CYBERSECURITY & RANSOMWARE INCIDENT RESPONSE MASTER PLAYBOOK

A website-ready educational guide and customizable operational template

PURPOSE

This master document explains how organizations can prepare for, identify, contain, eradicate, recover from, and learn from cybersecurity incidents, with an expanded ransomware-specific response procedure. It is designed for publication as informational content and for internal customization.

Organization / Website	[Insert name]
Document owner	[Insert role or department]
Version	1.0
Effective date	[Insert date]
Review frequency	At least annually and after each significant incident or exercise

IMPORTANT NOTICE

This material is provided for general educational and planning purposes. It is not legal, regulatory, insurance, forensic, or professional advice. Every incident is different. Organizations should engage qualified cybersecurity, legal, privacy, insurance, communications, and law-enforcement professionals as appropriate. Do not use this document as a substitute for organization-specific plans, contracts, regulatory analysis, or expert judgment.

This document is an original synthesis informed by public guidance from NIST, CISA, the FBI, and other government resources listed in the References section. It does not reproduce any source playbook verbatim.

How to Use This Document

- Website use: publish selected educational sections, checklists, and FAQs. Remove internal-only fields, contact lists, and decision criteria before posting.
- Operational use: replace bracketed placeholders, assign named owners, validate contact information, align actions with your technology stack, and obtain legal and leadership approval.
- Exercise use: test the playbook through tabletop exercises at least annually and after major technology or business changes.
- Incident use: create an incident record immediately, assign an incident commander, preserve an accurate timeline, and document every material decision.

Table of Contents

1. Executive Overview
2. Incident Response Governance
3. Preparation and Readiness
4. Detection, Validation, and Triage
5. Incident Severity and Escalation
6. Containment
7. Investigation and Evidence Preservation
8. Eradication and Remediation
9. Recovery and Restoration
10. Communications, Legal, Insurance, and Reporting
11. Ransomware-Specific Response Playbook
12. Common Incident-Type Mini-Playbooks
13. Post-Incident Review and Improvement
14. Ready-to-Use Forms and Checklists
15. Website FAQ
16. References and Source Attribution

1. Executive Overview

Cybersecurity incident response is the coordinated process used to limit harm, preserve evidence, restore operations, meet obligations, and improve defenses after a suspected or confirmed security event. Modern incident response is not merely a technical activity. It requires coordination among leadership, IT, security, legal counsel, privacy, communications, human resources, finance, business operations, vendors, insurers, and —when appropriate—law enforcement.

NIST SP 800-61 Revision 3, finalized in 2025, integrates incident response across the six Cybersecurity Framework 2.0 functions: Govern, Identify, Protect, Detect, Respond, and Recover. This playbook uses that broader model while retaining the familiar operational flow of preparation; detection and analysis; containment; eradication; recovery; and lessons learned.

FIRST PRINCIPLE

Protect people first, then contain ongoing harm, preserve reliable evidence, maintain safe business operations, and restore services in a controlled manner. Speed matters, but uncoordinated actions can destroy evidence, alert an attacker, or expand business disruption.

Core Objectives

- Confirm whether an incident has occurred and determine its scope and business impact.
- Stop or reduce ongoing unauthorized activity without causing unnecessary damage.
- Preserve evidence and maintain a defensible record of facts, actions, and decisions.
- Restore critical services from trusted systems and data.
- Meet contractual, insurance, legal, regulatory, and notification obligations.
- Identify root causes and implement improvements that reduce recurrence and impact.

2. Incident Response Governance

The response structure should be established before an incident. During a major event, uncertainty over authority and ownership creates delay. The organization should document who may declare an incident, isolate systems, shut down services, engage external responders, authorize emergency spending, communicate externally, and make decisions regarding extortion demands.

