CompTIA

BUSINESS CONTINUITY AND DISASTER RECOVERY OVERVIEW

RESEARCH BRIEF

RESEARCH

SEPTEMBER 2013

www.comptia.org

About this Research

CompTIA's *Business Continuity and Disaster Recovery* research focuses on:

- Assessing where businesses stand with BC/DR adoption
- Assessing the factors driving and/or inhibiting BC/DR adoption
- Understanding the perspectives of IT channel partners in the BC/DR space

This research was conducted in conjunction with a CompTIA study on the Big Data market. It was conducted in two parts:

Part I:
The data for this quantitative study was collected via an online survey conducted during June 2013. The sample consisted of 500 U.S. IT and business executives responsible for technical or strategic decisions affecting data at their company. Within the IT industry, this type of survey respondent is commonly referred to as an end user. CompTIA employed the services of a dedicated research panel provider to procure the sample. The margin of sampling error at the 95% confidence level for the results is +/- 4.5 percentage points. Sampling error is larger for subgroups of the data.

Part II:
The data for this quantitative study was collected via an online survey conducted during April 2013. The sample consisted of 500 executives at U.S. IT firms, with most having some level involvement in the U.S. IT channel. The margin of sampling error at 95% confidence for aggregate results is +/- 4.5 percentage points. Sampling error is larger for subgroups of the data.

As with any survey, sampling error is only one source of possible error. While non-sampling error cannot be accurately calculated, precautionary steps were taken in all phases of the survey design, collection and processing of the data to minimize its influence.

CompTIA is responsible for all content contained in this series. Any questions regarding the study should be directed to CompTIA Market Research staff at research@comptia.org.

CompTIA is a member of the Marketing Research Association (MRA) and adheres to the MRA's Code of Market Research Ethics and Standards.

Related Resources:

- CompTIA's *2nd Annual Big Data Insights and Opportunities* research study
- CompTIA's *11th Annual Security Trends research* study
- CompTIA's *Business Continuity and Disaster Recovery Quick Start Guide* for solution providers

These resources can be accessed at no charge by CompTIA members in the member area of CompTIA.org.

Key Points

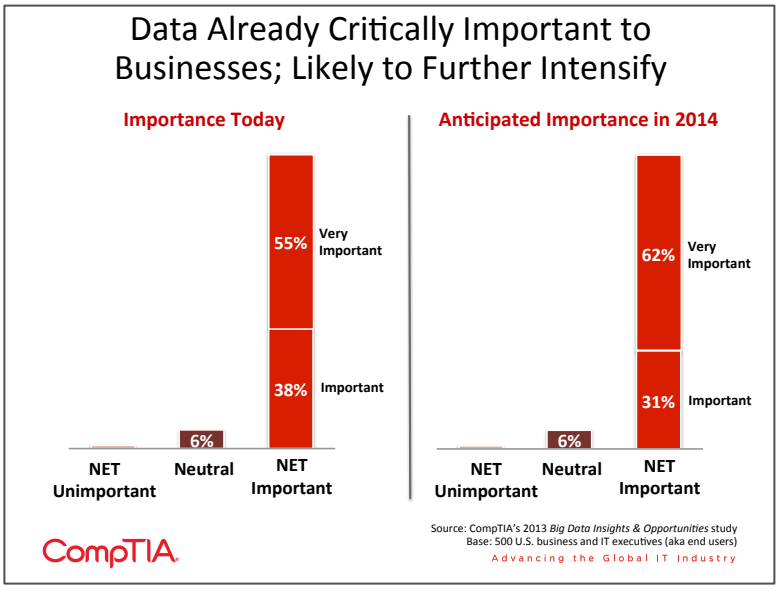
- The research indicates many companies continue to take unnecessary chances with their data and business operations. Overall, slightly less than half of companies report having a comprehensive business continuity and disaster recovery (BC/DR) plan in place. For small businesses, the rate falls to 31%.

- Three-fourths of businesses indicate data is one of their most valuable assets. Consequently, for nearly half of companies without a comprehensive BC/DR strategy process in place, protecting data and access to it, have prompted them to take action. The other key drivers for the BC/DR market include regulatory compliance and meeting end customer expectations for performance and reliability. Conversely, inadequate BC/DR strategies often involve challenges in the areas of expertise and execution.

