Hilco Global
AN ORIX COMPANY

SMARTER PERSPECTIVE: CYBERSECURITY

From the Boardroom to the Breach: Why Critical System Awareness Is the Foundation of Cyber Resilience

By Bob Olsen and Alexander Niejelow

June 2026

After hundreds of conversations with the executives responsible for protecting and running some of the most complex organizations in the world, we have arrived at an uncomfortable conclusion: most of them do not know which of their systems are truly critical. Not in the way that matters. They have asset inventories and risk registers and vendor lists but they lack a clear, operationally grounded understanding of which systems, if disrupted, would stop the organization from functioning. That distinction matters enormously, because organizations that attempt to secure and plan for everything equally accomplish neither well. Resilience is not about covering every surface. It is about knowing exactly where you cannot afford to fail and building your continuity strategy from that point outward.

Prevention Is Not a Survival Plan

The cybersecurity industry has spent two decades selling organizations on the idea that a strong enough defense will hold. It will not – not always, not reliably, and not against an adversary that is patient, adaptive, and increasingly well-armed. Yet the vast majority of security budgets remain weighted toward keeping threats out, with almost nothing reserved for the moment that strategy fails. That moment will come. The organization that has not reckoned with that reality is not secure. It is simply unprepared.

Continuity Planning Has a Credibility Problem

Business continuity and disaster recovery programs exist in most organizations in the same way that gym memberships exist in most households. They are purchased, documented, and largely unused. Plans are stored in SharePoint folders last touched before the most recent reorganization. Recovery runbooks reference systems that were decommissioned two years ago. The team that would execute the plan has never run a drill that felt remotely close to an actual crisis. This is not a technology failure. It is a leadership and governance failure. Organizations often treat continuity planning as a compliance artifact rather than an operational capability, leaving it underfunded, deprioritized, and insufficiently tested. The result is a plan that might look credible on paper but collapses under any real pressure, resulting in a significant and potentially catastrophic impact on the organization.

The Adversary Already Knows Your Weak Points

Modern threat actors are not simply trying to breach an organization. They are studying how it operates, where its dependencies lie, and which systems would cause the most immediate damage if disrupted. Ransomware operators have long understood that backup infrastructure is a more valuable target than the primary environment. Disabling the recovery path before triggering the attack is not a sophisticated technique, it is a standard one. What this means is that an organization whose resilience strategy amounts to "restore from backup" is already playing from behind. The adversary has planned for that move. The organizations that recover quickly are the ones that planned further ahead by building manual fallback procedures, isolating recovery environments, and testing degraded-mode operations before they are needed.

The Questions That Paralyze Leadership

When a critical system goes down, the technical response is rarely what breaks an organization. What breaks organizations is the absence of clear answers to the questions no one thought to rehearse:

- Who has authority to invoke continuity procedures, and is that person reachable at 11 p.m. on a Friday?
- Do we understand our critical systems and how they interoperate within our organization?
- Do key vendors and partners have their own resilience posture and does the organization actually know what it is?
- Which business functions can continue operating without the affected system, and for how long?
- What are the legal, regulatory, and contractual notification obligations, and who owns them?

These questions do not require sophisticated technology to answer. They require deliberate preparation, cross-functional ownership, and the organizational will to treat the exercise as real rather than theoretical. Most organizations have none of these things in place at the moment they are needed most.

Resilience Is a Capability, Not a Purchase

This is not a problem that can be remediated with a vendor solution or insurance policy. Resilience is not a platform, a subscription, or a feature in the next contract renewal. It is an operational capability that must be deliberately built, regularly stress-tested, and owned by leaders with both the authority and accountability to act when systems fail.. That means executives who understand continuity as a material business risk and not an IT inconvenience. It means operational teams that have practiced running core business functions under degraded conditions. It means third-party relationships assessed not just for security controls, but for their own ability to sustain service when under pressure. And it means communication and decision-making frameworks that do not depend on the systems currently offline.

The Window for Getting This Right Is Narrowing

The threat environment is not static. The tools available to adversaries are advancing rapidly, enabling faster exploitation, more precise targeting, and more disruptive outcomes at lower cost and skill thresholds. The organizations still debating whether cyber resilience deserves serious investment are making an implicit wager that disruption, when it comes, will be manageable without preparation. History suggests otherwise. The organizations that have suffered the most prolonged and damaging incidents share a common thread: they had not genuinely asked themselves what survival looked like, and so they had no real answer when the question was forced on them. Resilience does not guarantee that an organization will avoid disruption. It determines whether the organization survives it.

BOB OLSEN, MBA, MS, CISSP, CCSP
MANAGING DIRECTOR
GLOBAL CYBER ADVISORS
PROFESSIONAL SERVICES

Bob can be reached directly at rolsen@hilcoglobal.com.

ALEXANDER NIEJELOW
EXECUTIVE DIRECTOR
GLOBAL CYBER ADVISORS
PROFESSIONAL SERVICES

Alexander can be reached directly at *aniejelow@hilcoglobal.com.*

Hilco Global
Asset Smarter

Find Additional Smarter Perspectives at hilcoglobal.com