

Continuity at machine speed: Why enterprises need a resilience control plane

Disruption may not always be machine-driven, but it now propagates across interconnected systems at machine speed. The result? A growing resiliency gap between intent and action that turns continuity into a board level risk.

The resiliency gap: Disruption moves faster than humans

Enterprises aren't failing because disruption is new, but because it now moves at machine speed while resilience still operates at human pace.

Disruption is no longer exceptional: it's constant and multi causal, with cyberattacks being only one source. We recently surveyed business leaders to gauge their opinion on the current state of play, with findings revealing that resilience readiness is not yet uniform. While 55%¹ say they can maintain critical operations during most disruptions, 44% still indicate gaps in resilience consistency, recovery readiness, or disruption handling.

Clearly, businesses are facing an uphill battle: contending with power outages, human-driven misconfigurations, physical events, software failures, and more, experiencing continuous operational barriers across hybrid estates. However, it's not only the frequency of disruption but the speed of its impact—and the growing lag in organizational response—that's keeping leaders up at night.

Even when the origin is human, regulatory, geopolitical, or physical, disruption to business propagates and compounds quickly. Think about the physical consequences of a natural disaster, for example. These immediately cascade into the digital realm. Governance failures, on the other hand, might not "move fast", but exposure, enforcement, and knock-on effects of this disruption do.

The increasing complexity of interconnected hybrid estates—combined with a growing cybersecurity skills gap—only amplifies disruption by slowing coordination and fragmenting control. As enterprise estates sprawl, visibility across them decreases, consistent enforcement of policies fragments, and human led coordination breaks down. **Resilience is being tested like never before, with consequences giving the C-Suite cause for concern.**

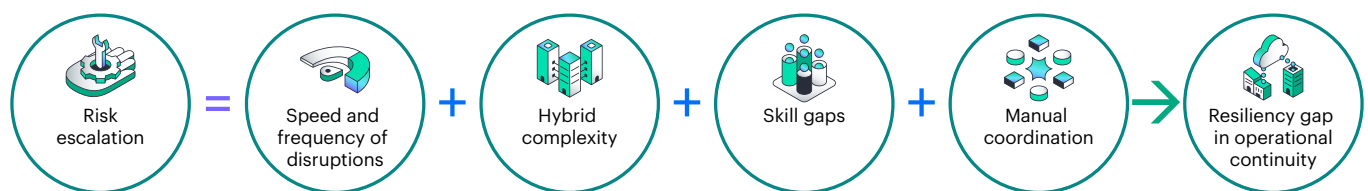


Figure 1. How resiliency gaps are created

What we're seeing is **a growing gap between human intent and machine speed action required to maintain security and continuity.** Importantly, this gap doesn't exist because organizations lack technology. It persists because there is no unifying system to coordinate intelligence, decisions, and action by that technology across operational domains in real time. **The problem is structural, not technological**—where latency is a symptom of something deeper: a lack of unified control.

This loss of control is playing out across the macroenvironment, not just in security. **Cost pressures** from unpredictable cloud spend and recent VMware® licensing shocks have pushed cloud infrastructure and operations (I&O) decisions into the boardroom. Meanwhile, **technology acceleration**—especially on the AI front—has intensified demands on hybrid estates, exposing the limits of brittle, VM-centric, tool-led operating models.

Together, cost pressures, technology acceleration, and risk escalation signal that the existing cloud I&O model no longer holds. And **the casualty is resilience.** This is what breaks first when I&O isn't designed to manage cost volatility, new technology demands, and escalating threats simultaneously. Rethinking I&O must therefore start with redefining resilience itself—because **you can't fix a problem you no longer fully understand.**

¹ HPE Business Transformers Community: The Security and Resiliency Imperative Customer Insights Survey, March 2026

The hidden risk: Coordination breakdown

Tooling can't fix what is fundamentally a coordination problem. When coordination breaks down, continuity fails, and the consequences surface at the board level.

Resilience must be broader than a security response and a set of security tools. In an era of disruption, the question is no longer: "How do we respond faster after something goes wrong?" but rather: "How do we keep critical operations running while disruption is happening?"

Framed this way, **resilience is no longer about faster recovery alone**. It is about maintaining control during disruption—which is now an always on condition, not an exception. So, if continuity is the goal, enterprises operating in siloes are at a clear disadvantage.

