The Pro Link Systems Incident Response Playbook

The plan we actually run when something goes wrong

Why we publish this

Most IT providers keep their incident process in their heads. We wrote ours down, and then we published it — because the moment to find out how your IT partner handles a crisis is **before** the crisis, not at 2 a.m. during one.

This is the playbook our team follows when a client is under attack, down, or unsure. It is deliberately calm. Panic is a choice, and in an incident it is the wrong one: it skips steps, destroys evidence, and turns a bad hour into a bad week. Our job is to be the steady hand — to already know the next move so you don't have to.

It's built on the incident-response lifecycle from **NIST SP 800-61** — Prepare, Detect & Analyze, Contain, Eradicate & Recover, and Learn — adapted for the real conditions of a small or mid-sized business.

What counts as an incident

An **incident** is any event that threatens the confidentiality, integrity, or availability of your systems or data. In plain terms: something is broken, exposed, or being attacked, and it needs a coordinated response — not just a help-desk ticket. We classify every incident by severity so the response matches the stakes:

Severity	What it looks like	Our response
SEV-1 — Critical	Active ransomware, confirmed breach, full outage of a critical system, funds at risk	Immediate all-hands. Incident Commander assigned. Owner called, not emailed.
SEV-2 — High	One compromised account, malware contained to a machine, a key system degraded, targeted phishing	Rapid response, senior engineer engaged, client notified within the hour
SEV-3 — Moderate	Suspicious activity, isolated outage, a failed backup, a lost device	Same-day investigation, monitored to resolution
SEV-4 — Low	A blocked threat, a single reported phishing email, a minor anomaly	Logged, reviewed, used to tune defenses

Severity can move in either direction as we learn more. We would rather over-classify for the first thirty minutes than under-react.

Who does what

In an incident, unclear roles cost time. We assign them immediately:

- **Incident Commander** — owns the response, makes the calls, keeps the timeline. One person, so decisions don't stall.
- **Technical Lead(s)** — the engineers doing the containment and recovery work.
- **Communications Lead** — the single point of contact for you, so your team gets one clear voice instead of five fragments.
- **Your business owner / decision-maker** — looped in from the start for any decision that affects operations, money, or legal exposure.

Because our help desk is **24/7, in-house, and US-based**, the person who picks up already works here and can escalate to a senior engineer in minutes — there's no offshore tier, no phone tree, and no waiting for business hours.

The response lifecycle

1. Prepare (before anything happens)

The best incident response is the work done on an ordinary day. For every client we protect, the baseline is: multi-factor authentication on email, remote access, and financial systems; endpoint detection and response (we run **SentinelOne**) on every managed device; a patch and vulnerability cadence; and **tested, off-site backups** with a documented recovery plan. An untested backup is not a backup — it's a hope, so we verify restores, not just backup jobs.

2. Detect & Triage

When an alert fires or a client calls, the clock starts. We confirm it's real, assign severity, name an Incident Commander, and open a live timeline. Our first-response target on any ticket is a **15-minute average**, and for a live SEV-1 the response is immediate. Then we ask three questions: *What is happening, what is affected, and is it still spreading?*

3. Contain

Stop the bleeding before cleaning the wound. Containment might mean isolating a machine from the network, disabling a compromised account, blocking a malicious address, or cutting a specific connection — always the least-disruptive move that stops the spread. **We preserve evidence while we contain:** we don't wipe or reboot a compromised machine before capturing what it can tell us, because that data decides how far the incident actually went.

4. Eradicate & Recover

Remove the cause — the malware, the foothold, the bad rule, the exposed credential — and confirm it's gone, not just quiet. Then restore from **known-clean, tested backups**, bring systems back in a deliberate sequence, and watch them closely for signs the threat returns. We don't declare “recovered” until systems are verified clean and stable, not merely powered on.

