EXECUTIVE SUMMARY

Strong Cloud Growth Driving Businesses to Change Their Thinking on Data Protection Solutions

Sponsored by: Acronis

Eric Burgener
August 2014

IDC OPINION

As organizations adapt to a new, more dynamic business environment, information technology (IT) services have higher availability requirements than ever. Awareness of the cost of downtime is at an all-time high, and more and more small and medium-sized businesses are managing their environments to strict recovery point objectives (RPOs) and recovery time objectives (RTOs). Flexible, easy-to-use, and affordable cloud technologies are allowing more of these businesses to implement their own disaster recovery (DR) strategies. To do this, businesses are leveraging private, public, and hybrid cloud options.

As data protection solutions evolve to accommodate new business requirements, it is clear that the use of the cloud support to store and protect data is becoming a critical baseline requirement. There can be a natural synergy between backup and DR solutions because they both manage the same data sets, just at slightly different points in the life cycle, but to enable this synergy, a data protection and recovery solution must include the right features. Based on how organizations are using cloud today, three features are becoming critical in a data protection solution: replication, cloud support, and the ability to easily copy and manage DR data to maintain copies in multiple locations (including an on-premise copy of the latest backup).

Businesses are dealing with increasing heterogeneity in their environments, including more widespread use of cloud technologies. A large percentage of businesses are simultaneously managing physical, virtual, *and* cloud environments; running multiple hypervisors and operating systems (OSs); and looking increasingly to workload specialists – instead of dedicated storage administrators – to implement multitiered recovery capabilities that include DR. As businesses grow and expand their IT infrastructure, data protection strategies need to evolve as well, just as people's insurance needs evolve over time. There is a strong trend toward integrated solutions that can manage all of these environments from a single interface, and small and medium-sized businesses need to keep all this in mind as they consider technology refreshes to their data protection and recovery capabilities to accommodate business growth.

METHODOLOGY

In May 2014, Acronis worked with IDC to sponsor a worldwide, cross-industry survey of small and medium-sized businesses (<1,000 employees) concerning their evolving data protection and DR needs. Cloud technologies played a prominent role in businesses' DR plans, and the survey drilled down into cloud-specific areas as well. Survey respondents were all IT personnel with responsibility for purchase decisions and overall management of the team that had responsibility for purchase decisions or that influenced purchase decisions in these areas. The total sample size was 401.

SITUATION OVERVIEW

Complexity in IT operations is not limited to large organizations. Small and medium-sized businesses are dealing with significant heterogeneity and have far fewer staff resources. While almost 80% of organizations still have physical servers, 37% of all organizations are simultaneously managing physical servers, virtual servers, *and* cloud-based operations — a "triple play" of computing environments. Of those that are managing virtual infrastructure, 54% have two or more different hypervisors, and the distribution of these hypervisors goes far beyond just VMware vSphere and Microsoft Hyper-V — 67% of businesses that have virtual servers are running at least one hypervisor other than the two market leaders. 42% of organizations have at least some of their data in the cloud, and among organizations that are backing up data to a remote location for DR purposes, 65% of them are leveraging cloud-based storage for at least some portion of that data. It is clear that administrators need data protection solutions that span all three areas — physical, virtual, and cloud — and work with many hypervisor platforms, not just Microsoft Hyper-V and VMware vSphere.

The demands of mobile computing, social media, and other 3rd Platform computing workloads are increasing overall availability requirements, driving changes in data protection strategies. Service-level agreements (SLAs) that define RPOs and RTOs are widely used in these organizations and have become ever more stringent as the importance of IT services availability increases. RPO defines the amount of data loss acceptable in the event of a failure, while RTO defines the time it takes to bring a failed application service back into normal operation.

As line-of-business managers drive more IT purchase decisions, small and medium-sized businesses are more aware than ever of the increasing cost of downtime. Just a few short years ago, many businesses did not specifically know their cost of downtime or their RPO/RTO requirements. Today, only 8% of organizations do not know their cost of downtime, and 65% of those organizations that do know their cost of downtime place it at $20,000–100,000 per hour for their most critical applications. Nearly 85% of them have RPOs of less than an hour, and 78% of them have RTOs of less than four hours.

