Forbes INSIGHTS

BUSINESS RESILIENCY: NOW'S THE TIME TO TRANSFORM CONTINUITY STRATEGIES

HOW EXECUTIVES ARE ADDRESSING CRITICAL APPLICATION RISKS ARISING FROM COMPLEX, HYBRID-IT ENVIRONMENTS

Mission-critical applications are the lifeblood of successful global businesses, but many enterprises don't devote enough attention to these vital resources when creating disaster recovery (DR) plans. Why? One of the biggest reasons is the "resiliency perception gap," or the gap between executives' perceptions of the effectiveness of their resiliency strategies and how successful these plans actually are at protecting against application outages or downtime. This resiliency perception gap can result in lost revenue and damaged brand reputations, and thus raises the question: How vulnerable are today's companies? Forbes Insights and IBM surveyed 184 senior IT executives throughout the world to find out, and the results are surprising.

Eighty percent of respondents fully expect that their disaster recovery plans can run their business in the aftermath of a disruption. Yet this confidence is questionable. Less than a quarter of these same executives say they include all critical applications in their DR strategies, which means 78% of enterprises face unplanned and unnecessary risks for these essential resources.

The reality is that many enterprises struggle to evolve their resiliency strategies quickly enough to address today's hybrid-IT environments and changing business demands. But in an always-on, 24/7-world, global enterprises gain competitive advantage—or lose market share—depending on how reliably IT resources serve core business needs.

The Resiliency Perception Gap: 80% of executives fully expect that their disaster recovery plans can run their business in the aftermath of a disruption, but only 22% include all mission-critical applications in their DR program.

While this resiliency perception gap is a glaring concern, enterprises face other significant risks as they move to modern hybrid-IT architectures. Increasing IT complexity, new types of cyber threats such as ransomware, and keeping resiliency strategies and DR runbooks up to date are also causing stress within C-suites and IT departments. In fact, less than a third of executives are confident they can meet desired recovery time and recovery point objectives (RTOs and RPOs, respectively) for essential applications.

"Many IT managers lack visibility across all their critical systems and still rely on manual processes to manage today's complex environments," says Chandra Pulamarasetti, IBM's vice president of resiliency strategy and resiliency orchestration software and services. "This occurs because of tight budgets or because organizations haven't found the right automation solution. So, even though organizations are implementing DR systems with specific RTO and RPO objectives, they're unable to meet these goals."

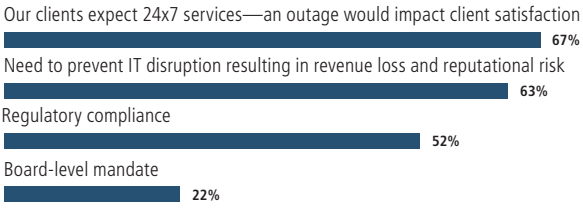
The Forbes Insights/IBM survey makes it clear that hybrid-IT environments require new resources to better protect business applications. In this executive brief, we'll detail the biggest availability gaps among global enterprises, look at the underlying causes and outline the tools being adopted by forward-looking organizations to meet today's business-resiliency realities and gain a competitive edge.

DIGITAL TRANSFORMATION SPAWNS SIGNIFICANT CHALLENGES

Concerns surrounding the protection of critical applications grow out of a heightened awareness by enterprise executives that resiliency is more important than ever for business success. For companies of all sizes across all industry segments, customers expect services to be available whenever they're ready to complete a transaction. Client satisfaction suffers when a company can't meet that threshold, and that then opens the door for competitors to steal business. Avoiding this scenario has

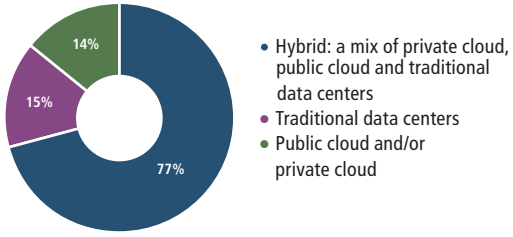
become a primary goal for the vast majority of executives. In fact, 63% of respondents see a direct link between IT disruption, lost revenue and damaged reputations (Fig. 1).

FIGURE 1: THE MAIN DRIVERS FOR BUSINESS CONTINUITY AND DISASTER RECOVERY PROGRAMS



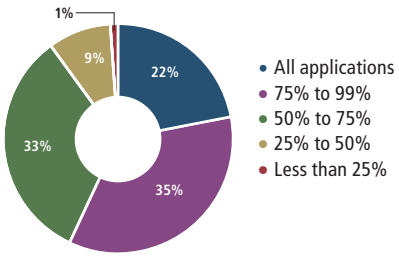
Unfortunately, meeting marketplace expectations for always-on services requires demanding RTOs and RPOs, and that is more difficult in today's dynamic, hybrid IT environments, where nearly three-quarters of enterprises are mixing private and public clouds with traditional, on-premise data centers (Fig. 2).