What do we mean by siloed? Again, it's not a technological problem, but a structural barrier. Most enterprises already have capable security tools, backup platforms, and automated monitoring systems that support four critical operational domains—data, network, workloads, and sovereignty. The problem is that these domains are often still designed, operated, and optimized as separate disciplines, rather than coordinated as a single system. And this is reflected in our survey data, with only 26%² of organizations saying they coordinate these operational domains.

As a result of siloed operations, decisions that affect the entire digital estate are slow. Coordination breaks down because response depends on humans stitching together signals, decisions, and actions across fragmented teams and tools—often under pressure, and often too late.

"Our biggest challenge is not a lack of tools; it is getting security, networking, and infrastructure teams to move as one during an incident. Better coordination would significantly improve our response."

— **Response from business decision-maker on the desired outcomes of future resilience operating models**, from HPE Business Transformers Community: The Security & Resiliency Imperative Insights Survey³

The reason isn't lack of capability. It's that human scale decision-making can't keep pace with what we've already established is machine speed disruption. This is where today's operating model fails.

Reframe resilience from recovery to continuity

- **Recovery** = Reactive, episodic, after-the-fact. Humans assess → decide → act
- **Continuity** = Proactive, policy-driven, always-on. Humans define intent → systems coordinate execution

Think about it this way: just as the brain sends intent to the nervous system so reflexes can act instantly, leaders must define security and continuity policies that resilient architecture translates into coordinated, AI-driven action at machine speed. Without that architecture, intent stalls—and coordination unravels.

^{2,3} HPE Business Transformers Community: The Security and Resiliency Imperative Customer Insights Survey, March 2026

