THREATNEXIS | SMALL BUSINESS CYBERSECURITY

Incident Response for Small Teams

A Practical Playbook for Detecting, Containing & Recovering from Cyberattacks

207 Days
Average time to identify a breach without an IR plan

58%
reduction in breach costs for businesses with a tested IR plan

60%
of small businesses never reopen after a major cyber incident

FREE EDITION | threatnexis.com | 2025 Edition | For businesses with 1–250 employees

What's Inside This Playbook

- What incident response is — and why it matters
- The 6 phases of incident response explained simply
- A ready-to-use incident response checklist
- Roles and responsibilities for small teams
- Communication templates for incidents
- The 5 most common incident types & how to respond
- Common IR mistakes to avoid
- Quick wins you can implement today

1. Overview

A cyberattack is not a question of if — it is a question of when. For small businesses, the difference between a manageable incident and a business-ending catastrophe is not the size of your IT team. It is whether you have a plan.

Incident response (IR) is the structured process your team follows when a security incident is detected: how you identify what happened, stop the damage, recover your systems, and learn from the experience. Businesses with a tested incident response plan contain breaches 58% faster and spend significantly less on recovery.

The good news: you don't need a dedicated security operations center or a 50-page enterprise playbook. This guide gives you a practical, plain-English incident response framework designed for teams of 1–20 people with no dedicated security staff.

2. Why This Matters

REAL-WORLD SCENARIO

A dental practice in Ohio was hit with ransomware on a Monday morning. They had no IR plan, no designated contact list, and no backups tested in over a year. By the time they reached their IT provider, three days had passed. Recovery took six weeks and cost $180,000 — including ransom, forensics, and lost revenue. A written response plan with current contacts could have saved months of pain.

The Business Case for Incident Response

Without an IR Plan	With an IR Plan	The Difference
• Panic and confusion • Wrong people contacted first • Evidence destroyed by accident • Regulators find out from press • Recovery takes weeks or months • Insurance claim denied	• Calm, coordinated response • Right people alerted immediately • Evidence preserved for forensics • Proactive stakeholder communication • Recovery in hours or days • Insurance claim supported	• 58% faster containment • Dramatically lower breach cost • Preserved legal standing • Client trust maintained • Operational continuity • Regulatory compliance

3. Key Definitions

Before diving into the playbook, it's helpful to understand a few key terms. These aren't just vocabulary exercises — they shape how your team thinks and communicates during an incident.

Term	Plain-English Definition
Security Incident	Any event that actually or potentially compromises the confidentiality, integrity, or availability of your data or systems. This includes ransomware attacks, phishing compromises, unauthorized access, and data leaks.
Security Event	A general observation or log entry that may or may not indicate a problem. Not every event is an incident — but all incidents start as events.
Threat Actor	The person or group responsible for the attack. Could be an organized criminal gang, a disgruntled employee, an automated bot, or a nation-state attacker.
Indicator of Compromise (IoC)	Evidence that a system has been compromised. Examples: unusual login times, unfamiliar processes running, files encrypted, large data transfers to unknown destinations.
Containment	Stopping the spread of an incident. Like quarantining a sick employee — you isolate the affected systems before the infection spreads further.
Eradication	Removing the threat from your environment entirely. This means removing malware, closing unauthorized access, patching vulnerabilities, and resetting credentials.
Recovery	Restoring affected systems and data to normal operation, verifying integrity, and resuming business operations.
Post-Incident Review	The 'lessons learned' session held after an incident to understand what happened, how it was handled, and how to prevent recurrence.

4. Roles & Responsibilities for Small Teams

You don't need specialized security staff to respond to incidents. You need clear role assignments so everyone knows exactly what they're responsible for before an incident occurs. The following roles can be filled by existing team members.

> **CRITICAL PREPARATION TIP**
> The biggest IR mistake small businesses make is assuming someone else will lead the response. Assign these roles now, in writing, before an incident happens. Post the contact list somewhere accessible even when systems are down (printed or on a shared phone note).