FIGURE 2: TYPE OF IT INFRASTRUCTURE BUSINESSES RELY ON NOW, OR ARE PLANNING FOR THE NEXT 12 MONTHS



But the Forbes Insights/IBM survey also finds a disconnect in attitudes among respondents. As noted earlier, less than a quarter of organizations include all critical applications in their resiliency strategies (Fig. 3).

FIGURE 3: PERCENTAGE OF CRITICAL APPLICATIONS INCLUDED IN YOUR RESILIENCY PROGRAM



Given this vulnerability, why are senior executives so confident about their resiliency plans? "Many people don't fully understand all the interdependencies that threaten their systems," Pulamarasetti says. "A company may successfully test a core financial system, for example, so that everyone thinks this critical asset is safe. However, a failure in another system, such as a power outage, may cascade into failures in various other areas, including the financial platform."

THE SIX ROADBLOCKS BEHIND RESILIENCY AND CONTINUITY PROBLEMS

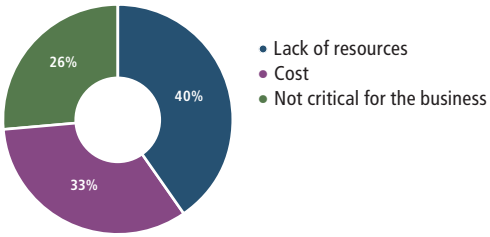
Even IT managers who fully understand the complex interdependencies of hybrid environments face significant challenges when trying to overcome resiliency and continuity problems. The reason: a mix of outdated technology, limited resources and budgetary challenges standing in the way. The Forbes Insights/IBM survey identified six roadblocks in particular that IT managers must address going forward.

Roadblock #1: Enterprises Don't Have the Means—or Desire—to Fully Protect Critical Assets

DR competes for funding with many other areas of enterprise operations, forcing executives to make difficult choices about priorities. One consequence is that 73% point to shortfalls in funding and other resources as impediments to covering all critical applications within resiliency programs

(Fig. 4). In addition, another quarter of executives don't even consider it essential to cover 100% of their critical applications.

FIGURE 4: FACTORS PREVENTING COMPANIES FROM INCLUDING ALL CRITICAL APPLICATIONS IN THEIR DR PROGRAM



Note: Does not add to 100% due to rounding.

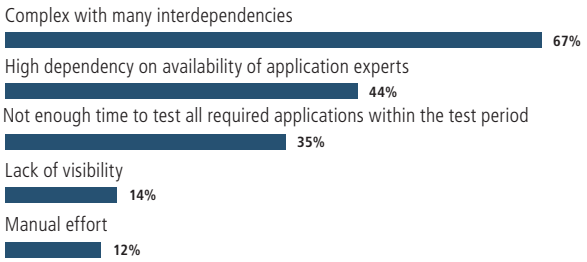
Personnel issues also factor into recovering high-value assets. When asked to identify their biggest application recovery challenges, nearly half of executives say their organizations are challenged by the availability of application experts.

Resource constraints help explain why many mission-critical applications remain vulnerable to disruption. And as shown earlier, this contributes to acute concerns about lost revenue and damaged corporate reputations. Because all organizations struggle with priority dilemmas, executives who strive to be market leaders must find ways to better protect critical assets even without a significant infusion of new funding.

Roadblock #2: Dynamic Environments Thwart Application Recovery Activities

For years, CIOs have been battling increasing IT complexity, but the challenge is greater than ever when data and applications flow among onsite and cloud resources. Survey respondents acknowledge this pain: More than two-thirds say their biggest application recovery challenge arises from complexity and the many interdependencies created when end-to-end business processes cross multiple departments, applications and hybrid-IT environments (Fig. 5).

FIGURE 5: BIGGEST APPLICATION RECOVERY CHALLENGES

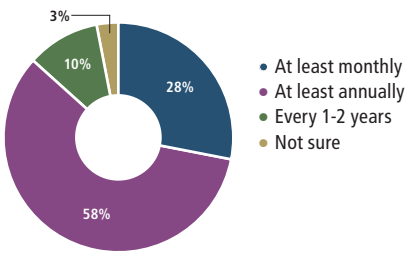


An underlying problem is that disrupted business processes and applications must be recovered in the correct sequence to avoid extended downtime.

