Ransomware response playbook

Playbook | English · Template to adapt | v3.0 · 2026-10-16

Template version: 3.0. Preparation assumes an organization of approximately 80 staff, potentially outsourcing IT and monitoring. Roles are functions that may be combined with deputies. An internal decision maker retains business-risk acceptance. Providers execute only authorized actions within their actual access and contracted scope.

How to use this playbook. Sections 1–6 give the short sequence. Apply sections 7–8 on responsibilities and dependencies before isolation, and sections 10–11 before recovery. Section 9 guides preservation; section 12 provides the example. Use these references at the relevant action, not after closure. Urgent preauthorized protection remains possible within its limits; record missing checks or information.

Type: adaptable operational procedure. This playbook supports the incident response policy. It covers suspected malicious encryption or data extortion affecting authorized endpoints, servers, cloud services and backups. It contains no automatic deletion or recovery commands. Assign the bracketed responsibilities and test the steps before relying on them during an incident.

Approval and preparation

Field	Value to complete
Organization, reference, version	[TO COMPLETE: organization, reference, version]
Owner and approver	[TO COMPLETE: security lead, management]
Approval and next review	[TO COMPLETE: dates]
Covered services and systems	[TO COMPLETE: scope, exclusions]
Incident and response lead	[TO COMPLETE: reference, name, deputy]
Independent crisis channel	[TO COMPLETE: tested channel, offline directory]

Management arbitrates major interruptions. The incident lead coordinates; the SOC assesses scope and tracks propagation. Systems, identity, network and backup teams execute authorized measures. Business owners set continuity priorities. Communications and legal advisers validate messages and applicable obligations with the relevant contacts. These assignments must match actual authority and supplier responsibilities.

Prepare critical asset inventories, recovery dependencies, emergency access and responder contacts before an incident. Check availability without relying solely on normal email. In industrial, healthcare or other safety-sensitive environments, physical safety and operating procedures take priority over mechanically applying this document. Record unavailable capabilities so the plan does not assume resources that nobody has committed.

1. Activate and assess

☐ Open the incident workbook and timestamp the first report.

☐ Record symptoms, hosts, affected paths, messages and detection sources.

☐ Check a sample without opening suspicious files on an ordinary workstation.

☐ Identify unavailable services and confirmed business impact.

☐ Activate coordination using [TO COMPLETE: thresholds, escalation arrangements].

Visible encryption does not necessarily mark the beginning of the intrusion. Investigate account compromise, backup deletion, persistence and possible exfiltration as well. Extortion can occur without encryption. Keep confirmed loss, suspected access and missing evidence distinct; an attacker's statement is not independent confirmation of the data they claim to hold.

2. Limit propagation

Use proportionate containment, record its authorization and verify the result. CISA guidance favors network isolation of affected systems; shutdown is a fallback when disconnection is unavailable and needed to stop propagation. Shutdown can destroy volatile evidence. Have the incident lead arbitrate this tradeoff using urgency, dependencies and safety constraints, rather than prescribing a universal power-off action.

☐ Isolate identified hosts using controlled methods; verify the actual effect.

☐ Restrict risky shares and remote access after assessing impact.

☐ Protect backup repositories and their administration accounts.

☐ Revoke or restrict compromised accounts with the identity team.

☐ Check remote-site and cloud coverage of containment measures.

☐ Record exceptions required for safety or continuity.

Do not reconnect a host simply to see whether it works. Avoid mass deletion of files or logs. Do not submit samples containing organizational information to a public service without authorization. If containment depends on a supplier, name the internal owner responsible for confirming execution and following up unanswered requests.

3. Preserve and understand

Question	Proposed collection, subject to authority	Owner
What is affected?	Inventory, alerts, shares and cloud resources	[TO COMPLETE: team]
What was the initial access?	Identity, remote-access, email and exposed-service logs	[TO COMPLETE: team]
How did activity progress?	Network, endpoint, administration and account-change logs	[TO COMPLETE: team]
What data may be lost?	Read/export records, transfers and data inventory	[TO COMPLETE: team]

Preserve ransom notes, timestamps, authorized samples and backup-change records. Memory or disk acquisition requires appropriate methods and skills. Record collection, integrity, storage, access and limitations in the workbook. Distinguish evidence of exfiltration from indicators and unavailable data. Prioritize evidence according to its volatility and the decisions it supports, without delaying urgently needed protection merely to complete a checklist.

4. Organize crisis decisions

Maintain a shared service status: unavailable, isolated, rebuilding or validated. Set an update cadence [TO COMPLETE: frequency] and a decision maker for each tradeoff. Competent advisers identify notifications and contacts according to jurisdiction, sector, contracts and affected data; no universal reporting deadline applies to every organization. Keep uncertainty visible in situation reports and record the next decision expected.

This template does not recommend paying a ransom. Any decision about an extortion demand requires specific governance and competent advice. An attacker's promise does not guarantee recovery or deletion of stolen data. Preserve any exchanges in a controlled channel; analysts must not improvise commitments on behalf of the organization.

