REPORT EXCERPT

ENJOY THIS COMPLIMENTARY EXCERPT

If you are interested in reading the complete report, please reach out to sales@451research.com

THOUGHT LEADERSHIP

Growing Disaster Recovery Needs Change the Role of Data Backup

MAR 2017

Steven Hill, Senior Analyst, Storage

Data protection in the form of backup and recovery remains one of the key tools in a company's disaster recovery/business continuity toolbox. However, the increasing adoption of cloud-based IT options has also added a new set of challenges for managing and protecting business processes that can extend beyond the datacenter. There's an increasing need for contingency plans that address the potential loss of mission-critical services, as well as the applications and data itself.

ABOUT 451 RESEARCH

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

NEW YORK
1411 Broadway
Suite 3200
New York NY 10018
P 212-505-3030
F 212-505-2630

SAN FRANCISCO
140 Geary Street
9th Floor
San Francisco, CA 94108
P 415-989-1555
F 415-989-1558

LONDON
Paxton House
(Ground floor)
30, Artillery Lane
London, E1 7LS, UK
P +44 (0)207.426.1050
F +44 (0)207.657.4510

BOSTON
75-101 Federal Street
5th Floor
Boston, MA 02110
P 617-598-7200
F 617-357-7495

ABOUT THE AUTHOR

STEVEN HILL
SENIOR ANALYST, STORAGE

Steven Hill is a Senior Analyst of Storage technologies. He covers the latest generation of hyperconverged systems, cloud-based storage and business continuity/disaster recovery solutions for enterprise customers.

REPORT EXCERPT

Key Findings

Customers of every size struggle with the challenge of providing business continuity (BC) in the event of an interruption of IT service, due in part to the substantially increased complexity of protecting an IT environment based on a growing mix of on-premises and cloud-based workloads.

Traditional backup vendors are expanding their offerings to include a variety of disaster recovery (DR) and BC capabilities that extend to protecting virtualized workloads and cloud services as well as data.

A growing number of vertical markets face legal compliance issues that require protections for availability as well as data security and protection for key applications. This typically includes a requirement for regular testing and validation of testing results.

Many cloud-based SaaS vendors do not offer data protection as part of their licensing agreements, and many cloud-based SLA contracts only define baseline availability terms and provide no protection for recovering business losses due to data loss or service interruptions.

There is a growing interest in changing the backup model to one more focused on data visibility in order to extract continued value out of all forms of corporate data. Traditional mass backup technology only offers limited access to information that can be stranded in large backup sets, making enhanced metadata an important key to data intelligence that spans all storage tiers.

The increasing use of storage alternatives such as the cloud raises a new set of issues when it comes to creating common and enforceable access and security policies for managing data that can reside both inside and outside the enterprise firewall.

Service providers are rapidly becoming key sources of disaster-recovery-as-a-service, and DR/BC needs can often be the initial SP engagement for enterprises. Backup/recovery and DR are becoming the most desired managed services for business customers, and should look to provide greater and more proactive customer assistance in terms of business-specific needs and high-touch support.

REPORT EXCERPT

Table of Contents

451 Research®

1. The Next Generation of Business Protection

MOVING BEYOND BACKUP

The development of computer systems for business and research applications changed more than the speed and accuracy of handling complex tasks. It also introduced a new and important challenge in the need to protect computing data production from the eventualities of physical system failures. Unless processing results were output in physical form, all of the digital information held within computing systems was intangible and at risk, as were all the hours of work that went into building the programs that generated it. As such, data protection technology was forced to adapt in tandem with the changing capabilities of computing. It evolved system-specific features like storage mirroring, replication and snapshot capabilities to protect data within the storage systems themselves that protected data up until a backup option was available.