Roadblock #3: Outdated Runbooks Are Common

Complexity also challenges enterprises to keep resiliency policies current with changing IT environments. One indication of this: 58% of enterprises go almost a year—and sometimes longer—between tests of their continuity and DR plans. Only 28% of companies run assessments monthly (Fig. 6). As a result, 47% of the executives say that DR drills or actual events showed the runbook was out of sync.

FIGURE 6: FREQUENCY OF TESTING BUSINESS CONTINUITY/DISASTER RECOVERY PLANS



Note: Does not add to 100% due to rounding.

Nearly 50% of executives find their DR runbooks are out of sync with their DR configuration.

"Many enterprises don't have a way to capture the ongoing configuration changes that regularly happen in their IT environments and then to ensure the same changes are done into DR," Pulamarasetti says. For example, someone may upgrade a system or move a production resource to a hybrid cloud. "So recoveries can fail even if the organization believes the DR strategy is ready to respond to an outage," he says.

In a world where IT managers are continuously adding, moving and consolidating resources, runbooks must reflect a similar pace to ensure critical applications get the protection they need to support demanding business operations.

Roadblock #4: Testing Disrupts Organizations

If tests are so important, why are many IT managers conducting them only annually or sometimes beyond that? A collection of logistical and practical problems get in the way of due diligence. Almost half (46%) of the executives surveyed say testing disrupts their organizations, and the cost of running tests keeps another quarter from testing more frequently (Fig. 7).

"Testing is an essential component of overall DR management, but industry studies show that an average of one in three DR drills encounter unexpected problems," Pulamarasetti says. "An organization may set aside eight hours to complete a DR test, but a series of failures due to an outdated inventory of IT resources pushes the drill beyond its allotted time. When that happens, organizations reschedule the test for another day, which causes further disruption to the business."

Roadblock #5: Overreliance on Manual Processes

The survey finds that resiliency strategies aren't becoming automated as quickly as production processes, leaving 31% of enterprises struggling with manual DR resources. Even many of the more mature organizations have only pockets of automation. For example, 33% of the enterprises automate DR but aren't taking advantage of resiliency orchestration (Fig. 8).

FIGURE 7: FACTORS PREVENTING COMPANIES FROM TESTING BUSINESS CONTINUITY/DISASTER RECOVERY PLANS MORE FREQUENTLY

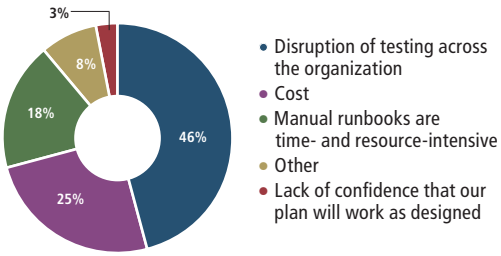
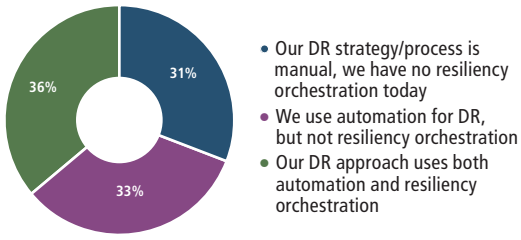


FIGURE 8: FACTORS PREVENTING COMPANIES FROM INCLUDING ALL CRITICAL APPLICATIONS IN THEIR DR PROGRAM



Note: Does not add to 100% due to rounding.

Forbes
INSIGHTS

DEFINING KEY CONCEPTS

In the Forbes Insights/IBM survey, automation and resiliency orchestration were defined as follows:

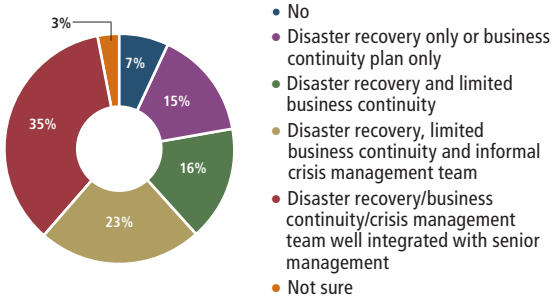
Automation: Codifying a set of manual steps via the creation of scripts that drive singular actions at independent component levels.

Resiliency Orchestration: An intelligent workflow composed of individual automated actions with an awareness of the entire disaster recovery process. Orchestration sits higher in the stack than automation, overseeing the entire process and ensuring the coordination of all required activities. Unlike traditional disaster recovery solutions that often focus on manual recovery for the IT infrastructure level, resiliency orchestration elevates resiliency to the business process level—it helps protect the end-to-end business process dependencies across applications, data and infrastructure components.

