SPOTLIGHT
Sponsored by: Object First

**Robust backup and recovery systems are critical to cyber-resilience, as they provide recovery when all else fails.**

# The Danger of Deferring Backup and Recovery Investments

*June 2026*

**Written by:** Johnny Yu, Research Manager, Infrastructure Software Platforms

## Introduction

In an era defined by increasingly frequent and sophisticated cyberthreats, backup and recovery remains the true last line of defense when security architecture gets breached. Yet, when faced with economic pressure from external forces alongside budget getting re-allocated toward AI investments, organizations may make the mistake of scaling back their backup and recovery investment, weakening their cyber-resilience posture.

### AT A GLANCE

#### KEY TAKEAWAYS

- Backup and recovery is the last line of defense. When all else fails, it restores operations.
- Budget pressure must not deprioritize backup, as the cost of ransomware far exceeds the cost of investing in resilient infrastructure.
- Robust backup and recovery supports the pillars of cyber-resilience: guaranteed data survival, data integrity, and rapid recovery.

Cyber-resilience is often understood as a layered strategy consisting of security components such as access controls, threat monitoring, and intrusion/anomaly detection, but all these components are focused on preventing an attack. Backup and recovery is often seen as an insurance policy or a compliance checkbox, but in practice it is foundational to cyber-resilience. Backup and recovery focuses on ensuring data and business survivability, which is no less important. When all else fails, a robust backup and recovery system allows organizations to endure an attack and return to normal operations with minimal disruption.

It is therefore a strategic error for organizations to treat backup and recovery any differently from the rest of the cyber-resilience arsenal. Cybercriminals recognize the importance of backup and recovery systems and often target them during their attacks. It would be a mistake for this final, critical line of defense to be under-funded.

### Budget Woes

Organizations across industries are facing a challenging macroeconomic environment. Geopolitical conflicts, persistent supply chain disruptions, and inflationary pressures have forced IT leaders to scrutinize every line of their budgets. In this environment, the temptation to defer or reduce investment in infrastructure components perceived as "insurance" rather than active business enablers is significant.

Backup and recovery is particularly vulnerable to this temptation. It operates in the background and only becomes visible during a crisis, unlike security controls that generate continuous alerts and observable activity. Organizations may therefore rationalize increased investment in prevention-oriented security tools at the expense of backup infrastructure, arguing that conditions and costs may improve if they wait.

However, waiting for macroeconomic conditions to "return to normal" before addressing backup gaps is not a viable strategy. Historically, global conflicts and material shortages that increase the cost of procuring IT infrastructure do not cause an anomalous spike that simply settles back down over time. Instead, the higher cost becomes the new normal, and organizations must adjust their budget planning accordingly.

Meanwhile, threat actors are not waiting. The appropriate response is therefore to build a cyber-resilience posture that can sustain operations through economic cycles as well as through evolving threat landscapes. Notably, cyber-resilience as a category has demonstrated relative resistance to budget cutbacks even in downturns: an IDC survey found 33.5% of organizations expect to see the most significant increase in spending on cyber-resilience in 2026.

Additionally, the costs of suffering a ransomware attack often add up to more than the cost of maintaining or deepening investments in backup and recovery. The financial impact isn't limited to the cost of the ransom itself. Operational downtime from an attack translates to lost business opportunities, reputational damage, productivity loss, and many other consequences.

### *A Solid Foundation*

Rather than scale back or postpone their backup and recovery investments and jeopardize their cyber-resilience foundation, organizations should ensure their backup and recovery systems are robust enough to guarantee the survival, integrity, and rapid recovery of critical data. Such a system should possess several attributes:

- Granular recovery point objectives (RPOs) that match the data timeliness and operational requirements of each workload
- Guaranteed clean copies of backup data residing in immutable storage with zero trust-enforced access controls
- Multi-factor and multi-person authentication for high-risk tasks to prevent unauthorized deletion or modification of backup data
- A combination of recovery orchestration and performant hardware to ensure recovery time objectives (RTOs) are met
- Recovery playbooks and methods of testing recovery plans against RTOs to ensure objectives are met
- Software and hardware combinations that allow for multiple tiers of recovery to optimize resources

## *Benefits*

A well-architected backup and recovery strategy delivers measurable benefits that extend across operational, financial, and regulatory dimensions.

### *Immutability for Absolute Data Survival and Integrity*

Immutability is important because it guarantees two critical properties: data survival (the backup copy exists and can be used to recover operations) and data integrity (the backup copy has not been tampered with). Even if a threat actor successfully compromises primary systems and injects corrupted data that propagates into backup, an immutable architecture preserves prior clean recovery points. Organizations can recover to a known good state with confidence.

It is important to note that not all immutability is created equal. Hardware-enforced immutability, where the storage device itself physically prevents or simply cannot accept changes to data, ensures that backup data cannot be altered, encrypted, or deleted, even by privileged administrative accounts. This is different from software-based immutability, which can potentially be circumvented by disabling or reconfiguring the immutability at the software layer. Software immutability can be defeated at the OS or firmware layer via root access or factory reset, or even be disabled by changing the system clock.

