# Modify Your Backup/Recovery Plan to Improve Data Management and Reduce Costs

**Published:** 14 February 2017 **ID:** G00324422

**Analyst(s):** Dave Russell

## Summary

I&O leaders responsible for storage must rethink their backup procedures to realize cost savings and improve backup infrastructure resource utilization. Cloud services can help your infrastructure modernization initiative, as they alleviate the burden on the data center backup infrastructure.

## Overview

### Impacts

I&O leaders responsible for storage who back up more data than required to meet SLAs are seeing increases in storage backup costs, failure rates and backup window times.

When I&O leaders responsible for storage back up data to a cloud service, they decrease the load on the primary data center backup infrastructure.

I&O leaders responsible for storage can save money by backing up less data and retaining backup data for shorter time periods.

### Recommendations

I&O leaders responsible for infrastructure modernization:

Re-examine the data and applications being protected, especially SLA terms such as backup include/exclude lists, number of versions of a file to retain and backup retention.

Move remote office/branch office (ROBO), desktop/laptop, departmental, and small or midsize business (SMB) backup workloads to the cloud.

Adopt a layered or tiered backup and recovery approach, backing up the lowest tier less frequently; perform fewer full backups for static data, such as every two weeks instead of weekly.

Deploy an archiving solution to capture and manage static data, or data that needs to be

retained longer than one year.

## Strategic Planning Assumption

By 2018, the number of enterprises using the cloud as a backup destination will double, up from 13% at the end of 2016.

