Microsoft Security

Ransomware incident response playbook framework

Learn how to build a ransomware IR playbook to prepare and protect your organization

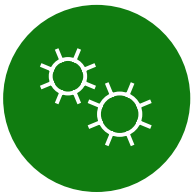
What is a ransomware incident response (IR) playbook?

A step-by-step guide that *serves* as a single source of truth to proactively mitigate, detect, respond, and recover from ransomware incidents. The playbook defines key stakeholders, processes, policies & prevention plans to defend your organization. Additionally, the playbook should be accompanied by other appropriate plans to ensure their processes are in place to restore normal operations quickly and to comply with applicable regulatory requirements.

Why is a ransomware IR playbook needed?

Be prepared to act in the event of an attack

Limit incident impact to save data, time, and money



Return to normal business operations as quickly as possible

Proactively reduce the risk of future attacks

Who plays a role in playbook development?

Security & Risk Management professionals

Chief Information Security Officer (CISO), Chief Technology Officer (CTO), Chief Audit Executive (CAE), Chief Information Officer (CIO), Chief Compliance Officer (CCO), Chief Security Officer (CSO), IT & security operations teams.

Finance

Discuss ransom payment options, including crypto, and prioritize decisions based on circumstance and business priorities so you're prepared to act.

Legal counsel

Provide guidance related to law enforcement engagement and documentation requirements in compliance with federal agencies and customer reporting.

Procurement

Communicate existing cyber insurance coverages. Procurement can assist with cyber insurance onboarding if a policy was not already in place to deliver necessary services.

Communications

Develop a plan that provides detail on how information will be communicated internally and externally—before, during, and after an incident.

How often to refresh a playbook?

Playbooks are most effective when they stay current, evolve with organizational changes and act as living documents. It's crucial to identify necessary updates, ownership, process improvement opportunities on a consistent basis. As threat landscapes and ransomware tactics are constantly changing, playbook updates are recommended on a semi-annual basis, or if any of the following occur:

- A ransomware incident
- Tabletop exercises, or other dry-runs/simulations
- Changes in key business stakeholders
- Major changes in the ransomware ecosystem

IR playbook framework

Ransomware IR playbooks should be structured with incident response framework principles in mind. This IR framework is based on guidance from the National Institute of Technology (NIST) Computer Security Incident Handling Guide, SP800-61 Rev 2. Per NIST's guidelines, four primary phases of security incident response should be included to develop an effective incident response playbook.

Preparation | **Detection and analysis** | **Containment, eradication, recovery** | **Post-incident response**

Phase 1: Preparation

Preparation is a foundational component to building effective incident response capabilities. This section provides an overview of the processes in place to help mitigate the risk of ransomware, and the roles and responsibilities of key stakeholders. It's recommended that the outlined sections in this phase are customized to fit your organization and thoroughly documented.

Roles and responsibilities

Clearly define key stakeholders, provide up-to-date roles and responsibilities, and outline necessary actions if a ransomware attack is detected.

Security awareness training

Implement company-wide required security training to communicate dangers of malicious threats and guidance on identifying suspicious activity with steps to protect. Educate users on how to report questionable activity to security teams.

Data backups and recovery

All important data and metadata must be backed up periodically in a vault that is immutable, air-gapped and caged. Partial drills are recommended to make sure data is valid and recoverable.

Endpoint protection

Ensure programs, policies, and procedures are in place to manage endpoint and mobile device security so devices are more resilient to ransomware and other malware infections. Examples: harden requirements, install antivirus and antimalware solutions, update operating systems and applications, etc. Invest in XDR-driven solutions like Microsoft Defender for Endpoint to secure your devices.

Network protection

Ensure programs, policies and procedures are deployed to monitor and secure entry and egress points to the network: firewalls, use of least privilege access, enforce strong authentication methods such as multifactor authentication (MFA), antispam solutions for email, physical security, etc. Invest in a SIEM-powered software like Microsoft Sentinel for access to advanced insights with built-in behavioral analytics to get ahead of attackers.

Security policies

Security policies should be kept current and be enforced for all identities, users, and accounts that have access to company assets and resources.

Documentation and drills

Full recovery procedures should be documented and updated with every major service release. Implement full drills to confirm key stakeholders are prepared to jump into action if an incident occurs.

Phase 2: Detection and analysis

Stay informed in common attack vectors used in ransomware attacks. Strategize and document security detection and response plans, they may differ depending on the method of attack. In addition, create process flow to show the end-to-end process of incidents detected, reported, triaged, and resolved.

