ELEVATE
SOLUTIONS

PLAYBOOK · CYBERSECURITY

Ransomware Response Playbook

The first 60 minutes

Exactly what to do when ransomware hits. Print it, tape it to the wall, train your team.

01 — MINUTES 0–15

Isolate

Ransomware was present in 44% of breaches last year, up 37% year over year. Verizon DBIR 2025 When it hits your firm, the first hour decides how bad it gets. Work the steps in order. Do not skip ahead.

BEFORE YOU NEED THIS — FILL IN NOW, NOT DURING THE INCIDENT

Incident response contact (name / 24×7 phone) _____

Cyber insurer hotline / policy number _____

Breach counsel (firm / attorney / phone) _____

Off-network copy of this playbook stored at _____

The goal of the first 15 minutes is containment, not diagnosis. Stop the spread, protect the backups, preserve the evidence. Resist the instinct to "fix" anything yet.

- [ ] **Disconnect affected machines from the network. Now.** 1
  Pull the network cable, disable Wi-Fi, or shut the switch port. Use your EDR's network-isolation function if you have one — it keeps the security agent connected while cutting everything else. Disconnect, do not shut down.
- [ ] **Disable the affected user accounts.** 2
  Disable sign-in and revoke active sessions and tokens for every account seen on an infected machine — including service accounts and any admin account used there. Reset comes later; disable comes now.
- [ ] **Isolate the backups and verify they are untouched.** 3
  Disconnect backup servers and repositories from the production network. Confirm the most recent backup jobs completed and that retention points have not been deleted or encrypted. Attackers hunt backups first — these are your recovery.
- [ ] **Preserve. Do not power off infected machines.** 4
  Memory holds encryption keys, attacker tooling, and active connections — all lost at power-off. Leave machines on and isolated. Do not reboot, wipe, reimage, or "clean" anything.
- [ ] **Note the time and the visible scope.** 5
  Record when ransomware was first noticed, who reported it, which machines and shares show encrypted files or ransom notes. One sentence per fact. You will need exact times for the insurer and regulators.
- [ ] **Start an incident log on a clean device.** 6
  Open a notebook or a document on a phone or machine that is not on the affected network. Log every action, decision, and time from this point forward. Assign one person to keep it current.

DO NOT WIPE OR REIMAGE BEFORE EVIDENCE CAPTURE

Reimaging destroys the forensic record your insurer, counsel, and investigators need — and you may rebuild the same hole the attacker used. Nothing gets wiped until forensics says so. That instruction comes in writing.

02 — MINUTES 16-30

Communicate

The spread is contained. Now get the right people on the phone — in this order. Calls, not email: assume the attacker can read anything on the compromised network.

- [ ] **Work the internal escalation tree.** 7
  Call the incident lead, then ownership/management, in the order your plan defines. Phone or SMS only. State facts: what is encrypted, when it started, what is isolated. No speculation about cause or blame.

- [ ] **Call the cyber insurer hotline — before any remediation.** 8
  Most policies require notice before you act and route you to approved forensics and ransom negotiators. Remediating first can jeopardize coverage. Read the policy number from the box on page 2 and make the call.

- [ ] **Call breach counsel.** 9
  Counsel directs the investigation under privilege and owns the notification analysis — HIPAA, state breach statutes, client contracts, ethics duties. If you have no breach counsel on retainer, your insurer can assign one. Engage them in hour one, not week one.

- [ ] **Call your IT team or managed services provider.** 10
  Brief them on scope and what is already isolated. Their first jobs: hold containment, pull EDR and firewall logs, and stand by for the insurer's forensics team. No rebuilds yet.

- [ ] **Designate a single spokesperson. Send no broadcast emails.** 11
  One person speaks for the firm — to staff, clients, and press. Everyone else says nothing. Do not send all-staff email from compromised systems: the attacker may read it, and careless wording becomes evidence. Brief staff verbally or via an out-of-band channel.

> **DO NOT PAY — OR CONTACT THE ATTACKER — BEFORE COUNSEL AND INSURER SIGN OFF**
>
> Paying a sanctioned entity can itself be a federal violation, payment does not always produce working decryption, and amateur contact weakens negotiation. The ransom decision belongs to counsel, the insurer, and ownership together — documented, never made alone in the first hour.

