# Leaders expect to contain attacks, but few can reach network gear quickly when the main network fails



An Opengear survey of 514 CIOs and CISOs finds that confidence in isolating attacks far exceeds the ability to reach critical network equipment quickly when the primary network is down.

- Opengear surveyed 514 CIOs and CISOs; only a small share could get secure management access immediately or nearly so when the primary network fails.
- In the better-prepared group, 93% were confident they could isolate compromised systems, yet only 15% could get secure access right away.
- Nearly three in four respondents delayed, scaled back or paused an AI, edge or distributed infrastructure project over resilience, remote access or recovery concerns.
- About one in six organizations do not formally test network resilience, and fewer than one in four consider it from the first planning stage.

> - Out-of-band management, a separate connection that stays up when the main network is down, is the remedy the researchers point to.

A survey by Opengear of 514 CIOs and CISOs points to a gap between confidence and capability. Most organizations cannot quickly obtain secure management access to critical network infrastructure once the primary network goes down.

## Why the gap matters

During a ransomware attack or a faulty update, engineers must log in, cut off what is compromised and restore services. If the only route to the equipment runs over the failed network, recovery waits until someone can attend in person. The July 2024 CrowdStrike outage is cited as an example, where millions of Windows machines had to be fixed largely by hand.

Access is only the first step. Teams must still triage, locate the fault and decide on a response, so delayed access delays all of that work.

## What the survey found

Respondents were split into two groups by remote recovery ability, testing frequency and reliance on onsite engineers. In the better-prepared group, 93% were confident they could isolate compromised systems while keeping access to the rest, yet only 15% could get secure management access immediately. The figures are self-reported, so the confidence number is the softer one.

Nearly three in four respondents had delayed, scaled back or paused at least one AI, edge or distributed infrastructure project in the past year over resilience, remote access or recovery concerns. Fewer than a third in either group had secure remote access and recovery in place before such systems went live. About one in six do not formally test network resilience, and fewer than one in four consider it from the first planning stage.

The researchers suggest out-of-band management, a separate connection that remains available when the main network fails.

## What to do now

1. Check whether your teams can reach core network, firewall and branch equipment if the primary network is unavailable, and record how long it would take.
2. Evaluate out-of-band management for critical and remote sites, so a separate access path exists during an incident.
3. Include a test with the primary network disabled in regular resilience and recovery exercises, and document the results.

4. Require secure remote access and recovery to be in place before any new AI, edge or branch project goes live.
5. Reflect these access dependencies in business continuity and incident response plans, and treat self-reported confidence as unverified until tested.