

Data resilience — not to be conflated with IT resilience, digital resilience, or business resilience — helps organizations reduce the risk of data loss and provides the data availability that leads directly to better business outcomes.

Understanding the Data Resilience Challenge

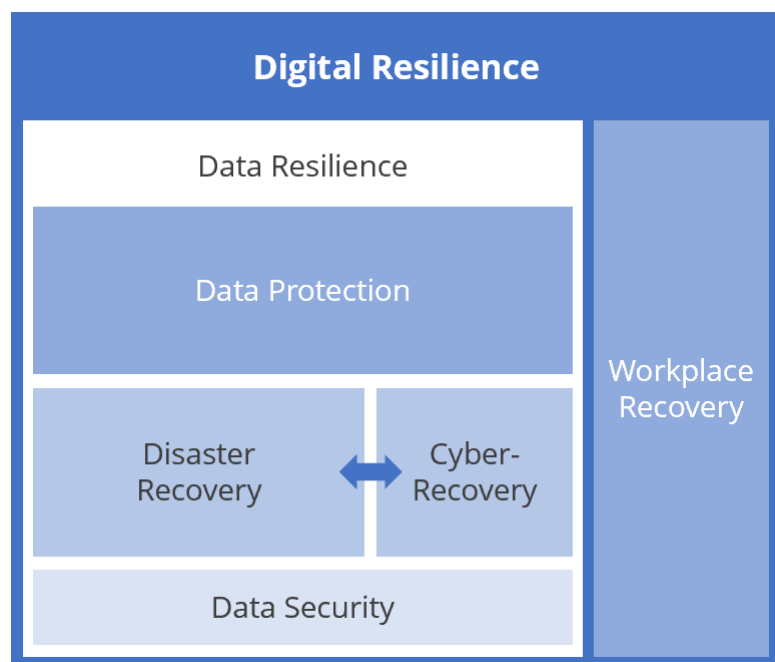
April 2022

Written by: Phil Goodwin, Research Vice President, Infrastructure Systems, Platforms, and Technologies Group

Introduction

Data resilience must be understood in the context of *digital* resilience. IDC defines digital resilience as the highest-level term referring to the comprehensive nature of a business' ability to conduct operations, including people, processes, and technology. As such, data resilience is part of digital resilience. With data being the lifeblood of organizations, data resilience is foundational to, and an essential component of, digital resilience. Figure 1 illustrates the digital resilience environment and how data resilience fits into it.

FIGURE 1: ***Data Resilience as Part of Digital Resilience***



Source: IDC, 2022

AT A GLANCE

WHAT'S IMPORTANT

Data resilience is foundational to business resilience and digital transformation. Organizations that exceed their peers in data resilience are also likely to exceed them in business outcomes.

KEY TAKEAWAYS

With data spread across core, cloud, and edge, organizations face added risk of data loss and unavailability. IT leaders need solutions that provide data resilience consistency as well as rapid, certain recovery from ransomware.

As Figure 1 illustrates, data resilience incorporates disaster recovery and cyber-recovery as supported by data protection and data security. Increasingly, data security is being tied to data resilience due to the growing risk and severity of malware, especially ransomware.

Given that data resilience is foundational to digital resilience and an organization's ability to conduct business, it is essential to any digital transformation initiative and the effective data leverage. Data resilience delivers reliable access to accurate data, regardless of security attacks, disasters, and human error.

In terms of threats to data resilience, ransomware is top of mind for both IT and businesspeople alike. IDC research shows that 90% of organizations have been attacked by malware and that 87% of those have been attacked successfully. In a survey conducted in December 2021, fewer than one-third of organizations that were victims of ransomware were able to fully recover their data without paying the ransom. Because of these grim statistics, organizations are seeking solutions that can provide assured data survival with certain, rapid recovery in the event of an attack.

