



EXECUTIVE SUMMARY

Complexity and Data Growth Driving Small and Medium-Sized Environments Toward a New Generation of Data Protection

Sponsored by: Acronis

Eric Burgener
June 2014

IDC OPINION

An increasingly dynamic business environment demands a much more agile IT infrastructure, and this is driving changes in a number of different areas, including data protection and disaster recovery (DR). As businesses have added virtual and cloud technologies to their physical infrastructure, managing heterogeneous environments has become a fact of life. Even small and medium-sized businesses are struggling with protecting physical, virtual, and cloud environments and multiple operating system platforms in the face of increasing availability requirements for both local and remote recovery capabilities.

Traditional backup products do not meet the needs of these small and medium-sized environments very well. They are very complex to manage and require buy-in to an entire platform up front, which is very costly and often overkill for them. Ease of use and complete support across physical, virtual, and cloud environments are paramount for small and medium-sized businesses, and a new generation of data protection solution that takes these needs into account is very attractive to the workload specialists who are managing more and more of the storage (and therefore data protection) infrastructure in these organizations. Recent survey results from IDC indicate that nearly 50% of respondents expressed a strong interest in a next-generation data protection solution that was easy to use and could provide the kind of comprehensive coverage needed in today's heterogeneous environments.

As explosive data growth challenges already overburdened administrators to provide business continuity strategies that protect the business from a wide range of losses, failures, and disasters, the data protection and recovery market will be moving to a new generation of comprehensive, easier-to-use data protection over the next several years. Point products that protect only a certain application or environment and lack the flexibility to accommodate burgeoning complexity and data growth will find it increasingly difficult to compete.

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. Survey respondents were all IT personnel with responsibility for purchase decisions and overall management of the team that had responsibility for these areas or that influenced purchase decisions in these areas. The total sample size was 401.

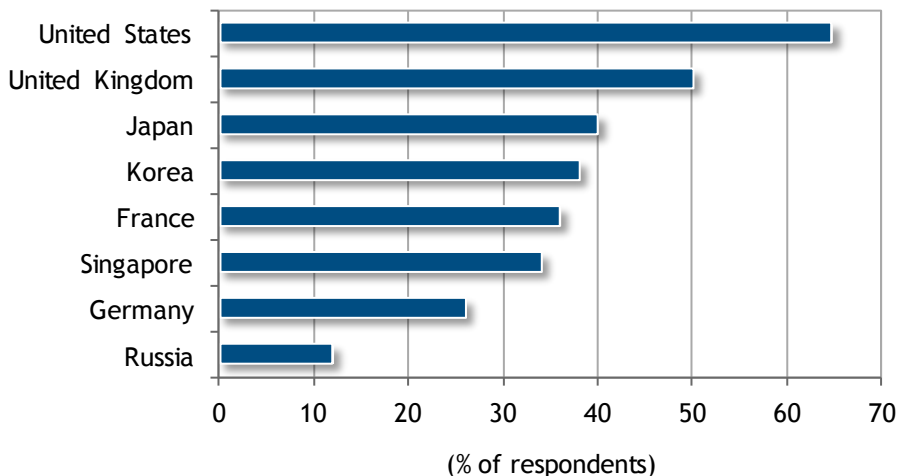
SITUATION OVERVIEW

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 nearly 80% of all organizations 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.

Figure 1 presents triple-play computing environments by country, and Figure 2 shows hypervisor usage by country.

FIGURE 1

Triple-Play Computing Environments by Country



n = 135

Base = all respondents

Notes:

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

Data is not weighted.

