



DRaaS Bridges Executive and IT Practitioner Gap in DR Practices

LONG A BACK-BURNER ISSUE, disaster recovery (DR) has recently become a corporate strategic priority. However, top execs, removed from day-to-day DR oversight, may be overconfident in their organization’s ability to execute a sustainable DR plan, according to a new survey from IDG Research.

A spate of high-profile data breaches like those that hit Target, Sony, and the IRS, as well as natural disasters like Hurricane Sandy, have thrust cyber threats and business continuity into the spotlight. In fact, regulatory changes and economic conditions are cited alongside cyber threats as the top-ranked concerns of board members and company executives for this upcoming year, based on a new report, “Executive Perspectives on Top Risks for 2016,” underwritten by North Carolina State.

Yet while top IT execs and the C-suite have increasingly started turning their attention to high-level issues surrounding data loss, theft, and noncompliance, IT practitioners immersed in the work of disaster recovery and cybersecurity are more concerned about the state of day-to-day operations. Specifically, the survey reveals that this segment of IT is struggling to practice proactive disaster recovery versus scrambling to address problems in a reactive fashion, after an event occurs.

Seventy-one percent (71%) of top executives responding to the IDG survey rank the prevention of data loss or theft as a critical or high priority, but only half (50%) are worried about their organization’s ability to deliver continuous, uninterrupted access to data, regardless of where it resides. These execs, under constant pressure from internal and external constituents such as regulators and boards, tend to turn their attention to issues that have a direct impact on the business, such as e-commerce website downtime.

In contrast, while 86% of IT directors and managers share executives’ concerns about data loss and theft, an even larger number (89%) cite continuous, uninter-

rupted data access as a higher priority. This finding appears to correlate with IT’s current mandate to maximize system uptime and performance and ensure employee productivity.

A Noticeable Disconnect

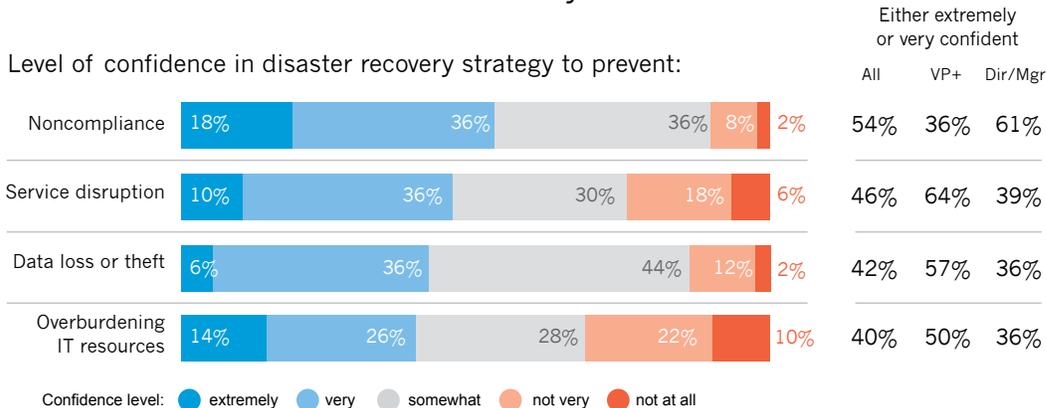
The gap between how IT and DR practitioners and senior executives view disaster recovery performance is apparent in other areas of the IDG research as well. For example, top executives say they are extremely or very confident in their firm’s ability to leverage DR practices to prevent service disruption (64%) or data loss and theft (57%). What’s more, half (50%) believe that existing disaster recovery practices don’t present a burden to their IT staffers when it comes to the day-to-day work of testing, monitoring, and managing DR plans.

IT implementers, on the other hand, see things differently. Only 39% of these respondents feel confident in their ability to ward off service disruptions, and about a third (36%) are not convinced they are adequately prepared for data loss and theft.

Noncompliance is the only area where senior IT execs have more concerns than mid-level IT managers: Here, only 36% of senior executives are extremely or very confident in this function of disaster recovery compared with 61% of IT managers. This finding appears to support senior management’s emphasis on the high-profile, strategic aspects of disaster recovery, as opposed to proactive service delivery. Moreover, since top execs have oversight and visibility into DR budget and resource allocations, they assume the bases are sufficiently covered, while mid-level IT professionals immersed in the work have daily insight into potential shortfalls.

The two groups are influenced by different challenges as they actively formulate DR strategies. As a whole, 76% of survey respondents make DR

How IT Practitioners View Disaster Recovery vs. Senior Execs



strategy decisions based on the threat of data loss or compromise; prompted by pressure from internal and external parties, including clients and regulators, they must deliver 24/7 service. In that same vein, 74% of all respondents evaluate DR strategies with an eye toward keeping data secure, while still ensuring easy access for end users.

The disconnect begins to surface when considering how a disaster recovery solution will impact IT staffers: IT managers grapple with the pain points of implementation, while top executives worry about additional housekeeping tasks that distract from value-creation activities for the business. Specifically, 85% of top execs say their DR decisions are guided by concerns about putting more manual work on IT's plate, while only 67% of IT staffers say the same. In the meantime, IT managers have more practical influences—70% of those surveyed say that DR is time consuming to test, monitor, and manage; 64% say DR is complex and difficult to deploy; and 69% believe the practices are not proactive enough in nature.

Both Camps Align Around DRaaS

Disaster recovery has long been viewed as an expensive insurance policy, and that attitude remains a barrier to garnering new investments. IT directors responding to the IDG survey are five times more likely than their senior executive counterparts (36% vs. 7%) to see that sentiment as a roadblock for funding and as the impetus for reactionary DR practices.

Yet a 2014 survey on the "State of IT Resiliency and Preparedness," put forth by Forrester Research and *Disaster Recovery Journal*, highlighted shifting corporate perceptions of DR risks and the costs of downtime. The survey found that 1 in 3 companies had declared a disaster in the past five years, and only 31% lacked experience with such an event (down from 36% in 2010).

As disaster recovery issues increase in number and

variety, the monthly subscription and OPEX business model of Disaster Recovery as a Service (DRaaS), coupled with its direct access to proven business processes and expertise, can quickly add up to an economically sound business case for once-skeptical executive management. Analysts report considerable growth in the DRaaS segment over the last couple of years and forecast 50% increases in market share annually through 2020.

For top executives and IT managers alike, DRaaS presents a tried-and-tested DR solution—a requirement cited by 72% of IDG survey respondents. Specifically, DRaaS addresses many of DR practitioners' most pressing concerns, including: failover and fallback capabilities to avoid being trapped in the cloud when disaster strikes (83%); offloading deployment, testing, monitoring, and management tasks (78%); providing a more proactive DR approach (72%); and providing visibility into metrics such as cost objectives and RPO/RTO (64%).

Not all DRaaS offerings are equal, however, so it's critical for companies to look beyond the technology stack to important differentiators in the areas of DR domain expertise and proven processes. For example, DRaaS partners should be versed in specific DR planning and testing requirements across a range of environments, and offer ready access to documentation and domain experts in order to serve as an extension of any internal IT/DR team.

Conclusion

Bolstering disaster recovery proficiency has become a top priority for both IT executives and mid-level managers, despite their varying takes on enterprise readiness and prowess. By partnering with a DRaaS provider that couples state-of-the-art technology with proven processes and expertise, organizations can bridge that gap and move confidently ahead with proactive DR strategies that deliver tangible business benefits.



For more information visit www.bluelock.com