FLYGHT

MANAGED IT SERVICES | TOLEDO, OHIO

Ransomware Incident Response Checklist

The First 72 Hours — What to Do, Who to Call, What to Save

A practical, step-by-step checklist for Toledo and NW Ohio businesses to follow the moment a ransomware attack is discovered. Print it. Share it. Keep it offline.

flyght.support | (419) 670-7100 | support@flyght.support

How to Use This Checklist

If you are reading this during an active ransomware incident: stay calm, stop typing, and start at Phase 1. Do not power off infected machines, do not pay the ransom, and do not start restoring backups until you finish the assessment phase.

If you are reading this before an incident: print a copy and store it somewhere your team can reach it without network access — a binder, a fire safe, a phone screenshot. The single biggest predictor of a smooth recovery is having this plan ready before you need it.

Each phase below has time-bound actions, the people you need to call, and the evidence you must preserve. Work through them in order. The order matters.

DO NOT

- Power off infected machines (destroys forensic evidence and may prevent decryption).
- Wipe, reimage, or restore systems before forensic images are captured.
- Pay the ransom or contact attackers without involving your cyber insurance carrier first.

01 PHASE 1: HOUR 0 — IMMEDIATE ISOLATION

Stop the spread. Every minute of network connectivity means more encrypted files.

- [ ] Disconnect affected machines from the network — unplug ethernet cables and disable Wi-Fi
- [ ] If the scope is unclear, shut down the network switch entirely to halt lateral spread
- [ ] Leave infected computers powered ON — do NOT shut down or reboot them
- [ ] Disconnect external/USB drives, but do NOT erase or reformat them
- [ ] Take affected file shares, servers, and backup repositories offline
- [ ] Pause or disconnect cloud sync clients (OneDrive, Dropbox, Google Drive, SharePoint)
- [ ] Disable scheduled backup jobs so the next run does not overwrite a clean restore point
- [ ] Tell every employee: stop working, stay off computers, do not open email or attachments
- [ ] Photograph the ransom note(s) on every affected screen — use a phone, not a screenshot tool
- [ ] Note the exact time of discovery and who discovered it (you will need this for insurance and law enforcement)

02 PHASE 2: HOURS 1–4 — WHO TO CALL

Make these calls in order. Do not skip the insurance step — it can void your coverage.

- [ ] Call your IT provider or MSP — they begin forensic triage and contain the incident
- [ ] Call your cyber insurance carrier BEFORE engaging outside vendors or paying anything
- [ ] Have your policy number, retention amount, and panel-vendor list ready when you call
- [ ] Notify your CEO/owner and document the executive who authorizes incident response decisions
- [ ] Engage your attorney — ideally one experienced with data breach notification law
- [ ] Report to FBI IC3 at ic3.gov (federal agencies sometimes hold decryption keys)
- [ ] Call the FBI Cleveland Field Office (216-522-1400) for Ohio-based businesses
- [ ] Report to CISA at cisa.gov/report if you operate in critical infrastructure
- [ ] Notify any third-party vendors or MSP partners whose systems may also be at risk
- [ ] Designate ONE spokesperson — no public statements, social posts, or customer emails until counsel approves

03 PHASE 3: HOURS 4–24 — EVIDENCE PRESERVATION

What you save now determines your insurance claim, legal position, and decryption odds.

- [ ] Do NOT delete, wipe, or reimage any affected machine until forensic images are captured
- [ ] Preserve the ransom note files exactly as left (.txt, .html, README files in encrypted folders)
- [ ] Capture sample encrypted files (do not modify them — the file extension identifies the variant)
- [ ] Preserve firewall logs, VPN logs, and remote access logs (these expire — export them now)
- [ ] Preserve endpoint logs, Windows Event Logs, and EDR/antivirus alerts from the prior 30 days
- [ ] Preserve Microsoft 365 / Google Workspace audit logs and sign-in logs for the prior 90 days
- [ ] Document every affected machine: hostname, IP, user, OS, location, encryption status
- [ ] Identify the ransomware variant via the note format and file extension (check nomoreransom.org)
- [ ] Maintain a written incident timeline — every decision, every call, every cost, with timestamps
- [ ] Designate one person to keep the timeline. Do not rely on memory or chat scrollback later

04 PHASE 4: HOURS 12–48 — BACKUP ASSESSMENT

Backup integrity is the single biggest factor in your recovery timeline and ransom decision.

