CONTINUITY HUB • ACTION PRINT PACK ($7)

Small Business Incident Response: First-24-Hours Action Kit

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

INCIDENT COMMAND • HOURS 0–1 ACTION CHECKLIST

Discovery Moment Protocol: The person who discovers the incident must execute immediate network isolation, preserve volatile memory, and escalate to the designated Incident Commander. Fill out every field in real time.

Incident Identification & Incident Commander Assignment

RECORD

Incident Reference ID:	.....	**Exact Date & Time Discovered:**	.....
Discovered By (Name/Role):	.....	**Designated Incident Commander:**	.....
Initial Symptom Observed:	.....		
Affected Machines / IPs:	.....		

Hours 0–1 Step-by-Step Execution Verification

MANDATORY VERIFICATION

Done	Action Item	Execution Standard & Rationale	Time & Verified By
☐	**1. Network Severance**	Unplug physical Ethernet cable. Toggle hardware/software Wi-Fi switch to OFF. Turn off Bluetooth. *Cuts spread highways immediately.*	Time: _____ Init: ___
☐	**2. Power State Preserved**	**DO NOT POWER OFF OR REBOOT.** Leave machine running. Powering off destroys volatile RAM containing unencrypted keys and active connections.	Time: _____ Init: ___
☐	**3. Screen Evidence Capture**	Photograph all error screens, ransom notes, and dialog boxes using a smartphone camera. Do not click buttons or dismiss alert dialogs.	Time: _____ Init: ___
☐	**4. Storage & Sync Isolation**	Disconnect external backup drives and USB storage. Pause Dropbox / OneDrive / Google Drive sync client to prevent encrypted file replication.	Time: _____ Init: ___
☐	**5. Central Escalation**	Call business owner or designated decision-maker. Enforce command discipline: one voice, all actions logged, zero unauthorized tampering.	Time: _____ Init: ___

Initial Observer Statement & First Observations

FORENSIC LOG

Describe what was observed on screen, exact filenames with changed extensions, any ransom text displayed:

[Observer narrative / screen observations / specific unusual activity noted]

CONTINUITY HUB • ACTION PRINT PACK ($7)

Hours 1–4 Calls-In-Order Worksheet & Call Record Log

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

LEGAL, INSURANCE & TECHNICAL SEQUENCE

The Call Sequence Rule: Making calls in the wrong order costs coverage and complicates legal defense. Insurer first to secure panel coverage; counsel second for privilege; response firm third for technical work; bank fourth if funds are in motion.

Designated Emergency Call Register (Fill Before Incident)

EMERGENCY DIRECTORY

Contact Entity	Provider Name & Contact	Emergency Numbers	Account / Policy #	Tested Date
1. Cyber Insurer Prompt notice required	Carrier: _____ Broker: _____	Hotline: _____ Alt: _____	Policy: _____ Deductible: ____	___/___/2026
2. Breach Counsel Directs under privilege	Law Firm: _____ Attorney: _____	Direct Cell: _____ Office: _____	Retainer Ref: _____ Bar #: _____	___/___/2026
3. Incident Response Forensics & eradication	IR Firm: _____ Lead Tech: _____	Emergency Line: _____ Helpdesk: _____	Contract Ref: _____ SLA Tier: _____	___/___/2026
4. Commercial Bank Wire recall desk	Bank: _____ Officer: _____	Fraud Line: _____ Direct Desk: _____	Operating Acct: ___ Payroll Acct: ___	___/___/2026

Hours 1–4 Live Call Documentation Log

CALL RECORDS

Time Placed	Called Party & Rep Name	Claim / Ticket # Issued	Instructions, Guidance & Assigned Resources
___:___ AM/PM	Insurer Claim Intake: Rep: _____	Claim Ref #: _____	Assigned panel counsel? ☐ Y ☐ N Assigned IR firm: _____
___:___ AM/PM	Breach Counsel: Attorney: _____	Privilege Matter #: _____	Instructions: _____ Regulatory clock: _____
___:___ AM/PM	IR Firm / MSP: Engineer: _____	Triage Ticket #: _____	Triage steps: _____ Remote access authorized? ☐ Y ☐ N
___:___ AM/PM	Bank Fraud Desk: Officer: _____	Recall Case #: _____	Recall initiated for Wire/ACH # _____ Accounts frozen: ☐ Yes ☐ Pending

CONTINUITY HUB • ACTION PRINT PACK ($7)

Hours 4–12 Scope-and-Stabilize Sheet & Business Workaround Plan

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

TECHNICAL CONTAINMENT & OPERATIONS CONTINUITY

Scope and Stabilize: With professional guidance established, define in-scope systems, reset critical credentials from clean off-network devices, and configure manual business workarounds to keep operations running tomorrow.

Clean-Device Credential Reset Protocol

CLEAN DEVICE ONLY

CRITICAL SECURITY RULE: Never reset passwords from a computer on the affected network. Use an uncompromised mobile phone or off-site computer.

