ITVORTEX
SIMPLIFY. PROTECT. EVOLVE.

INCIDENT RESPONSE · EMERGENCY ACTION POSTER

The First 60 Minutes.

When something's wrong, work top to bottom. Contain first, communicate on clean channels, and write nothing off the record.

STEP BY STEP

The first hour, in order

0 TO 5 MINUTES

1 Isolate.
Disconnect affected systems from the network. Do not power them off.

5 TO 15 MINUTES

2 Activate.
Call the Incident Commander and stand up the response team.

3 Preserve.
Capture logs, images, and the ransom note before touching anything.

15 TO 30 MINUTES

4 Assess.
Scope what's hit. Confirm backups are isolated and intact.

30 TO 60 MINUTES

5 Notify.
Call your cyber insurance carrier first, then law enforcement (FBI / IC3).

6 Contain.
Reset credentials, close the entry point, plan a clean recovery.

ESCALATION

Call tree: who calls whom

WHOEVER FINDS IT
First responder

▼ calls

OWNS THE TECHNICAL RESPONSE
IT Lead

▼ calls

DECISION AUTHORITY FOR THE INCIDENT
Incident Commander

▼ activates

Leadership	Legal & Comms
MSP / IR Retainer	Cyber Insurance

Golden rule: reach the Incident Commander first. Every other call flows from that one. One person owns the decisions, or six people make conflicting ones.

UNDER PRESSURE

Do this. Not that.

DO

+ Isolate immediately, keep systems powered on
+ Log every action with a timestamp
+ Call your insurance carrier before remediating
+ Communicate on out-of-band channels

DON'T

x Power off or reboot infected systems
x Pay or contact the attackers on your own
x Email about the incident from compromised systems
x Restore into a dirty environment

YOUR EMERGENCY CONTACTS

Incident Commander _____

IT Lead _____

MSP / IR Retainer _____

Cyber Insurance (policy #) _____

Legal / Comms _____

The first hour is reaction. Build the plan for the other 23. Book a readiness audit: **kb.theitvortex.com/meetings/lou-corriero**

www.theitvortex.com · (201) 225-8670 · 237 W Midland Ave, Paramus, NJ 07652 · info@theitvortex.com

ITV-IR60-2026 · v1.0
Print at 100% on Letter, landscape