Where Security Meets Innovation®

PRINT THIS. FILE IT. HOPE IT STAYS FILED.

Incident Response: The First Hour

For the manager who discovers it - no security background required. Full guide: **www.crccloud.com/blog/small-business-incident-response-guide/**

0-10 MIN - CONTAIN: disconnect affected machines from the network.
Pull cable / kill Wi-Fi. Do NOT power off - memory holds evidence; reboots can corrupt.

10-15 MIN - PROTECT BACKUPS: verify the offsite/immutable copy is intact.
Rotate backup credentials if they match any compromised account.

FROM MIN 10 - START THE TIMELINE: one person writes everything down.
What was seen, when, what was done, who was called. Notes are evidence.

15-40 MIN - CALL, IN ORDER:
1) IT/security provider emergency line 2) cyber-insurer hotline 3) legal counsel

DO NOT: mass-email staff or clients, or announce plans from possibly-compromised email.
Phone/text for the first hours. One voice, short sentences, counsel approves external messages.

40-60 MIN - FREEZE MONEY PATHS: bank on the phone, wires held.
Warn payment approvers - follow-on wire fraud loves post-incident chaos.

FILL IN NOW - BEFORE YOU NEED IT:

IT/security emergency line: _____ **Cyber-insurer hotline:** _____

Legal counsel: _____ **Leadership cell:** _____ **Bank:** _____

Keep a printed copy at leadership homes - the incident may take your file shares down with it.