Role	Responsibilities	Who Fills This	Backup Contact
Incident Commander	Leads the overall response. Makes final decisions. Communicates with leadership. Keeps the team calm and on track.	Owner / Senior Manager	Named backup person
Technical Lead	Investigates the incident, isolates systems, collects evidence, coordinates with IT provider or MSP.	IT Staff / MSP	IT provider on-call
Communications Lead	Handles internal and external communications. Notifies clients, regulators, and insurers as required. Manages messaging.	Office Manager / HR	Owner
Documentation Keeper	Records a timeline of all actions taken during the incident. Preserves evidence. Maintains the incident log.	Admin / Any staff	Secondary staff member
Business Continuity Lead	Ensures critical business operations continue or are restored as quickly as possible during the incident.	Operations / COO	Owner

Fill-in exercise: Write the actual names and mobile numbers for each role in your organization. Store this list printed in a physical binder and in a shared secure note accessible from any device.

5. The 6 Phases of Incident Response

Every incident response framework — from NIST to SANS — follows the same fundamental phases. Here they are adapted for a small business team with no dedicated security staff.

PHASE 1 **PREPARATION** *Before an incident occurs*

Preparation is the most important phase — and the only one you control entirely before an incident happens. Everything you do now determines how well you respond when it counts.

- Create and distribute a written incident response plan with contact lists
- Assign IR roles to specific people and ensure everyone knows their responsibility
- Maintain an up-to-date asset inventory: devices, software, cloud services, data locations
- Verify backups are working and tested — confirm you can actually restore from them

- Enable logging on critical systems: Microsoft 365 audit logs, firewall logs, endpoint logs
- Keep cyber insurance policy and contact information easily accessible
- Establish a relationship with a trusted IT provider or MSP before you need one
- Conduct a brief tabletop exercise at least annually — walk through a scenario as a team

PHASE 2 DETECTION & ANALYSIS

First hours of an incident

Something has happened — or may have happened. This phase is about determining whether you have a real incident and how serious it is. Resist the urge to immediately start fixing things; you may destroy evidence.

Detection Signals — What to Watch For

- Systems suddenly encrypted or files with unusual extensions (.locked, .encrypted, .crypted)
- Employees report they cannot access systems or receive ransom messages
- Unusual logins: unfamiliar locations, times outside business hours, multiple failed attempts
- Antivirus or EDR alerts that look unusual or describe threats you haven't seen before
- Unexplained data transfers — large uploads to unfamiliar IP addresses or cloud services
- Emails bouncing or clients reporting they received suspicious emails from your domain
- Financial transactions you don't recognize or wire transfer requests that seem unusual
- Systems running very slowly or crashing repeatedly without explanation

Initial Analysis Steps

1. Take a screenshot or photo of anything suspicious — do not delete it
2. Document when the issue was first noticed and by whom
3. Determine scope: is this one device, one user, one office, or widespread?
4. Check if this is an active attack in progress or a discovered past breach
5. Notify your Incident Commander immediately — do not try to handle it alone

PHASE 3 CONTAINMENT

Stop the bleeding

Containment means stopping the incident from spreading further. Think of it like a hospital isolating a patient with a contagious disease — you’re not curing the problem yet, you’re preventing it from infecting everyone else.

Short-Term Containment Actions

- Isolate affected devices from the network immediately — disconnect Ethernet, disable

Wi-Fi

- Do NOT turn off affected devices (you may destroy evidence needed for forensics)
- Change passwords for all potentially compromised accounts immediately
- Revoke active sessions for compromised accounts in Microsoft 365 or Google Workspace
- Block identified malicious IP addresses or domains at your firewall
- Disable any compromised email accounts or forwarding rules created by attackers
- Alert your IT provider or MSP — they should be your first external call

Evidence Preservation Checklist

- Do NOT wipe or reimage affected systems until forensics are complete
- Preserve system logs from affected devices and servers
- Screenshot all attacker activity, ransom notes, or suspicious emails
- Document all containment actions with timestamps
- Keep a written log of every action taken and by whom

PHASE 4 ERADICATION *Remove the threat*

Eradication is removing every trace of the attacker from your environment. This step must be thorough — attackers often leave backdoors so they can return after you think you've cleaned up.

