White Paper

The State of IT Resilience

Sponsored by: Zerto

Phil Goodwin Andrew Smith
August 2018

IDC OPINION

Many organizations view disaster recovery (DR) preparedness as an insurance policy and, therefore, an expense that is likely to have little payback. This approach to disaster recovery is inadequate for today's digital businesses. If DR tools and initiatives are viewed as a cost center objective and not as a business driver, an organization's cloud and digital transformation initiatives will be exposed to a higher rate of failure. In addition, digital businesses rely on data to operate and differentiate from the competition. Data must be efficiently collected, retained, and analyzed to reach the business' peak potential. Therefore, digital businesses must be prepared to manage and mitigate any event where there is potential for data to be corrupted or lost. Examples include but are not limited to malware attacks, ransomware attacks, and failures due to application or datacenter migrations and modernization. For these reasons, we believe it is necessary for information technology (IT) and business decision makers to advance their understanding of disaster recovery beyond natural disasters, extending to unplanned and planned disruptions as well.

The three key tenets of what we term *IT resilience* are the ability to protect data during planned disruptive events, effectively react to unplanned events, and accelerate data-oriented business initiatives. From a technology standpoint, IT resilience includes traditional disaster recovery and backup tools and also incorporates advanced analytics and security capabilities necessary for the success of any digital business in the 21st century. To better understand IT resilience, IDC conducted a worldwide survey of business and IT decision makers, sponsored by Zerto, that was designed to develop a more concrete understanding of the variables that determine IT resilience. The survey explored current disaster recovery preparedness, future needs, and perceptions of business disruption, digital transformation, and IT resilience. Detailed results can be found in the sections that follow. The following is a list of some of the key findings, including IDC's opinion on the overall results of the survey:

- More than half of the respondents are currently undertaking IT transformation or digital transformation projects and view IT resilience as foundational to the success of their effort. However, few respondents believe their IT resilience strategy is optimized.
- Most organizations surveyed have experienced tech-related business disruptions, which resulted in material impact in terms of either cost (to recover or for additional man-hours), direct loss of revenue, permanent loss of data, or damage to company reputation. Even more concerning is that many organizations are seeing new forms of disruptions, such as ransomware, cause considerable downtime.
- Many organizations use employee productivity, profit, and customer satisfaction as key performance measures to gauge the success of the business. These types of KPIs will be negatively impacted by tech-related business disruptions, as described in the previous bullet. This suggests an important correlation between the success of business KPIs and IT resilience–oriented initiatives.

In summary, given the close relationship between the success of business KPIs and the prevention of tech-related business disruptions, we believe it is in the best interest of today's IT and business decision makers to define what IT resilience means for their organization and develop a plan for implementation. Certainly there is no one-size-fits-all IT resilience solution — every organization will have unique needs based on its data and industry requirements, among others. But based on the survey results, we believe that organizations with highly mature IT resilience strategies will be in a better position to support the success of IT and digital transformation initiatives.

METHODOLOGY

The results presented in this study derive from an independent survey commissioned by Zerto and conducted by IDC. Zerto commissioned IDC to conduct the study in order to ensure the independence and validity of the results. IDC received responses from 500 senior-level IT and business managers. Respondents who indicated they are very familiar with or directly involved in their business' data protection (DP), disaster recovery, business continuity, and cloud computing strategies were selected to complete this survey.

The 500 respondents represented over 10 unique industries, with the top 3 industries being information technology, financial services, and manufacturing. Of the respondents, 60% were based in North America, 20% in Europe, and 20% in Asia. Regarding company size, 59.4% of respondents represented organizations with 1,000–4,999 employees, 27.4% represented organizations with 5,000–9,999 employees, and 13.2% represented organizations with 10,000+ employees. Readers should note that IDC does not endorse companies or products, and nothing in this study should be construed as such. The opinions and conclusions in this study are IDC's.