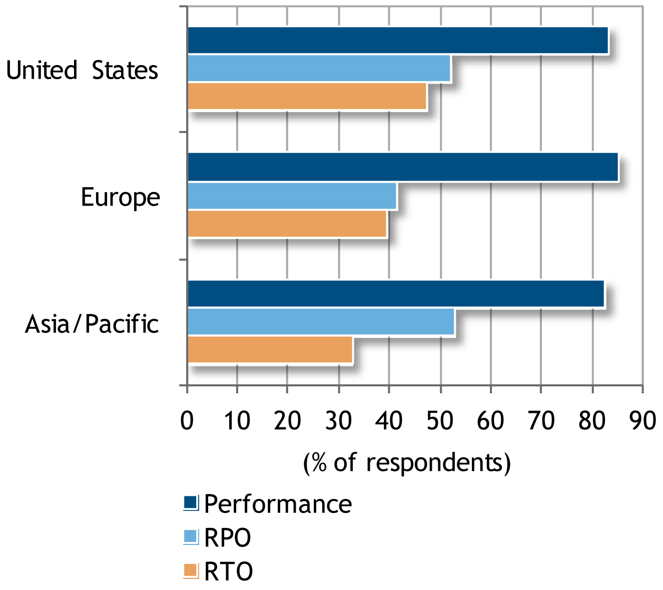
Understanding the true cost of downtime is important. Across industries, downtime may directly impact metrics as varied as revenue generation, manufacturing output, employee productivity, quality of customer service, brand reputation, or patient health. When downtime occurs, the ability to completely recover without losing data should not be taken as a given. The right data protection infrastructure needs to be in place to ensure that this can be done. IDC data over the years has indicated that as the length of an outage and the overall data loss increase for any given event, the higher the probability that a business will not recover and ultimately go out of business. As businesses evolve to rely more heavily on IT infrastructure to actually drive their business — not just support it — they need to modify their data protection strategies accordingly to ensure that their recovery capabilities keep up with their needs. In today's dynamic business environment, treating data protection as a static solution is very risky.

As availability has become more important, more small and medium-sized businesses than ever have instituted DR strategies. In recent years, increasing worldwide awareness of catastrophic disasters, such as earthquakes, hurricanes, tornadoes, and tsunamis, has also acted as a driver of DR deployments. 91% of respondents have a specific DR plan in place, and 83% of those respondents are testing their DR plans at least annually. 94% of organizations back up at least some portion of their data to a remote site, and fully 87% of those organizations want to also retain an on-premise copy of the most recent backup to facilitate granular recovery capabilities that administrators deal with on a regular basis. See Figure 1 for the drivers of onsite data retention by region. This customer need meshes nicely with data protection solutions that can manage on-premise and cloud-based data from a centralized interface and include features like efficient data capture, off-host snapshot-based backups, global deduplication, and replication.

FIGURE 1

Drivers of Onsite Data Retention by Region

Q. Why does your organization also retain an on-premise copy?



Backup performance is clearly the biggest driver of onsite retention across all regions.

n = 214

Base = respondents who retain an on-premise copy of most recent backup data

Note: Multiple responses were allowed.