03 — MINUTES 31-60

Investigate

Containment holds and the calls are made. Now build the picture the forensics team will need. Look — do not touch. Every finding goes in the incident log with a timestamp.

- [ ] **Identify the variant from the ransom note.** 12
  Photograph the ransom note and record the encrypted-file extension. Note text plus extension usually identifies the strain, which tells the response team the group's known tactics — including whether it typically steals data before encrypting.

- [ ] **Scope the encrypted shares and systems.** 13
  List every server, share, and mapped drive showing encrypted files — and what each holds: client files, PHI, financial records, email. This list drives both recovery priority and the notification analysis.

- [ ] **Check for signs of data exfiltration.** 14
  Look for large outbound transfers in firewall logs, uploads to file-sharing or cloud-storage domains, and staged archive files (.zip, .rar, .7z) in temp folders. Most ransomware groups now steal data before encrypting; assume exfiltration until disproven.

- [ ] **Pull and preserve EDR and firewall logs.** 15
  Export endpoint detections, firewall and VPN logs, and Microsoft 365 / identity sign-in logs to isolated storage now. Many systems retain logs for only days or weeks — capture before they roll off.

- [ ] **Identify patient zero and the entry vector.** 16
  Find the earliest infected machine and the earliest suspicious sign-in. Usual suspects: a phishing email and attachment, exposed RDP, a VPN or remote-access account without MFA, an unpatched edge device, or a third-party connection.

- [ ] **Capture volatile evidence before anything reboots.** 17
  If qualified staff are available, capture memory images, running processes, and active network connections from key infected machines. If not, leave machines on and isolated and wait for forensics. Never practice forensics for the first time mid-incident.

- [ ] **Assess backup integrity — verify, don't assume.** 18
  On an isolated machine, confirm restore points exist from before the infection window and test-restore a sample file. Check whether backup admin accounts were among those compromised. Report a tested fact, not a hope.

- [ ] **Document everything, with timestamps.** 19
  Variant, scope, exfil indicators, patient-zero findings, backup status, every call made and instruction received — into the incident log as it happens. This record drives the insurance claim, the notification analysis, and any later litigation.

AT MINUTE 60, YOU SHOULD BE ABLE TO SAY

What is isolated. What is encrypted. Whether backups survived. Whether data likely left. Who has been called. If any answer is missing, that gap is the next task — recovery starts only when forensics and counsel agree containment is real.

04 — AFTER THE INCIDENT

Documentation

The incident is not over when systems come back. Four documents turn a bad week into an insurable claim, a defensible notification position, and a firm that is harder to hit twice.

- [ ] **Incident timeline.** 20
  A single chronological record from first sign to full recovery: detection, isolation, every call, forensic findings, restore milestones. Build it from the incident log while memories are fresh. Insurers and regulators will ask for exactly this.

- [ ] **Decision log — including the ransom decision rationale.** 21
  Record each major decision, who made it, on whose advice, and why — above all the pay / don't-pay decision: backup status, exfiltration evidence, sanctions screening, counsel and insurer input. A documented rationale is defensible; an undocumented one is not.

- [ ] **Notification analysis, with counsel.** 22
  Counsel determines what the facts trigger: HIPAA breach notification, state attorney general notices, client contract clauses, professional ethics duties, carrier requirements. Document the conclusion either way — a written "no notification required" analysis matters as much as the notices themselves.

- [ ] **Lessons-learned review within 14 days.** 23
  One meeting, everyone involved, on the calendar before momentum fades. Three questions: how they got in, what slowed the response, what changes now — each fix with an owner and a date. Then update this playbook and re-run the drill.

Playbook owner _____

Last tabletop drill / next drill date _____

Elevate Solutions provides managed IT and cybersecurity for businesses that answer to regulators, clients, and courts.

Elevate Solutions

6230 Wilshire Blvd Suite 2120, Los Angeles CA 90048

(424) 400-6625 · support@elevatesolutions.io · elevatesolutions.io