cyber.encse

Ransomware Response Playbook

A step-by-step incident response guide for ransomware events — triage, containment, eradication, recovery, and post-incident review.

Version	1.0
Published	August 2026
Scope	Enterprise IT environments — Windows/Linux/hybrid cloud
Audience	Incident responders, SOC analysts, IT/security leadership

This playbook is a general-purpose framework, not a substitute for a tested, organisation-specific incident response plan. Adapt roles, tooling, and thresholds to your environment, and validate the plan with tabletop exercises before you need it for real.

Published by eNeoteric Consultancy Services · cyber.encse.com

Contents

1. Before an Incident — Preparation Checklist

Ransomware response is won or lost before the incident starts. Confirm the following are in place and tested.

- **Offline/immutable backups** exist for all Tier-1 systems, with restore tested in the last 90 days (3-2-1 rule: 3 copies, 2 media types, 1 offsite/offline).
- **Incident Response Plan** is documented, current, and every responder knows their role (IC, comms lead, forensics lead, legal liaison).
- **Out-of-band communications** channel is agreed (e.g. a Signal group or phone tree) — assume email/chat/AD may be compromised.
- **EDR/AV** deployed on all endpoints with centralised alerting and remote isolation capability.
- **Asset inventory** and network diagram are current — you cannot contain what you cannot see.
- **Cyber insurance policy** reviewed — know your insurer's incident hotline and any pre-approved IR/forensics vendors.
- **Legal counsel and law enforcement contacts** (local cybercrime unit / national CERT) are on file.
- **Retainer with an external DFIR firm** is in place, or at minimum, vetted vendors identified in advance.

2. Phase 1: Detection & Initial Triage (0–1 hour)

Goal: confirm scope and severity without tipping off the attacker or destroying evidence.

- Validate the alert — ransom note found, mass file renames/extension changes, EDR ransomware-behaviour alert, or unexplained encryption activity.
- Do **not** immediately power off affected machines — this destroys volatile memory (RAM) that may contain encryption keys or attacker artefacts. Isolate from the network instead (pull network cable / disable NIC / isolate via EDR).
- Activate the Incident Response Plan and declare a formal incident. Assign an Incident Commander (IC).
- Establish the out-of-band communications channel immediately — assume the primary email/chat system is compromised or monitored.
- Begin an incident timeline/log: every action, timestamp, and decision-maker, from the first minute.
- Identify patient zero and initial access vector if readily apparent (phishing email, exposed RDP, known CVE exploitation).

WARNING: Do not delete the ransom note, do not attempt to decrypt files yourself, and do not restart or reimage systems before forensic imaging — you may destroy the evidence needed for recovery, insurance claims, and law enforcement.

3. Phase 2: Containment (1–4 hours)

Goal: stop the spread. Isolate before you investigate further.

- Isolate affected hosts at the network layer (VLAN quarantine, switch port shutdown, or EDR network isolation) — not just the initially-known hosts, but anything that shares credentials, shares, or trust relationships with them.
- Disable or reset credentials for any accounts suspected of compromise, starting with domain admin and service accounts.
- Block identified command-and-control (C2) IPs/domains at the firewall and proxy.
- Disable inbound RDP/SMB from the internet if that is a suspected vector; review VPN and remote access logs for anomalous sessions.
- Snapshot or image affected systems before any remediation — this is your forensic evidence and your fallback if recovery attempts fail.
- Verify backup infrastructure has not been compromised or encrypted before relying on it — many ransomware families specifically target backup repositories first.
- Preserve logs: EDR, firewall, DNS, DHCP, authentication (AD/Entra ID), and any SIEM data — extend retention/export before rotation deletes it.

4. Phase 3: Investigation & Scoping

- Determine the ransomware family/variant if possible (ransom note format, file extension, encryption tooling artefacts) — this can inform whether a free decryptor exists (check *nomoreransom.org*) and typical actor TTPs.
- Identify initial access vector: phishing, exposed RDP/VPN, exploited public-facing application, supply-chain/third-party access, or valid stolen credentials.
- Map lateral movement: authentication logs, EDR process trees, Windows Event IDs 4624/4625/4648/4672, RDP/WinRM/PsExec usage.
- Determine data exfiltration: many modern ransomware groups exfiltrate data before encrypting (double-extortion). Review outbound traffic volume, cloud storage/file-sharing site access, and known exfil tooling (rclone, MegaSync, WinSCP).
- Identify the full blast radius: every host, share, and backup repository touched — do not assume containment scope equals total scope.
- If exfiltration is confirmed or suspected, engage legal counsel immediately for breach notification obligations.