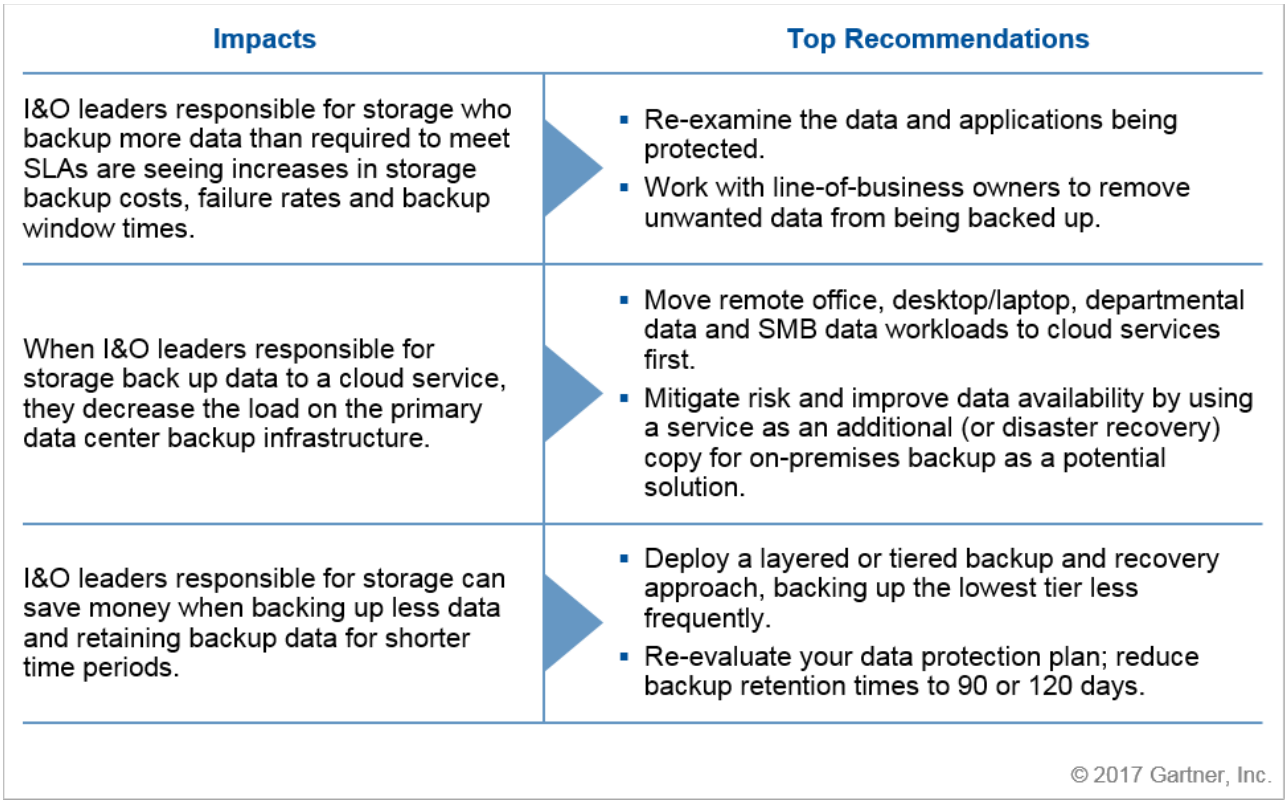
## Analysis

Data protection ranks high on every organization's priority list. However, lack of funding and staffing constraints can pose challenges for IT leaders who want to provide comprehensive and fail-proof services to their end users. To deal with these challenges, organizations need to implement a layered or tiered recovery approach, where backup and recovery is channeled between two or more service levels, each with a different quality of service (QoS) and cost structure.

This research is focused on optimizing the backup and recovery infrastructure (see Figure 1). [1] Perform a reclassification of the data being protected, rather than lowering QoS or reducing service-level agreements (SLAs) for all data. Implement techniques included in this research to help you meet tactical budget challenges and realize cost savings.

Do not alter backup policies and procedures in a way that would conflict with external regulations or internal corporate mandates. Regulatory and corporate requirements should still dictate how data is protected, and as always, consider an archiving solution for regulatory compliance when possible. Consideration of backup as a remediation for malware and ransomware needs to be taken in to account as well.

**Figure 1.** Impacts and Top Recommendations for Improving Data Center Backup




*Source: Gartner (February 2017)*

## Impacts and Recommendations

**I&O leaders responsible for storage who back up more data than required to meet SLAs are seeing increases in storage backup costs, failure rates and backup window times**

Organizations with broad, generalized "one size fits all" backup policies often consume significant resources. Storage administrators often back up and store data they did not intend to protect. For example, some organizations back up a user's entire drive, or all folders and directories.

However, leading organizations use software distribution solutions, imaging products or server virtualization offerings to deploy OS images. One means of protecting OS images is to use a bare-metal recovery (BMR) solution for filtering out OS files from the backup policy. Another approach is to exclude rich media files, such as Audio Video Interleave (AVI), JPEG and MP3 formats, unless there are business reasons to include them.

Storage managers and storage administrators need to revisit backup policies to exclude temporary and problem determination files, such as .tmp and .dmp files. Gartner also recommends that I&O leaders create and enforce desktop and laptop policies where only sanctioned data locations, such as a My Documents folder, are protected and backed up. I&O leaders can exploit recent backup solution enhancements that include the ability to

perform incremental-forever, virtual-full or synthetic-full backups that merge together data and consume less overall storage in the backup repository. To help contain costs, I&O leaders need to re-examine the types and amount of data being backed up.

