
BLACKTECHSTARTUP EDUCATION

The First 24 Hours After a Cyber Incident: A Small-Tech-Company Playbook

Panic destroys evidence and creates bad decisions. Prepare a first-day incident sequence that contains damage, preserves facts, triggers the right legal and contractual review, and gets the business operating safely again.

Panic destroys evidence and creates bad decisions. Prepare a first-day incident sequence that contains damage, preserves facts, triggers the right legal and contractual review, and gets the business operating safely again.

The first-day plan must exist before the incident

During a ransomware event, account takeover or cloud compromise, the team will have incomplete facts and time pressure. That is the worst moment to decide who has authority to isolate systems, contact counsel, call the insurer or tell customers. NIST SP 800-61 Rev. 3 treats incident response as part of broader cybersecurity risk management, not a binder that appears after compromise. A small company should have a one-page activation sheet with incident lead, technical lead, executive decision maker, legal contact, cyber-insurance contact, critical vendors and out-of-band communication methods.

First hours: contain without erasing the story

If an endpoint or account appears compromised, limit further access while preserving logs and evidence. Disable or reset credentials when appropriate, isolate affected systems, revoke suspicious sessions and preserve relevant cloud, endpoint, identity and network logs. Do not wipe machines or rebuild servers merely to make the alert disappear. Record who observed what, at what time, and every containment action. If you may need outside incident-response or forensic help, contact them early. Evidence quality affects both technical diagnosis and later contractual, insurance or legal questions.

Separate facts, hypotheses and decisions

Create an incident timeline with three columns: confirmed fact, working hypothesis and action.

'Admin account logged in from unfamiliar country' is a fact. 'Attacker stole customer data' may be a hypothesis until evidence supports it. This discipline prevents internal speculation from becoming a customer statement. Assign one person to maintain the record. For every major decision—taking a service offline, restoring a backup, notifying a partner—record who approved it and why. Small teams move fast; written decision history keeps speed from becoming confusion.

Trigger the notification map, not a mass email

Different incidents can create obligations under customer contracts, cyber-insurance policies, sector rules and state or federal law. Do not improvise legal conclusions from a blog post. Notify counsel and the insurer according to your plan and review the exact contracts and data involved. Some customers require rapid incident notice even before full root cause is known. Others require specific channels. Prepare templates that distinguish an initial factual notice from a final incident report. One uncontrolled employee message can create contradictions that are difficult to unwind later.

Recover from a known-good state and watch for re-entry

Restoring service quickly is not enough if the attacker still has credentials, persistence or an unpatched entry point. Before bringing systems back, rotate affected secrets, review privileged access, patch the exploited weakness where known, validate backups and increase monitoring. Prioritize the business services that matter most rather than rebuilding everything simultaneously. Document what remains uncertain. After restoration, watch identity, network and cloud logs for recurrence. Recovery is a controlled return to operation, not the moment the website comes back online.

Run the tabletop now

Choose a scenario: stolen administrator credentials, ransomware on a file server or exposed cloud token. Put the leadership team in a room for 60 minutes. At minute zero, reveal the alert. Ask who acts, which system is isolated, where logs live, who can reach the insurer, what the customer contract requires and how the team communicates if email is unavailable. Every time someone says 'we would probably,' write a corrective action with an owner. A rehearsal that exposes missing phone numbers and inaccessible logs is cheap. Discovering those gaps during a real attack is not.

Create the incident decision card

Print or securely store a one-page card that the incident lead can use under pressure. Include severity levels and the conditions that trigger each one; authority to isolate systems; forensic-preservation steps; emergency contacts; cyber-insurer notification instructions; outside counsel; cloud and identity vendor escalation paths; customer-notification decision owner; ransomware/payment policy authority; and the location of offline backups and credentials. Add three hard rules: preserve evidence before destructive cleanup when safe; do not make public attribution without evidence and leadership approval; and do not pay, promise or notify based on one person's guess. Then list the company's minimum operating services in recovery order—identity, communications, customer application, billing, internal file systems—and name the person who can declare each safe for restoration. Test the card twice a year and whenever vendors or staff change. During the exercise, deliberately remove a dependency: assume email is down, the CEO is traveling or the primary cloud console account is locked. The card should still work. This is not bureaucracy. It is a compact transfer of decision authority from a calm day to a chaotic one, which is exactly when a small company needs it most.

SOURCE DESK

Research behind this guide

Use the primary sources below to verify current rules, eligibility and program details before acting. Program terms can change.

NIST — SP 800-61 Rev. 3 Incident Response Recommendations and Considerations for Cybersecurity Risk Management



CISA — Federal Government Cybersecurity Incident and Vulnerability Response Playbooks



CISA — Cyber guidance for small and midsize businesses



NIST — Ransomware resources



Important: This article is educational information, not individualized legal, tax, investment or compliance advice. For decisions with legal or financial consequences, use a qualified professional who can review your facts.

SHARE THIS GUIDE ↗

POWERED BY: BLACK TECH STARTUP

blacktechstartup.com