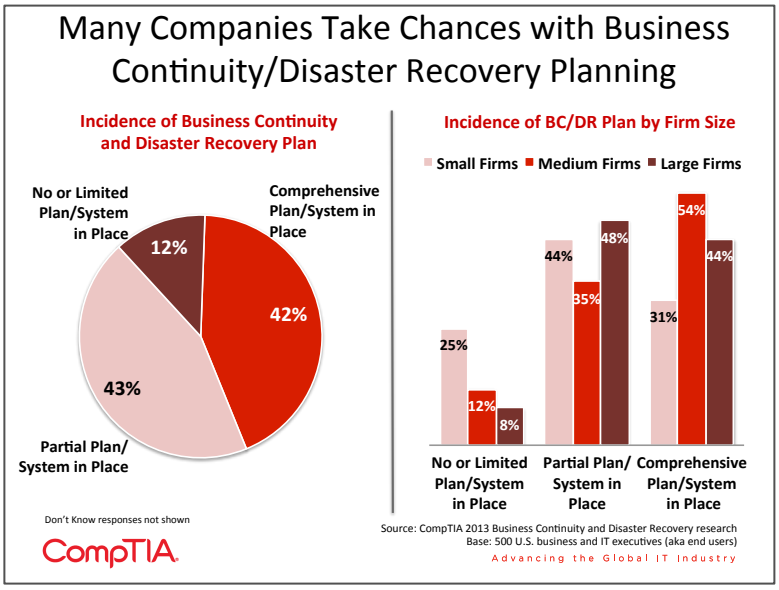
- According to CompTIA research, about 7 in 10 channel partners, encompassing VARs, solution providers, MSPs and related firms, offer some type of back-up and BC/DR service. For many channel partners, BC/DR is a natural extension of other offerings.

Overview

With IT systems and the data flowing through them growing in importance to businesses of all sizes, it logically follows that the cost of loss or disruption increases proportionally. At a minimum, costs may entail lost productivity. At the other extreme, disruption of business operations may result in millions of dollars of lost revenue or an incalculable hit to a company's reputation in the eyes of the customer.



Despite the slew of catastrophic natural disasters, as well as self-inflicted disasters such as security breaches, that heighten awareness of the need for business continuity and disaster recovery planning (BC/DR), the research indicates many companies continue to take unnecessary chances with their data and business operations.



Overall, slightly less than half of companies report having a comprehensive business continuity and disaster recovery (BC/DR) plan in place. This may cover everything from restoring data, applications and communications to detailed contingency plans for dislocated workers, disrupted supply chains and other functions.

A similar percentage (43%) reports having at least a partial plan in place, which is certainly better than nothing, but could be insufficient in practice or execution (e.g. expected vs. actual recovery time). In all likelihood, companies in this category probably don't know for sure whether their BC/DR plan is sufficient or not, which makes finding out the hard way even costlier.

As seen with many areas of IT, sophistication and investment is often correlated with firm size. This pattern generally follows with BC/DR; the smallest of companies have the lowest rates of preparedness. In a few limited cases, this may be justified, such as a highly mobile, virtual operation, but for most, it signifies a lack of know how, an unwillingness to devote the time and resources, or some combination of both.

Sizing the Market

According to the consultancy IDC, data protection and recovery software revenues increased during Q1 2013, growing at 7.6% year over year, reaching up to $1.3 billion. Storage and device management software revenues grew 7.3% year over year to $706.6 million. Compared to the modest growth rates of the overall storage market, data protection and recovery and archiving software have performed well.

