

EXECUTIVE GUIDE

Ransomware Response Playbook for SMBs

What to do in the first hours after a ransomware detection — and how to recover with less damage.

The First Hour

Speed and discipline in the first hour shape everything that follows. Isolate affected systems from the network immediately — disconnect, don't power off, since powered-off systems can lose forensic evidence. Activate your incident response plan and notify your incident commander, IT/security lead, and cyber insurance carrier right away; most policies require notification within 24-72 hours, and your insurer will often connect you with a breach coach and forensics team.

Containment

- Disconnect infected systems from the network — do not power them off
- Disable compromised accounts and reset credentials for affected systems
- Preserve logs and evidence — avoid actions that could destroy forensic data
- Identify and isolate the initial point of entry if known, to prevent re-infection

Assessing the Impact

Before making any recovery decisions, determine what was encrypted, what (if anything) was exfiltrated before encryption, and which backups remain viable and uninfected. This assessment — usually led by your incident response or forensics partner — determines whether you're dealing with a pure availability incident or a data breach that triggers separate notification obligations.

Should You Pay?

Paying a ransom does not guarantee data recovery or that stolen data won't be leaked, and it may carry legal risk if the threat actor is a sanctioned entity. This decision should involve legal counsel, your cyber insurance carrier, and law enforcement — not be made unilaterally under pressure. Many recoveries succeed without payment when backups are intact and isolated.

Notification Obligations

Depending on what data was affected, you may have notification obligations under HIPAA, state breach laws, or contractual requirements with customers and partners. Breach counsel should confirm your specific obligations and timelines — HIPAA, for example, generally requires notification within 60 days of discovery for affected individuals.

Recovery

Rebuild from clean, verified backups — never restore directly into a network that hasn't been confirmed clean, or the infection can recur. Validate systems are patched and the original entry point is closed before reconnecting to production.

Post-Incident Review

Once operations are stable, conduct a formal post-incident review: how did the attacker get in, how long did detection and containment take, and what controls need to change. This review is also typically required documentation for your cyber insurance claim.

Build Your Ransomware Response Plan Before You Need It

Cenova Cyber helps businesses prepare for — and respond to — ransomware incidents.

Contact us to get started.

www.cenovacyber.com