- [ ] Locate every backup repository: on-prem, cloud, immutable, and offline copies
- [ ] Verify backups are NOT encrypted — attackers commonly target backup systems before detonation
- [ ] Confirm the most recent CLEAN restore point (before initial compromise, not just before encryption)
- [ ] Validate backup integrity by performing test restores to an isolated environment — not production
- [ ] Document Recovery Point Objective: how much data was lost between last clean backup and attack?
- [ ] Document Recovery Time Objective: how long will full restoration take with current backup state?
- [ ] If backups are intact: do NOT consider paying. Begin clean-environment rebuild planning
- [ ] If backups are partial: list which systems can be restored vs. which must be rebuilt or accepted as lost
- [ ] If backups are unusable: notify insurance carrier immediately — ransom payment may enter discussion
- [ ] Never restore to compromised infrastructure — build a clean network segment first, then restore into it

05 PHASE 5: DAYS 1–7 — REPORTING & NOTIFICATION

Regulatory clocks start the moment you discover the breach. Miss them and penalties stack fast.

- [ ] Confirm whether personal data was exfiltrated, not just encrypted — most modern attacks do both
- [ ] Ohio Revised Code 1349.19: notify affected Ohio residents in the most expedient time possible
- [ ] Ohio AG: written notice required if more than 1,000 Ohio residents affected in a single breach
- [ ] HIPAA-covered entities: notify HHS within 60 days; affected patients without unreasonable delay
- [ ] HIPAA breaches affecting 500+ individuals: notify HHS and prominent media outlets within 60 days
- [ ] PCI-DSS: notify your acquiring bank and card brands within the contractually required window
- [ ] SEC public companies: assess Form 8-K Item 1.05 disclosure within 4 business days of materiality
- [ ] GLBA / NCUA / FFIEC regulated entities: follow your sector's specific incident reporting rules
- [ ] Notify customers, partners, and vendors per contractual breach-notification clauses
- [ ] Document all notifications sent — dates, recipients, content — for the regulator file

06 PHASE 6: AFTER RECOVERY — ROOT CAUSE & HARDENING

Restore and move on without fixing the root cause and you will be hit again — often by the same group.

- [ ] Identify the initial access vector definitively (phishing, exposed RDP, unpatched vuln, stolen creds)
- [ ] Conduct a written post-incident review with leadership, IT, legal, and insurance
- [ ] Rotate every password, API key, and service account credential across the environment
- [ ] Force-revoke all active sessions and OAuth tokens in Microsoft 365 / Google Workspace
- [ ] Enforce MFA on every account — no exceptions for executives, vendors, or service accounts
- [ ] Deploy or expand EDR coverage to every endpoint, including servers and remote workers
- [ ] Rebuild backup architecture using the 3-2-1 rule with at least one immutable or air-gapped copy
- [ ] Test restores quarterly going forward — a backup that has never been restored is a hope, not a plan
- [ ] Implement network segmentation so a future intrusion cannot move laterally without resistance
- [ ] Schedule security awareness training and run simulated phishing campaigns at least quarterly

Critical Contacts — Fill In Now

Fill these in BEFORE an incident. Print this page and store it where your team can find it without network access. During an attack, you will not have time to look up phone numbers.

IT Provider / MSP
(Flyght IT: 419-670-7100)
_____

Cyber Insurance Carrier
Policy #:
_____

Insurance Broker
_____

Legal Counsel
(data breach experience)
_____

FBI Cleveland Field Office
(216) 522-1400
_____

FBI IC3 Online
ic3.gov
_____

CISA Reporting
cisa.gov/report
_____

Ohio Attorney General
(800) 282-0515
_____

Internal Executive Authority
(authorizes payment / outside vendors)
_____

Internal Communications Lead
(only authorized spokesperson)
_____

The Best Time to Use This Was Yesterday.

Most Toledo businesses we meet only think about ransomware after they have been hit. By then, the question is not how to prevent it — it is how much was lost.

Flyght offers a free security gap assessment for businesses across NW Ohio, Michigan, and Indiana. We will review your backups, monitoring, and incident response readiness — honestly, with no pitch.

BOOK A FREE GAP ASSESSMENT

flyght.support/contact

(419) 670-7100

support@flyght.support

7430 W Central Ave., Toledo, OH 43617