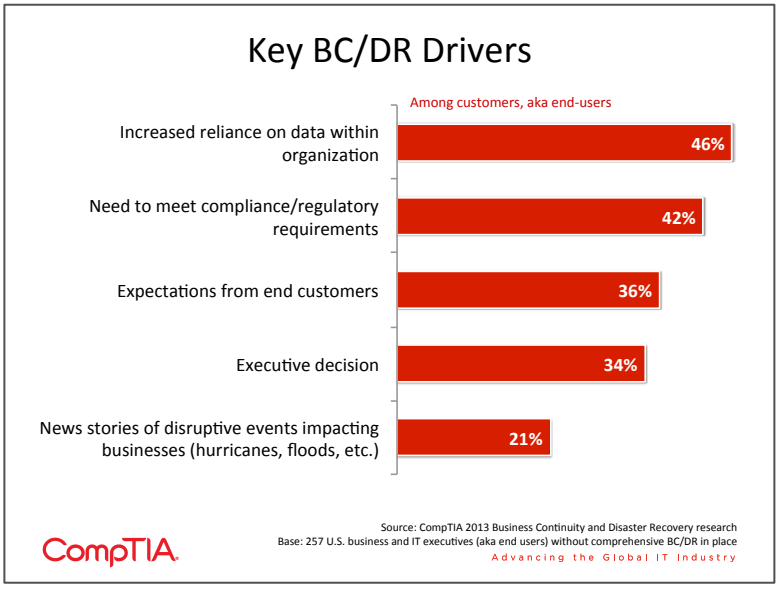
Additionally, ABI Research projects the global business continuity and disaster recovery market to reach $39 billion by 2015. Note: it is unclear what ABI includes in their estimate. It is likely a range of hardware, software and services go into the figure.

Traditional backup and recovery systems typically included an on-premise storage component supplemented with an off-premise component, such as tape backup. While some businesses still rely on this approach, increasingly, the cloud has become the option of choice. The research firm MarketsandMarkets predicts the global cloud storage market will grow from $5.6 billion in 2012 to $46.8 billion in 2018. This translates to a compound annual growth rate of 40%.

Of course, as with many cloud-based systems and applications, it can be difficult to classify certain types of revenue. For example, SaaS applications such as Office 365, Google Docs, and Box.net all have a storage component, but they also do much more. Should they be classified as productivity software, storage or general SaaS revenue? While the exact size of the cloud storage market remains fuzzy, there remains little doubt about its growth and impact on data backup and recovery.

BC/DR Market Drivers

Although a significant number of businesses acknowledge having an incomplete BC/DR plan in place, the research indicates a possible change in mindset is underway.



Three-fourths of businesses indicate data is one of their most valuable assets. Consequently, for nearly half of companies without a comprehensive BC/DR strategy/ process in place, protecting data and access to it, have prompted them to take action.

The past decade has seen a wave of new regulations covering data security, privacy, breach notification, ownership, archiving and more. In many situations, the pace of innovation gets ahead of lawmaking and companies find themselves navigating a shifting regulatory landscape. Compliance serves as the other top driver of BC/DR activities – 4 in 10 companies report it influencing their decision to take action.

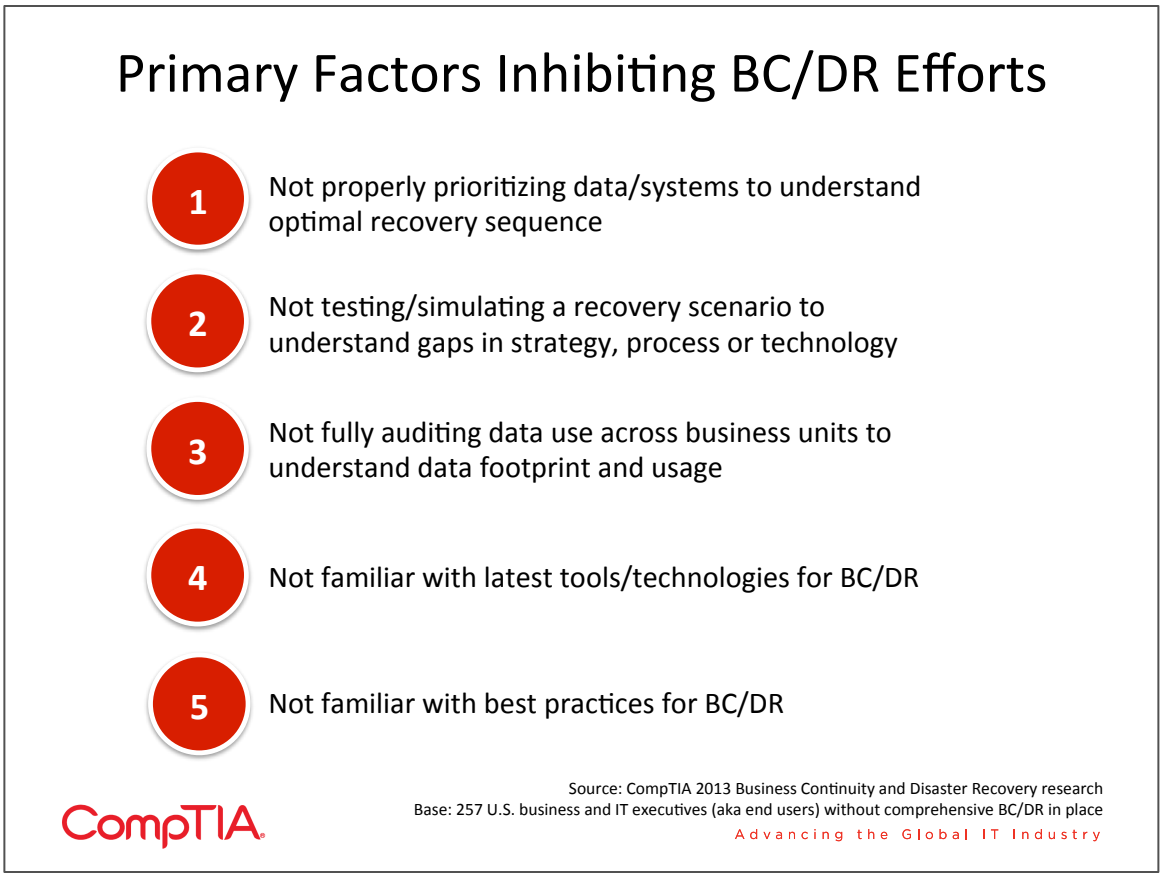
Customer expectations factor heavily into how companies view IT systems and data, thereby serving as another important driver of BC/DR adoption. When customers expect anytime, anywhere access to websites, ecommerce platforms, mobile apps, information portals (e.g. EMR) and so fourth, even a minor disruption can result in material losses.