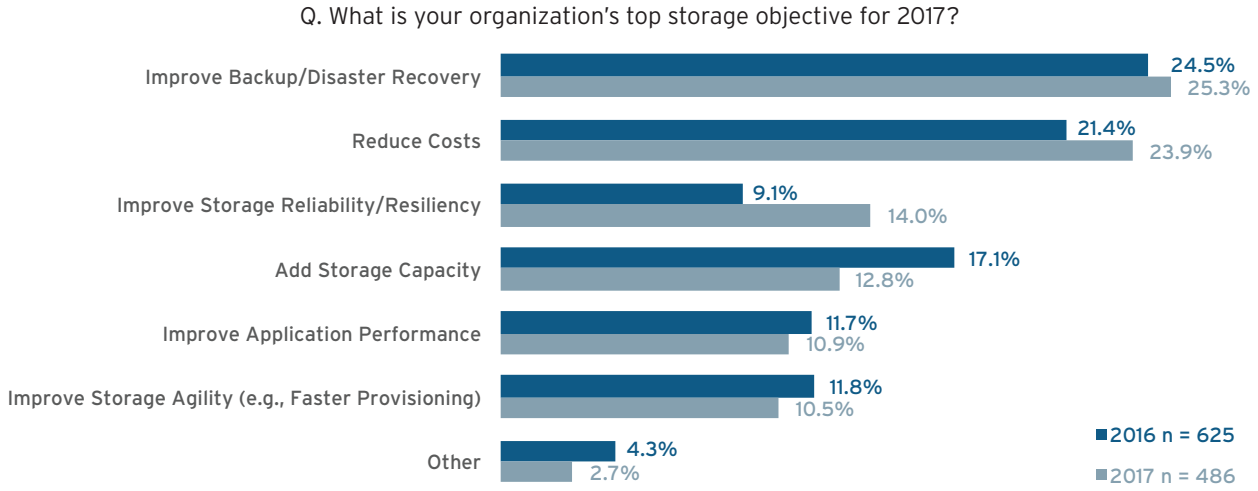
As a rule, data protection was based on a backup model where data was written to a separate system that could be isolated from the primary storage system. This met the need for key data to exist in multiple locations and on multiple systems for redundancy, but also created challenges as systems evolved and the volume of data increased. Many companies continue to make backup copies of all data their systems generate (with limited exceptions) because the lack of useful information about the data itself makes it too difficult to identify important information in the growing mountain of general data that is now part of business computing.

Traditional backup remains a key model for structured data from databases, which presents a different set of challenges when it comes to protecting data in a constant state of change. Databases commonly have a number of data files open concurrently, requiring that backup systems be able to maintain precise synchronization between these files in order to provide functional restoration in the event of a system failure. Fortunately, database and backup vendors alike have options for protecting databases on the fly – with or without a quiesce process – and offering highly granular roll-back capabilities for restoring data.

As storage needs continue to evolve and grow, the importance of protecting mission-critical data remains a top priority. Polling information supports this: Improving and updating existing data backup and DR capabilities is a serious concern for one in four business customers (see Figure 1).

Figure 1: A Quarter of Business Customers Are Concerned with Updating and Improving DR and Data Backup

Source: 451 Research's Voice of the Enterprise: Storage Budgets and Outlooks, 2016



Companies are realizing that traditional data backup becomes problematic as storage needs grow. Many customers are also finding that their existing backup methodologies are unable to keep up with the increasing data needs of business. New DR/business continuity (BC) offerings now provide faster RTO and RPO capabilities, making them capable of protection for critical workloads as well as data – an advantage that data backup methodologies alone can't offer.