DEFINITIONS/TERMINOLOGY

- **IT resilience:** IT resilience refers to an organization's ability to protect data in the event of any unplanned or planned disruption and, simultaneously, support data-oriented initiatives for business modernization and digital transformation.
- **Digital transformation:** Digital transformation describes the process of transforming decision making with technology. Digital transformation is an enterprisewide, board-level strategic reality for companies that are serious about ensuring their businesses deliver an exceptional customer experience and becoming leaders in the digital economy. Digital transformation is a multiyear effort, with specific goals and objectives around markets and customers, revenue, and profit growth.
- **Data protection:** Data protection refers to the protection, restoration, and recovery of data in the event of physical or logical errors. This includes products and services that support both physical and virtual infrastructures.
- **Disaster recovery:** Disaster recovery is a combination of solutions that provide replication of physical or virtual servers and failover workload recovery in the event of a hardware failure or man-made or natural catastrophe. Disaster recovery solutions typically provide replication of data and applications with assigned recovery point objectives, where data and applications will have a set "age" where recovery from backup storage for normal operations can occur if a server, system, or network suffers a failure. Solutions also have a recovery time objective, which is the time frame in which the enterprise will regain normalized access to the data and applications being supported.

- **Hybrid cloud:** Hybrid cloud is an application deployment environment that utilizes both on-premises private cloud resources (i.e., local datacenter) and off-premises public or managed cloud resources to deliver the totality of the application functionality.
- **Multicloud:** Multicloud is an infrastructure deployment environment that utilizes two or more off-premises public or managed cloud resources for complete or partial application delivery.

IN THIS WHITE PAPER

This white paper introduces readers to IT resilience and its importance in the context of operational continuity and data management and its relation to cloud adoption and digital transformation. The white paper uses findings from the survey to illustrate some of the key tenets of IT resilience and the challenges and opportunities organizations face when trying to achieve resilience. By the conclusion of the white paper, readers will have a firm understanding of IT resilience and its benefits on both business and IT operations and how those benefits stack up for survey respondents. Finally, we identify essential first steps to consider on the road map to IT resilience and highlight key challenges and opportunities.

SITUATION OVERVIEW

IDC estimates that as many as 50% of organizations could not survive a disaster event. Many organizations do not have properly protected and staged offsite data, have not tested the DR environment, or do not have automated DR processes as part of documentation and planning. The reasons for this are complex, but principal among them are typically cost, time, and training. IDC's *Worldwide Business Resilience Readiness Thought Leadership Survey* uncovered several statistics illustrating the business impacts of disasters and data loss and how organizations are currently prepared to respond:

- **93% of respondents have experienced tech-related business disruption in the past two years.** The fact remains that data disruption happens, and the negative impacts can be significant. Of those respondents who experienced a tech-related disruption, 17% categorized the disruption as "severe" — the highest choice on a scale of "no impact" to "severe." The impact of these disruptions varied, with employee overtime and loss of employee productivity being the two most common consequences (see detailed list in Figure 1). Even worse, 20% of respondents experienced major reputational damage and permanent loss of customers as a result of business disruptions.

FIGURE 1

Consequences of Tech-Related Business Disruptions Vary in Severity

n = 465

Base = respondents who indicated their organization experienced technology-related business disruptions

Notes:

This survey is managed by IDC's Quantitative Research Group.

Multiple responses were allowed.

Data is not weighted.

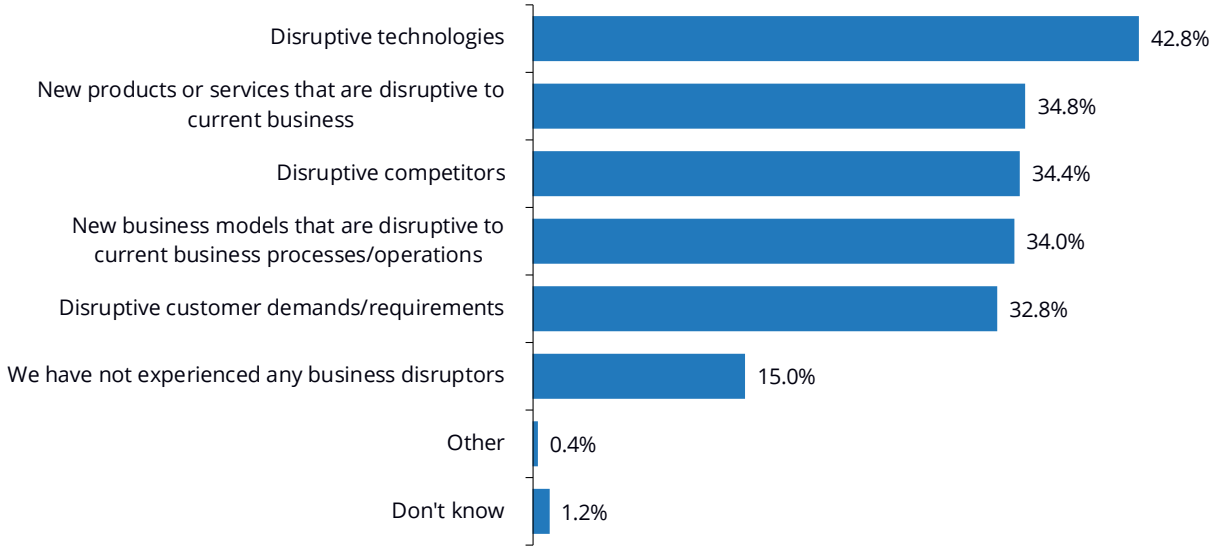
Use caution when interpreting small sample sizes.

