SECURITY GUIDE · 02

Building an Incident Response Plan

Be ready before something goes wrong

A clear, practical playbook for preparing your business to detect, contain, and recover from a cybersecurity incident — so a bad day stays a manageable one.

Wagner Cybersecurity LLC
www.wagnercybersecurity.com · joe@wagnercybersecurity.com

Contents

Why every business needs a plan

The question is not whether your business will face a security incident, but when — and whether you will be ready to handle it calmly.

An incident can be anything from a ransomware attack that locks your files, to an employee falling for a phishing email, to a lost laptop full of customer data. What separates a minor disruption from a business-threatening crisis is rarely the attack itself. It is whether the people involved know what to do in the first few hours.

An incident response (IR) plan is the difference between scrambling and executing. It removes guesswork at the exact moment when stress is highest and clear thinking is hardest. This guide shows you how to build one that fits a small or mid-sized business — short enough to actually use, complete enough to matter.

> **The cost of not planning**
> Disorganized response extends downtime, increases the chance of mistakes, and can turn a contained problem into a reportable breach. Most of the damage from an incident accrues while no one is sure who is in charge.

What an incident response plan is

An incident response plan is a written, agreed-upon document that answers four questions before an incident happens:

- **Who is in charge?** Named people and their backups, with contact details.
- **What counts as an incident?** How you recognize one and how serious it is.
- **What do we do?** The concrete steps to contain, investigate, and recover.
- **Who do we tell?** Staff, customers, regulators, insurer, and when.

A good plan is practical, not theoretical. It lives somewhere everyone can reach it — including on paper or on a phone, because the network may be exactly what is down. It is reviewed and rehearsed, not written once and filed away.

The incident response lifecycle

Most established plans follow a simple four-phase lifecycle. You will move through these phases — sometimes looping back — during any incident.

Phase	What happens	Goal
1. Preparation	Build the plan, assign roles, train staff, and put safeguards and backups in place.	Be ready, before anything happens.
2. Detection & analysis	Notice the incident, confirm it is real, and understand its scope and severity.	Know what you are dealing with.

Phase	What happens	Goal
3. Containment, eradication & recovery	Stop the spread, remove the cause, and restore clean systems and data.	Limit damage and get back to normal.
4. Post-incident activity	Review what happened, capture lessons, and improve the plan and defenses.	Be better prepared next time.

Preparation is where the real leverage is. Every hour spent here saves many during an actual incident.

Who does what: roles and contacts

During an incident, ambiguity is costly. Assign these roles in advance — in a very small business, one person may wear several hats, and that is fine, as long as it is written down.

Role	Responsibility
Incident lead	Owns the response, makes decisions, and keeps everyone coordinated. The single point of accountability.
Technical lead	Investigates, contains, and recovers systems. Often your internal IT person or managed IT provider.
Communications	Manages messaging to staff, customers, and the public. Prevents mixed signals.
Executive / owner	Approves major decisions (e.g., taking systems offline, paying for outside help) and owns business risk.
External partners	IT/security provider, cyber-insurance contact, and legal counsel — lined up before you need them.

> **Build your contact sheet now**
> Keep one page with names, mobile numbers, and after-hours contacts for every role above — plus your insurer's claims line and IT provider's emergency number. Store a copy offline.

Classifying incidents by severity

Not every event deserves an all-hands response. A simple severity scale helps you respond proportionally and decide who to wake up.

Level	Description	Example
Low	Minimal impact; contained and routine.	A single phishing email reported and deleted, no clicks.
Medium	Limited impact to some users or data; needs prompt attention.	One workstation infected; no spread confirmed.
High	Significant impact to operations or sensitive data.	Business email account compromised; fraudulent messages sent.
Critical	Severe, business-wide impact or confirmed data breach.	Ransomware across multiple systems; operations halted.

Define in advance who must be notified at each level and how fast. For example: High and Critical incidents notify the owner and IT provider immediately, day or night.

The first 24 hours: a response runbook

When an incident is confirmed, work through these steps. Resist the urge to skip straight to fixing — a few minutes of containment and documentation protects you later.

1. **Stay calm and activate the plan.** Notify the incident lead. Do not let individuals freelance fixes that destroy evidence.
2. **Contain first.** Isolate affected systems — disconnect from the network rather than powering off, which can erase useful evidence. Disable compromised accounts.
3. **Assess scope and severity.** What is affected? What data is involved? Assign a severity level and notify accordingly.
4. **Preserve evidence.** Take notes with timestamps, capture screenshots, and avoid wiping systems until you know whether you must investigate or report.
5. **Engage your partners.** Bring in your IT/security provider and notify your cyber-insurer early — many policies require prompt notice and can supply expert help.
6. **Eradicate and recover.** Remove the cause, then restore from known-good backups. Reset credentials. Confirm systems are clean before reconnecting.
7. **Communicate per the plan.** Keep staff informed; notify customers or regulators if and when required (see the next section).
8. **Document throughout.** A clear timeline supports insurance claims, legal obligations, and your post-incident review.