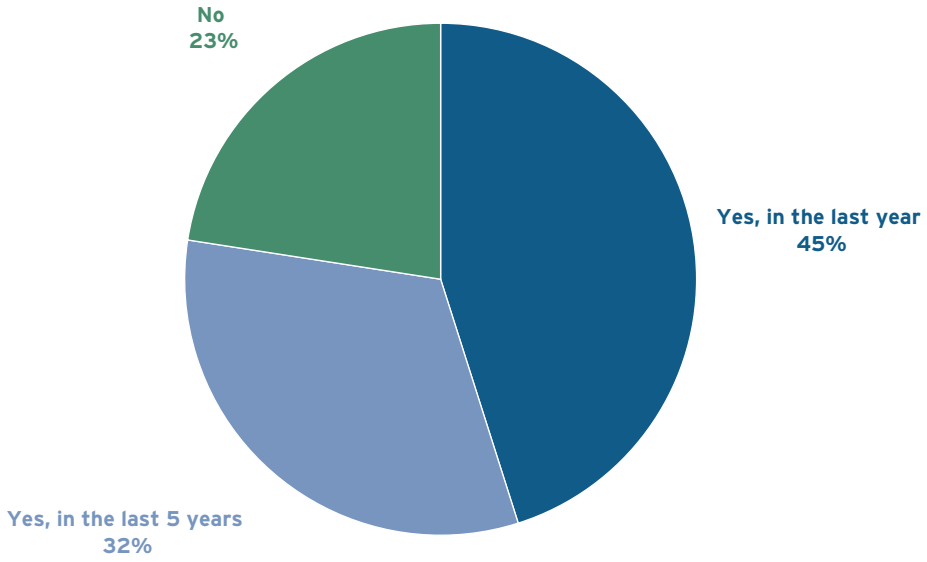
IT INTERRUPTION IS SERIOUS BUSINESS

There is no doubt that our IT systems have become far more reliable over the years, but the loss of data is still a far too common occurrence. Unfortunately, as business becomes more dependent on IT, and systems grow and become more complex, the number of potential failure points actually increases. This is a demonstration of the classic 'airplane rule' from aircraft design: Adding a second engine seems better on the surface, but also doubles the number of things that can go wrong. In an increasingly distributed IT environment, the addition of new technology and services without appropriate due diligence can lead to unexpected consequences if availability fails. As business IT becomes more dependent on off-premises resources such as cloud storage, it faces a new set of challenges: ensuring that systems can remain resilient through an interruption of underlying service dependencies. In a poll commissioned by Fujitsu America, about 77% of organizations had experienced data or productivity losses in the last five years (see Figure 2).

Figure 2: Most Organizations Have Experienced Data or Productivity Losses in the Last Five Years

Source: 451 Research, Commissioned by Fujitsu America, 2016

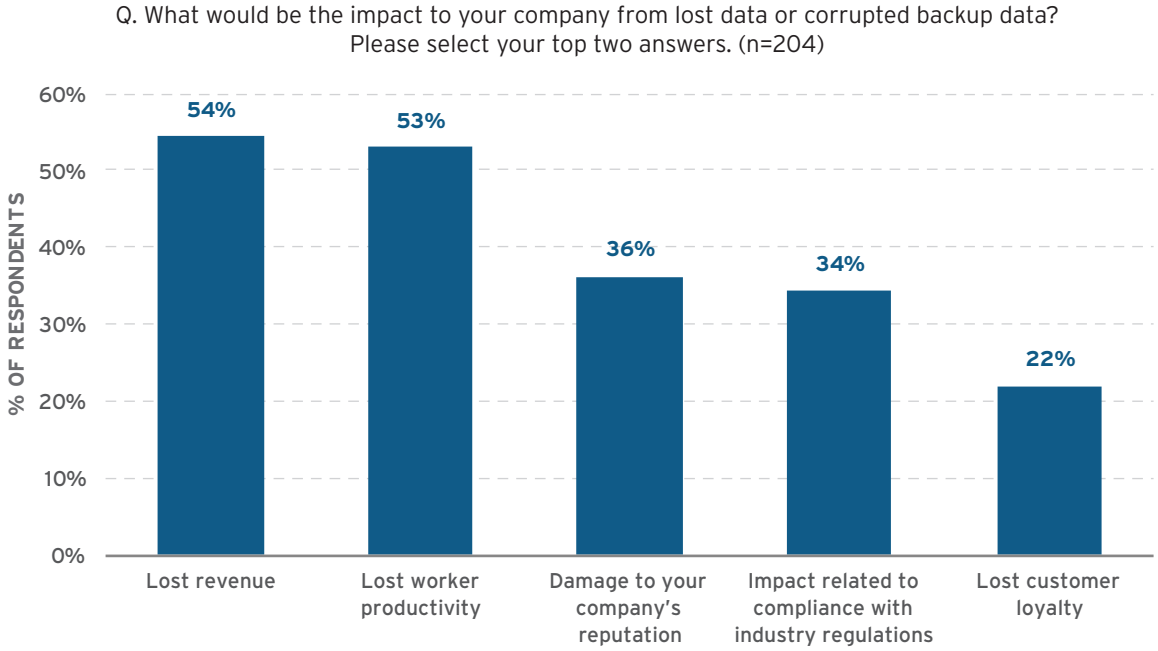
Q. Has your organization lost data or worker productivity related to data protection inefficiency? (n=204)



Further research showed that the loss of data had a direct and serious impact on the company in terms of lost revenue, worker productivity, reputation and customer loyalty, not to mention the issues specific to industry compliance (see Figure 3).

