keepit

Key takeaways

Resilience under fire

How to safeguard against hybrid attacks

Hybrid warfare, nation-state attacks, and increasing cyber risk — how resilient is your organization?

As the line between physical and digital conflict blurs, CISOs and IT leaders face mounting pressure to protect critical infrastructure from sophisticated and ever-evolving threats. In a rapidly shifting threat landscape where cybercrime, system failures, and hybrid attacks are increasing in scale, sophistication, and impact, resilience becomes paramount. As global dependencies deepen, even small disruptions can have cascading consequences.

This was the key focus of a recent Keepit webinar, where Kim Larsen, CISO at Keepit, and Ken Bonefeld Nielsen, Senior Cyber Security and Resilience Advisor at Norlys, explored how true resilience requires preparation, prioritization, and the ability to recover fast when the unexpected happens.

The threat landscape: What to consider

The threat landscape is changing rapidly

Cybercriminals are more capable than ever — now supported by powerful AI — and organizations must be prepared to deal with state actors, supply chain risks, and accidental outages. The world is deeply interconnected, meaning local disruptions trigger global consequences.

Hybrid attacks blur the line between peace and conflict

Nations and organizations are being disrupted without formal declarations of war. Hybrid attacks combine cyber, physical, economic, and information domains to create maximum impact. Resilience starts with mental resilience: understanding the threat and the scenarios to prepare for.

You can't protect everything — prioritize what matters most

Mission-critical systems and data must be identified, classified, and protected first. Trying to defend every asset equally leads to wasted resources and slow recovery, becoming a threat to business continuity.

Recovery is as important as defense

Absolute prevention is impossible. The true resilience test is how fast you can restore operations when you're under attack. Immutable backups, clear RPO/RTO objectives, and tested recovery plans are essential.

What this means for your organization

- Interdependencies across telecom, energy, infrastructure, and cloud services increase systemic risk — and no provider can guarantee 100% uptime.
- Organizations must be prepared for both accidental incidents and intentional attacks — the root cause matters less than the ability to recover.
- Exercises, scenario planning, and tabletop simulations expose vulnerabilities before a real incident does and are your best chance to train resilience.
- Backup and recovery is the final safety net — losing data has lasting consequences for your business and needs to be avoided at all costs.

"Your battlefield is your infrastructure, your critical systems, your delivery, your data. And the most important thing here is to exercise, learning about your infrastructure, learning how to recover in different scenarios."

Kim Larsen
CISO, Keepit

Resilience starts with intelligent choices

To build continuity and cyber resilience, follow these steps to make sure your organization can defend itself:

Map your critical infrastructure and know your dependencies — this includes servers, key staff, key assets, suppliers, and more.	☐
Map the risks to your infrastructure and conduct scenario planning: If this scenario happens, then how can you keep your business running?	☐
Classify data and understand where it lives — including SaaS applications outside IT's direct control. Establish a governance structure and data classification across your organization.	☐
Define priorities for data and systems so mission-critical services can be recovered first in the event of an attack.	☐
Involve business stakeholders — governance cannot be left to IT alone, but must be a coordinated effort across the business.	☐
Test recovery plans and learn from controlled failure before it's too late. Define your RPOs and exercise thoroughly to be prepared in case of emergency.	☐

Take control of your data

Read our data governance report for more insight into how to best classify, protect, and recover your data so you can ensure operational continuity.

Download now

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.

For more information visit www.keepit.com or follow Keepit on Linkedin