System / Account	Reset From Device	MFA Enforced?	Time & Verified By	Status
Domain Admin / Active Directory	Clean Mobile / Off-site	☐ Yes ☐ No	Time: ____ By: ____	☐ Reset Completed
Microsoft 365 / Google Workspace Admin	Clean Mobile / Off-site	☐ Yes ☐ No	Time: ____ By: ____	☐ Reset Completed
Cloud Infrastructure / AWS / Azure	Clean Mobile / Off-site	☐ Yes ☐ No	Time: ____ By: ____	☐ Reset Completed
ERP / Accounting / Banking Portals	Clean Mobile / Off-site	☐ Yes ☐ No	Time: ____ By: ____	☐ Reset Completed
Backup Repository Root Account	Clean Mobile / Off-site	☐ Yes ☐ No	Time: ____ By: ____	☐ Reset Completed

Tomorrow-Morning Business Workaround Matrix

OPERATIONS

Operational Function	Manual / Workaround Method	Staff Lead	Hardware / Tools Used
Customer Phone Lines	Forward main numbers to external mobile phones	_____	Cellular phones
Invoicing & Orders	Paper order forms / standalone offline laptop	_____	Isolated clean device
Fulfillment / Shipping	Manual packing slips; call courier directly	_____	Physical paperwork
Payroll & Banking	In-person bank branch processing or external portal	_____	Clean off-site laptop

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

THE DO-NOT LIST

5 CRITICAL RULES DURING A SUSPECTED CYBER INCIDENT

1. DO NOT RESTART COMPUTERS

Rebooting destroys RAM evidence, unencrypts memory keys, and may trigger automated file destruction or persistence payloads. **Disconnect cable and Wi-Fi, but leave machines running.**

2. DO NOT DELETE SUSPICIOUS FILES OR EMAILS

Deleting ransomware notes, phishing emails, or unknown scripts destroys the evidence needed by forensic investigators, insurance adjusters, and law enforcement. **Leave them untouched.**

3. DO NOT WIPE OR REINSTALL SYSTEMS PREMATURELY

Formatting hard drives before forensic imaging destroys all tracking data and leaves hidden attacker persistence alive on other network hosts. **Wait for forensic authorization.**

4. DO NOT COMMUNICATE WITH ATTACKERS DIRECTLY

Never attempt to email extortionists, visit dark web chat links, or negotiate ransoms independently. Ransom payments may violate federal OFAC sanctions. **Insurer panel experts manage this.**

5. DO NOT MAKE PUBLIC STATEMENTS WITHOUT COUNSEL

Never tell customers or social media "no data was compromised" on day one. Unverified claims create massive legal liability when forensic findings emerge. **Stick to cleared holding lines.**

POST THIS NEAR SERVER RACKS, ROUTERS, AND IT WORKSPACES • CONTINUITYHUB.ORG

CONTINUITY HUB • ACTION PRINT PACK ($7)

3 Core Scenario Recognition Cards & Specific Triage Playbooks

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

Scenario 1: Ransomware & General Network Compromise

NETWORK THREAT

Recognition Signs:	Encrypted files with new unfamiliar extensions; desktop backgrounds replaced with ransom notes; files failing to open; sudden high disk activity; antivirus disabled.	
First 5 Actions (In Order):	1. **Sever Network Connections:** Unplug Ethernet cables; disable Wi-Fi; keep machines powered ON. 2. **Isolate Shared Storage:** Unmount NAS drives and network shares immediately. 3. **Pause Cloud Sync:** Stop Dropbox / OneDrive / Box sync before encrypted files overwrite cloud version history. 4. **Protect Offline Backups:** Physically disconnect offline backup drives or verify immutable cloud lock. 5. **Escalate to Insurer & IR:** Call cyber insurer hotline; engage forensic triage team.	**Specific Do-Nots:** • Do NOT power off machines. • Do NOT connect clean backup media to infected machines. • Do NOT visit extortion chat sites.

Scenario 2: Business Email Compromise (BEC) & Financial Redirection

FINANCIAL THREAT

Recognition Signs:	Vendor reports changing banking details; customers report receiving unusual invoices; unexpected login notifications from overseas; mailbox rules moving mail to RSS/Deleted folders.	
First 5 Actions (In Order):	1. **Revoke User Sessions:** In M365/Google Admin, sign out of all active web/mobile sessions. 2. **Reset Password via Clean Device:** Reset password from mobile phone; verify MFA registration. 3. **Audit Mailbox Rules:** Search for and delete hidden forwarding, redirect, or delete inbox rules. 4. **Urgent Bank Recall:** If fraudulent wire was initiated, call commercial bank fraud desk immediately. 5. **Internal Financial Freeze:** Notify finance/accounting team verbally to suspend electronic fund transfers.	**Specific Do-Nots:** • Do NOT verify wire changes via email. • Do NOT delete attacker mailbox rules without taking screenshots. • Do NOT delay bank call.