Common attack methods according to NIST:

- Email attachments and embedded malicious links
- Web browser vulnerabilities
- Infected programs bundled with malware
- Portable USB devices

Incident response teams should implement consistent methods of evaluating and prioritizing ransomware events to determine required escalations. Create an incident impact matrix to determine required escalation.

Matrix example - incident impact and action

Critical, escalation required	High, escalation required	Moderate, notify appropriate personnel	Low, manage through normal IR process

Phase 3: Containment, eradication, recovery

Containment

A containment strategy should be created to define what actions should be taken once a system has been identified as potentially having ransomware. Single-system examples: shut down system, disconnect from network, disable certain functions. Multi-system examples: disconnecting broadly-impacted sites to prevent lateral movement if impact is isolated or disabling outbound connectivity at site level to cut attacker command and control.

Eradication

After an incident is contained, it's important to enforce procedures to eradicate ransomware from the environment. Eradication examples: delete malware, disable breached user accounts, and mitigate all exploited vulnerabilities.

Additionally, root cause analysis (RCA) should be performed to potentially help determine the type of ransomware and attack infiltration method to implement mitigation controls against future similar attacks.

Recovery

Containment and RCA activities should be performed before recovery procedures. Recovery plans should be documented to outline how affected files and data will be restored by reliable and secure backup sources.

Phase 4: Post-incident response

All security incidents should have a post-incident response (PIR) completed. In a PIR, security incident responders should work with responsible parties to:

- Identify the root cause of the incident and create high-level plans to prevent future incidents with similar patterns
- Implement mitigating technical controls to address identified gaps
- Identify technical or communication lapses, procedural failures, manual errors, and process flaws that could potentially influence a delay in threat response
- Evaluate response procedures for sufficiency and completeness of operating procedures
- Evaluate and improve cybersecurity training for employees
- Enforce company-wide security policies

Ransomware defense checklist

Prevent attackers from getting in

Remote access

- ☐ Secure multicloud and hybrid environments
- ☐ Get full visibility of your SaaS apps
- ☐ Maintain software and app updates
- ☐ Enforce Zero Trust user/device validation
- ☐ Configure security for third-party VPN solutions
- ☐ Deploy Point-to-Site (P2S) VPN
- ☐ Publish on-premises web apps with Application Proxy
- ☐ Secure cloud resource access

Email and collaboration

- ☐ Implement modern email security for the entire organization
- ☐ Enable attack surface reduction (ASR) rules to block common attack techniques

Endpoints

- ☐ Provide modern endpoint protection across all platforms
- ☐ Prevent device & system tampering
- ☐ Reduce the attack surface with rules that enable/disable specific device behaviors
- ☐ Block known threats at first sight
- ☐ Manage device settings at scale
- ☐ Apply security baselines to harden internet-facing servers, clients and applications
- ☐ Maintain updated software
- ☐ Isolate, disable, or retire vulnerable systems and protocols
- ☐ Block suspicious traffic with host-based firewalls and network defenses

Identities

- ☐ Protect your on-premises identities with cloud-powered intelligence
- ☐ Enforce strong MFA or passwordless sign-in for all users
- ☐ Strengthen password security to protect against breaches

Prevent attackers from escalating their privileges

Privileged access strategy

- ☐ Enforce end-to-end security for admin portals using conditional access
- ☐ Protect and monitor identity systems to prevent escalation attacks
- ☐ Detect and mitigate lateral traversal with compromised devices
- ☐ Use privileged identity management (PIM) time-based and approval-based role activation
- ☐ Use privileged access management (PAM) to limit access to sensitive data or critical configuration settings

Detection and response

- ☐ Gain visibility across your entire digital estate with a modern SIEM
- ☐ Automatically stop attacks and coordinate response across assets with XDR
- ☐ Combine SIEM+XDR to increase efficiency and effectiveness while securing your digital estate
- ☐ Gain access to global threat intelligence to identify external tools and systems used by attackers in SIEM+XDR incidents
- ☐ Provide high quality alerts, minimize friction and manual steps during response
- ☐ Prioritize common entry points and monitor for brute-force attempts like password spray
- ☐ Don't ignore commodity malware
- ☐ Monitor for an adversary disabling security (often part of an attack chain) such as:
  - Event log clearing, especially the security event log and Powershell Operational logs
  - Disabling of security tools and controls (associated with some groups)
- ☐ Integrate incident response experts with global threat intelligence to provide professional guidance
- ☐ Rapidly isolate compromised devices with advanced endpoint protection