While the aforementioned drivers will propel the BC/DR market forward, progress will be easier said than done due to a range of inhibitors that companies must overcome.

Approaches to BC/DR typically include the following elements:

- Data inventory / audit
- Risk assessment (including both internal and external risks)
- Creation of processes to address risk and compliance scenarios
- Deployment of BC/DR technology and procedures
- Review and testing

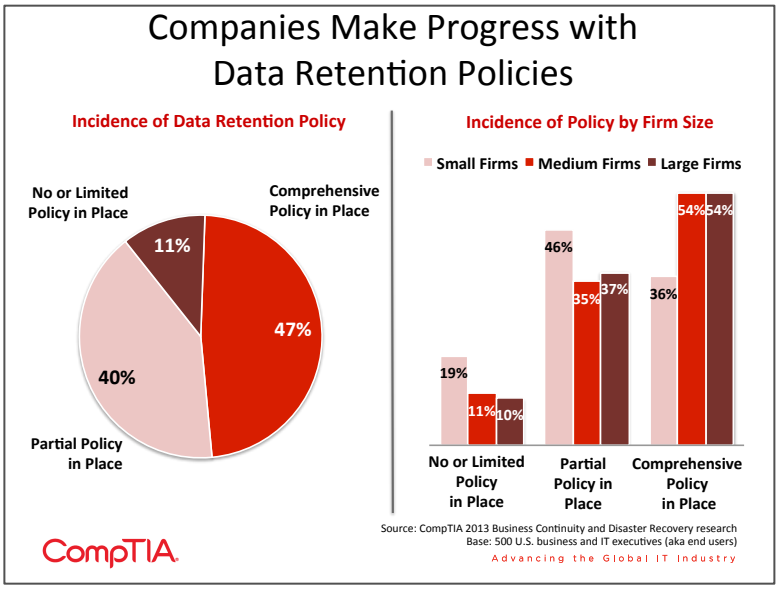
According to the research, businesses lagging with BC/DR efforts typically struggle with one or more of these elements.



The inhibitor ranking highest stems from challenges in identifying and prioritizing data and systems. Companies know certain types of data are more valuable than others. However, when it comes to storage and back-up, many organizations take an all or nothing approach, without fully thinking through the pros and cons of the strategy. Does the cost of storing the data exceed the value of the data itself? Does storing data indefinitely pose legal risks, such as keeping old emails beyond what is required by compliance or data retention policies? Does the "everything and the kitchen sink" approach introduce additional complexity into the system, hindering data analytics efforts?