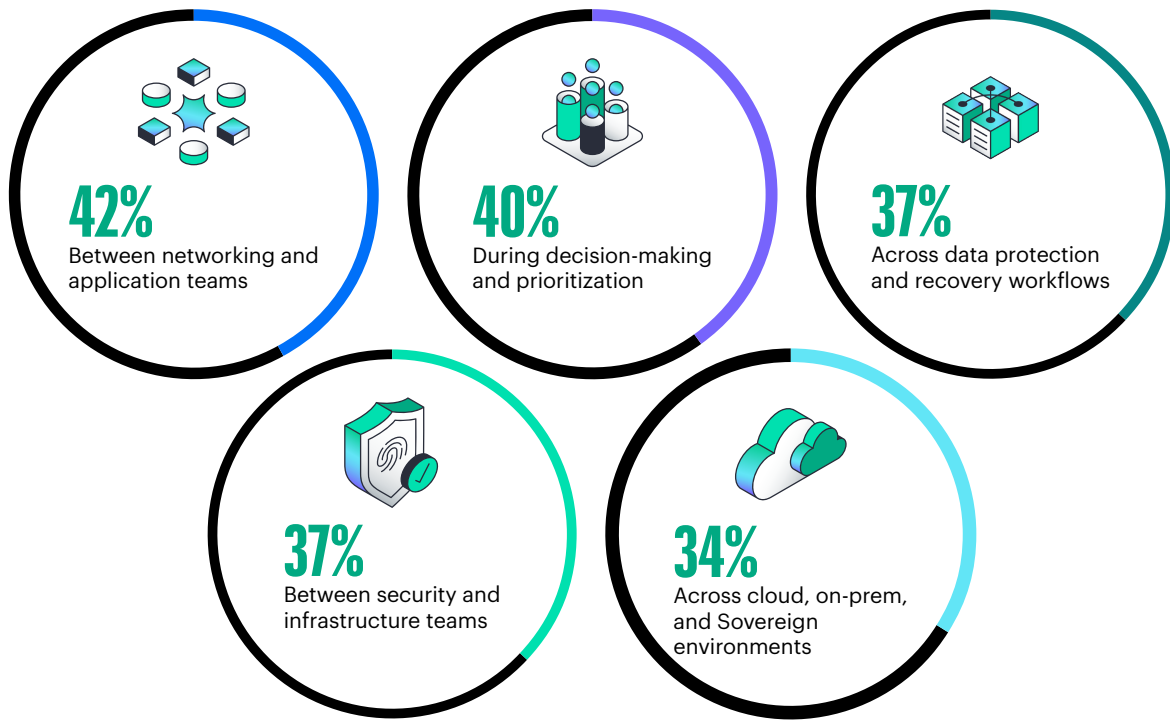


Figure 2. Biggest coordination bottlenecks

The impact of this operating-model failure isn't confined to IT downtime, and this is where board-level attention sharpens. **Continuity failures affect revenue protection, regulatory exposure, customer trust, and brand resilience.** The bottom line is clear: continuity doesn't break because tools are missing. It breaks because there is no unifying system for human-governed AI to accelerate coordinated intelligence, decisions, and action across operational domains in real time.



The board level mandate: Keep the business running

As disruption becomes the norm, continuity is no longer only an IT concern—it's a leadership responsibility that demands end-to-end control.

Across business and IT, decision-makers are wrestling with different concerns, rooted in the same coordination conundrum.

- **For the board and executive leadership**, the concern is about delivering continuity as a business mandate—they need to protect revenue, trust, regulatory standing, and brand reputation under constant disruption.
- **For I&O, security, and risk leaders**, the concern is more tactical, tied to their need to reduce operational fragility across hybrid estates while eliminating “human heroics” and proving control without a perimeter.

While concerns are expressed differently, the underlying requirement is the same: regaining control. This can only be achieved by establishing shared intent and policy that aligns SecOps, NetOps, and I&O around the same operational priorities.

“We still depend too heavily on manual handoffs and experienced individuals to keep response moving. A stronger resilience model should automate more of the coordination so we are not relying on heroics in every incident.”

— **Response from business decision-maker on the desired outcomes of future resilience operating models**, from HPE Business Transformers Community: The Security & Resiliency Imperative Insights Survey⁴

Regaining control end-to-end requires moving away from resilience as a collection of tools, toward a single system that coordinates security, networking, recovery, and governance to keep the business running. Essentially, **enterprises need to establish what we call a “continuity control plane”**.

The control plane isn't about a better dashboard or another product layer. It's about a better operating model designed to function under continuous disruption, not occasional failure.



⁴ HPE Business Transformers Community: The Security and Resiliency Imperative Customer Insights Survey, March 2026

When action is unified under a continuity control plane, the value of AI driven operations (AIOps) becomes apparent. Under this operational model, people-governed AI can coordinate intelligence, decisions, and execution across domains. This is the difference enterprises will need to reduce decision latency and enforce policy consistently crucially, at machine speed.

In practice, a continuity control plane works continuously across now-connected domains to ensure a **critical set of outcomes are met, simultaneously.**

1. Data is protected and recoverable.
2. Networks remain secure and available.
3. Workloads can be restored and moved without disruption.
4. Operations stay sovereign, compliant, and under customer control.

The resilience focus must be on resolving structural problems not addressing a perceived lack of technology. This is clear in the top 3 outcomes business leaders want from a future operating model: the ability to maintain operations during disruption, better cross domain coordination, and reduced decision latency.

Individually, each outcome above is necessary for a strong security posture. But businesses must unlock all outcomes because achieving only some isn't resilience—it leaves residual risk. **Resilience truly emerges when AI-driven operations unify the four key domains (and the individual outcomes) into a single, learning system.**



From human heroics to designed continuity

Continuity can no longer be improvised. It must be designed, supported by AIOps that delivers continuity at a pace manual intervention can't match.

Risks are escalating, costs are soaring, and technology is evolving rapidly. In this era of "disruption as the norm", continuity can no longer depend on human coordination across siloed security functions. This model of "human heroics" is neither secure nor sustainable.

The question to leaders: will you continue as you are, hoping your resilience model can keep up? Or will you embrace an architecture-first approach that embeds control, policy, and automation into cloud I&O?

The shift to a continuity control plane is both architectural and operational—and it's a journey that enterprises don't have to undertake alone.

When you're ready to make that shift, HPE is best placed to help you navigate it.

Learn more at

[HPE.com/security](https://hpe.com/security)



Visit [HPE.com](https://hpe.com)

[Chat now](#)

© Copyright 2026 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All third-party marks are property of their respective owners.

a00158260ENW

HEWLETT PACKARD ENTERPRISE

hpe.com

