ESG Brief

Why You Still Need Backup

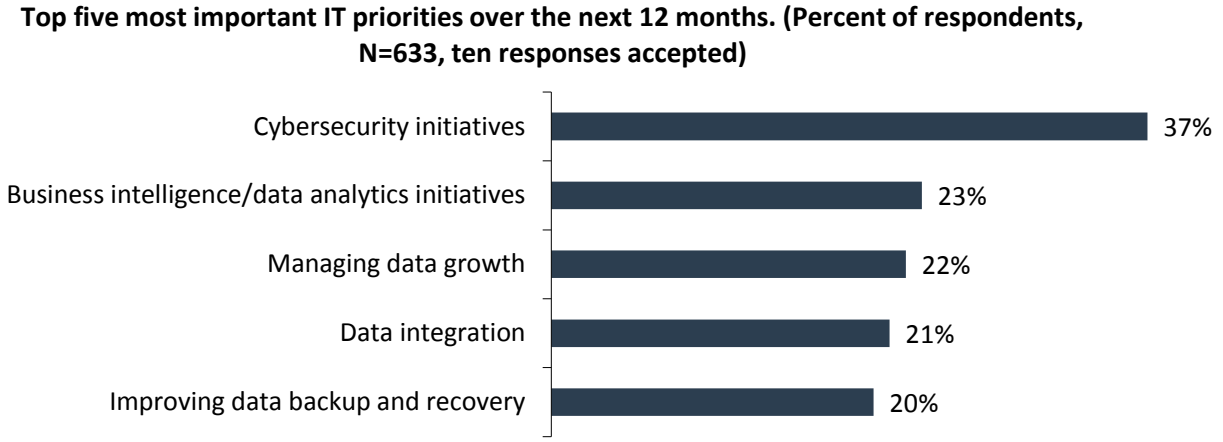
Date: February 2016 **Authors:** Jason Buffington, Senior Analyst; and Monya Keane, Senior Research Analyst

Abstract: *It's important for organizations to appreciate the differences between "backup" and processes such as file sync and share or deriving copies via storage-based snapshots and replicas. It's also important to know that even if a midsized organization is leveraging software-as-a-service (SaaS), it still must ensure proper preservation. This research brief describes the distinctive elements of three data protection scenarios, including covering how restoration and recovery fit into the picture.*

Overview

ESG research shows that for the past five years, improving data backup and recovery has consistently been one of the IT priorities most reported by respondent organizations (see Figure 1).[1]

Figure 1. Top Five IT Priorities for 2016



Source: Enterprise Strategy Group, 2016.

Tactical-level backup/recovery (as well as more strategic-level BC/DR efforts) continue to dominate mindshare for two main reasons:

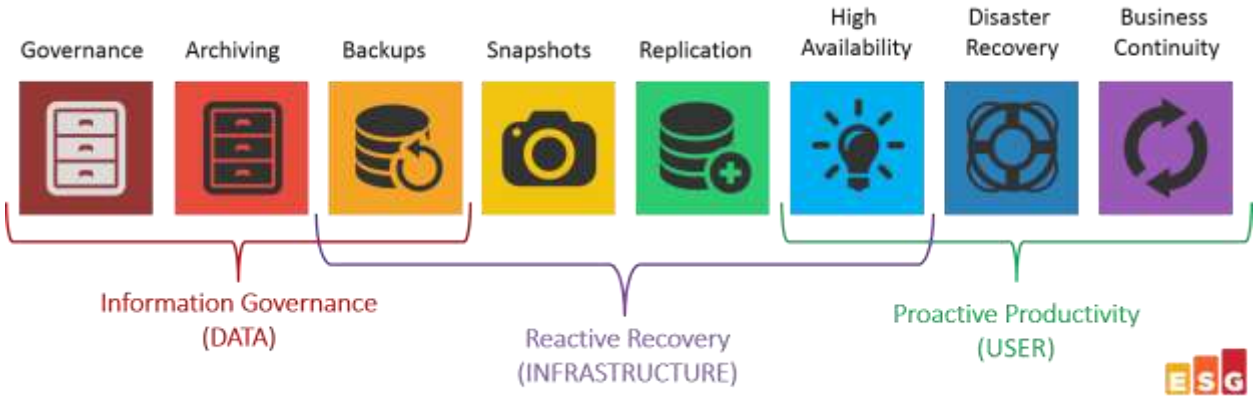
- As production workloads continue to evolve, legacy approaches for backup and recovery quickly become inadequate, thus driving the ongoing need for better data protection.
- Organizations of all sizes increasingly depend on their IT systems and services, thus requiring ever-increasing levels of IT durability.

With these considerations in mind, and particularly considering the evolving requirements for resiliency and recoverability, it should come as no surprise that many IT organizations are supplementing "traditional backup" with other forms of data protection (see Figure 2).