Roadblock #6: Gaps Exist in Management and Governance Activities

The sixth and final roadblock emerges as enterprises try, but fail, to holistically manage all the key elements of their resiliency strategies. Sixty-one percent of executives say business continuity, disaster recovery and crisis management are siloed rather than administered as they should be—as an interrelated whole (Fig. 9).

FIGURE 9: DO YOU HAVE DEFINED LEADERSHIP, MANAGEMENT AND GOVERNANCE OVER YOUR BUSINESS CONTINUITY PLAN (BCP)/DR/CRISIS MANAGEMENT PROGRAM?



RESILIENCY FOR AN ALWAYS-ON WORLD

To close the resiliency perception gap, meet demanding business requirements and fully protect critical assets, enterprises must overcome these six roadblocks—but how? For a growing number of organizations, the answer is with resiliency orchestration, a new, cloud-based approach that uses DR automation and a suite of continuity-management tools designed specifically for hybrid-IT environments. The comprehensiveness of resiliency orchestration gives enterprises six important benefits:

Better resource optimization: Software-based monitoring and management of DR processes significantly enhances the ability of the IT staff to test and update business systems. Prepackaged commonly used application and database patterns can be selected and assembled to create repeatable, reliable IT recovery workflows to scale up and streamline the recovery process.

Greater visibility into applications and IT systems: A centralized dashboard enables you to see your disaster recovery readiness in real time, test execution status and receive alerts based on your RTO and RPO.

Intelligent automation of DR workloads: By continuously monitoring the hybrid environment, resiliency orchestration services stay current with any data center changes that occur between formal DR tests and virtually eliminate human error.

Increased testing reliability: Resiliency orchestration services run incremental tests of DR subprocesses and identify areas where DR plans can be updated. This significantly reduces testing time for full DR drills, reduces disruption to the business and gives CIOs the confidence to run tests more often.

An alternative to manual processes: Resiliency orchestration not only automates formerly manual DR processes, but it also gathers and collates data for reports that document the effectiveness of resiliency policies. This replaces information collected by hand, and the inaccuracies that often result.

Insights for closing governance gaps: Enterprises can centrally monitor and manage resiliency activities, compare actual uptime levels against service-level agreements and take any corrective actions to increase availability.

Given these capabilities, cloud-based resiliency orchestration is quickly becoming top of mind for executives worldwide. As hybrid clouds reshape enterprise IT infrastructures, they will unleash new management and governance challenges that can potentially strain company resources and force organizations to leave critical systems exposed to downtime vulnerabilities. Yet progressive enterprises are finding an answer that keeps CIOs from having to endure these unacceptable risks: cloud-based resiliency orchestration services.

METHODOLOGY

The research in this report is based on a survey conducted by Forbes Insights, in association with IBM, of 184 senior IT decision makers responsible for disaster recovery programs within their companies. These leaders represent a wide range of industries. Global in nature, 33% of responses are from North America, 29% are from Asia-Pacific, 29% are from Europe, and 9% are from Latin America. Close to one-third are C-level executives, while 44% are vice presidents or directors. Twenty-two percent are at organizations with annual revenue exceeding $10 billion, and 45% represent companies with between $1 billion and $10 billion in revenue. Another 33% report between $100 million and $1 billion in revenue.

Forbes
INSIGHTS

ABOUT FORBES INSIGHTS

Forbes Insights is the strategic research and thought leadership practice of Forbes Media, a global media, branding and technology company whose combined platforms reach nearly 75 million business decision makers worldwide on a monthly basis. By leveraging proprietary databases of senior-level executives in the *Forbes* community, Forbes Insights conducts research on a wide range of topics to position brands as thought leaders and drive stakeholder engagement. Research findings are delivered through a variety of digital, print and live executions, and amplified across *Forbes'* social and media platforms.

FORBES INSIGHTS

Bruce Rogers
Chief Insights Officer

Erika Maguire
Director of Programs

Andrea Nishi
Project Manager

EDITORIAL

Kasia Wandycz Moreno,
Director

Hugo S. Moreno, Director

Alan Joch, Briefing Author

Charles Brucaliere, Designer

RESEARCH

Ross Gagnon, Director

Kimberly Kurata, Senior Research Analyst

Sara Chin, Research Analyst

SALES

North America
Brian McLeod, Executive Director
bmcleod@forbes.com

Matthew Muszala, Manager

William Thompson, Manager

EMEA
Tibor Fuchsel, Manager

APAC
Serene Lee, Executive Director

499 Washington Blvd. Jersey City, NJ 07310 | 212.367.2662 | **www.forbes.com/forbesinsights**