Source: IDC's *Worldwide Business Resilience Readiness Thought Leadership Survey,* May 2018

- **83.8% of respondents have experienced some type of business disruption in the past two years.** Further complicating matters, businesses face a range of disruptive factors beyond just disasters. Many disruptions are because of new technologies, new products or services, disruptive competitors, or new business models. Certainly many of these types of disruptive events/technologies will be related to digital transformation initiatives as enterprises look to outpace their competition or avoid falling behind (see Figure 2).

FIGURE 2

Business Disruptions Occur Because of a Variety of Reasons



n = 500

Base = all respondents

Notes:

This survey is managed by IDC's Quantitative Research Group.

Multiple responses were allowed.

Data is not weighted.

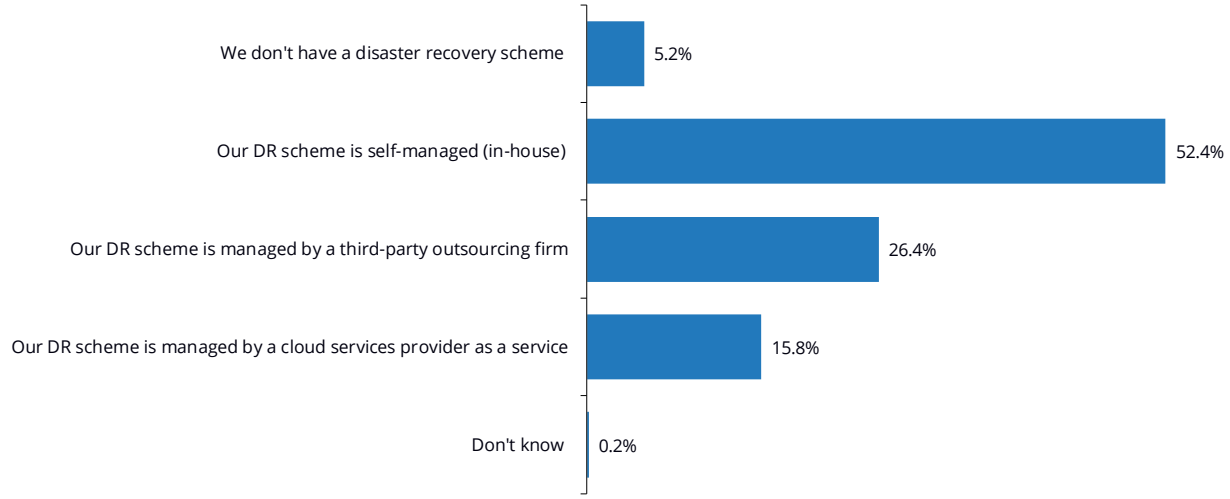
Use caution when interpreting small sample sizes.

Source: IDC's *Worldwide Business Resilience Readiness Thought Leadership Survey,* May 2018

- **55.2% of respondents believe their data protection requirements will be more complex in the coming years.** Respondents will face pressure to cost effectively manage the complexity associated with data availability. More than half of the respondents still manage their DR schemes in-house, without any third-party assistance. But in-house management is only going to get more time consuming and costly. There is potential for the gap to widen between current data availability capabilities and future needs, pushing IT organizations to more third-party and cloud-managed solutions as a result (see Figure 3).

FIGURE 3

Disaster Recovery Schemes Managed In-House Will Become Increasingly Burdensome



n = 500

Base = all respondents

Notes:

This survey is managed by IDC's Quantitative Research Group.

Data is not weighted.

