keepit

Key takeaways

# The anatomy of recovery: An inspection of intelligent disaster recovery

In the realm of disaster recovery (DR), the adage "failing to plan is planning to fail" holds significant weight. Intelligent DR planning is a key building block for cyber resilience and business continuity. This was a central point of discussion during a recent Keepit webinar, where Paul Robichaux, Microsoft MVP, Kim Larsen, CISO at Keepit, and Martin Husslage, Disaster Recovery Consultant at Zerto, discussed real-world scenarios of data loss and how to best prepare for them.

Most importantly, the experts stressed that merely having a plan isn't sufficient: *"Testing is critical — you need to know your plan works, not just assume it will."* (Kim Larsen) Organizations need to validate the effectiveness of DR strategies and identify potential weaknesses before a real crisis occurs. By adopting an intelligent approach to DR — emphasizing regular testing and robust redundancy measures — organizations can safeguard against disruptions and maintain business continuity.

## Take action today to improve your DR planning:

**Perform risk assessments:**
Identify business-critical systems, potential risks, and dependencies. Classify and prioritize your data and identify the systems most critical for recovery so you can establish a prioritized recovery plan.

**Implement multi-tier backups:**
Protect your critical data with immutable backups stored in separate, secure locations away from the production environment, ensuring air gapping and redundancy in your backup strategy.

**Test your recovery plans:**
Testing recovery plans regularly and documenting outcomes provide both reassurance and external proof of compliance, safeguarding operations in an increasingly scrutinized world.

Read more about a real-world recovery case from one of our customers

## Navigating cyberthreats: Preparing for the inevitable

| Common causes of data loss | |
|---|---|
| Human error | Human error, such as accidental deletion or misconfigurations, consistently ranks as the leading cause of data loss. For example, a financial institution failed to identify a bug in their data retention policies, leading to the deletion of federally mandated records. This incident highlights the critical need for organizations to implement routine audits and automated safeguards to ensure compliance. |
| External threats: | External threats such as cyberattacks, including nation-state hybrid attacks, are increasingly sophisticated, targeting both on-premises infrastructure and cloud systems. These attacks exploit vulnerabilities across interconnected systems, making it imperative for organizations to adopt robust multi-layered defenses. |

To combat these challenges, organizations must establish proactive strategies, such as implementing zero-trust architecture and comprehensive backup solutions that include immutable storage. Regular testing and employee training further strengthen defenses. Commenting on the recent CrowdStrike outage, Martin Husslage noted, “*Testing patches beforehand might seem like a hassle, but those who did were spared major disruptions.*”

## Actionable strategies for intelligent disaster recovery

**1. Follow well-adopted frameworks:** Follow the guidance from government and industry by aligning recovery plans with compliance standard and implement frameworks such as NIST 800 and ISO 27001.

**2. Implement zero trust models:** Proactively monitor systems for internal and external threats.

**3. Prioritize recovery order:** Classify systems by criticality and define a recovery order. Choose a recovery solution that allows for granular, prioritized recovery following your individual DR plan.

**4. Evaluate backup integrity:** Regularly verify that your backups are tamper-proof to ensure reliable recovery when disaster strikes.

**5. Invest in employee training:** Make cybersecurity education relatable and engaging to minimize accidental breaches. Gamified phishing simulations and real-world incident reenactments can help to train your employees.

**6. Engage the C-suite:** Show leaders that the benefit of preparedness outweighs the cost and ensure DR planning is prioritized at the C-level.

> *“Recovery isn’t just about technology. It’s about trust, planning, and real-world validation.”*
>
> Martin Husslage, Disaster Recovery Consultant at Zerto

## Disaster Recovery Guide

Check out our 7-step guide for data recovery and business continuity

Download now

keepit

When disaster strikes

A guide to data recovery and business continuity

Keepit provides next-level SaaS data protection 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