*Recommendations:*

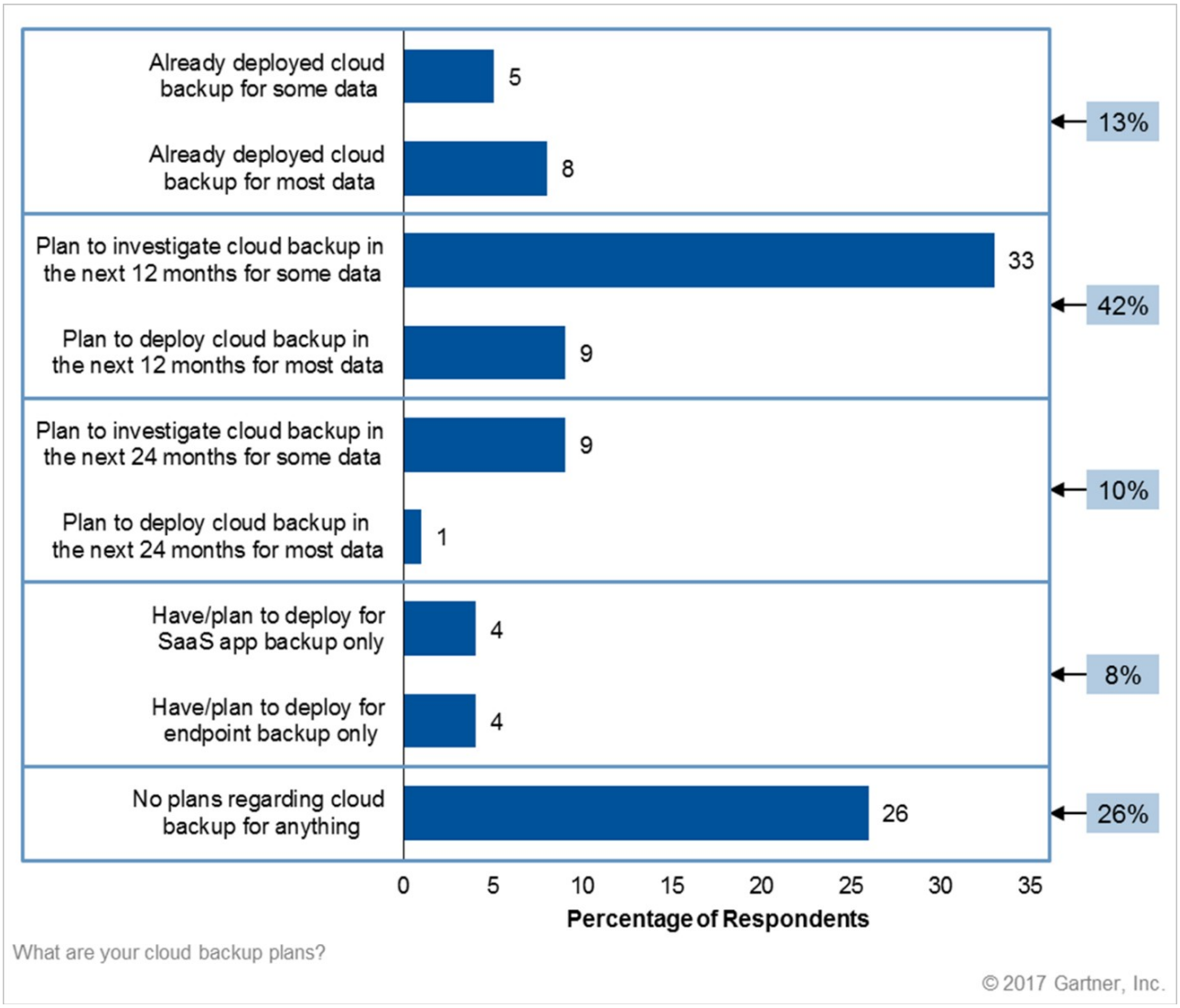
- Re-examine the data and applications being protected, especially SLA terms such as backup include/exclude lists, number of versions of a file to retain and backup retention.
- Work with line-of-business owners to create or review backup templates and policies for each group of users, applications or servers. Remove unwanted data from the backup workload. One way to encourage this is though implementing chargeback for all backup jobs or terabytes written to the backup application.
- Exploit backup solution enhancements that include the ability to perform incremental-forever, virtual-full or synthetic-full backups that merge data and consume less overall storage in the backup repository.
- Be cautious of changing backup policies and procedures in a way that would conflict with external regulations or corporate mandates. And of course, implement archiving solutions for long-term record retention.
- Perform data recovery testing at least once a year on a subset of data to ensure the backup strategy effectively meets the stated SLA projections.