Addressing these types of questions requires a bit of introspection, often facilitated with data audits and business impact analysis (BIA). This step is especially important in garnering support from executives across a range of functional areas. The CEO or CFO may rank the value of data or applications much differently than the CIO.

Closely rated, 1 in 3 businesses report not fully auditing their data across business units. Alternatively, companies may not fully know what data they have and what it is worth. CompTIA research uncovered disturbingly high rates of data silos and rogue/shadow data repositories across organizations (see Appendix for more).



Inadequate testing, review and simulation constitutes another critical problematic area. This especially applies to companies that fall into the mid-tier category of having a partial BC/DR plan in place.

Inadequate testing and review, such as omitting "what if" scenario analysis, can leave companies vulnerable when their BC/DR systems and processes are put to the test. Consider: what course of action would be required should the cloud service provider used for BC/DR data back-up goes out of business? Customers and channel partners using the Nirvanix cloud storage system experienced this worst-case scenario recently when the company abruptly announced it was shutting down. Users, including National Geographic and Fox Networks, were apparently given two weeks to retrieve or migrate their data to other providers.

Black swan events such as company closures or hundred year storms may be improbable, and yet, the organizations affected by them often wish they would have better addressed the risk.

Moreover, testing and review of BC/DR processes and systems helps companies to better understand the ramifications of their decisions. Recovery time objectives (RTO) and recovery point objectives (RPO) that may appear acceptable on paper, could be unacceptable in a real-world situation. Getting back to the example above, an organization such as National Geographic could have hundreds of terabytes, or even petabytes, of data. Estimates suggest moving 1 TB over a 1 GBPS line will take around 3 hours, or about 50 hours for 1,000 TB of data. Seen in this light, RTO/RPO requirements can quickly change.

While data recovery is obviously a vital component of the business continuity framework, what most companies really seek is a mechanism to ensure the quick restoration of data, systems and applications critical to business operations. For example, quick restoration of customer records will be important to the sales and marketing teams, but without access to their proposal building tools, their proprietary pricing calculator, or marketing campaign manager, business continuity is far from complete.

This holistic approach to BC/DR, sometimes referred to as operational resiliency, ensures companies think beyond the technology itself and consider big picture objectives as well.

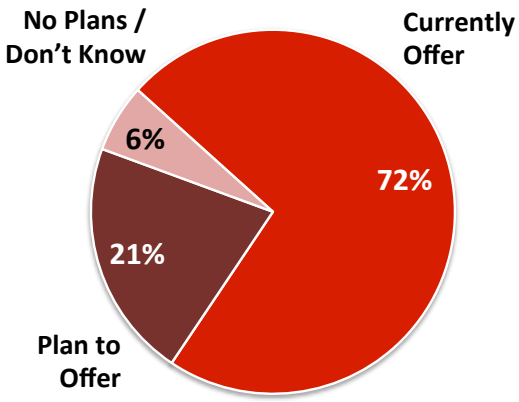
Channel Partner Perspectives

According to CompTIA channel research, about 7 in 10 channel partners, encompassing VARs, solution providers, MSPs and related firms, offer some type of back-up and BC/DR service. For many channel partners, BC/DR is a natural extension of other offerings. For example, an MSP that manages networks, endpoints and security for a customer, may opt to enhance the offering with the addition of BC/DR services.

Looking ahead to other complementary offerings, the greatest percentage of channel partners plan to begin providing cloud storage solutions (28%). This may entail acting as a reseller of any one of the growing number of cloud service providers, or white-labeling a solution and selling under their own brand.

Most Channel Partners Provide BC/DR Solutions

Incidence of Channel Partners Offering Back-up and BC/DR Solutions



Related Offerings Provided by Channel Partners

	Currently Offer	Plan to Offer
Data protection/mgt. (e.g. DLP)	70%	23%
Compliance management	66%	24%
On-premise storage solutions	61%	18%
Cloud-based storage solutions	52%	28%
Distributed storage solutions	48%	23%

Source: CompTIA 2013 Business Continuity and Disaster Recovery research
Base: 500 U.S. business and IT executives (aka end users)

CompTIA
Advancing the Global IT Industry

As noted above, lack of familiarity with the full range of BC/DR tools, technologies and best practices ranks as a top adoption inhibitor among customers.