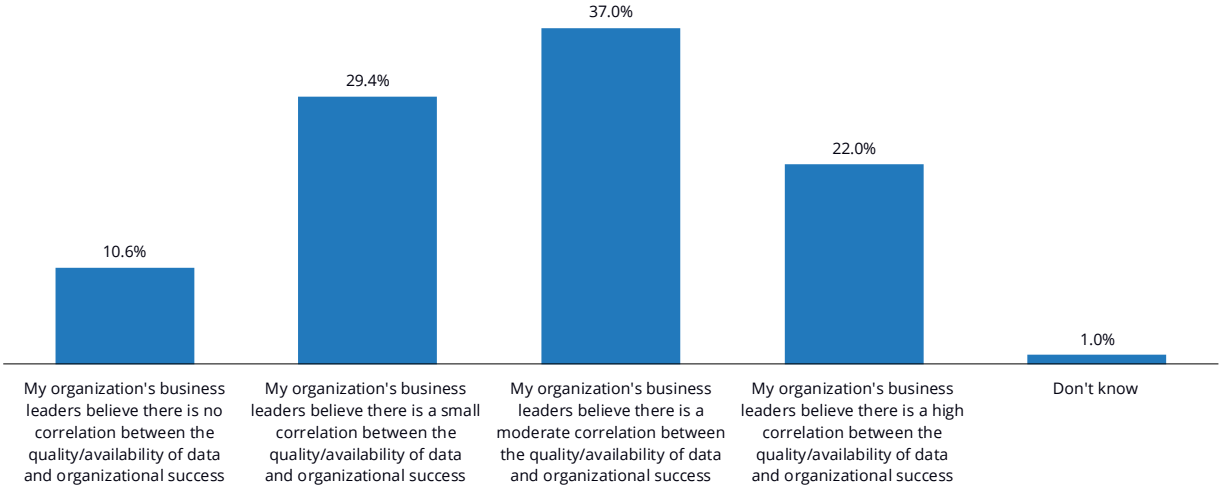
Use caution when interpreting small sample sizes.

Source: IDC's *Worldwide Business Resilience Readiness Thought Leadership Survey,* May 2018

- **Only 22% of respondents can be considered as representing "data-driven organizations."** As a result of this relatively low rate, we believe organizations will continue to struggle to convey the value of data between business and IT leaders and lack a consistent strategy for data availability and protection (see Figure 4).

FIGURE 4

Many Business Leaders See Little or No Correlation Between Data Availability and Success



n = 500

Base = all respondents

Notes:

This survey is managed by IDC's Quantitative Research Group.

This data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Worldwide Business Resilience Readiness Thought Leadership Survey,* May 2018

These key statistics indicate that most organizations continue to face a variety of technology and business-related disruptions and must work to improve data protection and disaster recovery environments while also conveying the value of this work to the organization's business leaders. The complexity of this task requires a rethinking of what it means for an organization to protect and recover business-critical data in a climate where transactions, IP, and the nature of business are increasingly digital. By leveraging IT resilience, organizations can efficiently define these requirements, gauge resilience maturity, and create a road map for implementation of data availability tools and services that ensure the success of the digital business. The sections that follow use additional survey results to illustrate which elements of IT resilience are most prevalent or lacking in today's enterprises. Finally, IDC groups these variables into a basic IT resilience maturity model to help readers compare their level of maturity with that of the respondents surveyed for this study.

Why Is IT Resilience Critical to Operations in the Digital Business Era?

Over the past 50 years, the average life span of S&P 500 companies has shrunk from around 60 years to closer to 18 years. To survive, companies have to be digital transformers while also managing the data required for new business initiatives. IDC estimates that worldwide spending on digital transformation technologies will expand at a CAGR of 17.9% by 2021 to more than $2.1 trillion.

This surge in digital transformation–based spending will drive adoption of public cloud/multicloud storage along with on-premises systems to harness massive amounts of business-related data. If organizations are not prepared to manage and protect this data in a resilient manner, they are effectively putting the business at risk, and this risk manifests in two key ways:

- **Short-term financial impact on an organization:** IDC has determined that the average cost of downtime is $250,000 per hour across all industries and organizational sizes. This number can vary widely and extend up to millions of dollars per hour for very large financial institutions. But for the purposes of this exercise, using this average, a collective eight hours of downtime per year would cost an organization $2,000,000. This includes the direct and indirect costs of lost revenue and lost productivity. The long-term impact on an organization's corporate reputation and customer goodwill may add significantly to this total over time.
- **Loss of competitive advantage:** Measuring the power of an organization's competitive advantage and how it fluctuates over time is a much more subjective exercise. However, we know that most modern digital transformation and cloud initiatives rely on data availability, causing the value of business-related data to increase and downtime to become less acceptable — and more visible — to the business. Our survey results support this assumption. Almost 50% of respondents indicated their "data demand" requirements are increasing compared with historical norms. Data demand requirements include the need for data to be leveraged internally for business purposes and the need for data to be protected and analyzed in real time. Furthermore, more than half of the respondents believed that data protection transformation is very important to their organization's digital and IT transformation projects. Without modern data protection solutions, many digital and IT transformation projects may simply be ineffective or unsuccessful, ultimately jeopardizing an enterprise's ability to compete.