Recommended Roles

Role	Primary responsibilities
Executive sponsor	Provides authority, resolves business priorities, approves high-impact actions, and keeps executive leadership or the board informed.
Incident commander	Owns coordination, objectives, decision cadence, workstreams, status reporting, and the authoritative incident record.
Technical lead	Directs technical investigation, containment, eradication, restoration, and validation.
Forensic lead	Preserves and analyzes evidence, documents collection methods, maintains chain of custody, and supports root-cause analysis.
IT operations / recovery lead	Maintains infrastructure dependencies, backups, rebuild sequencing, and controlled service restoration.
Legal and privacy counsel	Directs privilege strategy, assesses obligations, coordinates notifications, and advises on evidence, contracts, and communications.
Communications lead	Prepares consistent internal, customer, partner, media, and public messaging.
Insurance liaison	Notifies the carrier or broker, confirms consent requirements, tracks covered vendors and costs.
Business continuity lead	Coordinates manual processes, alternate operations, critical service priorities, and business impact decisions.
Human resources	Supports insider, employee, workforce, and policy issues.
Scribe / timeline manager	Records facts, timestamps, actions, decisions, owners, approvals, and outstanding questions.

Authority Matrix

Decision	Authorized role	Required consultation
Declare a major incident	[Insert]	Security, IT, legal, executive sponsor
Disconnect a critical system or site	[Insert]	System owner, incident commander, business continuity
Engage external incident response	[Insert]	Legal, insurance, procurement
Notify insurer	[Insert]	Legal, finance, incident commander
Contact law enforcement	[Insert]	Legal, executive sponsor
Approve public statement	[Insert]	Legal, communications, executive sponsor
Approve ransom or extortion decision	[Insert]	Executive authority, legal, insurer, law enforcement as appropriate
Restore production service	[Insert]	Technical lead, system owner, security validation

3. Preparation and Readiness

Preparation determines how effectively an organization can respond under pressure. Maintain the following capabilities before an incident occurs.

☐ An approved incident response policy, plan, and ransomware annex with clear activation criteria.

☐ A 24x7 reporting path for employees, customers, vendors, monitoring tools, and third parties.

☐ Current asset, identity, application, data-flow, dependency, and network inventories.

☐ Centralized logging with synchronized time, defined retention, protected storage, and tested search access.

☐ Endpoint detection and response, email security, identity monitoring, network visibility, and cloud audit logging.

☐ Offline or logically isolated backups, immutable copies where practical, documented recovery priorities, and routinely tested restores.

☐ Secure emergency communications independent of potentially compromised email, directory, or collaboration systems.

☐ Pre-negotiated contacts for external incident response, breach counsel, cyber insurance, crisis communications, restoration vendors, and law enforcement.

☐ Administrative access protections: phishing-resistant MFA where feasible, separate admin accounts, least privilege, privileged access controls, and emergency accounts.

☐ Tabletop exercises covering ransomware, data theft, cloud compromise, business email compromise, and destructive attacks.

Emergency Contact Register

Function	Primary contact	Alternate	Out-of-band method
Incident commander	[Name / mobile]	[Name / mobile]	[Method]
Executive sponsor	[Name / mobile]	[Name / mobile]	[Method]
Legal / breach counsel	[Firm / number]	[Alternate]	[Method]
Cyber insurance	[Carrier / policy / hotline]	[Broker]	[Method]
External IR / forensics	[Provider / hotline]	[Alternate]	[Method]
Cloud / hosting provider	[Provider / severity contact]	[Alternate]	[Method]
Law enforcement	FBI field office / IC3 / local authority	[Alternate]	[Method]
CISA	CISA reporting channel / regional contact	[Alternate]	[Method]

4. Detection, Validation, and Triage

Every report should be logged and evaluated. Initial responders should distinguish an observable event from a confirmed incident, but they should not delay reasonable containment when evidence indicates active harm.

Initial Triage Checklist

☐ Record who reported the event, when, how, and what was observed.

☐ Assign a unique incident identifier and open a protected incident record.

☐ Capture screenshots, alert details, filenames, hashes, IP addresses, domains, usernames, timestamps, ransom notes, and relevant logs.

☐ Determine whether the activity is active, ongoing, spreading, or affecting safety or critical operations.

☐ Identify affected users, endpoints, servers, networks, cloud tenants, applications, data, and third parties.

