Ransomware Recovery Checklist

For Small and Mid-Sized Businesses | Hour-by-Hour Response Guide

SAGE SOLUTIONS | sagesolutionsllc.net | (646) 886-7604

EMERGENCY

If you are reading this during an active incident, stop. Call your MSP immediately. If you do not have one, call Sage Solutions at (646) 886-7604. Then return to this checklist.

Print this checklist and keep it in your server room, IT binder, or incident response kit. At least two people in your organization should know where it is. This mirrors the runbook Sage Solutions executes for managed clients.

INCIDENT INFORMATION

Date of incident:		Time detected:	
Detected by:		Reported to:	
Incident commander:		Commander phone:	
Cyber insurance carrier:		Policy number:	
Carrier emergency line:		Breach counsel:	
Counsel phone:		MSP emergency line:	

Ransomware strain identified:

PHASE 1: FIRST 60 MINUTES -- CONTAIN THE BLAST RADIUS

Goal: stop the spread. Do not attempt recovery. Do not engage attackers. Do not power off machines (forensic data lives in memory).

- [ ] 1. Disconnect affected machines from the network (pull ethernet, disable Wi-Fi). Do NOT power off.
- [ ] 2. Isolate the affected network segment at the switch or firewall.
- [ ] 3. Pause all file sync clients (OneDrive, Google Drive, Dropbox, SharePoint) on EVERY machine. Sync will spread encryption to the cloud.
- [ ] 4. Notify leadership with a brief verbal update. Do not put detail in writing yet.
- [ ] 5. Open the incident log. Timestamp every action and note who performed it. This matters for insurance and law enforcement.
- [ ] 6. Do NOT engage the attackers. Do not click chat URLs or reply to ransom notes.
- [ ] 7. Photograph the ransom note on screen (helps identify the strain).
- [ ] 8. Document which systems show signs of encryption (changed file extensions, ransom notes present).

PHASE 2: HOURS 1-4 -- ASSESSMENT

Goal: understand what happened and determine recovery options.

- [ ] 9. Identify patient zero. Which machine was first affected? When did it start? EDR makes this trivial; without it, this is investigative work.
- [ ] 10. Identify the ransomware strain from the ransom note. Check nomoreransom.org for free decryptors.
- [ ] 11. Verify backup integrity:
  - [ ] Backups are reachable and accessible
  - [ ] Backups are recent (RPO is acceptable)
  - [ ] Backups are intact (not encrypted or deleted by attacker)
  - [ ] Backups are immutable (attacker cannot modify them)
- [ ] 12. Notify your cyber insurance carrier. Most policies require notice within 24-72 hours.
- [ ] 13. Notify or engage breach counsel. Your carrier will assign one if you do not have a relationship.
- [ ] 14. Document scope of affected systems:

Workstations affected (__ of __): _____ Servers affected (__ of __): _____

Data types potentially exposed: _____

PII involved? ☐ Yes ☐ No ☐ Unknown PHI involved? ☐ Yes ☐ No ☐ Unknown

PHASE 3: HOURS 4-24 -- DECISION AND NOTIFICATION

Goal: make the recovery decision and meet regulatory notification obligations.

- [ ] 15. Make the recovery decision (counsel and carrier must be involved for pay option):
  - [ ] RESTORE FROM BACKUP (preferred if backups intact)
  - [ ] DECRYPT (only if free/commercial decryptor exists for this strain)
  - [ ] NEGOTIATE / PAY (last resort -- carrier and counsel MUST lead)

Decision made by: _____ Time: _____

- [ ] 16. Notify regulators if required (counsel handles timing and content):
  - [ ] NY SHIELD Act (NY-resident PII exposed)
  - [ ] HIPAA Breach Notification Rule (PHI exposed)
  - [ ] PCI-DSS notification (cardholder data exposed)
- [ ] 17. Notify affected parties as directed by counsel: employees, customers, vendors.
- [ ] 18. Begin restoration in an ISOLATED environment. Do not restore to production until the entry vector is understood.

PHASE 4: DAYS 1-7 -- RECOVERY AND ROOT CAUSE

Goal: restore operations cleanly and close the door the attacker used.

- [ ] 19. Rebuild (not restore) affected endpoints from clean images. Restore data only, not full systems.
- [ ] 20. Reset ALL passwords:
  - [ ] Domain admin accounts
  - [ ] All service accounts
  - [ ] All user accounts
  - [ ] Force MFA re-enrollment for all users
- [ ] 21. Rotate all API keys, certificates, and secrets that the attacker could have exfiltrated.
- [ ] 22. Identify the entry vector:

- [ ] Phishing email
- [ ] Unpatched VPN or firewall appliance
- [ ] Compromised RDP / remote access
- [ ] Stolen credentials
- [ ] Supply chain compromise

- [ ] 23. Patch and close the entry vector permanently.
- [ ] 24. Scan all systems for persistence mechanisms (backdoors, rogue accounts, scheduled tasks).
- [ ] 25. Restore systems to production only after entry vector is closed and persistence is cleared.
- [ ] 26. Verify all restored systems are functional:
  - [ ] Email working
  - [ ] File shares accessible
  - [ ] Line-of-business apps operational
  - [ ] Backups running on rebuilt systems
  - [ ] EDR deployed on all rebuilt endpoints

PHASE 5: WEEKS 1-4 -- POST-INCIDENT

- [ ] 27. Complete forensics report: what happened, what was exfiltrated, root cause, full timeline.
- [ ] 28. Conduct blameless lessons-learned review with leadership and IT.
- [ ] 29. Submit insurance claim with complete documentation.
- [ ] 30. Implement permanent hardening based on findings:
  - [ ] EDR on every endpoint
  - [ ] MFA on every critical system
  - [ ] Immutable off-site backup
  - [ ] Network segmentation
  - [ ] Phishing training program
  - [ ] Automated patch management
  - [ ] Email security with DMARC enforcement
  - [ ] Privileged access management
- [ ] 31. Update the incident response plan based on lessons learned.
- [ ] 32. Schedule a tabletop exercise for 90 days out to test the updated plan.

PREVENTIVE CONTROLS AUDIT

Every "No" below is an open risk. Use this to track remediation after an incident -- or to prevent the next one.

- [ ] EDR on every workstation and server
- [ ] MFA enforced on all business-critical systems
- [ ] Immutable, off-site, air-gapped backup
- [ ] Backup restore tested within the last 90 days
- [ ] Cyber insurance with incident response retainer

- [ ] Documented incident response runbook (this document, filled out)
- [ ] Phishing simulation program running monthly
- [ ] Automated patch management (OS + third-party)
- [ ] Network segmentation between user/server/IoT segments
- [ ] DNS filtering at the network layer
- [ ] Email security with DMARC enforcement
- [ ] 24/7 SOC monitoring with human analyst escalation
- [ ] Annual third-party penetration test
- [ ] Privileged access management (PAM)
- [ ] Security awareness training at least quarterly

CRITICAL CONTACTS -- FILL THIS OUT BEFORE AN INCIDENT

During a crisis you will not have time to look up numbers. Keep this current.

Incident commander: _____

Backup incident commander: _____

CEO / business owner: _____

CFO / finance lead: _____

MSP / IT provider: _____

MSP emergency line: _____

Cyber insurance carrier: _____

Breach counsel: _____

FBI local field office: _____

PR / communications lead: _____

NOTES

This checklist is provided as a planning and response resource by Sage Solutions LLC. It does not constitute legal advice. Engage qualified legal counsel for compliance-specific guidance regarding breach notification, regulatory obligations, and liability. Sage Solutions does not pay ransoms. Version 1.0 | May 2026