5. Rebuild and restore

☐ Examine known or plausible initial access and address identified persistence paths. Document remaining uncertainty and obtain incident-lead acceptance of residual risk before recovery.

☐ Provide a separate recovery environment with trusted administration.

☐ Select backups using date, integrity and contamination risk.

☐ Address implicated access paths and vulnerabilities before service return.

☐ Restore a pilot service and test function and security controls.

☐ Obtain business-owner acceptance before expanding recovery.

☐ Maintain enhanced monitoring and a practicable fallback.

Record which systems and dependencies were tested, what failed and what remains unknown. A successful restoration does not independently establish that every hostile access path has been removed. Avoid reusing unverified administration credentials or reconnecting restored systems to a suspected environment without a controlled decision.

6. Close and exercise

Document known loss, uncertain periods, restored services and residual risks. Assign owners and due points to corrections. Exercise this playbook using unavailable email, a doubtful backup and a compromised administrator account. Judge the exercise by traceable decisions and verified recovery, not merely server restarts. Track exercise gaps until the responsible owner demonstrates the agreed correction.

Limitations: actions must respect authority, business constraints and specialist procedures. This template does not prove complete eradication or regulatory compliance. It must be adapted for the affected technologies, supplier arrangements and safety needs.

Decision gates

The incident lead adapts these gates to severity and safety constraints. They make progress explicit without imposing identical timelines or demanding absolute certainty. Accepted residual risk records the available facts, uncertainties, decision maker and next check.

Proposed gate	Evidence and authority to complete
Initial containment	[TO COMPLETE: isolated systems, exceptions, checks, decision maker]
Reconstruction authorized	[TO COMPLETE: trusted scope, access addressed, accepted unknowns]
Pilot recovery	[TO COMPLETE: technical tests, business acceptance, monitoring]
Agreed operating state	[TO COMPLETE: residual risks, owners, stop conditions]

If suspicious indicators reappear, pause expansion and reassess scope. A new alert does not automatically establish reinfection; retain its source and compare it with the changes made. Recovery reports identify services actually tested and unverified dependencies. Temporary access and fallback environments receive an owner and a removal condition.

7. Coordinate outsourced response

Before adoption, connect this playbook to actual endpoints, remote workers, files, identity, email, SaaS, hosting and backups. For each service, identify the business owner, technical executor, contract owner and route to an out-of-hours decision. Do not assume an on-call service exists unless its availability and resources are confirmed.

Decision	Proposed internal authority	Execution and evidence
Isolate a noncritical endpoint	Coordinator within delegation	Authorized operator or provider; isolation checked
Stop a shared service	Business owner or management	Operator; dependencies and consequences recorded
Restrict identity or backup access	Designated authority with relevant owners	Authorized administrator; necessary access and lockout risk checked
Approve rebuild and recovery	Management or delegated business owner	Provider; technical/business criteria met or residual risk accepted

The coordinator activates a channel independent of the suspect environment and verifies responders using known contact details. Assign a common case reference to IT, MSSP, host and backup requests. Record requested, executed, verified or impossible states. An MSSP may lack administrative access; forwarding an alert is not containment.

If a provider does not respond, use its backup contact and contractual escalation route. Record attempts, consequences and protection available without additional privileges. The internal authority decides whether to suspend activity or wait with protection, within safety limits. Do not share emergency credentials in a group conversation simply to bypass an unavailable contact.

8. Check dependencies before disconnection

Build a short dependency map: identity needed by administrators, networks needed for backups, business service dependencies and communications. Keep it readable outside the suspect system. Identify circular dependencies, such as a vault accessible only through the unavailable identity it is meant to restore. Decide before an incident how authorized people can recover essential capabilities.

Dependency	Question before action	Decision and record
Identity and administration	Will isolation remove emergency access or collection?	[TO COMPLETE: authorized solution, owner]
Backup and storage	Can compromised accounts or networks modify copies?	[TO COMPLETE: verified protection, retained access]
Business and safety	Is abrupt interruption unsafe?	[TO COMPLETE: decision, degraded operation]
Providers and remote work	Who can act on off-site systems?	[TO COMPLETE: coverage, contact, limitation]

Active propagation may require initial isolation before the map is complete. Record assumptions, authority, intended effect and next verification. An unavailable measure must not stop every decision: propose a narrower scope, business interruption or access restriction that can actually be performed. Check compensating protection rather than merely announcing it.

Examine backup administration as its own scope: console, accounts, repository, remote copies and recovery capabilities. StopRansomware recommends backup protection; owning a backup product does not establish that these components are unreachable by the attacker. Ask the owner to demonstrate protections and record limits. Do not destroy a doubtful copy before its preservation and recovery value are assessed.

