RANSOMWARE RESPONSE

How To Respond To A Ransomware Attack On A Small Business

Plain-English how-to. ~First 72 hours playbook. Step-by-step under pressure.

Ransomware against small businesses has become an industrialized crime. According to CISA, over 60% of small businesses hit by ransomware close within 6 months. The difference between the ones that survive and the ones that don't usually comes down to the first 72 hours.

If you've never been hit, this guide is your insurance policy: read it now, print the playbook, store it offline. If you are hit — open this immediately. Every section is a step you take in order.

By the end of this guide you'll have a printed incident-response runbook for ransomware, with contact info pre-filled, decision flowcharts, and the FBI / CISA contact path. You'll know exactly what to do — and just as importantly, what NOT to do.

Quick snapshot

What you'll learn	The first-72-hours playbook for ransomware response in a small business.
Skill level	Owner / IT lead · Use during incident OR preparation
Time required	1 hour to prepare; immediate response during incident
What you'll need	This printed guide, contact info pre-filled, cyber insurance policy
Risk if you skip this	Business closure within 6 months (60% of SMBs hit)
PDF kit	■ Download at the bottom of this page

Why this matters

Ransomware is the most likely catastrophic cyber event for a small business. The combination of encrypted files, threatened data leak, ransom demand, and operational shutdown creates extreme pressure to make bad decisions fast.

Prepared organizations recover. Unprepared organizations pay ransoms (often without getting decryption) and still fail. The FBI strongly recommends never paying, but the decision is yours — preparation gives you the option to recover without paying.

Most ransomware incidents follow a predictable pattern: initial access via phishing or RDP, dwell time of days to weeks while attackers map your network, exfiltration of data for double-extortion, then encryption. Detection

during dwell time stops the worst outcomes.

Before you start

Pre-fill this playbook with: cyber insurance carrier phone number, your IT provider's emergency contact, your attorney's contact, your CPA's contact, the FBI Internet Crime Complaint Center (ic3.gov), and CISA's reporting line.

Print three copies: one in the office safe, one at the owner's home, one with the attorney. Yes, paper — your digital copies may be encrypted during an event.

Verify that your backups are tested and survivable. Without working backups, every other step is harder. See our Small Business Backup how-to.

Step 1 — First 15 minutes: STOP. ISOLATE. DON'T PANIC.

Disconnect affected systems from the network immediately: unplug Ethernet, turn off WiFi adapters. Do NOT shut down. Modern ransomware can lose decryption ability if shut down before encryption finishes.

Take a photo of any ransom note with your phone (timestamp it). Don't click anything, don't reply, don't pay yet. Most decisions in the next 72 hours need to be deliberate.

Step 2 — First 30 minutes: assemble the response team

Call: (1) your cyber insurance carrier (they have an incident hotline — they activate immediately), (2) your IT provider, (3) your attorney, (4) leadership.

If you don't have cyber insurance and IT response on retainer: call CISA at 1-844-Say-CISA (1-844-729-2472) or visit cisa.gov/stopransomware/report. They provide free guidance for SMBs.

Step 3 — First hour: scope the damage

Identify: which systems are encrypted? Which are intact? Were backups reached? Has data been exfiltrated (look for unusual outbound traffic in any monitoring you have)?

Document everything you find. Time-stamp every action. This documentation matters for insurance claims, FBI reports, and post-incident review.

Step 4 — First 4 hours: notify the FBI

File an Internet Crime Complaint at **ic3.gov**. The FBI takes ransomware seriously and may have decryption keys from prior cases. Reporting is free, confidential, and doesn't force any decision on you.

If credit card data, healthcare info, or other regulated data was potentially exposed, also notify the relevant regulator (state AG offices, HHS for HIPAA, your payment processor for PCI).

Step 5 — Day 1: assess recovery options without paying

With your IT provider/incident responder, test backup restoration on a clean (rebuilt) system. Can you restore data and rebuild? Time it.

Check **nomoreransom.org** — a free decryption project that has keys for over 150 ransomware strains. Sometimes the strain that hit you is already broken.

Step 6 — Day 2-3: decide on payment (rarely; with counsel)

The FBI advises against paying — funds criminal organizations, no guarantee of decryption, often re-targeted later. About 30% of paying organizations never receive a working decryptor.

If you must consider payment, do so only with cyber insurance, attorney, and an incident response firm. There are also OFAC sanctions to check — paying certain ransomware groups is illegal even if you're trying to save your business.

Step 7 — Day 3-7: rebuild and recover

Rebuild systems from clean media. Restore data from verified backups. Reset every credential (every password, every API key, every certificate) on the assumption attackers have them all.

Test critical business processes one by one before announcing 'we're back.' Premature reopening often leads to a second infection from the same persistence the attacker left behind.

Step 8 — Day 7+: notify customers and post-incident review

If customer data was exposed, you likely have legal notification obligations. Your attorney handles this. Done well, transparency rebuilds trust; done badly, lawsuits follow.

Run a thorough post-incident review: how did they get in? What controls would have stopped them? Implement those fixes immediately. The first attack is bad; the second one is the one that closes you.

