

PRACTICAL TOOLS FOR BUSINESS OWNERS

THE FIRST 24 HOURS

A Cyber Incident Preparation & Coordination Kit

Prepare the contacts, decisions, and communication routes before a suspicious event becomes a business crisis. A calm command team beats an improvised rescue mission.

The Power to Connect and Control

Use this kit with your team. Record decisions and owners, then bring the gaps to a Free IT Risk Review.

calendly.com/jdavis-connexiom/30min

WHEN YOU SUSPECT AN INCIDENT

Pause. Report. Preserve the facts.

Use a known reporting route

Contact the designated IT/security incident lead through a known number or approved channel. If company email or messaging may be compromised, use the planned alternate route. Report what you observed even if you are unsure.

Record the first facts

Time discovered / time zone: _____

Person reporting / safe callback: _____

Affected device, account or process: _____

Observed message, behavior or action: _____

What has already been done: _____

Keep response decisions coordinated

Follow your organization's incident plan and the designated responder's instructions for containment. Do not improvise cleanup, delete evidence, negotiate with an attacker, or independently send public statements. Preserve relevant messages and logs through the approved process.

It's a trap: the helpful stranger

Verify anyone offering emergency support through a known independent route. Do not send passwords, payment, remote access, or sensitive files to an unverified caller. If you shared something, include that fact in the report.

YOUR COMMAND TEAM

Name the people before the emergency.

Primary response contacts

Incident lead / safe phone: _____
Alternate technical contact: _____
Business decision-maker: _____
Insurer / broker / policy contact: _____
Legal/privacy adviser: _____
Critical application/vendor escalation: _____

Decision ownership

Who can authorize emergency spending? _____
Who decides which operations stop or resume? _____
Who approves employee/customer communications? _____
Who coordinates insurer and adviser requirements? _____

Keep a reachable copy

Maintain these contacts in an approved location available when normal systems are unavailable. Keep the list current and access-controlled. The incident lead coordinates reporting obligations, insurance conditions, and outside assistance with qualified advisers.

THE COORDINATION LOG

Stay on target. Keep one record.

First coordination checkpoint

What is known, what remains unconfirmed, and which systems or accounts may be affected? Record the incident lead, the next update time, and actions assigned. Do not let a rumor become the incident report.

Business-priority decisions

Which operations must continue? What can pause safely? What dependencies, backups, replacement systems, staff access and vendor support are needed? Confirm recovery choices with responders; a successful restore alone does not establish that an environment is ready to resume.

Track each action

Time / action / authorized by: _____

Assigned owner / status: _____

Evidence location / access restrictions: _____

Next update time / communication owner: _____

Coordinate communications

Use approved facts and the designated spokesperson. Legal, privacy, contractual, insurance, and reporting requirements vary; have the appropriate advisers determine what applies. Employees should know where to get the next authorized update.

PRACTICE BEFORE YOU NEED IT

The Jedi Council tabletop exercise.

A realistic scenario

An employee reports an unexpected MFA prompt and a supplier reports a changed bank-details email. Can the team identify whom to call, how to communicate safely, who approves containment and spending, and what facts to record?

A useful 20-minute rehearsal

- [] Reach the incident lead without company email
- [] Find critical systems and vendor contacts
- [] Identify decision and communication owners
- [] Explain how evidence will be preserved
- [] Name the next action and update time
- [] Record gaps, owners and follow-up dates

Reference and next step

This preparation worksheet complements your current incident plan; it is not a substitute for incident-response leadership. Technical references: CISA #StopRansomware Guide, cisa.gov/stopransomware/ransomware-guide; NIST CSF 2.0 Small Business Quick-Start Guide, doi.org/10.6028/NIST.SP.1300.

Ask Connexiom to help review readiness, recovery dependencies and the gaps revealed by your exercise.