☐ Check for evidence of privileged-account use, persistence, lateral movement, data staging, exfiltration, encryption, or destructive activity.

☐ Estimate initial business impact and identify critical dependencies.

☐ Assign severity, activate the appropriate team, and establish the next briefing time.

☐ Preserve volatile evidence where feasible before power-off or destructive remediation.

☐ Use an out-of-band communication channel if email, identity, or collaboration services may be compromised.

Questions to Answer During Scoping

- What is the earliest known suspicious activity?
- What initial access method is suspected?
- Which identities or credentials are compromised?
- Which systems and environments are confirmed affected, suspected affected, or verified clean?
- Is the attacker still active?
- Was data accessed, collected, staged, or transferred?
- Are backups, hypervisors, identity systems, security tools, or management platforms affected?
- Are customers, vendors, regulated data, or critical services involved?
- What can be safely contained now, and what business risk would that action create?

5. Incident Severity and Escalation

Severity	Typical characteristics	Response expectation
SEV-1 Critical	Widespread ransomware or destructive activity; threat actor active with privileged access; critical operations or safety affected; material data theft likely; major customer impact.	Immediate full-team activation; executive, legal, insurance, and external IR engagement; frequent situation reports.
SEV-2 High	Confirmed compromise of important systems or privileged identity; limited encryption; significant data exposure possible; major service degradation.	Rapid activation of core team; legal and leadership notification; external support considered.
SEV-3 Moderate	Contained malware, compromised standard account, isolated cloud or application incident, limited operational impact.	Security-led response with documented scope, containment, remediation, and management reporting.
SEV-4 Low	Suspicious event or policy violation with no confirmed compromise and minimal impact.	Routine investigation, documentation, corrective action, and monitoring.

Severity should be reassessed as facts change. A technically small incident may warrant high severity because of the data involved, regulatory exposure, customer impact, threat actor, or business timing.

6. Containment

Containment should interrupt attacker access and prevent additional harm while preserving the organization's ability to investigate and recover. Use the least destructive action that effectively reduces immediate risk, but do not allow evidence preservation concerns to override safety or ongoing material harm.

Potential Containment Actions

- ☐ Isolate affected endpoints through EDR or network controls; disconnect network cables or disable wireless only when remote isolation is unavailable or untrusted.
- ☐ Disable or restrict compromised accounts, revoke sessions and tokens, rotate credentials, and block unauthorized authentication methods.
- ☐ Block malicious IP addresses, domains, URLs, email senders, hashes, certificates, tools, and command-and-control patterns where appropriate.
- ☐ Disable exposed remote services, malicious forwarding rules, unauthorized OAuth applications, rogue devices, and persistence mechanisms.
- ☐ Segment affected network areas and restrict administrative protocols, east-west traffic, VPN access, and remote management paths.
- ☐ Protect backups, hypervisors, domain controllers, cloud control planes, security consoles, and privileged access systems.
- ☐ Preserve firewall, identity, EDR, email, cloud, DNS, proxy, VPN, and application logs before retention windows expire.
- ☐ Create temporary business workarounds and prioritize safety-critical or revenue-critical operations.

CAUTION

Avoid immediately reimaging every affected device, deleting malware, rebooting critical systems, or broadly resetting accounts without a coordinated plan. These actions may remove evidence, trigger destructive behavior, eliminate access needed for analysis, or fail to remove attacker persistence.

7. Investigation and Evidence Preservation

The investigation should establish an evidence-supported timeline, identify initial access, determine the attacker's actions and objectives, define affected assets and data, and provide actionable findings for containment and recovery.

Evidence Sources

- Endpoint telemetry, memory captures, disk images, event logs, registry and persistence artifacts.
- Identity-provider sign-in, MFA, session, conditional access, privileged activity, and audit logs.
- Firewall, VPN, DNS, DHCP, proxy, network flow, packet capture, and intrusion-detection data.
- Email headers, mailbox audit, message trace, forwarding rules, delegated access, and OAuth grants.
- Cloud control-plane, workload, storage, SaaS, API, and application audit logs.
- Hypervisor, backup, RMM, PSA, monitoring, vulnerability management, and security platform logs.
- File-access, database, data-loss prevention, and data-transfer records.
- Threat intelligence and indicators, used as leads rather than proof by themselves.