Scenario 3: Lost or Stolen Laptop, Tablet, or Smartphone

ENDPOINT THREAT

Recognition Signs:	Company device missing from employee possession, vehicle, hotel room, or conference; repeated failed biometric login alerts; unexpected geolocation alerts.	
First 5 Actions (In Order):	1. **Trigger MDM Remote Wipe:** Issue remote wipe or lock command via Intune, Jamf, or Google Endpoint. 2. **Revoke Cloud Tokens:** Terminate user's OAuth tokens, M365 session tokens, and VPN certificates. 3. **Verify Full Disk Encryption:** Check inventory records to confirm BitLocker / FileVault was active. 4. **File Police Report:** Obtain official police report number (required for insurance and proof of loss). 5. **Breach Assessment with Counsel:** Determine whether cached PII or health data requires statutory notice.	**Specific Do-Nots:** • Do NOT assume password protects unencrypted hard drive. • Do NOT delay remote wipe hoping device turns up.

CONTINUITY HUB • ACTION PRINT PACK ($7)

Recovery Checkpoints Gate Sheet: Return-to-Production Authorization

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

THE 4-GATE RECOVERY PROTOCOL

Strict Gatekeeper Requirement: Systems must NOT be reconnected to the production network or returned to service until all four recovery gates are independently verified and signed off. Reconnecting early invites secondary re-encryption.

Gate 1: Containment Confirmed

GATE 1

Check	Verification Requirement	Evidence / Test Result	Sign-Off
☐	All compromised hosts identified and isolated from network.	Total isolated endpoints: _____	Init: ____ Date: ___
☐	Attacker command-and-control (C2) domains blocked at DNS/firewall.	Firewall sinkhole verified? ☐ Yes	Init: ____ Date: ___

Gate 2: Eradication Confirmed

GATE 2

Check	Verification Requirement	Evidence / Test Result	Sign-Off
☐	Malicious binaries, persistence tasks, and backdoors removed.	Forensic scan clean? ☐ Yes	Init: ____ Date: ___
☐	Operating systems rebuilt from clean media or verified uncompromised.	Rebuild image hash verified? ☐ Yes	Init: ____ Date: ___

Gate 3: Clean Credential Reset

GATE 3

Check	Verification Requirement	Evidence / Test Result	Sign-Off
☐	All administrative, service, and user passwords reset from clean hardware.	100% directory reset confirmed? ☐ Yes	Init: ____ Date: ___
☐	Multi-Factor Authentication (MFA) re-enforced for all external access.	MFA policy applied to 100% users? ☐ Yes	Init: ____ Date: ___

Gate 4: Backups Validated & Safely Restored

GATE 4

Check	Verification Requirement	Evidence / Test Result	Sign-Off
☐	Target backup verified clean of ransomware binaries before restoration.	Backup timestamp: _____	Init: ____ Date: ___
☐	Restoration completed in isolated VLAN; system integrity verified.	Record counts & DB integrity OK? ☐ Yes	Init: ____ Date: ___

Return-to-Production Authorization Sign-Off

By signing below, the response team certifies all four gates have passed verification:

Incident Commander: _____ Date: __/__/2026 **Technical Lead / IR Firm:** _____ Date: __/__/2026 **Legal Counsel:** _____ Date: __/__/2026

CONTINUITY HUB • ACTION PRINT PACK ($7)

Communication Drafts Fill-In & Regulatory Notification Log

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

CONTROLLED COMMUNICATIONS • LEGAL DISCIPLINE

Pre-Drafted Words Prevent Self-Inflicted Wounds: Improvised communications in a breach become the story. Drafted, counsel-cleared messages protect customer trust and prevent premature statements that create liability.

1. Internal Staff Notice Template

INTERNAL ONLY

"Team: We are currently managing a technical disruption affecting our internal network systems. Our primary focus is investigation and safe stabilization alongside specialized external security partners.

Immediate Staff Instructions:
1. Do not attempt to log into internal servers or restart workstation computers until instructed.
2. If you notice any unusual prompts or emails, report them immediately to **[Incident Commander Name]**.
3. Please maintain professional confidentiality: do not discuss this issue on personal social media or with external parties.
4. For outside inquiries, use the cleared holding sentence below. We will provide our next internal briefing at **[Time]**."

2. Customer & Partner Holding Line

CUSTOMER COMMS

"Dear [Customer / Partner Name]: We are currently experiencing an unexpected technical disruption affecting some of our communication and processing systems. Our team is actively working alongside specialist technical partners to resolve this disruption securely.

Our core operations remain available via our alternative contact line at **[Phone Number]**. We appreciate your patience while we complete our verification and will share further operational updates as soon as confirmed information is available."

3. The Single Sentence for Outside Inquiries

PUBLIC DISCIPLINE

"We are actively investigating a potential 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."

Official Regulatory & Law Enforcement Reporting Record

REPORTING LOG

Agency / Channel	Date & Time Filed	Tracking / Confirmation #	Assigned Agent / Contact
FBI IC3 (ic3.gov)	___/___/2026 __:__	IC3 Ref: _____	FBI Field Office: _____
CISA Incident Report	___/___/2026 __:__	CISA Case: _____	Analyst: _____
State Attorney General	___/___/2026 __:__	Notice Filing Ref: _____	Consumer Protection Desk: ___
Local Police Department	___/___/2026 __:__	Police Incident #: _____	Officer / Badge: _____