- Identify and remove all malware, malicious files, and attacker tools
- Close every unauthorized access point, account, or software the attacker used
- Reset ALL passwords across your environment — not just the obvious accounts
- Revoke and reissue any API keys, application credentials, or tokens that may be compromised
- Patch every vulnerability that was exploited during the attack
- Review and remove any unauthorized email forwarding rules, OAuth app permissions, or admin accounts
- Conduct a full scan with your EDR tool before declaring systems clean
- Consider engaging a third-party forensics firm for significant incidents

CRITICAL WARNING

Never restore from backup into a compromised environment. Eradicate the threat completely, verify the environment is clean, then restore. Restoring into a compromised system can immediately reinfect your recovered data.

PHASE 5 RECOVERY *Restore normal operations*

Recovery is bringing your systems and business operations back online safely. Patience here is critical — returning to normal too quickly, before the environment is truly clean, can restart the entire incident.

- Restore systems from verified clean backups — confirm backup integrity before restoring
- Rebuild any systems that cannot be fully verified as clean
- Re-enable user accounts only after passwords are reset and MFA is confirmed active
- Test all restored systems thoroughly before reconnecting to the production network
- Monitor restored systems closely for the first 30 days for signs of reinfection
- Validate that business operations are functioning normally before declaring the incident closed
- Notify clients, partners, or regulators as required by law or contract
- Update your cyber insurance carrier on the incident status and recovery timeline

PHASE 6 **POST-INCIDENT REVIEW** *Learn and improve*

The post-incident review is one of the most valuable activities in your entire security program. This is where you turn a painful experience into durable protection. Schedule this meeting within two weeks of incident closure.

Post-Incident Review Questions

- How and when was the incident first detected? Could it have been detected earlier?
- What was the initial attack vector? How did the attacker gain access?
- Were response times adequate? Where did the process slow down?
- Did our IR plan work? What was missing or unclear?
- Was communication effective — internally and with clients/regulators?
- What controls, if we had them, would have prevented or reduced the impact?
- What immediate security improvements should we prioritize?
- Do we need to update our IR plan, contact lists, or backup procedures?

6. Incident Response Checklist

Print this checklist and keep it in a physical binder accessible even when your systems are down. Walk through it in sequence when an incident occurs.

IMMEDIATE — First 30 Minutes

☐	Stay calm. Do not start deleting or wiping anything.
☐	Take screenshots / photos of any ransom notes, error messages, or suspicious activity
☐	Note the exact time and date the incident was discovered
☐	Disconnect affected devices from the network (Ethernet cable out, Wi-Fi off)
☐	Notify your Incident Commander
☐	Call your IT provider / MSP on their emergency number

SHORT-TERM — First 4 Hours

☐	Change all passwords for potentially compromised accounts
☐	Revoke active user sessions in Microsoft 365 / Google Workspace Admin console
☐	Contact your cyber insurance carrier to open a claim
☐	Begin documentation: timestamped log of every action taken
☐	Determine scope: how many devices, users, systems are affected?
☐	Notify your attorney if client data may be involved

ONGOING — First 48 Hours

☐	Work with IT provider to eradicate malware and close all unauthorized access
☐	Reset ALL employee passwords across all systems
☐	Determine if breach notification is legally required (attorney guidance)
☐	Send pre-approved communications to affected clients if data was involved
☐	Begin verified backup restoration process
☐	Document all costs for insurance claim purposes

RECOVERY — Days 3–14

☐	Restore systems from clean backups into clean environment
☐	Test all restored systems before returning to production
☐	Monitor restored systems for 30 days for signs of reinfection
☐	File formal breach notifications to regulators if required
☐	Notify clients of resolution and steps taken to prevent recurrence
☐	Update cyber insurance carrier with final incident details

LEARN — Within 30 Days

☐	Hold post-incident review meeting with all role holders

☐	Update IR plan with lessons learned
☐	Implement security improvements identified during review
☐	Update contact lists if anything was missing or wrong
☐	Schedule a tabletop exercise within 60 days to test improvements

7. The 5 Most Common Incident Types

These are the most frequently reported incident types for small businesses. Knowing the specific response actions for each type helps your team react faster and more effectively.

