CONTINUITY HUB • FIELD INCIDENT CARD

First-24-Hours Incident Card: Small Business Cyber Emergency Fast Protocol

Current version — Oct 31, 2026
Update history: continuityhub.org/cyber-incident-response...

DAY ONE VICTORY CONDITION • PROFESSIONAL RULE

Contained, Documented, Covered, and Still Trading. The first 24 hours of incident response are a containment-and-calls exercise, not a recovery exercise. Trying to fix or restore systems on day one destroys forensic evidence and re-exposes the business to an attacker still inside. Follow the four jobs in strict order.

Hours 0–1: Isolate, Preserve, Escalate

DISCOVERY

Whoever finds the incident: stop spread, protect RAM, establish single commander.

- **Disconnect Network Cables & Wi-Fi:** Unplug Ethernet cables, disconnect Wi-Fi on affected machines. Cut spread roads immediately.
- **LEAVE MACHINES ON:** DO NOT power off, restart, or pull power plugs. Volatile RAM holds active connection evidence, injected malware, and keys.
- **Photograph Screens:** Take photos with a smartphone rather than clicking through prompts, closing windows, or clearing alerts.
- **Log Time & Details:** Note discovery time, visible filenames, unusual extension, user account, and affected shared folders.
- **Escalate to Single Voice:** Notify the owner or named decision-maker immediately. One person in charge; zero freelancing.

Hours 1–4: Calls In Strict Order

PROTECT POSITION

The order your plan sets protects legal, financial, and insurance standing.

1. **Cyber Insurer Incident Line:** Call FIRST if covered. Timely notice preserves coverage; insurer assigns panel counsel and forensic firm.
2. **Breach Counsel / Attorney:** Directs investigation under legal privilege; determines statutory breach notice clocks across jurisdictions.
3. **Incident Response Firm / IT Provider:** Directs technical containment, forensic imaging, and eradication. (Regular IT assists under IR direction).
4. **Bank Fraud Desk:** If funds, invoices, payroll, or BEC are involved. Wire fraud recall is a race measured in hours; freeze transfers instantly.

Restraint Rule: Professionals direct what gets touched. The evidence is the case.

Hours 4–12: Scope and Stabilize

CONTAINMENT

- **Clean-Device Credential Reset:** Reset admin, M365/Google Workspace, and remote access passwords *only from an uncompromised device*.
- **Staff Holding Line:** Instruct team using drafted words: explain systems are undergoing maintenance; prohibit speculation and outside discussion.
- **Customer Holding Statement:** Provide factual holding message cleared by counsel. Never say "no data was taken" on day one.
- **Tomorrow's Workaround:** Activate continuity runbook: paper invoices, alternative phones, isolated loaner laptops. Maintain trade.

Hours 12–24: Shape of Coming Days

DAY ONE CLOSE

- **Containment Holding:** Verify severed network links remain isolated; monitor firewall logs for abnormal beaconing attempts.
- **Eradication Sequencing:** Confirm forensic images are captured before any wipe; plan rebuild milestones from verified clean baselines.
- **Notification Clocks:** Counsel logs statutory deadlines (e.g., state AGs, HIPAA, GDPR, customer contract SLAs).
- **Day-Two Roster:** Document decision-maker shifts, check-in calls, and staff communications before anyone sleeps.

Immediate Emergency Decision-Maker Call Directory

Keep physical copies in phone & off-site

Entity / Role	Contact Name / Provider	Direct 24/7 Phone	Policy / Account Ref
1. Cyber Insurer Incident Line	Carrier Claims Department	1-800-XXX-XXXX	Policy #: _____
2. Breach Counsel / Attorney	Lead Privacy Attorney	Direct Cell: _____	Retainer / Case Ref: _____
3. IR Firm / Managed IT	Designated Technical Lead	Emergency Desk: _____	Service SLA Ref: _____
4. Bank Commercial Fraud Desk	Relationship Mgr / Fraud Line	Wire Recall Direct: _____	Acct #: _____

CONTINUITY HUB • FIELD INCIDENT CARD

The Do-Not List, Core Scenarios & Federal Incident Reporting Channels

Current version — Oct 31, 2026
Update history: continuityhub.org/cyber-incident-response...

THE CRITICAL DO-NOT LIST: 5 IRREVERSIBLE ERRORS

NEVER DO THESE

Every one of these is something a well-intentioned person does instinctively. Each destroys your recovery.

Irreversible Action	Operational Risk & Forensic Impact	Correct Immediate Protocol
1. DO NOT RESTART	Destroys volatile memory (RAM), kills active network sockets, erases encryption keys held in memory, and triggers scheduled malware execution.	Pull network cable / turn off Wi-Fi. **Leave the computer powered ON.**
2. DO NOT DELETE	Deleting encrypted files, suspicious emails, or scripts destroys evidence required by insurers, law enforcement (FBI), and legal defense.	Leave files untouched. Note full path names and timestamps for forensic staff.
3. DO NOT WIPE	Reimaging before forensic images are captured destroys root-cause proof, hides persistence backdoors, and voids insurance claim payouts.	Keep compromised systems segregated until forensic imaging is completed.
4. DO NOT NEGOTIATE	Ransomware negotiation carries federal OFAC sanctions risks. Unskilled communication invites extortion escalation and secondary attacks.	Never message extortionists independently. Let insurer panel negotiators handle.
5. DO NOT ANNOUNCE	Improvised public notices or premature statements ("no data was taken") become legal liabilities when forensics uncover contradictory facts.	Use the single cleared outside sentence. Counsel controls external timing.

3 Core Small Business Scenario Recognition Cards

FIELD TRIAGE

Ransomware / Compromise

Signs: Encrypted file extensions, desktop ransom note, sudden CPU spike.

- Unplug Ethernet / turn off Wi-Fi.
- Disconnect external hard drives.
- **Pause cloud sync** immediately.
- Isolate network shared drives.
- Verify offline backup status.

Email Compromise (BEC)

Signs: Strange inbox forwarding rules, fake invoice sent, MFA fatigue prompts.

- Revoke all active user sessions.
- Reset password from a clean phone.
- Check & delete hidden inbox rules.
- Call bank if wire instructions sent.
- Warn financial team verbally.

Lost or Stolen Device

Signs: Laptop, tablet, or executive phone missing from transit or vehicle.

- Send remote MDM wipe/lock command.
- Revoke corporate account tokens.
- Verify BitLocker / FileVault state.
- File police theft report (for insurance).
- Notify counsel if PII was cached.

Federal & Law Enforcement Reporting

REPORTING

Reporting runs in parallel with response; counsel directs mandatory duties.

- **FBI IC3 (ic3.gov):** Federal intake for cybercrime, wire fraud, and ransomware patterns. Enables federal asset freeze tracing.
- **CISA (cisa.gov):** Federal technical assistance door and incident alert repository. Complementary to IC3.
- **Local Law Enforcement:** File police report for stolen physical hardware or local fraud documentation.

The Single Outside Sentence

PUBLIC COMMS

Every staff member uses this exact sentence for outside inquiries:

> *"We are actively investigating a technical disruption with specialized forensic experts and our partners. We are focused on continuity and will share verified updates as soon as confirmed facts are available."*