Evidence Handling Principles

- Record collector, date and time, source, method, tool, destination, and cryptographic hash where appropriate.
- Store evidence in access-controlled, integrity-protected locations separate from production.
- Maintain original evidence and analyze verified working copies when feasible.
- Document time zones and known clock differences.
- Coordinate with counsel when privilege, litigation, notification, employee monitoring, or privacy issues may apply.
- Do not attribute an attacker or claim data theft solely from a ransom note or threat-actor statement; corroborate claims.

8. Eradication and Remediation

Eradication removes attacker access and the conditions that enabled compromise. It should be based on a sufficiently complete understanding of scope. Remediation that begins too early may leave hidden persistence or cause the attacker to change tactics.

☐ Remove malicious software, persistence, scheduled tasks, services, accounts, keys, tokens, applications, rules, and configurations.

☐ Patch exploited vulnerabilities and remediate exposed services and insecure configurations.

☐ Rebuild systems from trusted images when integrity cannot be established.

☐ Rotate compromised credentials, service-account secrets, API keys, certificates, recovery codes, and signing keys in dependency-aware order.

☐ Review privileged groups, trust relationships, federation, application consent, conditional access, and remote administration.

☐ Update detection logic and hunt across the environment for related behaviors and artifacts.

☐ Validate that security tooling is functioning and has not been disabled, bypassed, or tampered with.

☐ Document residual risks, accepted exceptions, owners, and due dates.

9. Recovery and Restoration

Recovery should restore business services from trusted infrastructure and data while maintaining visibility for signs of recurrence. The recovery plan should be driven by business priorities and technical dependencies, not merely by which system is easiest to restore.

Recovery Sequence

1. Establish a trusted recovery environment and secure administrative access.
2. Validate identity, DNS, networking, time, certificate, logging, EDR, backup, and management foundations.
3. Confirm the selected recovery point predates compromise and is free of known malicious artifacts.
4. Rebuild or restore systems in dependency order using trusted media and configurations.
5. Apply patches, hardening, monitoring, and credential changes before production access.
6. Perform technical, security, data-integrity, and business-owner acceptance testing.
7. Reconnect services in controlled stages with heightened monitoring and rollback criteria.
8. Communicate restoration status and remaining limitations.
9. Continue threat hunting and monitoring through a defined stabilization period.

Recovery Acceptance Criteria

☐ Root cause and major persistence paths have been addressed.

☐ Affected credentials and trust relationships have been remediated.

☐ Systems are built from trusted sources and meet current configuration requirements.

☐ Required logging and security controls are enabled and reporting.

☐ Backups and restore processes have been validated.

☐ Business owners confirm function and data integrity.

☐ The incident commander and technical lead approve production release.

10. Communications, Legal, Insurance, and Reporting

Communications should be accurate, consistent, timely, and limited to verified facts. Use a single source of truth and an approval process. Avoid speculation, premature attribution, unsupported statements about data access, and promises that cannot be guaranteed.

Stakeholder Communication Matrix

Audience	Typical content	Owner / approval
Employees	What happened at an appropriate level, required actions, approved workarounds, phishing warnings, and reporting instructions.	HR / communications / legal
Executives / board	Business impact, scope, actions, risks, decisions required, recovery forecast, financial and legal considerations.	Incident commander / executive sponsor
Customers / partners	Verified impact, service status, protective actions, support channels, and notification information where required.	Communications / legal / business owner
Insurer	Prompt notice, incident facts, vendors, approvals, cost tracking, and coverage-related documentation.	Insurance liaison / legal
Law enforcement / government	Indicators, timeline, attacker communications, payment information if relevant, and requested evidence.	Legal / incident commander
Media / public	Approved holding statement or updates based on verified facts.	Communications / legal / executive

Reporting and Notification Considerations

- Notify cyber insurance promptly and follow policy requirements before retaining vendors or incurring major costs when feasible.
- Engage counsel early to assess contractual, privacy, sector, state, federal, international, employment, and litigation obligations.
- Report ransomware to appropriate law-enforcement and government channels. In the United States, FBI reporting options include the Internet Crime Complaint Center (IC3) and local FBI field offices; CISA also accepts cyber incident reports.
- Preserve copies of all notifications, submissions, approvals, and communications.