In summary, organizational data — whether it is application-level data, machine-generated data, operational data, or customer data, stored in the cloud or on-premises — is the fuel for today's digital transformation initiatives. Having a comprehensive IT resilience strategy that supports these initiatives should be considered essential to an organization's success.

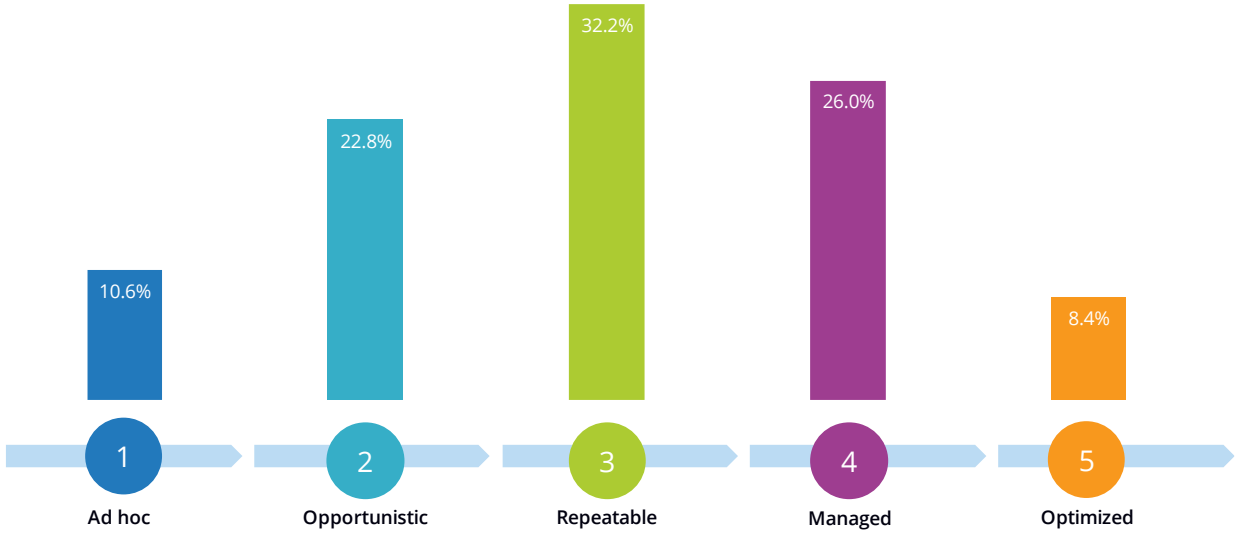
IT Resilience Maturity Rankings

We have established the definition of IT resilience and its relationship to modern IT, cloud, and digital transformation initiatives. But the definition of IT resilience will be unique to each organization. Respondents were asked to self-assess their IT resilience maturity based on the general definition of the term. Over 90% of respondents classified themselves below the top tier of maturity (see Figure 5):

- **Ad hoc — 10.6%:** Business and IT initiatives for IT resilience are disconnected and poorly aligned with enterprise strategy.
- **Opportunistic — 22.8%:** Business and IT initiatives for IT resilience may be identified, but execution is on a project basis. Progress is neither predictable nor repeatable.
- **Repeatable — 32.2%:** Business and IT goals are aligned at the enterprise level around the creation of IT resilience but are not yet focused on maximum and integrated IT resilience.
- **Managed — 26.0%:** Integrated, synergistic business and IT management disciplines deliver IT resilience on a continuous basis.
- **Optimized — 8.4%:** The enterprise and both business and IT leaders are aggressively disruptive in the use of new digital technologies and business models to affect maximum IT resilience. Ecosystem and feedback are constant inputs to business innovation.