That being said, it would be easy to erroneously presume that if backup can be supplemented by such a wide variety of other methodologies, perhaps it is no longer required. *This presumption could not be further from the truth.*

[1] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, to be published 2016.

Figure 2. The Spectrum of Data Protection



Source: Enterprise Strategy Group, 2016.

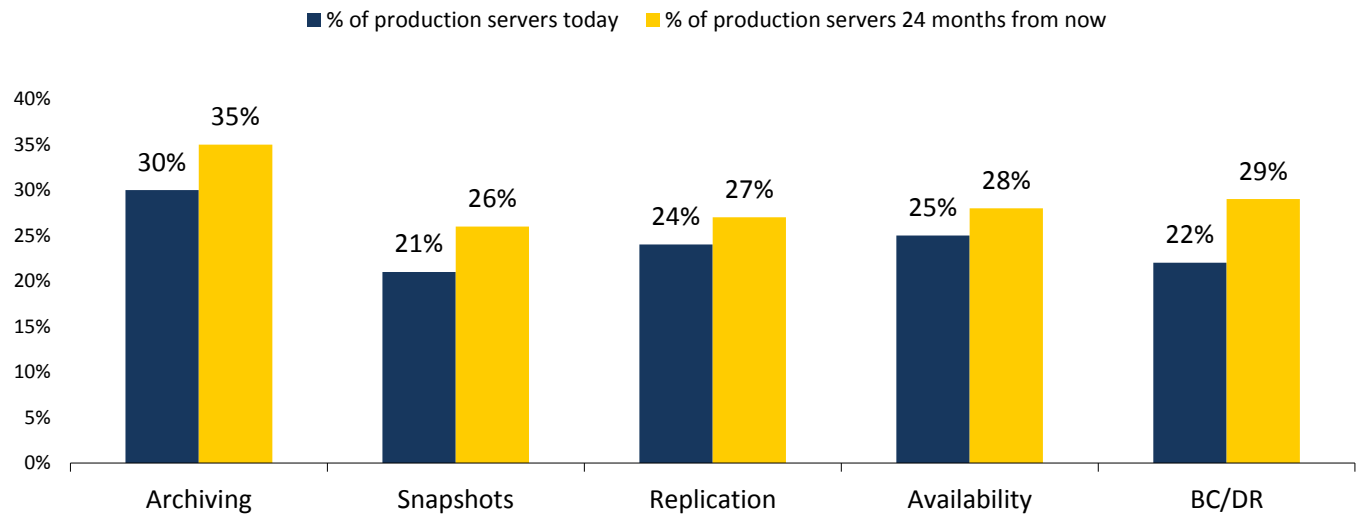
How Snapshots and Replicas Complement Backup

ESG research respondents recently revealed that more than a third (35%) of servers operating within modern IT infrastructures have per-outage downtime tolerances of 15 minutes or less. Roughly another third (32%) are marked by downtime tolerances of between 15 minutes and two hours.[2] Neither server category could be recovered reliably using traditional means of backup, thus necessitating secondary forms of replication—i.e., snapshots and replicas. Both of those processes often boast a much lower recovery time objective than what legacy backup approaches can achieve.

In fact, organizations of all sizes are not only leveraging that broad range of data protection methods seen in Figure 2, but also appear committed to increasing their use of them over the next two years (see Figure 3).[3]

Figure 3. Approximate Percentage of Production Servers with Data Protection Activities Applied to Them: Today and 24 Months from Now

For each of the following data protection activities, please indicate the approximate percentage of your organization's production servers (physical or virtual) that have those technologies being applied to them today. How do you expect this to change over the next 24 months? (Mean, N=366)



Source: Enterprise Strategy Group, 2016.

[2] Source: ESG Research Report, *The Evolving Business Continuity and Disaster Recovery Landscape*, February 2016.
[3] Source: ESG Research Report, *2015 Trends in Data Protection Modernization*, September 2015.

Both snapshots and replicas provide faster IT resiliency than legacy backup approaches because legacy backup solutions tend to transform the production data into a format that is more efficiently stored but not as agile in reuse. In contrast, both snapshots and replicas keep the data in a more usable format, making it more agile for recovery:

- **Snapshots** provide near-immediate recovery but are almost always retained within the same production storage system as the primary data itself. Thus, although recoveries to previous points in time are faster, any impact to the storage system also affects both the production data and the locally stored snapshots. In addition, because snapshots use capacity within primary storage systems (which are typically more expensive), the length of retention by most snapshotting mechanisms is typically measured in days. Backups usually exist for weeks, months, or years.
- **Replicas** provide data survivability across town or the country. However, all the copies are typically kept in near-unison *by design*. Hence, any incorrect data or corruption affecting the primary copy will in short order affect all replicas. Backups, conversely, are *by design* reflective of previous points in time.