Protect your critical data from access and destruction

Secure backups

- ☐ Automatically backup all critical systems on a regular cadence
- ☐ Protect backups against deliberate erasure and encryption:
  - Strong protection: require out of band steps (MFA or PIN) before modifying online backups
  - Strongest protection: store backups in online immutable storage and/or fully offline or off-site
- ☐ Regularly exercise your business continuity/disaster recovery (BC/DR) plan
- ☐ Protect supporting documents required for recovery such as restoration procedure documents, your configuration management database (CMDB) and network diagrams

Data protection

- ☐ Migrate your organization to the cloud:
  - Move user data to cloud solutions like OneDrive/ SharePoint to take advantage of versioning and recycle bin capabilities
  - Educate users on how to recover their files by themselves to reduce delays and cost of recovery
  - Designate protected folders
- ☐ Review your permissions:
  - Discover broad write/delete permissions on file sharing solutions. Broad is defined as many users having write or delete permissions for business-critical data.
  - Reduce broad permissions while meeting business collaboration requirements
  - Audit and monitor to ensure broad permissions don't reappear

Supercharge your defense with built-in AI, automation, and global threat intelligence

Automatic attack disruption and response to ransomware at machine speed

PREVENT

Industry-leading ransomware prevention with threat-based configuration recommendations that incorporate AI and machine learning to automatically stop threat actors in your environment. Block ransomware before it harms your business.

DETECT

AI-driven detection capabilities with automatic attack disruption. Stops progression and limits the impact of an attack across devices, identities, apps, email, data and cloud workloads.

RESPOND

Optimize SOC efficiency with a unified investigation and remediation experience. Deploy automated data backup capabilities that let you resume operations as quickly as possible.

Why Microsoft?

- AI-powered automatic attack disruption & response
- Hybrid environment protection that delivers visibility and risk remediation for managed and unmanaged devices
- Insightful, actionable alerts and posture recommendations to reduce attack surface
- SIEM+XDR integration to protect the entire kill chain

Microsoft security products are chosen over any other brand by security decision-makers to protect against ransomware and cyber extortion[1]

Microsoft 365 Defender
Stop attacks and coordinate response across assets with XDR

Hybrid Identities | Endpoints & IoT | Email & Collaboration
Cloud Apps | Data Loss Prevention

Microsoft Sentinel
Gain visibility across your entire digital estate with a modern SIEM

Infrastructure | Devices | Users | Application | IoT/OT

Microsoft Defender for Cloud
Secure your infrastructure

DevSecOps | Cloud Security Posture Management
Cloud Workload Protection

Microsoft Defender Threat Intelligence
Understand and eliminate modern threats with dynamic threat intelligence

Enhanced Detection & Remediation | Latest IoCs
Advanced Investigations | Raw & Finished Intelligence

[1] Microsoft Internal Research

Microsoft Incident Response

Your first call before, during, and after a cybersecurity incident.

What is Microsoft Incident Response?

Microsoft Incident Response provides fast, flexible services that will remove a bad actor from your environment, build resilience for future attacks, and help mend your defenses after a breach. Our global team of incident responders leverage expertise from Microsoft product engineers, security analysts, and threat researchers, along with governments around the world, to help customers keep their most sensitive, critical environments secure.

Incident response needs vary, and Microsoft provides service options for proactive attack preparation, and reactive crisis response, and compromise recovery so you can regain full control of your environment after damage is contained.

Available services:

Proactive incident response services

Compromise Assessment

Receive a point-in-time, deep analysis of your environment, including proactive investigation for persistent threats and security risks.

Crisis Readiness Exercise

Assist your team with exercises based on real-world observations and mitigation tactics. These include the identification and remediation of high-privileged identities to reduce the risk of compromise.

Reactive incident response services

Incident Response

Get global investigation and guidance—all day, every day—to help evaluate incident scope, contain attacks, and restore critical systems, with options for onsite and remote.

Compromise Recovery

Remove attacker control from an environment, regain administrative control after a cybersecurity incident, and tactically harden high-impact controls to help prevent future incidents.

Incident Response Retainer

Retain Microsoft expertise to respond and recover fast

Get peace of mind with the Incident Response Retainer, which provides flexible prepaid hours to help you prepare for and respond to cybersecurity attacks.

IR Retainer

Learn more → https://aka.ms/MicrosoftIR

Interested in purchasing? Email us at MicrosoftIR@Microsoft.com

Learn more

Ransomware | Microsoft 365 Defender | Microsoft Sentinel | Microsoft Incident Response