FIGURE 5

IT Resilience Maturity Rankings — Respondents' Self-Assessment



n = 500

Base = all respondents

Notes:

This survey is managed by IDC's Quantitative Research Group.

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Worldwide Business Resilience Readiness Thought Leadership Survey,* May 2018

Certainly very few organizations have highly managed or optimized IT resilience processes. But this has the potential to change drastically. 93.8% of respondents indicate they expect to invest more in IT resilience capabilities (e.g., backup, replication, DR, and cloud) over the next two years. Bigger budgets, coupled with growing cloud adoption, will drive maturity and understanding of IT resilience across the business. However, organizational challenges may also hinder IT resilience maturity, and these are explored in depth in the section that follows.

FUTURE OUTLOOK

The maturity assessment shows us that most respondents have not implemented highly managed or optimized IT resilience practices. As a result, many backup and disaster recovery solutions may still be interpreted as cost center tools by business stakeholders. Owing to this predominant but antiquated view of DR, we recommend that IT and business decision makers focus on the scenarios discussed in the sections that follow when assessing IT resilience maturity for their organization, as the future impact will be significant.

Identify the Gap Between Your Organization's Digital Transformation Initiatives and Perceived Value of Data

One important prerequisite to advance up the ranks of IT resilience maturity is to identify and close the gap between digital transformation initiatives and the organization's perceived value of data. Successful IT resilience programs will combine both technology and business processes to recover from planned and unplanned events in a coordinated manner, which ensures true business continuity. For many organizations, getting business and IT decision makers to agree on the importance of data availability will be a good first step to improving IT resilience maturity. 30% of survey respondents indicate that their organization's business leaders believe there is little to no correlation between the quality/availability of data and organizational success. By contrast, 60% of respondents currently undergoing digital transformation and/or IT transformation projects believe data protection transformation is very important to the success of their digital transformation/IT transformation projects.

Consider these two data points illustrative of a perception gap that exists in many organizations undergoing digital transformation and IT transformation projects. Many business leaders have never dealt with the intricacies of data availability and continuity (excluding help desk requests to restore lost files, etc.) until they are faced with a digital transformation or IT transformation initiative that changes the way business-critical applications and data are accessed. Public cloud services are a great example of this shift. As additional external and internal parties beyond traditional IT are added to the mix, and a greater amount of application ownership and management is offloaded from IT onto the business unit and the services provider, responsibility for the availability and continuity of the data and application is also spread among the additional parties. These types of deployment changes require additional time and training — specifically for line-of-business owners — to make sure they understand the data protection requirements of applications and services. Ultimately, the complexity of this process may delay the deployment of IT resilience initiatives as higher volumes of applications and services outside the walls of traditional IT must be integrated and managed under a single business continuity plan.

Closing this perception gap between the importance of data availability and success of digital transformation/IT transformation initiatives is essential because there will be a lot of money on the line; 93.8% of respondents indicate they expect to invest in their IT resilience initiatives over the next 12 months. Appropriate spending and implementation of these funds require IT and business decision makers to be aligned on what it means to be IT and business resilient.

Identify Cloud-Based Tools and Services That May Be Absent or Underutilized for IT Resilience Purposes

IT buyers are steadily shifting toward cloud-first strategies, and nearly all are reevaluating their IT best practices to embrace hybrid and multicloud construction and operations, secure data management, end-to-end governance, updated IT skills, and improved multivendor sourcing. The ability to integrate and manage data across environments will be a fundamental requirement for operating not just as an IT group but also as a business.

Survey results reinforced the growing importance of cloud- and SaaS-based capabilities. Cloud-based data protection was named as one of the highest-priority IT initiatives for respondents over the next 12 months. Furthermore, over 90% of respondents believe cloud will play a role in their organization's disaster recovery or data protection plans.

Although this future focus on cloud-based protection solutions is important to the future of IT resilience initiatives, the fact is that 55% of respondents already have cloud backup solutions. Given this high rate of current adoption, we can assume that respondents' continued focus on cloud-based data protection is part of a long-term initiative, not something that will fall off the organization's road map in a year or two. Clearly, cloud-based disaster recovery and data protection solutions have currency and staying power within many organizations. This is because of several factors, including ease of use and deployment, integration with a variety of data sources, and alignment with other cloud application and infrastructure-as-a-service (IaaS) subscription pricing. Business and IT leaders should focus on leveraging cloud DR and DP solutions as key pillars of their IT resilience strategy for their message to resonate with the organization from both cost and functionality perspectives. In other words, "cloud" should be considered an essential part of the IT resilience equation, alongside on-premises solutions.