9. Preserve for specific questions

Ask providers for records needed to establish plausible initial access, identity changes, affected systems and backup changes. Specify period, time zone, source and export format. Preserve ransom notes and

detection identifiers without unnecessarily reproducing sensitive data in crisis messages. Record who can explain an export and answer completeness questions after the original operator leaves.

For volatile or disk acquisition, the executor describes risk, method, tool and authority. The coordinator records when urgency requires losing a collection opportunity. Do not improvise specialist acquisition on a critical server. If logs expired or are missing, consider other relevant authorized sources; do not fill the gap with certain attribution.

SaaS providers may have their own procedures and contractual response arrangements. Obtain a request reference, exportable scope, preservation time and available checks. “No alert” does not establish no access: ask what was actually monitored. Tie each conclusion to its period and sources rather than describing an entire environment as clean without qualification.

10. Rebuild in a controlled scope

Reconstruction begins with a decision, dependency inventory and authorized administration. Prioritize systems by business need; check identity, network, name resolution, applications, keys and required permissions. Authorized people must be able to retrieve emergency instructions and associated secrets without relying exclusively on the suspect domain. Keep access to these materials restricted while ensuring the agreed recovery path works.

Stage and input	Expected action	Failure and exit evidence
Approved reconstruction scope	Prepare separated networking and administration according to assessment	If isolation or access is unverified, pause admission; retain check and decision
Trusted image or installation media	Install, patch and configure selected systems	If origin is doubtful, obtain trusted media; record versions and checks
Candidate backup	Examine date, integrity and relevant indicators in test scope	Preserve unresolved copy; choose another path or obtain explicit acceptance of limits
Restored pilot service	Test business function, security and dependencies	Do not expand after failure; record defect, owner and retest

A backup predating encryption is not necessarily earlier than every compromise. Choose recovery points using the available timeline and its unknowns. The recovery lead explains data loss, estimated time with limitations and alternatives. The business authority accepts the tradeoff before restoration expands; technical staff must not silently make that business-risk decision.

Order account, secret and supplier-access changes to avoid losing remediation capabilities or reintroducing compromised access. Exact operations belong in an approved technical procedure, not a universal command from this template. After sensitive changes, check essential access and failure of the specific access paths the measure was intended to remove.

11. Return-to-service checks

☐ Pilot scope and dependencies are identified with tests actually completed.

☐ Known or plausible initial access and identified persistence have treatment or accepted limitations.

☐ Administration and backup access have been reviewed with owners.

☐ Business staff perform a representative operation and verify data consistency.

☐ Relevant protections and alerts are tested with a named recipient.

☐ Exceptions identify risk, verified compensation, authority, expiry and reassessment.

☐ Temporary access, fallback environments and restrictions have removal owners.

☐ Reappearing indicators have an escalation route and suspension condition.

Recovery exception	Value to complete
Service, gap and business effect	[TO COMPLETE: scope, missing protection, consequences]
Compensation and evidence	[TO COMPLETE: restriction, completed check, limits]
Decision	[TO COMPLETE: authority, rationale, date]
End	[TO COMPLETE: expiry, reassessment trigger, remediation owner]

12. End-to-end scenario — entirely fictional

Workshop-80, a fictional 80-person business, discovers encrypted files on a share at 09:00 UTC. IT is outsourced; the MSSP sees endpoint alerts but does not administer storage. The internal coordinator opens EX-R1 and calls the provider's verified contact. Because email is suspect, decisions use the agreed fallback channel. None of these results describes a real operation or customer experience.

At 09:08 UTC, the provider confirms isolation of two fictional endpoints. It cannot yet act on a powered-off remote laptop; that device remains uncontrolled. The business owner authorizes stopping the affected share and processing orders manually. The backup console is not declared clean: its owner separately examines access and changes.

Fictional decision	Rationale and authority	Evidence and uncertainty
EX-D1: stop the share	Limit changes; delegated management	Access check completed; initial intrusion unknown
EX-D2: preserve export and candidate copy	Investigation and recovery preparation; coordinator	Export received; period completeness still unverified
EX-D3: restore a separated pilot	Priority business need; order-processing owner	Test operation succeeds; remote device and earlier period unchecked

The fictional previous-day backup supports pilot preparation, but its age does not exclude earlier intrusion. IT explains available checks and management accepts limited recovery without reconnecting the uncontrolled device. Business staff reconcile orders created after the restored point before expansion. Exception EX-X1 covers unavailable historical logs, with targeted monitoring, ownership and a locally agreed reassessment point.

Accept the exercise if a replacement responder can find decisions and evidence, business staff demonstrate a consistent operation and unknowns remain visible. Fail it if a sent ticket counts as completed isolation, a backup is presumed clean or management is unaware of residual risk. Assign corrective actions before calling the playbook ready; a successful demonstration must not conceal untested dependencies.

Working references

Part 2 of the CISA StopRansomware Guide provides a response checklist, including isolation and preservation; the guide also covers prevention, extortion and recovery. ANSSI's incident remediation guidance provides a remediation framework. The proposed checklists and responsibilities require local adaptation and testing.