### *Accelerated Recovery and Reduced Downtime*

The financial value of reduced downtime is substantial. Beyond direct revenue loss, organizations facing prolonged outages experience compounding impacts: lost customer opportunities, reputational damage, regulatory scrutiny, lowered employee morale, and productivity loss. Each hour of recovery time avoided represents meaningful cost avoidance.

Additionally, with a backup and recovery system and a clear response plan that has been tested to meet RTO requirements, organizations do not have to consider if paying a ransom might result in a faster recovery.

### *Insurance and Compliance Alignment*

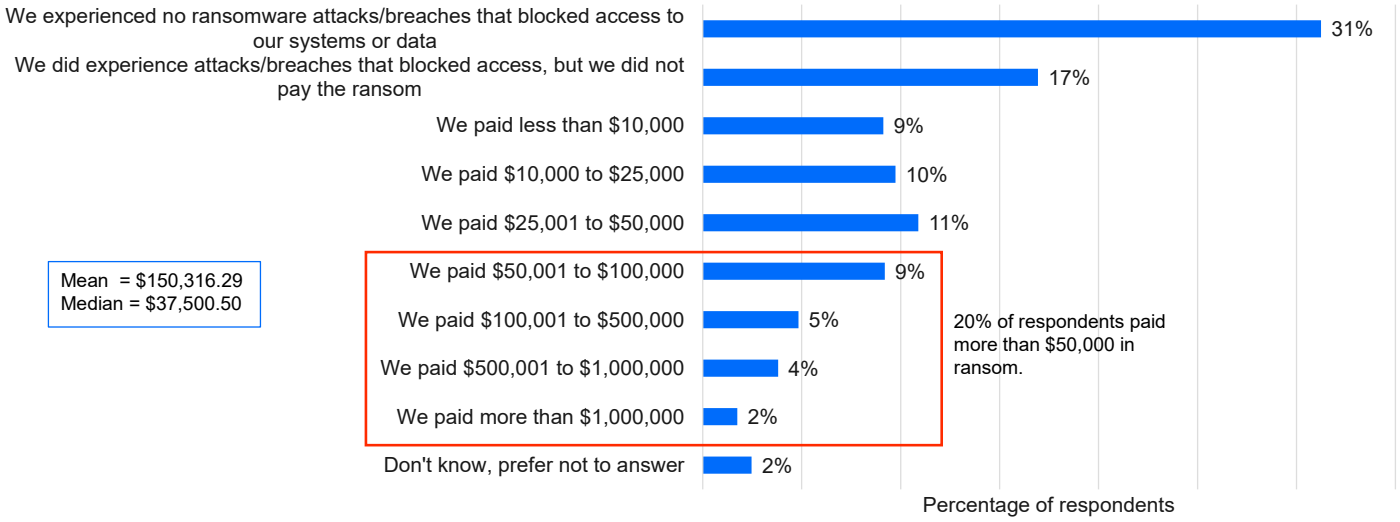
Cyber insurance underwriters increasingly scrutinize backup and recovery maturity as part of policy underwriting and renewal. Organizations that can demonstrate immutable backup storage, documented recovery procedures, and tested RTOs are likely to secure more favorable policy terms or lower premiums.

Additionally, regulatory compliance obligations in sectors including financial services, healthcare, and critical state infrastructure impose data retention and recovery requirements. A cyber-resilient backup and recovery architecture supports ongoing compliance and reduces the risk of regulatory penalties following an incident.

## Trends

Figure 1. **Average ransomware payments in the past 12 months**

**Q** ***If your organization paid a ransom in the past 12 months to regain access to systems or data, how much was paid? If multiple ransoms were paid, please include the TOTAL amount.***




Base = all respondents (n = 885)

Notes: Managed by IDC's Global Primary Research Group.; Data Weighted by IT Spending by country; Use caution when interpreting small sample sizes.

Source: IDC's *Future Enterprise Resiliency & Spending Survey Wave 5*, June 2025

Ransomware remains a major threat for organizations of all sizes across all sectors. The IDC data in Figure 1 shows the cost of the ransom demanded by the attacks, but it understates the total incident cost. The full cost of a ransomware incident includes quantifiable elements beyond the ransom itself, such as operational downtime and associated revenue loss, IT recovery labor and any third-party recovery services costs, data reconstruction where recovery is incomplete, mandatory customer notification and regulatory reporting, and reputational damage.

Notably, there are less easily quantified but equally significant consequences to paying ransoms. Organizations that pay are more likely to be attacked again, ransom payments fund the criminal infrastructure that enables future attacks, and payment may trigger legal and regulatory penalties, particularly where sanctioned threat actors are involved. Payment also does not guarantee complete data recovery. Combined, these costs amount to far more than investing in bolstering backup and recovery systems.