Benefits

If data resilience is foundational to digital resilience, then data protection and recovery is foundational to data resilience. It stands to reason that organizations that can recover faster from any given data outage and with less data loss will be positioned to better utilize that data. IDC research shows that one-third of organizations have suffered a cyberattack that prevented access to data or systems within the past 12 months (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 11*, December 2021). Thus data resilience is directly linked to competitive positioning in the marketplace.

A major challenge to data resilience is data silos. In fact, most organizations deal with more than 10 different silos. Having so many silos increases the risk of data loss due to increased intrusion opportunities and disparate or inconsistent data protection policies.

These silos often require separate data protection products, leading to redundant purchases, inefficient operations, and excessive maintenance.

Consolidating data protection tools and operations across the enterprise can solve the problem of inconsistent data protection due to silos and thereby can improve data resilience, reduce the risk of data loss, and improve recovery times regardless of the reason for the outage. Consolidated data protection also enables more efficient data management operations and better use of human resources.

Considerations

Improved data resilience begins with establishing key performance indicators (KPIs), followed by measuring and monitoring them on an ongoing basis. Specific KPIs include total application uptime, recovery time objective (RTO), and recovery point objective (RPO). RTO and RPO are particularly important because lower RTO offers greater data availability, while lower RPO indicates less data loss. Other measures include backup/recovery job success and failure. In fact, our research shows that restore job failure is the number 1 cause of data loss indicating the need to prioritize implementing reliable backup tools and operations.

If data resilience is foundational to digital resilience, then data protection and recovery is foundational to data resilience.

The cloud has come to play a very important role in data protection and resilience. IDC predicts that by 2025, 55% of organizations will have migrated their data protection systems to a cloud-centric model to centrally manage core, edge, and cloud data protection from the cloud. This shift from on-premises data protection to cloud data protection is driven by faster data growth in the cloud as well as the flexibility and consumption-based subscriptions that have become the preferred engagement model for many organizations. Common cloud data protection–related services include backup as a service (BaaS), disaster recovery as a service (DRaaS), and archive as a service (AaaS). Using the cloud for backup and disaster recovery can enhance data resilience as an offsite repository to help ensure data survival and facilitate recovery in the cloud against any onsite disruptions. Backup sets in the cloud can also be repurposed for analytics and test/dev or staging.

Trends

Digital transformation (DX) projects continue to be among the most important organizational initiatives. DX projects are designed to make organizations data driven and, in 70% of cases, cloud-first. About half of DX projects involve improvements to data resilience, which accounts for 30% of the project budget. To improve data resilience, most organizations will begin with enhancements to data protection and especially cyber-recovery. This will include modernizing systems and solutions with the emphasis on fast, certain recovery with minimal data loss.

Conclusion

To fully achieve digital resilience, organizations must first ensure data resilience. Data resilience begins with sound backup and recovery for any eventuality, whether simple human error or sophisticated malware/ransomware. Success demands assured data integrity, data survival, and rapid recovery with minimal data loss. Those organizations able to achieve superior data resilience compared with their peers can expect competitive advantage in a marketplace where data leverage is critical.

About the Analyst



Phil Goodwin, Research Vice President, Infrastructure Systems, Platforms, and Technologies Group

Phil Goodwin is a Research Vice President within IDC's Infrastructure Systems, Platforms, and Technologies Group, with responsibility for IDC's infrastructure software research area. Mr. Goodwin provides detailed insight and analysis on evolving infrastructure software trends, vendor performance, and the impact of new technology adoption. His focus is on multicloud data management, data logistics, on-premises and cloud-based data protection as a service, cyber protection and recovery, recovery orchestration, and more.

MESSAGE FROM THE SPONSOR

About Druva

Druva enables cyber, data and operational resilience for every organization with the Data Resiliency Cloud, the industry's first and only at scale SaaS solution. Customers can radically simplify data protection, streamline data governance, and gain data visibility and insights as they accelerate cloud adoption. Druva pioneered a SaaS-based approach to eliminate complex infrastructure and related management costs, and deliver data resilience via a single platform spanning multiple geographies and clouds.



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

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2022 IDC. Reproduction without written permission is completely forbidden.

IDC Research, Inc.

140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com