Figure 3: Data Loss and Outages Have Direct and Serious Effects

Source: 451 Research, Commissioned by Fujitsu America, 2016



Of course, it's difficult to predict the actual costs of an incident of data loss or service interruption to a given business, because they can vary greatly based on the length of interruption, the amount of data lost and the nature of the affected applications. However, those are the factors that must be taken into account when evaluating the need for a proactive DR/BC solution, and they affect businesses of every size without exception. Operating in today's IT-dependent business environment without considering the ramifications of system failure is very much like driving without insurance: It's less of a question of 'if,' and more of 'when' and 'how bad.' The challenges only become greater as IT needs become more and more reliant on outside services, and they can add a substantial amount of complexity to the DR/BC model.

THE RISE OF DRAAS

The need for DR/BC and backup/recovery capabilities has pretty much always been a part of enterprise IT, but the SMB segment is experiencing the same growing dependence on systems without the benefit of larger companies' IT capabilities. While the challenges may be smaller in scale, keeping up with the growing needs of business computing is just as critical and just as difficult. The presence of a strong IT strategy – much less a well-designed backup/recovery or DR/BC environment – becomes less and less likely at the smaller end of the SMB scale, and many companies simply don't have the experience or budget to develop a functional DR/BC approach. This has provided a perfect opportunity for the growing number of vendors, service providers and VARs that offer convenient, attractively-priced online file backup and sync and share services, but many of these low-cost services don't cover deeper DR/BC capabilities and requirements.

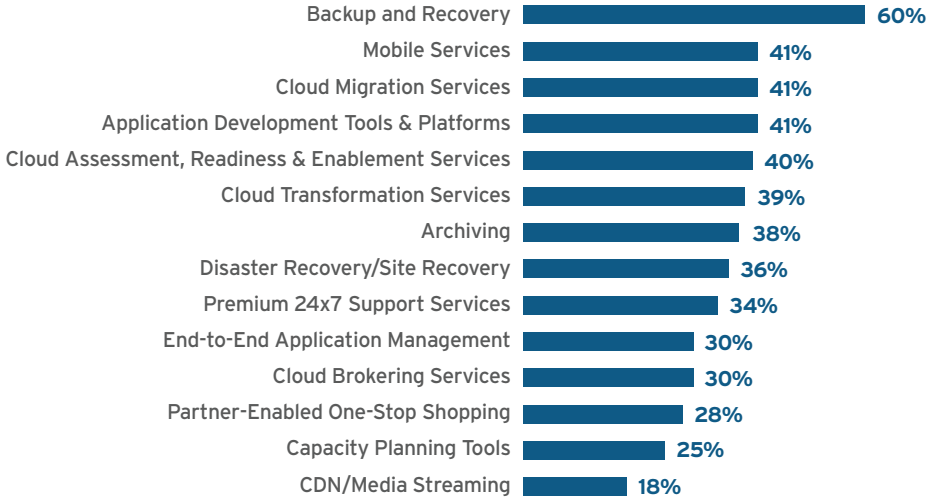
A growing number of traditional IT resources are now becoming available as 'as-a-service' offerings, and DRaaS can provide value for a broad range of IT customers. However, at least in the case of DRaaS, a service provider or VAR should take a more hands-on approach to addressing the varying needs of the SMB customer, adding value beyond the basic, metered consumption model. Most customers probably don't understand the ramifications of DR/BC, and should be able to count on their service partners to help them best address the specific needs of their business environments. We understand that this can be a challenge and can add upfront costs for the end customer, but we feel that this difference can elevate DRaaS above commodity online backup offerings.