CHALLENGES/OPPORTUNITIES

IT resilience and its methods for implementation will remain a work in progress for many organizations. Relating the value of IT resilience to business and digital transformation initiatives will be key to the success of long-term IT resilience endeavors. Based on our survey results, the sections that follow provide a summary of additional challenges and opportunities we believe organizations should consider as they develop a strategy for IT resilience.

Challenges

- Modernization, transformation, and cloud-first strategic initiatives rely on data availability, and yet most businesses still experience a high degree of disruption. Minimizing these events must be the first step for any IT resilience plan.
- Complex legacy licensing will hinder cloud-based DR/DP purchases or — at worst — any purchase. In addition to contending with the people and process roadblocks laid out in this white paper, the reality of legacy licensing will also play a large part in dictating how and when organizations are able to implement the tools needed to achieve IT resilience.
- The expansion of cloud and multicloud storage environments is relentless, adding complexity to an organization's backup, DR, and DP environments and IT resilience plans. Reiterating this point, more than half of the survey respondents expect the complexity of their data protection requirements to increase in the coming years. Any IT resilience plan will be challenged to balance this complexity with a timely and successful implementation.
- The emergence of nontraditional data types requires innovative backup and recovery methodologies. Application data, machine learning data, and data gathered from sensors — ranging in format from structured to unstructured — will all be relevant to an organization's IT resilience strategy, creating an ongoing data management and visibility challenge.
- Staffing and training requirements will be strained to continuously keep pace with IT resilience requirements. The perception gap discussed previously is one factor in this equation. But agile IT shops focused on cost savings will struggle to implement the additional tools and people skills needed to enable IT resilience. 85% of respondents indicated they need to invest in additional training or personnel — or both — in order to meet their organization's requirements over the next two years.

Opportunities

- New compliance regulations like the GDPR and MiFID II can be leveraged to build the business case for IT resilience now. Organizations are budgeting time and money to meet new compliance regulations like the GDPR. IT and business leaders can use this as an opportunity to develop strategies that not only meet new compliance requirements but also help contribute to the organization's overarching goal of IT resilience.
- As data demands become more complex, putting a strain on IT budgets and staffing levels, opportunities to automate and simplify existing processes will be extremely important. Improving the automation of DR and DP functions can help organizations limit the cost and time associated with additional personnel and training. Adoption of cloud-based services for DR and DP may be a natural opportunity for many organizations. For example, 24% of survey respondents indicate they plan to deploy disaster recovery-as-a-service (DRaaS) solutions in the next 12 months.
- Optimized IT resilience requires a combination of business and IT operations and processes. The convergence of previously discrete storage workloads creates opportunity for backup and DR admins to extend their reach with complementary, integrated, and cloud-enabled solutions and services that optimize the value of organizational data and facilitate digital transformation initiatives.
- The emerging nature of many data protection and disaster recovery-as-a-service solutions gives buyers the ability to influence vendor and partner product road maps to match their security and compliance requirements, business initiatives, and data types. Many cloud-based services are constantly being improved by the software and services providers that deliver them. This allows buyers to match current and road map technology features with their unique requirements for IT resilience.

CONCLUSION

IT resilience remains a nascent concept for many organizations. The maturity model indicates that most organizations possess some level of IT resilience, starting with tools for data protection, availability, and continuity. Increasingly mature levels of IT resilience depend on the ability of IT and business units to coordinate recovery operations in a way that minimizes downtime and data loss. Optimized IT resilience models coordinate the people, processes, and technologies needed to eliminate data loss while also delivering levels of data availability that can support the organization's digital transformation initiatives.

The survey results indicate that most respondents have not optimized their IT resilience strategy, evidenced by the high levels of IT and business-related disruptions. However, the majority of organizations surveyed will undertake a transformation, cloud, or modernization project within the next two years. This illustrates the need for all organizations to begin architecting a plan for IT resilience to ensure the success of these initiatives. Without such a plan, the high prevalence of disruptive events, unplanned downtime, and data loss indicated by respondents will continue to put cloud and transformation initiatives at risk of delay or failure — creating a financial burden and negative impact to an organization's competitive advantage. A data protection strategy grounded in IT resilience allows organizations to simplify the people, process, and technology requirements necessary for digital transformation initiatives to succeed over the long term with minimal disruption to the business.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com