This pain point dovetails perfectly with channel partners seeking to develop a trusted advisor relationship with their customers. It's easy to imagine customers having many questions about BC/DR, ranging from the strategic to the technical. A few examples:

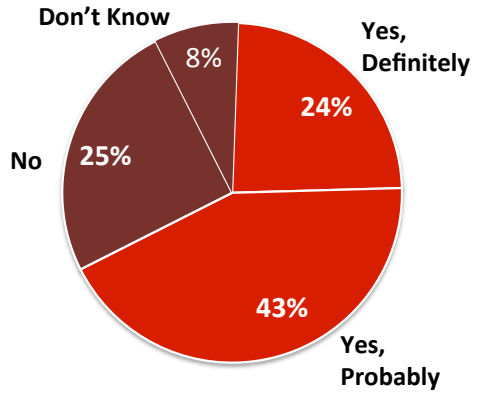
- What strategies can be used to quantify the ROI of a BC/DR solution and/or the cost/benefits of doing nothing?
- What are the best ways to think about risk, cost and operational resiliency?
- What are the tradeoffs in RTO/RPO among the different BC/DR options? For a business my size, what are the appropriate RTO/RPO benchmarks?
- How do BC/DR strategies for large enterprises compare to those for medium or small businesses?
- How can BC/DR solutions be tailored to my particular needs in my particular industry? (think healthcare sector vs. retail sector)
- What is Disaster Recovery-as-a-Service (DRaaS) and how might it be a good option for SMBs with limited in-house IT capacity?
- What are the pros and cons of the emerging range of cloud options vs. traditional tape back-up solutions?
- What about consumer-oriented cloud services such as DropBox? As DropBox and similar services mature, adding more enterprise level features and security, how do they compare to established vendors?
- In a worst-case scenario whereby a cloud provider goes down for a period of time or goes out of business, how does that impact cloud-based BC/DR solutions?
- Beyond restoring data and server assets, how do BC/DR solutions handle a situation whereby staff may need to work from home for an extended period of time?

This short list of example questions illustrates the many nuances of developing and implementing a BC/DR strategy. Channel partners equipped to connect the dots between business objectives and technical solutions, well be best positioned to meet customers' needs.

Appendix

Rogue/Shadow Data Repositories Complicate Data Management Strategies for Many Businesses

Perceived Likelihood of Rogue/Shadow Data Repositories Within Companies



Rogue/Shadow Data Repositories: any instance of employees storing company data outside of approved applications or policies. For example, an employee storing customer records in a private CRM or cloud-based storage account.

Large Firms report the greatest level of concern over rogue data repositories. This may stem from larger companies having more organizational and geographic complexity, as well as more IP and possibly more regulatory requirements, making a breach more costly.

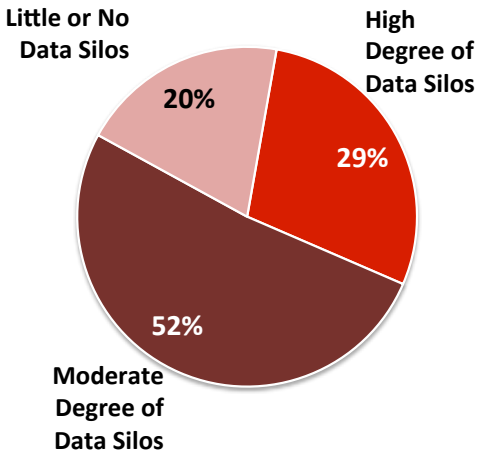
Interestingly, firms that self-rate as **ahead of the curve** in managing/using data report higher rates of rogue databases. This could be a case of greater self-awareness than firms that are still getting up-to-speed on managing/using data.

Source: CompTIA 2013 Business Continuity and Disaster Recovery research
Base: 500 U.S. business and IT executives (aka end users)