Traditional IT vendors like IBM and Hewlett Packard Enterprise, data protection vendors like Commvault and Veritas, and service providers like SunGard, CSC and Accenture have always offered a variety of high-touch DR/BC services that could be classified as DRaaS. However, these high-end services can be priced beyond the capabilities of many SMB customers. A growing number of new vendors in the DR/BC space produce DRaaS-enabling software products, but depend on service providers and channel partners to provide high-touch, direct customer support services. This is fine, provided that these partnerships offer additional value beyond simply reselling commodity products. Recent 451 Research data shows that data backup and recovery and DR/BC have become two of the most commonly requested offerings from service providers, and these needs can often be a key first opportunity for engagement between service providers and enterprises (see Figure 7).

Figure 7: Enterprises Want More than Compute and Storage from Providers

Source: 451 Research, Commissioned by Microsoft, 2016

Top Cloud and Hosting Services: Cloud Services



REPORT EXCERPT

2. The DR/BC/Backup Application Vendor Landscape

THE CLOUD AS AN ALTERNATIVE STORAGE PLATFORM

The rise of cloud-based compute and storage services has revolutionized the IT industry more than nearly any other advancement in business computing. There's no doubt that the cloud consumption model is appealing: Features like on-demand availability, usage-based billing, virtually limitless scalability and very attractive pricing would make it seem to be a slam-dunk decision for business uses. But there are still a number of reasons that supporting a traditional IT infrastructure makes perfectly good sense for many vertical applications. Maintaining physical control of a company's IT systems can alleviate a number of concerns over cloud storage performance, availability, compliance and security that aren't issues for on-premises systems. A flexible hybrid cloud offering that combines on-premises and cloud-based services can offer the best of both worlds.

On-premises or in the cloud, storage has a somewhat greater need for resilience than the applications that utilize it. A failed application can simply be re-started, but lost data is lost forever, demanding a different level of vigilance to ensure that it either persists or can at least be reconstructed in the event of a systems failure. Data protection has always been the key task of storage administrators, and a very large segment of the business has dealt with systems to both protect the data within the applications and provide a model for replicating that data to another location. All initial DR/BC and data backup models revolved around this closed-loop approach to protecting data within the on-premises systems first and foremost and then writing that data to another platform for off-premises storage, typically in the form of compressed large datasets on tape.

Of course, things are different in the cloud. Storage use has somewhat stratified into two major use cases: flexible, high-performance block/file primary storage for cloud-based production workloads and object stores for secondary storage uses with more flexible performance needs. Data protection for cloud-based block volumes can be accomplished using the mirroring and snapshot capabilities of on-premises SAN systems today, but the model is different for the object-based secondary storage capabilities of the cloud, and secondary storage makes up the vast majority by volume of cloud storage today. It's this second-tier object storage platform that's most rapidly affecting the model of DR/BC because of the nearly limitless capacity and economy of scale that it offers to the customer. In addition, the offsite nature of cloud storage addresses one of the key issues in DR/BC, which is geographical separation from the primary site. Ironically, utilizing the cloud for DR/BC is only a minor variation on the theme of co-location, which has been available as a more bespoke service for decades. Cloud systems offer similar reliability in an on-demand model and at a tiny fraction of the cost of co-location, but they also add a new degree of complexity to the DR/BC formula.

As systems grow they almost always become more complex, and though the cloud model is designed to mask that complexity from the end user, it doesn't eliminate it. Large systems can also equal large problems, especially systems like hybrid clouds that can have many interdependencies. Historically, the only way to protect systems from all forms of disaster was to build hot mirror sites. Of course, this costly process was only accessible to the largest and most important enterprises, but this system redundancy is now theoretically available, on demand, to every company regardless of size…in the form of cloud-based storage. However, with cloud-based storage, the loss of underlying services represents a new challenge for customers: Mapping those dependencies can be a never-ending process for resources that are falling more and more outside the corporate firewall, and thus beyond IT's direct control. The other side of that coin is the opportunity offered by the massive scale and global presence of cloud-based services. They offer a completely new set of options that could almost never be delivered in an on-premises IT model. Large cloud environments can provide a tremendous degree of resiliency and accessibility that addresses a number of DR/BC-oriented use cases, offering an IT platform that provides geographical separation as well as unprecedented redundancy.

Regardless of the degree of cloud adoption a company chooses, it's important to re-evaluate and update a DR/BC plan that addresses an entirely new set of interdependencies between on- and off-premises services, as well as to better adopt the new resiliency tools and services that cloud vendors are developing.