5. Learn (post-incident review)

Within days of resolution, we run a **blameless review**: a clear timeline, what worked, what didn't, and the specific changes that make the same incident less likely and less costly next time. The point isn't to assign fault — it's to make the whole environment stronger. Every incident improves the playbook.

The first 60 minutes

The opening hour sets the tone. Our checklist, in order:

1. **Confirm and classify** — is it real, and how bad? Assign severity and an Incident Commander.
2. **Open the timeline** — every action and finding, timestamped, from minute one.
3. **Contain, don't erase** — isolate what's spreading; preserve the evidence.
4. **Communicate out-of-band** — if email or accounts may be compromised, we reach you by phone or a channel the attacker can't see. We never discuss a live incident on a system that may be listening.
5. **Protect what matters next** — verify backups are intact and reachable before anything else touches them.
6. **Bring in the right people** — senior engineers, and where warranted, guidance on cyber-insurance and legal notification obligations.

Incident-type runbooks

Ransomware

Isolate affected machines immediately; do **not** power them down (it destroys evidence and can worsen encryption state). Identify patient zero and scope. Preserve samples and logs. **Do not pay or negotiate before assessing recovery options** — with tested backups, paying is usually avoidable, and payment carries legal and no-guarantee risk. Recover from clean backups, rebuild affected systems, rotate credentials, and monitor for reinfection.

Business email compromise / phishing

Reset the affected credentials and revoke active sessions immediately. Hunt for attacker-created mailbox rules (auto-forwarding and auto-delete are the classic hidden footholds). Check for fraudulent wire or payment-change requests — **any payment or banking change gets verified out-of-band, by voice, no exceptions.** Notify anyone the compromised account may have targeted.

Account or credential compromise

Disable the account, revoke sessions and tokens, reset the password, and re-enroll MFA. Review what that account could reach and whether it was used to move laterally. Assume the credential is public and rotate anything it shared.

Data breach or exfiltration

Contain the access path first. Determine what data, whose data, and how much — this drives legal and notification obligations. Preserve evidence rigorously. Engage the client's decision-maker early; breach notification is a legal question with deadlines, not just a technical one.

Major outage or infrastructure failure

Establish what's down and the business impact. Work the restore in priority order — decide the sequence before you need it, not during. Communicate status on a steady cadence so silence never reads as “still broken.” Fail over where a plan exists; recover from backups where it doesn't.

Lost or stolen device

Remotely lock or wipe the device, revoke its access and sessions, and rotate any credentials it held. Assess what data it could reach and whether encryption was enabled (it should have been). Log it and confirm the gap is closed.

Our commitments during an incident

You reach a real person, fast. Our help desk is 24/7, in-house, and US-based, and calls are answered live — no phone tree, no hold queue. Average ticket first response: 15 minutes.

We resolve, and quickly. 90% of issues solved on first contact, with a sub-one-hour average resolution time — and in an incident you get proactive updates, not silence.

No surprises. One clear point of contact and a straight account of what’s happening, what we’re doing, and what we need from you.

We tell you the truth. Including when the news is bad, and including what we’ll change so it doesn’t happen again.

We've done this since 1999 — through real outages, real ransomware, and real recoveries, for Los Angeles businesses.

The baseline that prevents most of this

Most incidents we see would have been stopped, or made trivial, by five things being in place beforehand:

1. **MFA everywhere** it matters — email, remote access, financial systems.
2. **EDR on every endpoint**, monitored — not just antivirus.
3. **Backups that are off-site and actually tested** by restoring them.
4. **Patching and vulnerability management** on a real cadence.
5. **People who can spot a phish** — the best-defended network still has a front door made of human judgment.

Want us to pressure-test your incident readiness?

We'll do a **free 15-minute review** — a straight read on where you're exposed and what to shore up first, no pitch. Because the best time to meet the team that answers at 2 a.m. is long before you need them.

prolinksystems.com/contact • 1-800-890-6133

This playbook is a general framework, adapted to each client's systems, obligations, and risk. It is guidance, not a substitute for a response plan built for your specific environment.