Basically, no data protection conversation should be "backups *or* snapshots *or* replicas." Each should be viewed as complementary to the others in providing IT organizations with many recovery options to satisfy the many recovery requirements that business units demand.

How Enterprise File Sync and Share Complement Backup

Particularly in the case of endpoint data protection (e.g., protecting data on laptops), it would be easy to mistakenly assume that using an enterprise file sync and share (EFSS) technology is an acceptable replacement for backup services—specifically, the backup-as-a-service (BaaS) capabilities provided by various cloud providers. Admittedly, at first glance, EFSS and BaaS do have very similar plumbing:

- A lightweight agent is (typically) deployed through a consumer-style app store to a wide variety of heterogeneous devices.
- That agent identifies changed data, transmitting it periodically across an Internet connection to a cloud-based service.
- The cloud-based service, which often charges clients by how much storage they consume, operates with or without IT oversight (depending on the service offering).

In terms of actual architecture—from agent, through internet, to cloud storage—EFSS and data protection seem nearly identical. But if they are so similar architecturally, then why aren't EFSS offerings not officially considered "data protection solutions"? Often, the differences boil down to a lack of retention, disposition, central control, and multiple copies. Significant differences also center on the level of flexibility or agility of the cloud store:

- **To enable the productivity of individual users, a synchronization cloud service** ensures data is consistent and accessible across desktop, laptop, tablet, and smartphone devices.
- **To enable the collaboration of multiple users, a sharing service** gives multiple people access to the same documents across myriad devices.
- **To ensure data validity, regulatory compliance, and proper information governance**, **data protection services** retain multiple versions of files over an extended period of time.

Certainly, there are various service-based platforms that offer combinations of the business-value capabilities—ideally using a consolidated agent and a single cloud-based data store for multiple purposes. ESG expects to see continued convergence of these services over time because of the natural synergy offered in providing a broader range of cloud-based data management services from a single provider (i.e., BaaS, EFSS, DRaaS, etc.).

Why SaaS Needs Backup

According to recent ESG research, 62% of current cloud BC/DR service users report leveraging the built-in resiliency capabilities of the applications they are consuming as a service.[4]

Many data protection initiatives focus on either reactive or proactive availability as the outcome (including rapid restores, clustering technologies, and failover technologies), but SaaS-based platforms are often presumed to be "natively" durable. For example, although IT organizations use many methods to ensure the uptime of their MS Exchange email servers, most assume that Office 365 mail "just doesn't go down." And in fact, most cloud-based services do have multiple points of presence and operate at levels of resiliency that are unattainable by most IT organizations (e.g., Office 365 data may be hosted in parallel in at least three locations to ensure availability).

Unfortunately, because cloud-based services' resiliency is based on replication technology, erroneous data and/or deletions of data can and will affect all resilient copies nearly instantaneously—thus rendering those copies non-compliant with any level of regulatory compliance, information governance, or operational retention requirement.

Many organizations incorrectly assume that providers of large SaaS-based platforms (including Office 365, Google Apps, and Salesforce.com platforms) perform their own backups. None do.

Many organizations incorrectly assume that providers of large SaaS-based platforms (including MS Office 365, Google Apps, and Salesforce.com) perform their own backups. None do.

Just like many of the platform transitions that IT has seen over a matter of decades, the data protection of new platforms is frequently an afterthought, and organizations that are not protecting their *service*-based data with the same thoroughness and commitment as their *server*-based data run the risk of exposing their organizations to huge data losses and resulting negative business impacts.

The Bigger Truth

Availability of IT services has always been the goal. Throughout its entire evolution, the data protection industry has consistently been about shrinking the amount of downtime and data loss that IT organizations and their business users must endure.

That kind of proactive availability is achieved through durable IT architectures. And reactive availability comes via the many data protection options available to organizations of all sizes, with backup as the mainstay of them all.

With such a diverse set of resiliency, recovery, and retrieval requirements faced by business units today, it is reasonable that most IT organizations will use multiple methods of data protection and availability to meet those goals.

In some cases, "backup" will be supplemented by other data protection mechanisms, but that does not diminish the organization's requirement for long-term retention and recoverability. In other cases, organizations will erroneously presume that backup is no longer required because of other productivity- or availability-centric mechanisms. Doing so puts the business unit, senior leadership, and the IT professionals themselves in peril.

The good news is that there are more ways to ensure the agility and durability of your data and IT services than ever before—but don't forget the foundational requirement to routinely create and retain versions of data in a highly efficient and adept manner: *backups*.

[4] Source: ESG Research Report, *The Evolving Business Continuity and Disaster Recovery Landscape*, February 2016.