ITVORTEX
SIMPLIFY. PROTECT. EVOLVE.

FREE RESOURCE · INSTANT DOWNLOAD

The Ransomware Recovery Checklist.

Fifteen steps, in the order that actually matters, for the first hour and the first week after an attack. The malware is rarely what decides the outcome. The sequence is. Built for the 50 to 500-seat businesses we protect across NJ, NY, and CT.

SEQUENCE
15
ordered steps, isolation through hardening

PHASES
4
contain, preserve, recover, harden

FIRST HOUR
1 hr
the window that sets the trajectory

VERIFIED BACKUPS
0
errors after a verified test restore

ITV-RW-RECOV-2026 · v1.0

The first hour. In sequence.

The first hour decides whether this is a bad week or a closed business. Ransomware doesn't just encrypt your production data, it hunts your backups first, so the early moves you skip are the ones you can't undo. Work these in order. Don't jump to recovery before you've contained, preserved, and verified.

PHASE 1 · FIRST MINUTES

Contain & isolate

- [ ] **1** Isolate infected systems from the network now, but **do not power them off**. Pull the cable, disable Wi-Fi, or quarantine the host through your EDR. MAKE-OR-BREAK

  WHY THIS DECIDES IT Shutting a machine down can wipe volatile evidence and encryption keys held in memory. Network isolation stops the spread without destroying what investigators need.

- [ ] **2** Cut remote access and disable shared or privileged accounts. Kill VPN, RDP, and any standing admin sessions.

- [ ] **3** Disconnect and protect your backups before they're reached. Take repositories offline and confirm your immutable or air-gapped copies are intact and unmounted. MAKE-OR-BREAK

  WHY THIS DECIDES IT Modern ransomware targets backups first. Protecting them is what preserves any path to recovery at all.

PHASE 2 · FIRST HOUR

Preserve evidence & notify

- [ ] **4** Activate your incident response plan and stand up the team: IT lead, leadership, legal, communications, and your MSP or IR retainer.

- [ ] **5** Preserve evidence before you clean anything. Capture system images, memory, logs, the ransom note, and sample encrypted files. MAKE-OR-BREAK

  WHY THIS DECIDES IT You can only investigate, recover, and satisfy insurers and regulators if the evidence survives the cleanup.

- [ ] **6** Keep a timestamped incident log from minute one. Record what you saw, when, and every action taken.

- [ ] **7** Call your cyber insurance carrier before you remediate. Engage their breach response process and use their approved vendors. MAKE-OR-BREAK

  WHY THIS DECIDES IT Most policies require carrier notification and pre-approval first. Acting alone can forfeit coverage you've already paid for.

- [ ] **8** Notify law enforcement and assess your legal duties. Report to the FBI through IC3, and evaluate breach-notification obligations under HIPAA, state law, and your contracts. Use clean, out-of-band channels.

Operational guidance, not legal or insurance advice. Confirm notification duties and carrier requirements with your counsel, compliance officer, and cyber insurance provider.

Clean recovery. Then resume.

PHASE 3 · HOURS TO DAYS

Assess scope & recover clean

- [ ] **9** Find the scope and the entry point. Map every affected system, account, and dataset, and identify how they got in: phishing, exposed RDP, or an unpatched vulnerability. MAKE-OR-BREAK

  > **WHY THIS DECIDES IT** Recover without closing the door they walked through and you'll be doing this again next week.

- [ ] **10** Confirm clean backups exist and validate them against **3-2-1-1-0**: three copies, on two media types, one offsite, one offline or immutable, with zero errors after a verified test restore. MAKE-OR-BREAK

  > **WHY THIS DECIDES IT** A backup you haven't test-restored is a hope, not a recovery plan.

- [ ] **11** Rebuild clean. Never restore into the compromised environment. Reimage from known-good media into a clean, isolated environment.

- [ ] **12** Eradicate persistence and rotate every credential. Remove backdoors, rogue accounts, and scheduled tasks, then reset all passwords, keys, and tokens. MAKE-OR-BREAK

  > **WHY THIS DECIDES IT** Operators plant several footholds. One missed account is all it takes for them to walk back in.

- [ ] **13** Restore in priority order and validate each system before reconnecting. Bring back critical services first, verify integrity, then reconnect in controlled waves.

PHASE 4 · DAYS TO WEEKS

Harden & resume

- [ ] **14** Close the gap before full reconnection. Patch the exploited vulnerability, enforce MFA everywhere, segment the network, and tighten backup immutability. MAKE-OR-BREAK

  > **WHY THIS DECIDES IT** The same weakness that let them in stays open until you deliberately close it.

- [ ] **15** Run a post-incident review and harden what failed. Turn the incident into specific, tested changes to your plan, your backups, and your controls.

Recovery is architecture, not luck.

Good recovery isn't improvised at 3 a.m. It's built in advance: tested backups, a recovery environment that's ready to take the load, and a plan your team has actually rehearsed. That's the difference between executing this checklist and scrambling to invent it. Here's where each step of it gets easier when the groundwork is already in place.

Disaster Recovery (DRaaS)

theitvortex.com/disaster-recovery-as-a-service/

Failover that's been tested ahead of time, so recovery runs from a runbook instead of a gamble.

Backup as a Service (BaaS)

theitvortex.com/veeam-baas-offerings/

Veeam-powered, immutable, and verified against the full 3-2-1-1-0 standard, not just scheduled.

Security as a Service (SECaaS)

theitvortex.com/secaas/

Close the entry points before they're used: MFA, segmentation, and managed detection and response.

Managed IT Services

theitvortex.com/managed-it-services/

Monitoring, patching, and response so an alert gets handled before it ever becomes an outage.

Talk it through with our team: (201) 225-8670 · www.theitvortex.com

BEFORE THE NEXT ATTACK

Walk your recovery plan with an IT Vortex engineer and find the gaps now, while they're still cheap to fix. We'll pressure-test your backups, your sequence, and your last line of defense.

BOOK A READINESS AUDIT