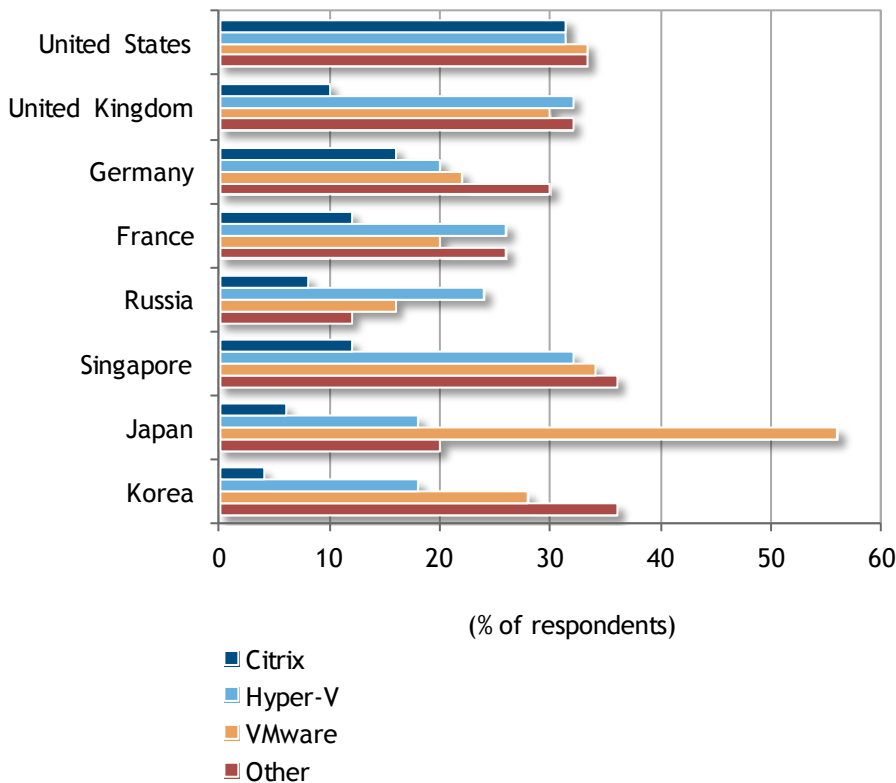
Multiple responses were allowed.

Use caution when interpreting small sample sizes.

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

FIGURE 2

Hypervisor Usage by Country



n = 243

Base = respondents who have virtual server IT infrastructure

Notes:

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

Data is not weighted.

Multiple responses were allowed.

Use caution when interpreting small sample sizes.

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

Common challenges administrators face when crafting solutions to back up these hybrid (physical, virtual, and cloud) environments include managing complexity, solutions cost, and the movement of data and systems between physical, virtual, and cloud environments. As economic pressures trim IT staff head count, administrative tasks are migrating more and more to distributed IT workload specialists – particularly in small and medium-sized businesses. These workload specialists typically have server and applications management skills but are less familiar with the storage management operations they are increasingly taking on.

Over 70% of surveyed organizations have multiple backup applications in use. Administrators look to match data protection solutions to application considerations, targeting solution specificity, ease of

use, and cost as primary purchase criteria. Well over 40% purchased a separate backup product designed specifically for virtual environments. Ease of use in a data protection solution is of particular importance as workload specialists assume a more comprehensive application management role that includes areas with which they are not generally familiar, like backup and DR.

With business operations increasingly dependent upon IT services, administrators are very focused on managing downtime to a minimum. IT is more aware than ever of critical metrics like the cost of downtime, and managing availability to service-level agreements (SLAs) is commonplace. Among small and medium-sized businesses, nearly 60% put the cost of downtime for the most critical application at \$20,000-100,000. Nearly 85% of them have recovery point objectives (RPOs) of less than one hour, while 78% have recovery time objectives (RTOs) of less than four hours. 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.

Small and medium-sized businesses have to prepare for a range of possibilities with their data protection strategies. Regular backups enable quick recoveries from small events, such as a corrupt or inadvertently deleted file. File-level recovery events are quite common, with 64% doing at least several a week and over 30% performing one at least once a day. Not surprisingly, overburdened administrators would be very or extremely interested in a backup solution that could safely enable file-level recoveries by end users, allowing them to focus more on other tasks.

The widespread use of virtual infrastructure, combined with cloud, has made DR strategies easier and more cost effective than ever to put into place. A legacy of costly, complex-to-configure DR solutions had most enterprises providing a DR solution only for their most mission-critical applications, but this is changing rapidly as businesses become more dependent on IT services. Just over 30% are backing up 75% or more of their data to a remote location to enable recovery from a catastrophic disaster, and an additional 33% are locating 50-74% of their backup data remotely. While remote backup is rapidly gaining adoption, businesses show a distinct desire to keep remote data within close physical proximity in the same geographic region, with 85% of them expressing this preference because of performance, regulatory, and other requirements.

DR is part of the comprehensive data protection regimen businesses need to put in place to ensure business continuity even in the face of catastrophic but thankfully rare disasters. In recent years, a number of catastrophic disasters – earthquakes, floods, hurricanes, tornadoes, and tsunamis – have received widespread press coverage. More small and medium-sized businesses, very aware of the impacts of these types of events, are putting DR plans into place, leveraging virtual infrastructure and cloud providers as necessary. Replication has become a key technology to move the data in a timely manner to offsite locations, and being able to manage offsite data movement from the same user interface used to schedule and manage backups is becoming increasingly important.

