

SMARTER PERSPECTIVE: Cybersecurity When Cyber Readiness Becomes a Trust Advantage

By Taran Lucker

October 2026

Most companies approach cyber risk the same way they approach a regulatory audit. They document the controls, check the boxes, and earn certification through regulatory frameworks. These frameworks provide value by creating a common language, satisfying customer diligence, and demonstrating that security is being managed seriously. But they are a starting point rather than a finish line, and the gap between the two is where organizations risk exposure.

A real cyber incident does not unfold inside a policy document. It unfolds under pressure, with degraded systems, incomplete information, anxious stakeholders, and decisions that cannot wait for the next committee meeting. In that environment, containment matters, but it is not the whole challenge. The larger test is credibility, which depends on two things: whether your organization can operate through a disruption, and whether it can communicate through one. The organizations that get both right are the ones that come out the other side with trust intact.

The Preparedness Gap

Compliance frameworks provide an important foundation, but they do not fully replicate the operational realities of a cyber crisis.

An organization can have a documented



incident response plan, mature security policies, clean access reviews, and a successful audit while still struggling with more practical questions: Which systems must be restored first? Can critical services operate if technology dependencies are unavailable? Are backups actually recoverable? Who has authority to make consequential decisions before the full scope of the incident is known?

Cyber incidents rarely progress according to plan. Initial assumptions change, supposedly unaffected systems may prove compromised, and third-party dependencies can fail at the worst possible time.

Organizations that discover these dependencies and decision gaps during an incident have already waited too long.

Build Around the Business, Not Just the Controls

The most resilient organizations use security frameworks as a foundation rather than the boundary of preparedness.

That requires shifting from control-centric security toward service-centric resilience. Organizations need to understand which business services are truly critical and map the technology, data, vendors, credentials, personnel, and facilities required to sustain them.

Critical services should receive prioritized attention. Recovery objectives must be realistic, single points of failure identified, backups validated, and alternative operating procedures established before they are needed. Third-party dependencies should be incorporated

directly into recovery planning rather than treated as external variables.

Sector-specific threat intelligence is another important marker of technical preparedness. Industries face unique threats, attack methods, operational consequences, and regulatory expectations. A manufacturer preparing for ransomware-driven plant disruption faces different recovery priorities than a financial institution responding to account compromise or a professional services firm dealing with sensitive client data theft.

Effective preparedness is therefore business-specific, not simply framework-driven.

Recovery Has to Be Proven

Ultimately, technical readiness is demonstrated through testing.

Tabletop exercises should be used to confirm that critical systems can actually be restored within acceptable timeframes and in the correct sequence. They should force technical teams and executives to make decisions with incomplete information and test degraded conditions, including the loss of email, identity infrastructure, cloud services, collaboration tools, or critical third parties.

The objective is not to prove that the plan works exactly as written. It is to identify where it fails.

Testing may expose unclear recovery priorities, invalid backup assumptions,

fragmented decision authority, overlooked dependencies, or response procedures that rely on systems that may themselves be unavailable.

Preparedness Is an Operating Capability

Cybersecurity frameworks remain essential to a mature security program, but an audit or certification should not be mistaken for proof of resilience.

Real preparedness means understanding what must remain operational, knowing what those services depend on, establishing viable recovery options, and regularly testing those assumptions under realistic conditions.

When an incident occurs, containing the threat and restoring technology is critical. However, the broader objective is maintaining the organization's ability to operate through uncertainty and recover without allowing a technical event to become a prolonged business crisis.

Cyber resilience is built before an incident occurs. Organizations should regularly validate whether critical services can withstand disruption, whether recovery assumptions hold under pressure, and whether technical and business leaders are prepared to make decisions with incomplete information. The time to identify gaps in recovery, coordination, and communications is during testing and tabletop exercises, not during an active incident.



TARAN LUCKER
SENIOR DIRECTOR
GLOBAL CYBER ADVISORS
PROFESSIONAL SERVICES

Taran can be reached directly at
TLucker@hilcoglobal.com



CO-WRITTEN WITH C STREET ADVISORY
GROUP

C Street Advisory Group is a strategic advisory firm built by people who have lived the most consequential moments in business, and trusted by senior leaders when the stakes are highest.