PRO TIP

Isolate, Don't Shut Down.

Unplugging from the network stops further spread without losing decryption potential.

Shutting down kills the ransomware process — sometimes that breaks the decryption.

Photograph ransom notes; don't click anything in them.

FBI reporting is free, confidential, and doesn't force any decision.

If you want to go further: power-user upgrades

Power-user upgrade #1 — Retain an incident response firm in advance

CrowdStrike Falcon Complete, Sophos MDR, Arctic Wolf, or smaller regional firms. Pre-arranged means they show up in hours, not days.

Trade-off: retainer fees (sometimes covered by cyber insurance).

Power-user upgrade #2 — Implement EDR / XDR

Endpoint Detection and Response (Microsoft Defender for Business, CrowdStrike, Sentinel One) catches ransomware behaviors before encryption.

Trade-off: $5-15/endpoint/month.

Power-user upgrade #3 — Cyber insurance with ransomware coverage

Most policies cover incident response, legal fees, business interruption, ransom payment if approved.

Trade-off: premiums; requirements to qualify (MFA, backups, training).

Power-user upgrade #4 — Run tabletop exercises quarterly

Scenario: 'It's 2 AM Sunday; you get the ransom note. Walk through the playbook.' Builds muscle memory.

Trade-off: 1-2 hours per quarter.

Power-user upgrade #5 — Implement network segmentation

Separate VLANs for accounting, operations, guest WiFi. Ransomware in one segment doesn't reach others.

Trade-off: requires managed switches and setup time.

Power-user upgrade #6 — Establish a clean 'recovery LAN'

Pre-built rebuild environment on different hardware, ready for emergency use.

Trade-off: hardware cost.

Common mistakes & pitfalls

Mistake — Shutting down systems instead of isolating.

Fix — Sometimes prevents decryption. Unplug network instead.

Mistake — Paying without exhausting options.

Fix — 30% of payers don't get working decryptors. Try backups + nomoreransom.org first.

Mistake — Not calling cyber insurance immediately.

Fix — They have the playbook, contacts, and resources. Call them first.

Mistake — Skipping the FBI report.

Fix — Free, confidential, sometimes yields a decryption key.

Mistake — Reopening too fast.

Fix — Persistence mechanisms often remain. Second wave hits within weeks.

Mistake — Hiding the breach from customers.

Fix — Legal and PR damage compounds. Transparency wins long-term.

Mistake — No printed playbook.

Fix — Digital copies are encrypted. You need paper. Multiple copies.

Pro tips

Pro tip 1. Cyber insurance carriers usually answer 24/7 — call them BEFORE the attack to know the process.

Pro tip 2. Bookmark nomoreransom.org — many strains are already broken.

Pro tip 3. If you use Microsoft 365, enable Defender for Business — ransomware behavioral detection is free with Premium plans.

Pro tip 4. Practice this playbook annually with a tabletop exercise.

Pro tip 5. Build the contacts list NOW. Looking up phone numbers during a crisis wastes critical minutes.

Frequently asked questions

Should I just pay the ransom to get back to work fast?

Rarely. 30% never get working decryptors. Many groups are sanctioned (illegal to pay). Insurance often won't cover it. Try backups + nomoreransom.org + IR firm first.

Will the FBI shut down my business?

No. The FBI takes reports confidentially. They're trying to catch criminals, not punish victims.

How long does recovery take?

With good preparation: 3-7 days. Without: weeks to months, often ending in closure.

Do I have to notify customers?

Depends on data exposed and your state/sector. Healthcare (HIPAA), payment cards (PCI), and most state breach laws require notification. Attorney decides timing and content.

Should I publicly disclose the attack?

Often yes — transparency wins customer trust long-term. Coordinate with attorney and PR.

Will my cyber insurance cover everything?

Most cover incident response, legal, business interruption. Coverage of ransom payments and customer notification varies. Read the policy NOW.

Can I prevent this from ever happening again?

Not 100%, but combining: MFA everywhere, EDR, backups with immutability, training, network segmentation — drops the probability to very low.

Quick recap — do these in order

DO THIS RIGHT NOW

The 8-step recap.

1. Isolate (unplug). Do NOT shut down.
2. Photograph ransom note. Document everything.
3. Call cyber insurance, IT provider, attorney.
4. Report to FBI via ic3.gov within 24 hours.
5. Check nomoreransom.org for free decryption.
6. Attempt recovery from backups before considering payment.
7. Rebuild from clean media; rotate all credentials.
8. Notify customers per legal counsel; run post-incident review.

Mini glossary

Ransomware: Malware that encrypts files and demands payment for decryption.

Double extortion: Ransomware that also steals data and threatens leak.

Decryptor: Tool that reverses the encryption — sometimes free, sometimes from ransom.

nomoreransom.org: Free project providing decryption keys for known ransomware strains.

OFAC: US Treasury office maintaining sanctions list; paying sanctioned groups is illegal.

IR / DFIR: Incident Response / Digital Forensics and Incident Response.