- Track deadlines from the moment facts are known; do not wait for the investigation to be fully complete before assessing obligations.

11. Ransomware-Specific Response Playbook

Ransomware incidents commonly involve more than encryption. Threat actors may steal data, disable security tools and backups, compromise identity systems, destroy recovery infrastructure, and use extortion threats. Treat ransomware as a potentially enterprise-wide compromise until evidence supports a narrower scope.

DO NOT

Do not communicate with the attacker, make promises, pay funds, run an unknown decryptor, delete ransom notes, or wipe systems without approval from the incident commander and coordination with legal counsel, insurers, forensic responders, and law enforcement as appropriate.

Immediate Actions — First 15 Minutes

☐ Declare a suspected ransomware incident and activate the incident commander.

☐ Use an out-of-band bridge or communication platform.

☐ Isolate actively encrypting or clearly compromised systems using EDR or network controls.

☐ If multiple systems are rapidly encrypting, consider emergency segmentation or targeted shutdown of affected network paths while protecting critical infrastructure.

☐ Protect backup systems, hypervisors, identity systems, security consoles, RMM tools, and cloud control planes from further access.

☐ Preserve ransom notes, filenames, screenshots, alert data, and initial logs.

☐ Notify legal counsel, executive leadership, the insurer, and external IR according to the activation matrix.

First Hour

☐ Identify confirmed encrypted systems, systems showing precursor activity, and systems with privileged or administrative access.

☐ Determine whether the attacker is still active and whether encryption is continuing.

☐ Block known malicious infrastructure and revoke clearly compromised sessions and accounts.

☐ Assess domain controllers, identity providers, VPN, email, backup, virtualization, RMM, and security-management platforms.

☐ Preserve volatile evidence from representative systems when safe and feasible.

☐ Identify the likely earliest compromise date and begin enterprise-wide threat hunting.

☐ Establish business-critical service priorities and manual workarounds.

☐ Begin a decision log and cost tracker.

First 4–24 Hours

☐ Determine initial access, privilege escalation, lateral movement, persistence, defense evasion, data staging, exfiltration, and encryption methods.

☐ Create lists of confirmed affected, suspected affected, and validated-clean assets and identities.

☐ Assess backup integrity, isolation, retention, recovery points, and restore capacity without connecting backups to an untrusted environment.

☐ Identify data potentially accessed or exfiltrated and the affected individuals, customers, systems, jurisdictions, and contracts.

☐ Coordinate law-enforcement and government reporting through counsel or the designated liaison.

☐ Develop a containment and eviction plan that addresses identity, endpoints, servers, network, cloud, remote access, persistence, and credentials together.

☐ Develop a clean recovery architecture and restoration sequence.

☐ Prepare approved internal and external holding statements.

Ransom / Extortion Decision Framework

The FBI does not encourage paying ransom, and payment does not guarantee data recovery, deletion, confidentiality, or safety from future extortion. Any decision must be made by authorized executives with legal, sanctions, insurance, law-enforcement, financial, operational, and ethical considerations evaluated by qualified professionals.

Question	Evidence / decision record
Can operations be restored safely without payment?	[Document]
What is the verified condition of backups and expected recovery time?	[Document]
Is there a credible threat to safety or critical services?	[Document]
What data is confirmed or reasonably believed stolen?	[Document]
What legal, sanctions, anti-money-laundering, or regulatory issues apply?	[Counsel determination]
What does the insurance policy require or cover?	[Carrier determination]
Has law enforcement been consulted?	[Document]
What are the risks of nonpayment, payment, failed decryption, repeat extortion, and public release?	[Document]
Who has final authority and what approvals are required?	[Document]

Ransomware Recovery Checklist

☐ Build a trusted administrative environment; assume previous administrative workstations and credentials may be compromised.

