#### keapit

## Data governance meets recovery: An intelligent approach to resilience

The surge in SaaS application usage, coupled with an exponential increase in data creation, has ushered in an era where businesses are constantly at the mercy of cyberthreats and evolving data compliance regulations.

In this evolving landscape, resilient disaster recovery plans must be anchored in a modern, intelligent approach to data governance.

This was a central point of discussion during a recent Keepit webinar, where Kim Larsen, CISO at Keepit, and Ulf Feger, vCISO and CISO Advisory Services, emphasized that data governance is no longer a backoffice task — it's a strategic, business-critical capability.



#### **Building blocks for intelligent resilience**

Most organizations unknowingly house their own Trojan horse — created by internal blind spots in data classification, ownership, and SaaS applications usage. Marketing, HR, and research teams often operate applications beyond the CISO's visibility, increasing exposure. Real resilience requires that business units — not just IT — own their data risks. CISOs must partner with functional leaders to ensure that data is handled, stored, and protected in accordance with its business value and risk level. Resilience is built on the following fundamental building blocks:



Data classification Prioritization as the cornerstone of future proofing



Data governance Structure as the basis for informed decision making



**Disaster recovery** Preparedness as the anchor of uninterrupted operations

"We need to make sure every data owner understands the data governance model, what data they put into the application, how it's governed and how they recover from something that happens to the application"

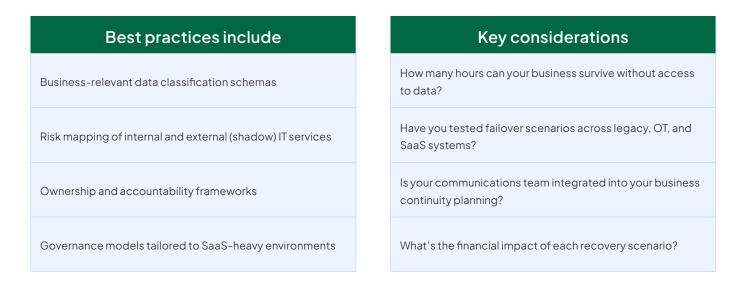
Kim Larsen, CISO at Keepit

# Governance as a pillar of cyber resilience

The NIST Cybersecurity Framework now recognizes 'Govern' as its sixth core function, sitting beneath Identify, Protect, Detect, Respond, and Recover. Modern data resilience hinges on understanding what data exists, where it lives, and how critical it is to operations.

#### Recovery in practice: Planning for the unknown

Disaster recovery is not about returning to normal — it's about handling disruption and ensuring continuity. Whether facing ransomware, data corruption, or critical vendor outages, organizations must weigh recovery speed against data completeness.



### 5 key takeaways to consider

- 1. Cyber resilience starts with intelligent data governance.
- 2. Risk ownership must be distributed across the enterprise.
- 3. Frameworks like NIST 800 and ISO27k provide a blueprint for maturity.
- 4. Recovery planning must balance speed, completeness, and cost.
- 5. CISOs must become strategic advisors, not just technical gatekeepers.

#### Data governance report

Read our data governance report for more insight into why taking control of your data is key for operational continuity

#### **Download now**

Intelligent data governance



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

For more information visit <u>www.keepit.com</u> or follow Keepit on <u>Linkedin</u>