1. Ransomware Attack

- Isolate ALL affected devices immediately — disconnect from network
- Do NOT pay the ransom without consulting your attorney and insurance carrier first
- Contact cyber insurance carrier immediately — most policies have IR firm on retainer
- Engage a professional ransomware response firm for decryption assessment
- Identify patient zero: which device/user was the initial point of infection
- Restore from clean offline backups after full eradication of malware
- Report to FBI Internet Crime Complaint Center (IC3) at ic3.gov

2. Phishing / Account Compromise

- Immediately reset the compromised account password and force sign-out all sessions
- Enable MFA if not already active — do this before re-enabling the account
- Review email account for unauthorized forwarding rules, sent emails, or deleted items
- Check for unauthorized applications connected via OAuth in Microsoft 365 / Google admin
- Notify anyone who received phishing emails from the compromised account
- Scan all devices used by the compromised user for malware
- Review audit logs for all actions performed using the compromised credentials

3. Business Email Compromise (BEC) / Wire Fraud

- Immediately contact your bank — you have minutes to 72 hours to potentially recover funds
- File a complaint with the FBI IC3 at ic3.gov — they work with banks to freeze

transfers

- Preserve all emails involved in the fraud chain — do not delete anything
- Identify how attacker accessed email or impersonated the executive/vendor
- Notify your insurance carrier — BEC coverage is often separate from general cyber policy
- Engage attorney immediately — wire fraud notification requirements vary by state
- Conduct full audit of all payment processes and email security controls

4. Data Breach / Unauthorized Data Access

- Determine what data was accessed, exfiltrated, or exposed
- Identify all affected individuals — name, contact information, type of data involved
- Engage attorney immediately — data breach notification laws vary by state and industry
- Preserve all evidence of how the breach occurred and what was accessed
- Notify your cyber insurance carrier and open a claim
- Prepare breach notification letters for affected individuals (attorney should review)
- For healthcare breaches: notify HHS Office for Civil Rights within 60 days of discovery

5. Malware Infection (Non-Ransomware)

- Isolate infected device(s) from the network immediately
- Run a full scan with your EDR tool to identify all malware components
- Do not attempt manual removal unless guided by a professional
- Determine if the malware has communicated with external command and control servers
- Change passwords for all accounts accessible from the infected device
- Rebuild from clean image if the device cannot be fully verified clean
- Investigate how the malware was installed: malicious email, website, USB drive, software?

8. Communication Templates

Having pre-written, attorney-reviewed communication templates eliminates one of the most stressful tasks during an incident: figuring out what to say to clients, staff, and regulators. These are starter templates — have your attorney review and customize them before use.

Template 1: Internal Staff Notification

Subject: IMPORTANT — Security Incident Underway — Action Required

Team,

We are currently responding to a security incident affecting [describe systems/scope]. Our IT team is actively working to contain and resolve the issue.

IMMEDIATE ACTIONS REQUIRED:

- Do NOT use [affected systems] until further notice
- Do NOT discuss this incident externally or on social media
- Report any suspicious activity or unusual system behavior immediately to [name/number]
- Check your email for your manager's updates

We will provide updates every [X hours]. Contact [Incident Commander name] at [phone] with any questions.

Thank you for your cooperation.

Template 2: Client Notification (Data Breach)

Subject: Important Notice Regarding Your Information

Dear [Client Name],

We are writing to inform you that [Company Name] recently experienced a security incident. We take the security of your information extremely seriously and want to be transparent with you about what happened.

What Happened: [Brief description of the incident without technical jargon]
What Information Was Involved: [Specific types of information]
What We Are Doing: [Steps taken to contain, investigate, and prevent recurrence]
What You Should Do: [Specific protective actions for the recipient]

We sincerely apologize for any concern or inconvenience this may cause. For questions, please contact [dedicated contact name] at [phone/email].

⚠️ **IMPORTANT: Have your attorney review and customize this template before sending.**

9. Common Incident Response Mistakes

⚠️ **Turning Off Affected Systems Immediately**

The instinct to power down a compromised computer is understandable but often harmful. Volatile memory (RAM) contains critical forensic evidence — active malware, attacker commands, encryption keys — that is permanently lost when you power off. Leave systems running and isolated unless specifically instructed otherwise by your IR team.

