Key takeaways

Resilience lessons from hybrid threats

What do you do when the cloud goes dark?

Outages used to be measured in hours. Now they can last days — and they rarely start where you expect. Power failures, cut subsea cables, cascading SaaS dependencies, and AI acting at scale are all changing what disruption looks like. Old assumptions no longer hold, and this reshapes what resilience means. In a recent Keepit webinar, a panel of experts explored the hybrid threat landscape and what organizations need to do now to survive when critical infrastructure fails. Read on for the key takeaways.

What the panel agreed on

Design resilience around what you can't control

The instinct is to build recovery plans around the systems you own and manage. The real exposure is the SaaS applications, cloud services, and third-parties outside your control. For organizations with operational technology environments — manufacturing, energy, critical infrastructure — this is essential.

The question isn't if, it's when and how fast you'll know

Whether it's a hybrid infrastructure attack, a natural disaster, or an AI agent acting at scale — something will happen. The panel was unanimous: preparedness isn't pessimism, it's reality. The organizations that fare best are the ones that know how they'll detect, communicate, and recover.

Criticality has to come from the business, not IT

IT cannot decide which systems matter most. That conversation belongs with operations, finance, production — whoever owns the processes that keep the business running. Without that alignment, recovery prioritization is guesswork, and people will be knocking on the wrong doors during an incident.

Governance frameworks are the foundation, not the ceiling

ISO 27001, NIS2, and similar frameworks are essential starting points, not finish lines. Certification answers the question of whether controls exist. Regular, realistic testing answers the question of whether they actually work. A resilience strategy that hasn't been validated is not a strategy — it's just a plan.

A practical framework for building resilience

Step 1: Know what's critical — with the business, not just IT

IT cannot define data criticality in isolation. Work with business owners to identify which systems and data must be recovered first, and in what order. Build that prioritization into your minimum recovery model before an incident forces the conversation.

Step 2: Design around dependencies you don't control

Resilience planning tends to focus on the systems organizations own. The larger risk is often the SaaS platforms, cloud services, and third-party components that fall outside direct control. Map those dependencies and build redundancy around them.

Step 3: Test, sequence, and test again

Recovery doesn't just have to work — it has to work in the middle of the night, in the right order, by people who may not have designed the process. Run tabletop exercises that include third-party and cloud dependencies and do it at least quarterly. Realistic testing surfaces gaps that documented plans don't — like whether your team can reach each other if primary communication channels go down, or whether the contact numbers they need live in the very systems that just failed. And factor in what happens to your people after a major incident: staff burnout after a prolonged recovery is a real continuity risk.

What good looks like

A resilient organization doesn't just have a plan — it has a practiced one. When something goes wrong, the difference between hours of disruption and weeks usually comes down to decisions that were made long before the incident.

- [ ] Do your recovery priorities reflect what the business needs, or what IT *assumes* it needs?
- [ ] Have you mapped the SaaS platforms and third-party services your recovery depends on, and what happens if those are the ones that fail?
- [ ] If your primary communication channels went down right now, would your team know how to reach each other?
- [ ] Could someone unfamiliar with your DR plans execute them correctly under pressure?
- [ ] Do you have access to clean, immutable backup data that no outage or attacker can reach?
- [ ] Have you had an honest conversation with leadership about how long recovery actually takes, and what it costs the people who make it happen?

If any of those answers are uncertain, that's where to start.

Is your SaaS backup strategy truly resilient?

We offer a no-obligation resilience readiness consultation — a focused conversation about your current setup, your business continuity plan, and any potential gaps. We'll assess how prepared your current approach is for recovery, compliance, and external threats and offer next-step recommendations tailored to your environment.

Book a session

keepit® Your data. Here today. Here tomorrow.

Keepit provides a next-level SaaS data protection platform purpose-built for the cloud by securing data in a vendor-independent cloud to safeguard essential business applications, boost cyber resilience, and future-proof data protection. www.keepit.com

bsi ISO/IEC 27001 Information Security Management CERTIFIED