**When I&O leaders responsible for storage back up data to a cloud service, they decrease the load on the primary data center backup infrastructure**

Storage managers find backup delivered as a service is becoming attractive for a portion of the organization's data. Bandwidth limitations are addressed through data reduction and network optimization techniques, as service-based features and functionality continue to improve. Organizations are actively considering SaaS and cloud-delivered solutions to protect data in ROBO environments, as well as test-and-development data and endpoints, including desktop, laptop and tablets. Some companies are evaluating these delivery models for regional areas and at least a subset of their primary data centers.

At Gartner's 2016 Gartner Data Center and Infrastructure and Operations Management Conference, 13% of those polled indicated that they had already deployed cloud backup for some of their data, and 42% indicated that they plan to investigate or deploy cloud backup for at least some of their data in 2017, as shown in Figure 2.

**Figure 2.** Cloud Backup Intentions




Question: What are your cloud backup plans? (n = 135)

*Source: Gartner (February 2017)*

Cloud infrastructure as a service is becoming a backup target for licensed software, either by design or customer initiative. However, adopters should ensure that overall costs are not compromised by egress (restore) charges. Organizations leveraging outsourcing and SaaS are comfortable with not owning the technologies used to enable their solutions. Some internal IT organizations will become contractors/brokers, managing not only their own IT, but also multisourced IT services from the cloud. IT leaders in enterprise ROBO, departmental and endpoint (desktop/laptop) environments and especially midmarket IT organizations, likely will back up these workloads to the cloud first.

*Recommendations:*

Move ROBO, desktop/laptop and departmental, and especially midmarket backup workloads to the cloud.

Mitigate risk and improve data availability by using a service as an additional, or disaster recovery, copy for on-premises backup as a potential solution. However, both total cost of ownership (TCO) over time and egress fees must be examined when evaluating these services.

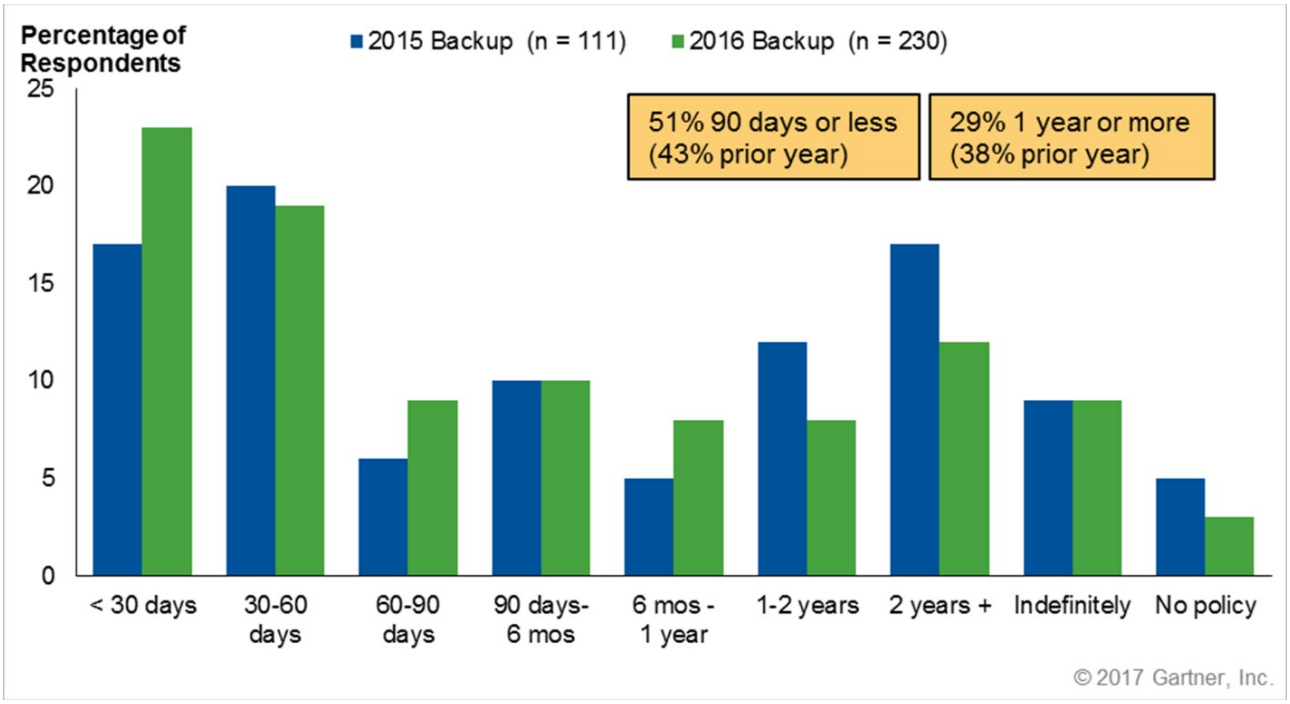
Assess the criticality of data you would like to move to a cloud or SaaS site before implementing the process, and pilot a cloud-based backup project using less-critical data.