To help optimize recovery capabilities and at the same time control costs, many businesses have established multiple recovery tiers. Meeting more stringent recovery requirements is typically more costly because of increased backup frequencies, but not all applications require this level of protection. Data protection strategies that define multiple tiers can more cost effectively meet application-specific recovery requirements. More than ever, businesses are establishing and managing multiple recovery tiers in an effort to optimize recovery capabilities and costs. Savings in lower tiers include less frequent backups and less required storage capacity.

FUTURE OUTLOOK

Given burgeoning complexity, increasingly stringent RPO/RTO requirements, the need for tiered recovery capabilities, and a more widespread awareness of the costs of downtime than ever, a new generation of data protection solutions is required. Such a solution would cover physical, virtual, and cloud infrastructures; major hypervisors including at a minimum Citrix XenServer, Microsoft Hyper-V, and VMware vSphere and at least one major open source distribution; common operating systems in use including Windows and Linux; and disk *and* tape. Replication should be at least a licensable feature of this solution so that remote data movement and storage can be managed in concert with the overall data protection plan for the business. Survey data bears this out: Nearly 50% of respondents expressed strong interest in a single product that would provide centralized management of a comprehensive backup and DR solution.

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. Survey respondents made clear what some of these features are:

- A comprehensive solution that covers physical, virtual, and cloud infrastructures and offers both on-premise and off-premise storage and flexible recovery options that address mobile, desktop, and server requirements
- Data capture options that minimize overhead and backup windows and offer integration with popular applications through snapshot APIs like Windows Volume Shadow Copy Service (VSS), VMware's vStorage APIs for Data Protection (VADP), and others
- Migration capabilities that allow any-to-any recovery (e.g., physical to virtual and virtual to virtual) across hypervisors supporting local, remote, and cloud environments, facilitating easy movement of workloads across environments
- Ease-of-use features that make it easy to assign new applications to predefined recovery tiers with the appropriate RPOs/RTOs for the application environment
- Features like compression and/or deduplication and encryption that enable the efficient movement of even large data sets securely over networks with limited bandwidth

Increasing complexity, an increasing span of administrative control among workload specialists, and economic considerations favor data protection solutions that are easy to use. They should provide comprehensive, centralized management and the flexibility to accommodate dynamic environments with multiple recovery tiers. It is a common occurrence in the computer industry that what were once separate products ultimately become features in newer, more comprehensive products, and this is happening in data protection. Combined backup and replication solutions, intelligently architected into a single, easy-to-use product that efficiently accommodates physical, virtual, and cloud infrastructures, will be compelling alternatives to legacy backup products as small and medium-sized businesses consider their next refresh cycle.

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 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 50 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.

APPENDIX

Key results from the user survey are shown by country in Table 1.

TABLE 1

Summary of Key Survey Results by Country (% of Respondents Reporting Activity)

	United States	United Kingdom	Germany	France	Russia	Singapore	Japan	Korea
Virtualization								
Currently utilizing two or more hypervisors when virtualizing servers	78	74	39	48	25	78	45	63
Complexity and variety of configurations are the major backup challenge	57	54	44	34	18	24	20	12
Virtual machines are backed up less frequently than physical machines	29	32	38	38	44	32	38	36
Backup decisions are fragmented and driven by each applications team	65	69	52	62	32	65	60	64
Cloud								
Percentage of companies backing up at least some data to the cloud	94	78	68	69	35	73	42	56
How often security is the major concern about backup to the cloud	33	64	40	53	71	46	44	45
Companies using public cloud backup for some workloads	61	46	24	30	2	28	22	40
Downtime								
Backup coverage								
Less than 75% of all data is backed up	51	46	36	34	40	62	32	34
100% of all data is backed up	2	0	0	0	0	8	4	0
Very or completely confident that all data can be recovered	92	72	80	72	70	74	32	56
Downtime cost								
More than \$60,000 per hour	49	30	34	38	48	42	44	54
More than \$20,000 per hour	98	96	88	94	82	86	76	90
Major requirement that the most critical systems cannot be down more than 7 hours	63	74	84	80	84	86	70	88
Need to perform file recovery at least once per week	98	96	100	100	80	92	96	98

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

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

Copyright Notice

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 2014 IDC. Reproduction without written permission is completely forbidden.