> **Do not pay or negotiate alone**
>
> If you face an extortion or ransomware demand, involve your insurer, legal counsel, and security provider before taking any action. There are legal, financial, and practical considerations that specialists handle every day.

Your communication plan

Poor communication can do as much damage as the incident. Decide in advance how you will handle each audience.

- **Internal staff:** Tell them what they need to know, what to do, and what not to say externally. Designate a single spokesperson.
- **Customers and partners:** Be honest, timely, and specific about impact and remediation. Silence breeds distrust; speculation creates liability.
- **Regulators:** Many jurisdictions and industries require notification of data breaches within set timeframes. Know your obligations before an incident, not during one.
- **Public and media:** Prepare a short holding statement template now. Route all inquiries to your spokesperson.

> **Have templates ready**
>
> Draft skeleton notices for staff, customers, and a public statement in advance. Filling in blanks

> under pressure is far easier than writing from scratch during a crisis.

Common incidents and first moves

A few scenarios cover most of what small businesses actually face. Knowing the opening move for each saves precious time.

Incident	Immediate first moves
Ransomware	Isolate affected machines from the network; do not pay or react alone; engage insurer and IT provider; recover from clean backups.
Business email compromise	Reset the affected account password and sign out all sessions; enable MFA; check for mail-forwarding rules; warn anyone who received messages.
Phishing (clicked link / entered credentials)	Reset that user's passwords immediately; enable MFA; scan the device; watch for unusual account activity.
Lost or stolen device	Remotely lock or wipe if possible; change passwords for accounts used on it; confirm whether sensitive data was stored and encrypted.
Suspected data breach	Contain access; preserve evidence; assess what data is involved; consult counsel and insurer about notification duties.

> **MFA is your safety net**
> Most email-compromise and credential-phishing incidents are stopped cold by multi-factor authentication. If it is not on everywhere, that is the highest-value fix you can make today.

Testing the plan before you need it

A plan no one has practiced is a document, not a capability. The simplest and most effective test is a tabletop exercise.

A tabletop is a guided, low-pressure discussion where your team walks through a realistic scenario together: "It is Monday at 9 a.m. and staff cannot open their files. What do we do first? Who calls whom?" You talk through each step, find the gaps, and fix the plan.

- Run a tabletop at least once a year, and after any major change to your systems or team.
- Keep it realistic and blameless — the goal is to improve the plan, not to grade people.
- Capture every gap you find and assign an owner to fix it.
- Confirm the basics actually work: can you reach the contact list, and can you truly restore from backup?

Quick-start checklist

If you are starting from nothing, this is enough to have a real plan in place quickly.

- Name an incident lead and a backup, with contact details.

- Build a one-page emergency contact sheet, including insurer and IT provider — stored offline.
- Define your severity levels and who gets notified at each.
- Write the first-24-hours runbook steps and keep them accessible without the network.
- Draft communication templates for staff and customers.
- Confirm backups exist and test a restore.
- Schedule a tabletop exercise on the calendar.

> **Done beats perfect**
>
> A short plan your team has read and rehearsed will serve you far better than a comprehensive one no one has opened. Start simple and improve it after every test.

Where to go from here

Preparation pays off precisely when everything else is going wrong. Assign the roles, build the contact sheet, write the runbook, and rehearse it once — you will have moved your business from improvising to executing.

If you would like help drafting your plan, facilitating a tabletop exercise, or being on call as your incident response partner, we are glad to help.

> **Talk to us**
>
> **Wagner Cybersecurity LLC**
>
> joe@wagnercybersecurity.com · www.wagnercybersecurity.com

Glossary

Incident — Any event that compromises the confidentiality, integrity, or availability of your systems or data.

Incident response (IR) — The organized process of preparing for, detecting, containing, and recovering from incidents.

Containment — Steps taken to stop an incident from spreading further.

Eradication — Removing the cause of an incident, such as malware or a compromised account.

Tabletop exercise — A discussion-based rehearsal where a team walks through a hypothetical incident to test the plan.

Business email compromise (BEC) — An attack where a business email account is taken over or impersonated, often to commit fraud.

Ransomware — Malicious software that encrypts your data and demands payment to restore access.