Source: IDC and Acronis *Disaster Recovery Survey,* May 2014

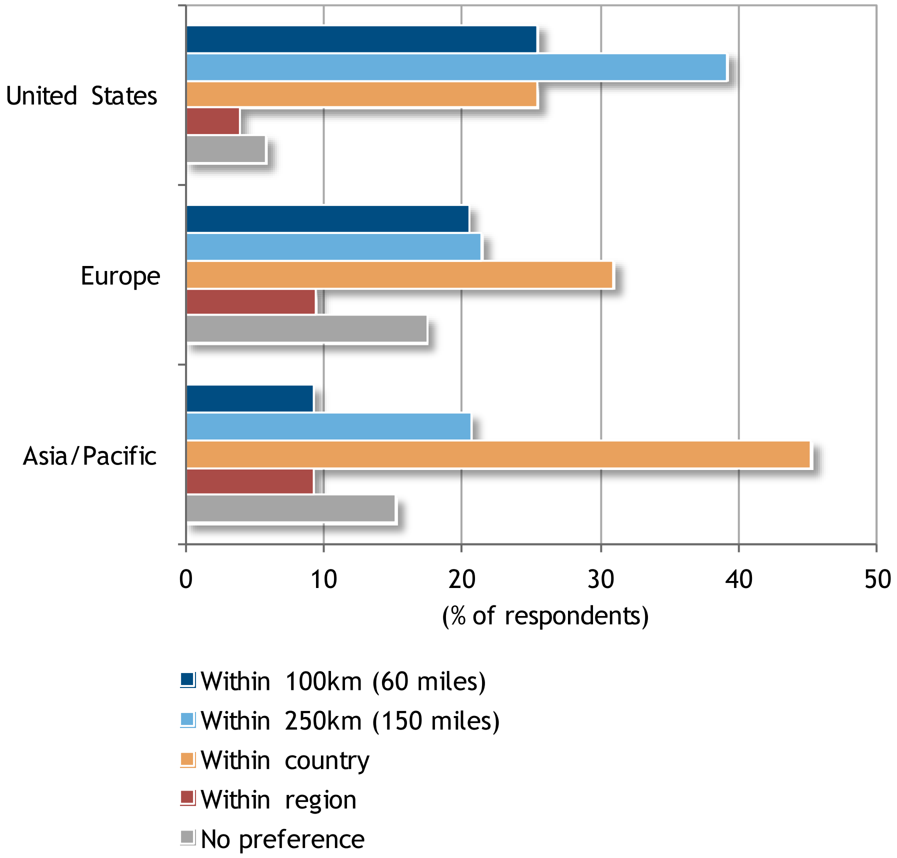
The type of replication that is most applicable to small and medium-sized businesses is an asynchronous, snapshot-based capability that opens up the option of locating data far enough away to ensure that catastrophic disasters do not affect both primary and secondary copies of business information. Asynchronous replication offers other benefits that are a good fit for the DR requirements of small and medium-sized businesses as well: the ability to securely create and maintain remote copies without impacting primary application performance, the flexibility to locate remote data hundreds of miles away from a primary site, and more efficient use of limited network bandwidth through an ability to leverage a variety of relevant storage efficiency technologies.

As businesses struggle to manage their IT operations on limited budgets, they have increasingly turned to cloud technologies to help establish cost-effective yet viable DR plans. 42% of organizations have at least some of their data in the cloud, and among organizations that are backing up data to a remote location for DR purposes, 65% of them are leveraging cloud-based storage for at least some portion of that data. Businesses want the data far enough away that even a catastrophic disaster at the primary site location will not affect the cloud site, but they also don't want the data too far away. In the United States, businesses want the data within around 150 miles (250km) of the primary site, while in Europe and Asia/Pacific, they want the data primarily within the same country as the primary site (see Figure 2). Particularly in the European Economic Community (EEC), regulations may be driving some of these requirements.

FIGURE 2

Offsite Data Location Preferences by Region

Q. Where does your organization prefer having your data stored in the cloud?



n = 401

Base = all respondents

Source: IDC and Acronis *Disaster Recovery Survey,* May 2014

These businesses are leveraging a variety of different cloud platforms — including private on-premise, private off-premise, public, and hybrid — to meet their top storage challenges. These challenges include, in order of importance, managing complexity across multiple platforms; the cost of disparate backup and DR solutions; moving data and systems between physical, virtual, and cloud environments; and the availability of appropriately skilled IT personnel. As virtualization technology penetrates more deeply into the enterprise, storage management is migrating away from dedicated storage administrators toward IT workload specialists, many of whom have limited storage experience. Ease of use is a key purchase criterion for this audience.

Given that RPO and RTO vary by application environment, and meeting more stringent RPO/RTO requirements generally requires more frequent backups and more storage capacity that adds cost, many IT shops are using multiple recovery tiers. Most small and medium-sized businesses have at least two backup tiers plus one DR tier (if they have a DR strategy), and the use of automation that makes it easy to deploy new applications to the appropriate tier is welcome. Multiple tiers give administrators the option to structure and pay for only the protection that a particular application environment requires.

Cloud technology is attractive to small and medium-sized businesses for a number of reasons. It gives them quick access to increased storage capacity without capital investments and provides the flexibility to expand or contract capacity as needed. Businesses pay only for the capacity they use. Cloud technology also offers an offsite location for data storage that gives businesses that might not otherwise be able to afford it a DR location. And it provides a lower cost per gigabyte to store data than many organizations could achieve with their own infrastructure, where they must not only purchase storage arrays but also allocate datacenter floor space and pay for energy costs. Survey data underlines the importance of cost as a driver of cloud usage — total cost of ownership (TCO) was rated as an important or extremely important driver of cloud usage by nearly 80% of respondents.