**Storage managers can save money by backing up less data and retaining backup data for shorter time periods**

Many organizations are striving to find ways to better protect data, which often includes capturing a copy of the data more frequently (as in more than once a day, perhaps hourly to every few hours). However, some data may not warrant the current backup policy, much less an improved recovery point objective (RPO). In these cases, due either to the low business-criticality of the data or the very low change rates of the data, we recommend less-frequent backup. Most backups are used for short-term operational recovery. Many recoveries are used to satisfy restore requests for data that was created recently or just deleted, or corrupted from a virus. In each of these cases, the latest data is being recovered, making longer retention of earlier backups unnecessary.

At the 2016 Gartner Data Center and Infrastructure and Operations Management Conference, 51% of the respondents to a survey regarding data retention indicated they are keeping backup data for 90 days (one calendar quarter) or less (see Figure 3). The trend toward 60-day and 90-day retention has been steadily increasing during the past ten years, according to Gartner surveys.

**Figure 3.** Backup Retention Timeframes: Retention for Backup Is Slightly Shorter Than One Year Ago




Question: Which of the following time frames best describes your organization's backup retention policies?

*Source: Gartner (February 2017)*

Unfortunately, we also still see organizations keeping backup data for more than two years. We recommend that data over one year old be moved, ideally to an archive product to provide a long-term records retention solution. An alternative is to examine storage tiering and storage-native (i.e., self-protecting storage) solutions (see "Can 'Self-Protecting' Storage and Hyperconverged Systems Replace Traditional Backup?" ).

*Recommendations:*

Deploy a layered or tiered backup and recovery approach, possibly backing up the lowest tier less frequently. Perform fewer full backups for static data, such as every two weeks, or even monthly instead of weekly.

Re-evaluate your data protection plan. If the primary goal of the backup strategy is to satisfy operational recovery requests, then reduce backup retention times to 90 days or 120 days. However, understand that recent malware and ransomware threats may make backup retention below 30 days or 60 days a risky consideration (see "Use These Five Backup and Recovery Best Practices to Protect Against Ransomware" ).

Even if there are operational reasons to keep longer-term copies of application data or month-/quarter-/year-end data, evaluate running a separate backup job and retention policy for that subset of data, so that all data is not subject to the elongated retention.

Deploy an archiving solution to capture and manage static data, or data that needs to be retained longer than one year.

## Evidence

[1] Our research is based on more than 1,000 client interactions conducted annually regarding how I&O leaders and storage managers back up and protect their data. We also polled nearly 200 Gartner clients at the 4Q16 Gartner Data Center and Infrastructure and Operations Management Conferences in the U.S. and Europe on their backup and storage methodologies.

firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity. (/technology/about/ombudsman/omb_guide2.jsp)"

---