3. Conclusions and Recommendations

A complex set of calculations should be part of the risk assessment process, and decisions for a DR/BC strategy should be based on much more than a temporary loss of underlying services, local system failures or any other single aspect. It's really about people, systems, resources, and connectivity and cost; even then, things can get missed until systems actually go down. Decisions regarding disaster recovery, business continuity and data protection ultimately come down to a risk vs. cost calculation that many customers will need skilled assistance to make.

The cloud has dramatically changed the formula of DR/BC in a substantial number of ways, but it doesn't really eliminate the challenges involved. It's likely that as IT systems continue to grow larger and more interconnected, they become even more susceptible to the laws of unintended consequences. Automation may well reduce the number of human errors, but also has the potential to dramatically increase the impact of errors when they do occur. A recent example is the rare three-hour outage of Amazon S3 storage services in the East Coast zone that occurred on February 28, 2017, and created havoc across the internet. This outage was quickly traced to a simple human error and no data was lost, but it illustrates the fact that even the best systems available today are still susceptible to unplanned outages; and that such outages can have a substantial footprint.

In business, there is no such thing as perfect, and there's no simple system or formula that can cover every contingency. The best thing to shoot for in DR/BC is mitigating losses when outages do occur. Ultimately, the cost of both freedom and business continuity is eternal vigilance; it remains up to customers to protect themselves, because there's no one else who will.

RECOMMENDATIONS FOR CUSTOMERS

- **Protect data first and foremost**. Make sure that storage platforms, both on-premises and in the cloud, have sufficient redundancy for insured data protection.
- **Re-evaluate and triage applications and data**. The rules of what constitutes mission-critical data are changing. Protecting database information remains important, but unstructured data in the form of documents, email and rich media are evolving to become nearly as important as classic systems of record.
- **Beware of missing dependencies**. The increasing use of hybrid cloud applications and services exposes new vulnerabilities in the form of service interruptions. Whether service involves access to storage or to the internet itself, contingencies need to be in place to ensure that both applications and their underlying network and storage requirements remain met.

The Advantages of Cloud-Native Backup and DR

A comprehensive answer to the challenges of merging backup with DR is a solution that is architected with the cloud in mind, leveraging the advantages of the public cloud in terms of instant availability, and long-term retention, while being optimized for bandwidth and storage to deliver against timely RTO and RPOs.

Cloud-native backup and DR achieves this by utilizing technologies such as global deduplication, and ever incremental backups, ensuring only a minimal footprint of data is needing to be stored at the greatest cost-benefit to the organization. By combining these capabilities, organizations see up to 80 percent bandwidth reduction that ensures that even remote office locations, potentially with suboptimal WAN speeds, can still be effectively protected.

Leveraging the efficiencies of public cloud vendors such as AWS allows companies to take advantage of tiered storage, with data automatically sorted into hot, warm, and cold storage depending on retention and recovery needs. This provides for longterm storage at an affordable price.

An integrated cloud backup and DR system also provides mechanisms for immediate failover to minimize downtime, using cloud-based disaster recovery, and enable quick spin-up of virtual machine instances using stored snapshots at a moment's notice to get business operations back up and running.

Druva has built a disaster recovery as a service capability into its Phoenix backup platform that allows companies to continuously protect data in the cloud. Using Amazon Web Services (AWS), the DRaaS builds on the ability of Druva Phoenix to back up and archive physical and virtual servers, removing the costly and complex burden of legacy infrastructure.

Learn how to execute your DR plan in the cloud at

https://www.druva.com/solutions/cloud-disaster-recovery/

About Druva

Druva is the leader in cloud data protection and information management, leveraging the public cloud to offer a single pane of glass to protect, preserve and discover information - dramatically increasing the availability and visibility of business critical information, while reducing the risk, cost and complexity of managing and protecting it.

Druva's award-winning solutions intelligently collect data, and unify backup, disaster recovery, archival and governance capabilities onto a single, optimized data set. As the industry's fastest growing data protection provider, Druva is trusted by over 4,000 global organizations and protects over 25 PB of data. Learn more at www.druva.com and join the conversation at twitter.com/druvainc.

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44.(0)20.3150.1722
APJ: +919886120215
sales@druva.com
www.druva.com