☐ Restore identity and core services first, with new credentials and validated configurations.

☐ Prioritize systems based on life safety, legal requirements, customer impact, revenue, dependencies, and recovery feasibility.

☐ Use trusted images and validated backups; do not simply decrypt and return compromised systems to production.

☐ Install EDR, logging, patches, and hardening before reconnection.

☐ Test restored data for integrity and application consistency.

☐ Reconnect in controlled waves and monitor authentication, remote execution, persistence, data transfer, and encryption indicators.

☐ Maintain a separate list of systems that cannot yet be trusted or restored.

☐ Continue investigation even after operations resume; recovery does not prove the attacker has been removed.

12. Common Incident-Type Mini-Playbooks

Business Email Compromise / Account Takeover

- Disable or restrict the account; revoke sessions, tokens, app passwords, and suspicious authentication methods.
- Preserve sign-in, mailbox, audit, message trace, inbox-rule, forwarding, delegate, and OAuth logs.
- Review fraudulent payments or changed banking instructions; contact financial institutions immediately through verified channels.
- Search for malicious messages sent internally or externally and warn recipients.
- Reset credentials from a trusted device; confirm MFA and recovery methods.
- Review other accounts for password reuse, shared sessions, consent grants, or lateral movement.

Malware on an Endpoint

- Isolate the endpoint and preserve alert details and volatile evidence as needed.
- Determine execution chain, user context, persistence, command-and-control, credential access, and lateral movement.
- Hunt for the same behavior across the environment.
- Rebuild when integrity cannot be established; otherwise remove artifacts and validate thoroughly.
- Reset exposed credentials and monitor for recurrence.

Cloud / SaaS Compromise

- Preserve control-plane, identity, audit, storage, API, workload, and application logs.
- Revoke compromised tokens and keys; disable malicious identities, applications, integrations, and access policies.
- Review changes to logging, security controls, federation, roles, network rules, storage permissions, and recovery settings.
- Assess data access and transfer using provider logs and application records.
- Restore secure configurations through reviewed infrastructure-as-code or trusted baselines.

Data Exfiltration / Privacy Incident

- Preserve records showing access, search, staging, compression, transfer, deletion, and external destinations.
- Identify the data types, owners, individuals, jurisdictions, contracts, and systems involved.
- Avoid unsupported precision; document confirmed, likely, possible, and ruled-out data separately.
- Coordinate notification analysis and communications through legal and privacy counsel.

13. Post-Incident Review and Improvement

Conduct a structured review after stabilization, and begin capturing lessons as soon as they are identified. The purpose is improvement, not blame.

Review Questions

- What happened, and what evidence supports the timeline?
- What was the initial access and root cause?
- Why did preventive or detective controls not stop or identify the activity earlier?

- What actions worked well, and which caused delay or confusion?
- Were authority, communications, vendor, insurance, and legal processes effective?
- Were logs and evidence sufficient?
- Did backups and recovery plans perform as expected?
- What technical, procedural, staffing, training, contract, architecture, or governance changes are required?
- Who owns each corrective action, by when, and how will completion be verified?

Corrective Action Register

Finding / lesson	Corrective action	Owner	Due date	Priority	Validation
[Example: MFA gap]	[Implement phishing-resistant MFA for admins]	[Owner]	[Date]	High	[Test / evidence]
[Finding]	[Action]	[Owner]	[Date]	[H/M/L]	[Method]
[Finding]	[Action]	[Owner]	[Date]	[H/M/L]	[Method]

14. Ready-to-Use Forms and Checklists

Incident Intake Form

Field	Entry
Incident ID	
Date/time reported and time zone	
Reporter and contact	
Detection source	
Summary of observed activity	
Affected users / systems / services	
Known indicators	
Business impact	
Current status: active / contained / unknown	
Initial severity	
Incident commander	
Next briefing time	

