

This is the short version of a cyber incident response plan, the part you would actually use in the first hour. Fill in the blanks with your own names, numbers, and systems, then keep a copy somewhere you can reach without a login.

1. Who does what names, not job titles

INCIDENT COMMANDER

Runs the response, calls the severity

Primary name and mobile

Backup name and mobile

TECHNICAL LEAD

Isolates, preserves evidence, restores

Primary name and mobile

Backup name and mobile

COMMUNICATIONS LEAD

Sends internal, client, regulator messages

Primary name and mobile

Backup name and mobile

EXECUTIVE SPONSOR

Approves spend, insurance, counsel, police

Primary name and mobile

Backup name and mobile

2. Who we call before we need them

IT PROVIDER

Main line and after-hours number

CYBER INSURER

Claims line and policy number

ATTORNEY

Who reviews notification obligations

BANK OR PAYMENT PROCESSOR

Fraud line, if funds may be involved

FBI REPORTING

ic3.gov, plus local field office if known

OTHER

Landlord, key client, regulator, board chair

3. The first 60 minutes check the box, write who did it

- ☐ Declare an incident and note the time. Everything downstream is measured from here. _____
- ☐ Isolate what is clearly affected. Do not wipe, reimage, or "clean up" anything yet. _____
- ☐ Preserve evidence: leave logs and affected machines intact, photograph screens showing ransom notes or errors. _____
- ☐ Tell staff what is happening and how to work in the meantime. Silence invites workarounds. _____
- ☐ Call the IT provider and the cyber insurer. Insurers often require notice before you incur costs. _____
- ☐ Start the log: what was seen, when, by whom, and every decision made from here on. _____

4. Systems, in the order they matter and what breaks if we take them offline

System or service · Can it be isolated immediately? · Workaround if not

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

5. What we say fill in the blanks now, send them later

To employees

We have identified a security issue affecting _____. Until further notice, do not _____. Use _____ instead. We will update you every _____. Report anything unusual to _____.

To clients

We are addressing a security issue that has affected _____. At this time _____. We expect to _____ by _____, and we will contact you again by _____ whether or not there is news.

Holding statement, if data may be involved

We are investigating a security incident and have engaged outside experts. We do not yet know whether _____ was affected. We will notify anyone whose information was involved, within the timeframe the applicable laws require.

WHO APPROVES MESSAGES BEFORE THEY GO OUT

6. Coming back online in this order, no shortcuts

- ☐ Confirm the backup predates the intrusion. Attackers target backups first. _____
- ☐ Restore in priority order, using the list on page one. _____
- ☐ Patch the hole that was used, reset credentials, tighten access rules. _____
- ☐ Test each restored system before anyone touches it. _____
- ☐ Say the all clear, to staff and to clients, only when it is genuinely true. _____
- ☐ Watch closely for weeks. A second attempt is common. _____

7. Within a week the step that makes the next one easier

WHAT WORKED

WHAT DID NOT

WHAT CHANGES IN THIS PLAN, AND WHO OWNS THE CHANGE

PLAN LAST REVIEWED

NEXT TABLETOP EXERCISE

CONTACT LIST VERIFIED

IF THIS PAGE HAS MORE BLANKS THAN ANSWERS

That is the normal starting point, and it is fixable in an afternoon. We build these with small businesses across Greater New Orleans, pressure test them, and sit in on the first tabletop so it is not the first time anyone has thought it through.

Book a 15-minute consultation: gocourant.timezest.com/darrin/sales-call-15

Or send us a message: gocourant.com/contact-us