5. Phase 4: Eradication

- Do not simply delete the ransomware binary and consider the job done — attackers commonly leave backdoors, scheduled tasks, new admin accounts, and persistence mechanisms for re-entry.
- Rebuild compromised systems from known-good gold images rather than attempting to "clean" them in place, wherever feasible.
- Rotate **all** credentials that may have been exposed — not just accounts directly observed in logs. Assume Kerberos tickets, cached credentials, and any stored secrets (browser-saved passwords, config files, CI/CD secrets) are compromised.
- Patch or remediate the confirmed initial access vector before reconnecting anything to production.

- Reset the krbtgt account (twice, per Microsoft guidance) if Active Directory was compromised, to invalidate all existing Kerberos tickets.
- Remove any newly created accounts, scheduled tasks, services, GPOs, or firewall rule changes made by the attacker.

6. Phase 5: Recovery

- Restore from backups verified to be untouched and from a point in time before the confirmed compromise — restoring an already-infected backup reinfects the environment.
- Bring systems back online in priority order per your Business Impact Analysis — not simply "whatever is fastest."
- Monitor restored systems closely for 2–4 weeks post-recovery for signs of reinfection or residual attacker access.
- Re-enable network connectivity in stages, validating each segment before proceeding to the next.
- Communicate a clear all-clear only after the eradication and monitoring criteria in this playbook are met — a premature all-clear that reintroduces the attacker is worse than a longer, verified recovery.

7. Phase 6: Post-Incident Review

- Conduct a blameless post-incident review within 2 weeks of recovery, covering: root cause, timeline, what worked, what didn't, and cost/impact.
- Update the IR plan, detection rules, and hardening baselines based on findings — every incident should measurably improve your defences.
- Report findings to leadership and, where applicable, the board — include quantified business impact and remediation roadmap.
- Fulfil any outstanding regulatory notification obligations (see Section 9) and close out with insurers/law enforcement.
- Verify all identified gaps (e.g. missing MFA, unpatched systems, weak backup isolation) have assigned owners and target dates.

8. Decision Point: To Pay or Not to Pay

Paying a ransom is a business and legal decision, not solely a technical one. Considerations include:

- **No guarantee of a working decryptor** — some victims who pay never receive a working key, or receive one that only partially decrypts data.
- **Legal/sanctions risk** — paying certain sanctioned threat actors or groups may violate national sanctions law (e.g. OFAC in the US); consult legal counsel before any payment is considered.
- **It funds future attacks** — payment does not guarantee the actor won't leak stolen data anyway, or won't target you again.
- **Check for free decryptors first** — the *No More Ransom* project (nomoreransom.org), run by law enforcement and industry, has free decryptors for many older ransomware families.
- **If payment is considered**, it should be a decision made jointly by legal counsel, executive leadership, and (where applicable) your cyber insurer — never a unilateral IT decision, and never made under artificial time pressure from the attacker's countdown.

9. Communication & Notification Matrix

Stakeholder	When to Notify	Who Owns It
Executive leadership / board	Immediately on incident declaration	Incident Commander
Legal counsel	Immediately if data exfiltration suspected	Incident Commander
Cyber insurer	Within policy-required window (often 24–72h)	Legal / Risk
Data protection regulator	Per applicable law (e.g. 72h under GDPR, 6h under India's CERT-In directions)	Legal / DPO
Affected customers/individuals	Per applicable breach notification law, after scoping	Legal / Comms
Law enforcement	As soon as practical, especially for extortion/exfiltration	Incident Commander
Employees	Staged — operational instructions first, full detail after containment	Comms lead

Note: notification timelines vary significantly by jurisdiction and sector. This table is a general framework — confirm exact obligations with legal counsel for your specific regulatory environment.

10. Appendix: Quick-Reference Command Cheat Sheet

Windows — isolate a host from the network (keep it powered on)

```
netsh advfirewall set allprofiles state on
netsh advfirewall firewall add rule name="ISOLATE" dir=in action=block
remoteip=any
netsh advfirewall firewall add rule name="ISOLATE-OUT" dir=out action=block
remoteip=any
```

Windows — reset krbtgt password (run twice, ~10 hours apart, after eradication)

```
Set-ADAccountPassword -Identity krbtgt -Reset
```

Linux — isolate a host (iptables)

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

Capture volatile memory before shutdown (Windows, via WinPmem or similar)

```
winpmem_mini_x64.exe memory.raw
```

Useful references

- No More Ransom — free decryptors: nomoreransom.org
- CISA #StopRansomware guide: cisa.gov/stopransomware
- MITRE ATT&CK for ransomware TTPs: attack.mitre.org