Incident Timeline Template

Date/time + zone	Source	Fact / action / decision	Owner	Evidence reference

Date/time + zone	Source	Fact / action / decision	Owner	Evidence reference

Situation Report (SITREP) Template

- Incident ID / title:
- Reporting period and time zone:
- Current severity and status:
- Executive summary:
- Confirmed scope:
- Suspected scope / open questions:
- Business and customer impact:
- Actions completed:
- Actions in progress and owners:
- Decisions required:
- Risks / blockers:
- Recovery outlook:
- Next update time:

Evidence Log

Evidence ID	Date/time	Collected by	Source / description	Method / tool	Hash / integrity	Storage location

Decision Log

Date/time	Decision	Alternatives considered	Decision maker / approver	Rationale / evidence

15. Website FAQ

What is a cybersecurity incident response playbook?

A playbook is a documented set of roles, decisions, and response actions for handling a suspected or confirmed cybersecurity incident. It helps teams act consistently under pressure while preserving flexibility for the facts of each event.

What should an organization do first after discovering ransomware?

Activate the incident response team, establish secure communications, isolate actively affected systems, protect identity and backup infrastructure, preserve evidence, and engage legal, insurance, forensic, and leadership contacts according to the organization's plan. Avoid indiscriminate wiping, rebooting, or attacker communication.

Should a ransomware victim turn off infected computers?

There is no universal answer. Network isolation is often preferable because powering off may destroy volatile evidence, while leaving a system connected may allow encryption or lateral movement to continue. The correct action depends on active harm, available isolation controls, system criticality, and responder guidance.

Should an organization pay a ransom?

Law-enforcement agencies generally discourage ransom payments. Payment does not guarantee recovery or deletion of stolen data and may create legal or sanctions risks. The decision requires authorized leadership and advice from legal counsel, insurers, law enforcement, and qualified incident-response professionals.

How often should an incident response plan be tested?

At least annually, after material changes to technology or business operations, and after significant incidents. High-risk organizations may test individual procedures more frequently.

Does restoring from backup end a ransomware incident?

No. Restoration addresses availability, but the attacker may retain access, stolen credentials, persistence, or exfiltrated data. Investigation, containment, credential remediation, trusted rebuilding, and continued monitoring remain necessary.

16. References and Source Attribution

The following authoritative public resources informed this original synthesis. Review the source websites for updates before relying on this playbook operationally.

Source	Resource	Public URL
National Institute of Standards and Technology (NIST)	SP 800-61 Revision 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (April 2025).	https://csrc.nist.gov/pubs/sp/800/61/r3/final
Cybersecurity and Infrastructure Security Agency (CISA)	StopRansomware Guide, including ransomware prevention and response best practices and a response checklist.	https://www.cisa.gov/stopransomware/ransomware-guide
CISA	Federal Government Cybersecurity Incident and Vulnerability Response Playbooks.	https://www.cisa.gov/sites/default/files/2023-02/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf
CISA	Incident Response Plan Basics.	https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf
Federal Bureau of Investigation (FBI)	Ransomware reporting and victim guidance.	https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware

Source	Resource	Public URL
FBI	Ransomware Prevention and Response for CISOs.	https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view
NIST	Ransomware Protection and Response resources.	https://csrc.nist.gov/Projects/ransomware-protection-and-response/publications

Source note: NIST SP 800-61r3 supersedes Revision 2 and reframes incident response as an organization-wide cybersecurity risk-management activity. CISA's StopRansomware Guide provides ransomware-focused preventive and response practices. FBI resources emphasize reporting and caution that ransom payment is not encouraged and does not guarantee recovery.

Document Customization Checklist

☐ Replace every bracketed placeholder.

☐ Insert company-specific technologies, escalation thresholds, network isolation procedures, and recovery dependencies.

☐ Validate all phone numbers, policy numbers, contracts, and out-of-band contact methods.

☐ Have legal counsel review notification, evidence, privacy, employee, and communications language.

☐ Have the cyber insurer confirm notice and vendor-consent requirements.

☐ Approve the authority matrix and ransom/extortion decision authority.

☐ Run a tabletop exercise and update the document from lessons learned.

☐ Create a sanitized public website version separate from the confidential operational version.