises with IT, security, and executive stakeholders.
	+ Educate staff on early reporting signs (e.g., ransom notes, inaccessible files).

**8. Pre-Approved Communication Templates**

* + Prepare internal and external comms templates (execs, staff, customers, media).
	+ Maintain alternate communication channels to be used in the event of email compromise.

**9. Cyber Insurance & External Resources**

* + Ensure cyber insurance covers ransomware events, including forensics and negotiation.
	+ Pre-engage an IR retainer with a specialist firm for rapid deployment.

**Trigger to Proceed:** Detection of potential ransomware indicators via monitoring, user report, or SOC alert.

### **2. Identification**

* **Indicators:**
	+ File encryption with unfamiliar extensions
	+ Ransom notes present
	+ Access errors or file corruption reports
	+ SIEM/EDR alerts, AV detections
	+ Complaints from users of unavailable files or services

**Key Actions:**

* + Document detection source and timestamp
	+ Capture affected systems and user accounts
	+ Save ransom note content and filenames
	+ Begin incident log (Appendix A)

**Trigger to Proceed:** Confirmed ransomware indicators AND severity score ≥3

### **3. Triage**

**Objective:** Validate incident, establish initial scope and risk level

**Checklist:**

* + Confirm encryption activity and ransom demand
	+ Determine number of impacted systems and users
	+ Identify initial access vector (if known)
	+ Check backup availability and integrity
	+ Assess if critical services are affected (AD, HRIS, Finance)

**Trigger to Proceed:** Scope validated, backups assessed, impact on operations confirmed

### **4. Analysis**

**Objective:** Determine root cause, scope of compromise, and attacker behaviour

**Investigate:**

* + Initial access vector (phishing, RDP, vulnerabilities)
	+ Malware strain and IOCs (hashes, domains)
	+ Lateral movement and persistence mechanisms
	+ Any signs of data exfiltration (network logs, external connections)

**Branching:** - If data exfiltration suspected, refer to Data Loss Battle Card

**Trigger to Proceed:** Threat understood, containment strategy validated, exec approval

### **5. Containment**

**Objective:** Prevent further spread while preserving evidence

**Key Actions:**

* + Isolate infected endpoints
	+ Isolate network segments, when the containment requires swift action.
	+ Disable compromised accounts
	+ Revoke credentials and tokens
	+ Block attacker IPs/domains
	+ Capture memory images if forensics are required, don’t shutdown systems.
	+ Initiate a company-wide scan

### **Escalation decision matrix (post-containment)**

A severity score helps to prioritise response efforts and supports escalation decisions:

| **Criteria** | **1 (Low)** | **3 (Medium)** | **5 (Critical)** |
| --- | --- | --- | --- |
| **Systems Affected** | Fewer than 2 endpoints | Several endpoints | Core systems (e.g. AD, ERP, finance) |
| **Data Sensitivity** | No sensitive data impacted | Internal documents only | Regulated or customer data affected |
| **Regulatory Exposure** | No reporting obligations | Possible contract impact | Confirmed legal/regulatory reporting required |
| **Operational Disruption** | No real impact | Minor delay to operations | Business downtime, financial loss |
| **Threat Propagation** | Fully contained | Limited lateral movement | Active spread across network |

1. Score each row (1, 3, or 5 — or interpolate with 2 or 4 if needed)

2. Add up the total score

3. Use the total to guide urgency and resourcing

| **Total Score** | **Severity Level** | **Response Guidance** |
| --- | --- | --- |
| 5–8 | Low | Monitor and contain |
| 9–12 | Medium | Escalate to IR team, start containment |
| 13–17 | High | Activate full IR plan, notify key stakeholders |
| 18–25 | Critical | Exec-level involvement, consider breach notification |

### **Roles & Responsibilities**

| **Phase** | **Lead** | **Contact Info** | **Supporting Roles** |
| --- | --- | --- | --- |
| Prepare | IT Team | [Phone/email] | IT Operations Manager, CISO, Solutions Architect |
| Identification | IT/Security team | [Phone/email] | Managed SOC provider, Helpdesk |
| Triage | Managed SOC | [Phone/email] | IT Ops, Customer CISO |
| Analysis | Managed SOC | [Phone/email] | Incident Manager, Forensics |
| Containment | Managed SOC | [Phone/email] | Network and Server Admin, Legal |
| Eradication | IT Lead | [Phone/email] | SOC, IT operations team  |
| Recovery | IT & Business | [Phone/email] | SOC, Exec Sponsor, IT Operations team |
| Review | Incident Manager | [Phone/email] | All involved parties |

### **6. Eradication**

**Objective:** Remove malware and eliminate attacker presence

**Key Actions:**

* + Reimage or clean affected hosts
	+ Remove malicious persistence (scripts, tasks, registry)
	+ Patch exploited vulnerabilities
	+ Reset passwords and MFA tokens
	+ Monitor all assets, network and user activity for IOCs consistent with the attack profile

**Trigger to Proceed:** Systems verified clean by AV/EDR scan, logs show no active threats

### **7. Recovery**

**Objective:** Restore systems and operations to trusted state

**Checklist:**

* + Restore validated backups
	+ Reconnect systems in staged approach
	+ Monitor for recurrence or reinfection
	+ Re-verify access control and segmentation
	+ Continue to monitor dark web and ransomware operator blog sites

**Business Engagement:** Include function owners in go/no-go decisions

**Trigger to Proceed:** All systems pass integrity and functionality checks, business sign-off obtained

### **8. Review**

**Objective:** Capture learnings, ensure continuous improvement

**Actions:**

* + Conduct post-incident review meeting
	+ Finalise root cause analysis
	+ Document incident in full (timeline, actions, roles)
	+ Identify gaps in tooling or detection
	+ Update playbooks, training, and preventative controls
	+ Consider notification to regulators or insurers if applicable
	+ Update company response plans, policies, standards and user training, review SOC processes.
	+ Setup continuous improvement program to address control failures and root cause

###

### **Appendix A – Incident Log Template**

| # | Timestamp | IR Phase | Action | Owner | Notes |
| --- | --- | --- | --- | --- | --- |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |

###

### **Appendix B – Ransomware Incident Questions**

* Was a ransom note present and what was the demand?
* Were files exfiltrated or exposed?
* Was double extortion or public shaming threatened?
* Were cyber insurers notified?
* Was law enforcement engaged?
* Are notifications (e.g., GDPR, DORA) required?