FUTURE OUTLOOK

In the data protection market, the trend toward integrated solutions that can manage the heterogeneity in today's IT environments is strong. Solutions need to simultaneously support physical, virtual, and cloud as well as more hypervisors than just Microsoft Hyper-V and VMware vSphere. They need to offer next-generation data protection technologies like flexible data capture, multiple recovery options and tiers, encryption, data reduction, and integrated replication with coverage for servers, desktops, and mobile devices. Unified solutions that require customers to buy into an expensive and complex platform up front may be a viable approach for large enterprises, but small and medium-sized businesses need solutions that are easier to install and use and that are more cost effective and do not require professional services during deployment.

Many businesses already have multiple recovery tiers, and this is also the wave of the future as they try to better match differing recovery capabilities to application requirements to get the most out of their budgets. Cloud technologies can be key contributors here with their flexibility, ease of use, and aggressive TCO for secondary data storage, making it easy to add a DR tier.

As data protection strategies evolve, many considerations about where remote data is located must be taken into account. A remote site should be far enough away to ensure survivability in the event that a disaster completely incapacitates a primary site, but near enough the primary site that employees can get to it to restart operations. Compliance and regulatory requirements about locating data within certain geographic zones must be considered. Survey data shows that most businesses want their DR sites within the same country and no more than around 150 miles (250km) away from the primary site. IDC does not expect this preference to change going forward, and this again underlines the need for cost-efficient asynchronous replication as part of the data protection solutions of the future.

Cloud usage is clearly on the rise as cloud services are used to supplement on-premise IT. In addition to the flexibility, cost, and ease-of-use benefits, cloud usage allows business to delegate much of the day-to-day management responsibility for services, including data storage, to a cloud provider whose business it is to manage IT services, freeing up organizations to focus more on their business priorities. All types of cloud — private, public, and hybrid — are already in wide use, but across all three regions (United States, Europe, Asia/Pacific), private on-premise clouds are more widely used. This will likely continue to be true, but smaller organizations that have smaller IT budgets are heavily leveraging public cloud providers like Amazon Web Services, Microsoft Azure, and Google instead of investing in their own IT infrastructure.

Developers of data protection solutions, regardless of whether they are targeting selling direct to businesses or through cloud and other managed service providers, need to consider this varied cloud usage. Replication should be integrated into the data protection product, along with support for all types of clouds. The industry is quickly moving to an era where cloud support will be thought of not as a separate feature but as part of the baseline data protection requirement, and the ability of vendors to provide a unified solution that covers physical, virtual, and cloud platforms; offers the requisite features; and is easy to use will figure prominently in their market success. Businesses considering how to evolve their data protection strategies to better fit the requirements of the 3rd Platform need to take these developments into account.

About Acronis

Acronis sets the standard for new-generation data protection through its backup, disaster recovery, and secure access solutions. Powered by the AnyData Engine and set apart by its image technology, Acronis delivers easy, complete, and safe backups of all files, applications, and operating systems across any environment — virtual, physical, cloud, and mobile. Founded in 2002, Acronis protects the data of more than 5 million consumers and 300,000 businesses in over 130 countries.

The Acronis AnyData Engine is a set of new-generation data protection technologies that capture, store, recover, control, and access data in virtual, physical, cloud, and mobile environments. The architecture of the Acronis AnyData Engine sets it apart from other data protection solutions designed to comprehensively cover heterogeneous environments that require an initial buy-in to a platform up front. With Acronis, customers can purchase an application-specific solution that stands on its own but can be integrated under centralized management (without the separate purchase of a platform) with any of the other Acronis data protection products for a complete solution. Acronis' data protection solutions cover physical, virtual (VMware, Microsoft, Citrix, Red Hat, and others), and cloud infrastructures; can protect Windows and Linux environments; and have additional solutions that can be integrated under centralized management for mobile, desktop, PC, and applications including mail and databases. Fueled by over 100 patents, the Acronis AnyData Engine powers all of Acronis' individual products, each optimized for individual workloads that all seamlessly blend into a total unified solution.

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-insights-community.com
www.idc.com