## Vendor Profile

Object First is a data resilience company focused on delivering purpose-built, ransomware-proof backup data storage for Veeam software. Founded in 2023 and headquartered in Denver, Colorado, Object First was established with the specific mission of providing backup storage that is secure by design, easy to deploy, and tightly integrated with the Veeam ecosystem. The company's flagship product, Ootbi, is an on-premises backup storage appliance engineered from the ground up to address the specific demands of cyber-resilient backup and recovery.

Veeam acquired Object First in January 2026.

Ootbi's core differentiator from other purpose-built backup appliances (PBBAs) is its hardware-enforced immutability. The distinction from and advantages over software-level immutability was detailed above, and Object First refers to this capability as "Absolute Immutability." Backup data written to Ootbi cannot be modified, encrypted, or deleted for the duration of the configured retention period. This architecture has been validated through third-party penetration testing.

Ootbi is designed and optimized exclusively for use with Veeam Backup & Replication, a market-leading enterprise backup software platform. This tight integration eliminates the compatibility uncertainties that arise when combining general-purpose storage with backup software from a different vendor. Ootbi is recognized by Veeam as a recommended repository, providing Veeam customers with a validated backup software-to-storage hardware integration with no additional tuning or compatibility testing necessary.

Object First offers Ootbi through both traditional capital expenditure models and a consumption-based, pay-per-use subscription model. The subscription option lowers the barrier to entry for organizations operating under constrained capital budgets, which is particularly relevant in the current macroeconomic environment. Organizations can deploy Ootbi and access its cyber-resilience capabilities without a large upfront investment, scaling capacity and cost as needs evolve.

Ootbi is designed for operational simplicity. Deployment from unboxing to first backup is intended to take approximately 15 minutes, with no specialized storage expertise required. The appliance is managed and updated automatically by Object First, removing the administrative overhead of maintaining storage firmware and software. This addresses a cyber-resilience weak point, as out-of-date systems introduce security vulnerabilities, and patching is a task that is often postponed in resource-constrained IT organizations.

## Challenges

IDC notes the following considerations for Ootbi and Object First as part of the backup and recovery architecture. Firstly, as a PBBA, Ootbi is only used for backup storage and cannot be repurposed for general storage. In environments where budget pressure encourages infrastructure consolidation, committing dedicated appliance capacity exclusively to backup may face resistance.

However, although PBBAs are commonly seen as storage optimization investments, this is not the primary benefit or focus of Ootbi. Organizations should instead consider Ootbi as a component of the broader cyber-resilience strategy and an investment against the quantifiable cost of ransomware incidents rather than evaluating it purely as a storage infrastructure line item. Object First has a messaging opportunity to clarify this difference and strengthen Ootbi's position as a cyber-resilience investment.

Ootbi is designed exclusively for Veeam Data Platform environments. Organizations that have standardized on alternative backup software platforms or use multiple backup tools from different vendors would need to acquire and deploy Veeam licenses to leverage Ootbi. This constraint limits Object First's addressable market to Veeam customers only and may present a hurdle for organizations undergoing backup platform consolidation.

Undoubtedly, organizations that have a sizeable investment in Veeam stand to benefit from Ootbi, but the completeness of the cyber-resilience offering of Object First alongside Veeam could encourage some organizations using multiple data protection tools to consolidate and deepen their investments in Veeam. Tool consolidation continues to be a common IT infrastructure goal, especially as economic pressure drives organizations to scrutinize their spending.

## *Conclusion*

The cyberthreat landscape has fundamentally changed the calculus of IT investment. Ransomware and other destructive cyberattacks are a near-certain operational risk that organizations must plan to survive rather than merely prevent. In this environment, backup and recovery is not a secondary consideration, but the last, most critical, line of defense.

IDC believes organizations that build their cyber-resilience strategies with robust backup and recovery at the foundation will be materially better positioned to withstand attacks, avoid ransom payments, and meet their recovery SLAs. Budget pressures are real, but the cost of underinvesting in backup infrastructure is demonstrably higher than the cost of maintaining it. Organizations that defer backup modernization in hopes of better economic conditions in the near future are essentially accepting a higher probability of an unrecoverable incident.

# About the Analyst

***Johnny Yu,*** *Research Manager, Infrastructure Software Platforms*

Johnny Yu is Research Manager within IDC's enterprise infrastructure global research domain and part of the core infrastructure subdomain. Johnny focuses on data logistics, protection and management vendors. His core research includes data protection, cyber resilience, archiving software, and container data management. Johnny's research also spans storage and data security, the impact of AI on cyber resilience and ransomware defense, and cost optimization as companies balance competing IT priorities.

## MESSAGE FROM THE SPONSOR

As this IDC Spotlight illustrates, ransomware is a near-certain operational risk, and backup and recovery is the last line of defense when prevention fails. Object First's on-premises backup storage with absolute immutability is the ultimate ransomware defense. Secure, simple, and powerful, we enable Veeam customers to be simply resilient against the risk of cyberthreats. To learn more, visit www.objectfirst.com.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

**IDC Research, Inc.**
One Beacon Street
Suite 33100
Boston, MA 02108, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com