Advancing the Global IT Industry

Silos Reduce Data Utility for Many Businesses

Degree of Data Silos

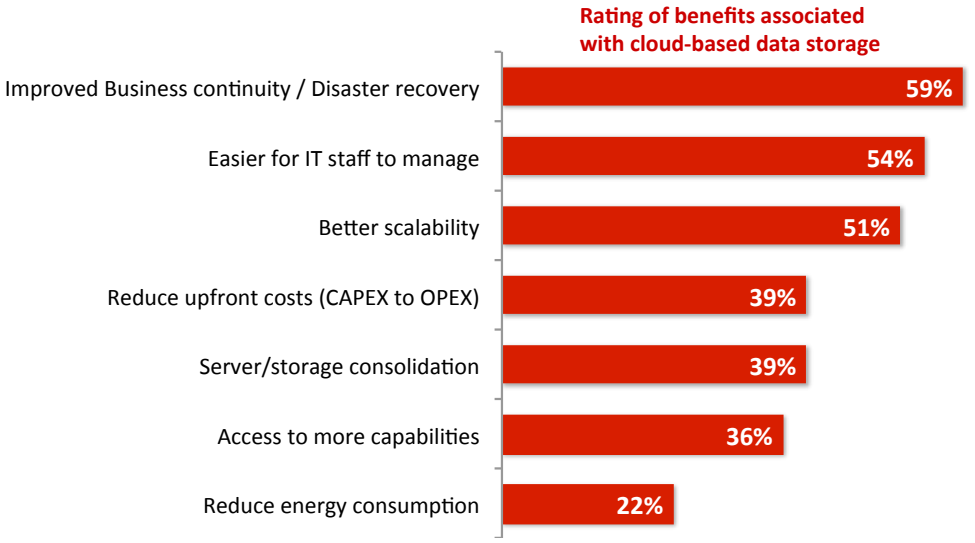


- The data indicates an increase in the number of firms reporting a high degree of data silos (29% in 2013 vs. 16% in 2012).
- Large companies report slightly higher degrees of data silos than medium-size or small companies.
- Interestingly, respondents self-reporting their analytics capabilities as 'advanced' have the highest level of data silos, possibly an indication they are most self-aware of their data shortcomings.

Source: CompTIA 2013 Business Continuity and Disaster Recovery research
Base: 500 U.S. business and IT executives (aka end users)

Advancing the Global IT Industry

Cloud-Based Data Storage Appeals to Businesses on Several Fronts

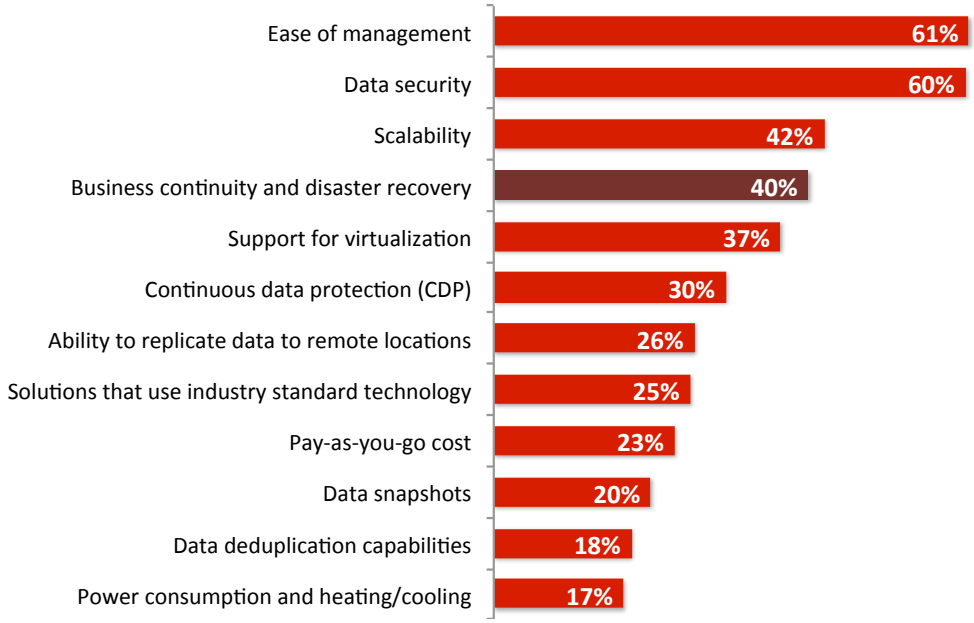


CompTIA

Source: CompTIA's 2012 *Big Data Insights & Opportunities* study
Base: 212 U.S. IT and business executives (aka end users) planning to increase usage of cloud storage

Advancing the Global IT Industry

Date Storage and Back-up Considerations



CompTIA

Source: CompTIA's 2012 *Big Data Insights & Opportunities* study
Base: 199 U.S. IT executives (aka end users) planning to invest in storage

Advancing the Global IT Industry