⚠️ **Trying to Handle It Internally Without External Help**

Small business owners often try to manage incidents without calling their IT provider, attorney, or insurance carrier to save time or money. This almost always makes the incident worse. Call

your IT provider and insurance carrier immediately — most cyber policies include a 24/7 IR hotline.

⚠ **Paying Ransom Without Professional Guidance**

Paying a ransom is not simply a financial transaction. It may violate OFAC regulations if the attacker is a sanctioned entity, and it does not guarantee you'll recover your data. Always consult your attorney and insurance carrier before making any payment decision.

⚠ **Delaying Client Notification**

Many business owners delay notifying affected clients to avoid embarrassment or panic. This backfires badly — delayed notifications increase legal liability, damage trust far more than the incident itself, and may violate breach notification laws with serious penalties.

⚠ **Failing to Preserve Evidence**

Wiping devices, deleting suspicious emails, and clearing logs to "clean up" are natural impulses but destroy the evidence needed for forensics, insurance claims, and legal proceedings. Preserve everything until your IR team and attorney say otherwise.

⚠ **Never Testing the IR Plan**

A plan that has never been rehearsed is not really a plan — it's a document. Conduct at least an annual tabletop exercise where your team walks through a realistic scenario. This surfaces gaps in the plan, confirms contacts are current, and builds the muscle memory your team needs in a real crisis.

10. Quick Wins: Build Your IR Readiness Today

You can meaningfully improve your incident response readiness in under two hours. Here are the five highest-impact actions that cost nothing but time:

#	Action	Time	Cost
01	Write down your three most important emergency contacts: IT provider, cyber insurance carrier, and your attorney. Store on paper AND in your phone.	15 min	Free
02	Assign IR roles to specific named individuals. Write it down, email it to the team, and confirm everyone knows their role.	30 min	Free
03	Verify your most recent backup by actually restoring a test file. If you can't restore, you don't have a backup.	30 min	Free
04	Locate your cyber insurance policy. Find the 24/7 claims hotline number. Save it in your phone right now.	10 min	Free

05	Enable audit logging in Microsoft 365: Admin Center > Compliance > Audit. This is turned off by default in many tenants.	15 min	Free

11. Resources & Next Steps

Essential External Resources

- FBI Internet Crime Complaint Center: ic3.gov
- CISA Incident Reporting: cisa.gov/report
- NIST Computer Security Incident Handling Guide (SP 800-61): csrc.nist.gov
- FTC Data Breach Response Guide: ftc.gov/datasecurity
- HHS Breach Notification Rule (Healthcare): hhs.gov/hipaa/breaches
- Cyber Readiness Institute (Free SMB Resources): cyberreadinessinstitute.org

THREATNEXIS INSIGHT

The best time to build your incident response plan was last year. The second best time is today. A one-page plan with current contacts, assigned roles, and a backup verification date is infinitely more valuable than a 50-page plan that's never been tested.

SEO & Content Strategy Reference

Primary Keyword:

- incident response plan for small business

Secondary Keywords:

- cyber incident response checklist small business
- what to do during a ransomware attack small business
- business email compromise response steps
- data breach response plan small team
- NIST incident response framework small business

SEO Title:

- Incident Response for Small Business Teams: Complete Playbook & Checklist [2025]

Meta Description:

- Step-by-step incident response guide for small businesses. Includes the 6 IR phases, ready-to-use checklist, response templates for 5 incident types, common mistakes, and quick-start actions.

SEO Slug:

- /incident-response-plan-small-business

People Also Ask:

- What should a small business do during a ransomware attack?
- Does a small business need an incident response plan?
- How do I create an incident response plan for a small team?
- What are the 6 phases of incident response?
- How do I report a cyberattack to the FBI?

Monetization Opportunities:

- Premium Incident Response Playbook (premium version of this guide)
- IR Tabletop Exercise Facilitation Service
- Annual Security Assessment & IR Plan Development
- Virtual CISO Retainer — ongoing IR plan maintenance
- Cyber Insurance Readiness Review
