CONNEX

OUT-OF-BAND INCIDENT RESPONSE · ENTERPRISE & PUBLIC SECTOR

When your war room is compromised.

Attackers often sign in with stolen credentials instead of breaking in. Once inside, they can read the same email, chat and SSO apps your team uses to respond. Your incident response needs a channel they can't see.

Veteran-owned. Veteran-operated. Built to execute.

THE DOCTRINE

Never run on one comms channel

In the military every communications plan has four layers: Primary, Alternate, Contingency, Emergency. If one is compromised, you move to the next without losing command. Most incident response plans only have a Primary.

Primary

Email, Teams, Slack, SSO apps. Likely compromised in a breach.

Alternate

A secure out-of-band command channel, separate from your network and identity.

Contingency

Plans, playbooks and contacts stored where you can reach them during an attack.

Emergency

Phone tree and in-person rally point, written into the playbook.

Connex sets up your Alternate and Contingency layers.

BEFORE YOU NEED IT

Three things to check

- ☐ **Where would your team meet if email and chat were compromised?** A personal group chat has no record, no access control and no plan.
- ☐ **Can you reach your response plan without SSO?** If it sits behind the login the attacker has, you may not be able to open it, and they may already have read it.
- ☐ **When did you last run a tabletop exercise?** A plan nobody has practised tends to fall apart in the first hour, when decisions matter most.

THE SERVICE

What's included

We design it, set it up and keep it ready. Your team gets a place to command the response that the attacker can't reach.

Secure command channel

Runs outside your network, email and SSO, so decisions happen where the attacker can't monitor them.

Response playbooks

Built ahead of time. They activate when an incident is declared and walk the team through each step.

Tabletop exercises

Realistic scenarios that expose the gaps in your plan before a real attack does.

One shared view

IT, legal and executives see progress in real time, and everyone knows their role.

Mass notifications

Critical updates reach every team at once.

Secure file storage

Crisis plans and key documents, available and current when your own systems aren't.

WHAT IT TAKES

From review to ready

1 Readiness review

We review your response plan, roles and contact lists, and find the gaps.

2 Setup

We configure the out-of-band channel, load plans and contacts, and build playbooks.

3 Tabletop exercises

We run realistic scenarios with your team, so first use isn't a real attack.

4 Keep it current

Plans, contacts and playbooks stay current as people and systems change.

WHO IT'S FOR

Organizations whose response team spans IT, legal and leadership: enterprise, public sector and municipalities, financial and professional services, and anyone whose cyber insurer or auditor is asking how they would respond to a breach. The platform is SOC 2 Type 2 certified.

13%

of Canadian businesses that reported a cyber incident in 2023 said ransomware was the method.

Source: Statistics Canada, via Canadian Centre for Cyber Security, Ransomware Threat Outlook 2025 to 2027.

Find out where your plan would break.

Book a Let's Talk I.T. call. We design it, you choose who runs it.

thinkconnex.com/lets-talk-it