

Backup and Disaster Recovery Modernization Is No Longer a Luxury, but a Business Necessity

John P Morency, Donna Scott, Dave Russell

For the first time, Gartner's CIO Survey included business continuity management (BCM), inclusive of disaster recovery and backup, as one of the business strategy priorities. As IT continues to modernize more business processes, IT resilience becomes all that much more critical to provide the required uptime of systems and applications.

Key Findings

- Business process transformation and increased visibility of worldwide disasters, and their impact is driving business demand for increased IT resilience.
- In the most recent Gartner CIO Survey, 87% of respondents had recovery time objectives (RTOs) of four hours or less for their mission-critical applications and services.
- Backup/recovery improvements and modernization remain a large end-user client inquiry topic, and they come out near the top in polling regarding overall data management priorities for 2011.
- BCM maturity is improving; more than 50% of respondents still have not achieved Level 3, which we consider "good enough" maturity.

Recommendations

- Invest in IT disaster recovery management (IT DRM) modernization to meet increasingly stringent business resilience requirements.
- Invest in classifying applications and services based on mission-critical requirements to develop appropriate recovery tiers that balance risk mitigation with affordability.
- Charter a backup modernization initiative to assess current recovery capabilities, scope present and future recovery requirements, and prepare enhancement service options to be addressed.
- Look to deploy, or more fully deploy, recent proven backup products, such as incremental forever or synthetic full processing, deduplication, server virtualization improvements, and snapshot and replication integration.

- Evaluate your IT DRM maturity level using Gartner's ITScore for BCM. If you score at Level 1 or Level 2, then invest to achieve a minimum of Level 3.

ANALYSIS

While CIOs have many business strategy priorities, including increasing enterprise growth (moving more of the IT budget from run the business to transform and grow the business), improving business continuity, risk and security came in at No. 10 in the 2011 Gartner CIO Survey, as published in "Reimagining IT: The 2011 CIO Agenda" (see Figure 1). In this year's survey, 2,014 CIOs responded, representing more than \$160 billion in CIO IT budgets and covering 38 industries in 50 countries. This goes to show that while growth and cost reduction projects are critical (and dominate the top 10 list), CIOs also want to ensure that their initiatives don't bring additional risk exposure to the enterprise. While the survey crossed all industries, some industries in particular see business continuity (inclusive of backup and disaster recovery) and risk management as key to achieving their business objectives — such as in healthcare, where they are moving away from paper records, or in financial services, where IT makes up a significant portion of business processes and products. As a result, resilience is seen as a means for business growth, not just as an insurance plan. In addition, interest stems from the increased visibility of worldwide disasters in 2010 and 2011.

Figure 1. Top CIO Business Strategies for 2011, and Projected for 2014

Business strategies place a new emphasis on growth

Business Strategies	Ranking of Business Strategies CIOs Selected as One of Their Top 3 in 2011 and Projected for 2014				
	2011	2010	2009	2008	2014
Increasing enterprise growth	1	*	*	*	1
Attracting and retaining new customers	2	5	4	2	3
Reducing enterprise costs	3	2	2	5	6
Creating new products or services (innovation)	4	6	8	3	4
Improving business processes	5	1	1	1	13
Implementing and updating business applications	6	*	*	*	12
Improving technical infrastructure	7	*	*	*	7
Improving enterprise efficiency	8	*	*	*	10
Improving operations	9	*	*	*	2
Improving business continuity, risk and security	10	*	*	*	23
Expanding into new markets and geographies	11	13	10	4	5
Attracting and retaining the workforce	12	4	3	6	8
Introducing and improving business	15	15	*	*	9

Source: Gartner (August 2011)

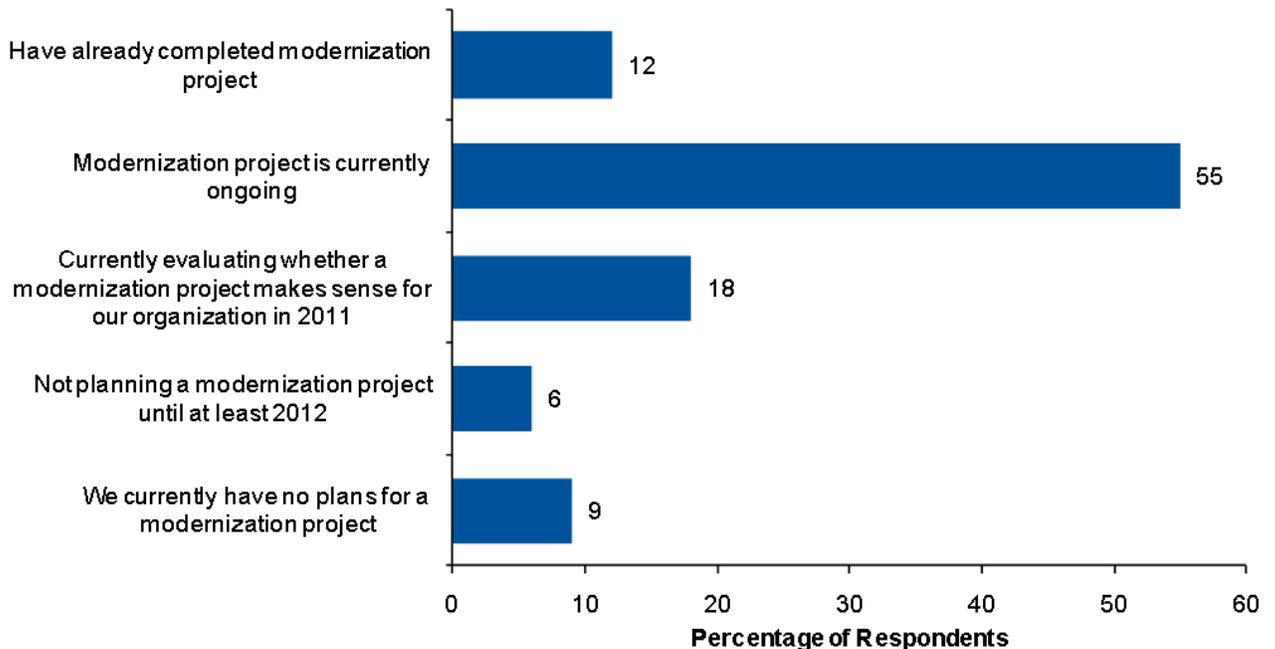
In December 2010, we surveyed our Data Center Conference attendees on the topics of IT DRM and backup, and found significant activity in support of the Gartner CIO Survey results.

IT DRM Modernization

Once considered either an afterthought or a very expensive insurance policy for a low-probability event, IT DRM is increasingly becoming an important data center initiative and an ongoing optimization priority for many client organizations.

During the past year, Gartner has seen a significant increase in both interest in and implementation of IT DRM modernization initiatives, based on the frequency with which the topic has come up in client inquiries and on-site workshops. The polling results, collected during Gartner's 2010 U.S. Data Center Conference session called "Operations Resilience: How Achievable Will It Be?" and depicted in Figure 2, showed that client implementation of related modernization projects was consistent with our survey results on BCM/IT DRM maturity, and that 12% of the session attendees had completed this specific initiative. As the results show, 55% of respondents are currently pursuing modernization, suggesting that the CIO focus enabled funding and implementation of IT DRM modernization. At present, it appears that most modernization projects for large enterprises focus on the logical extension of the in-house IT infrastructure, rather than leveraging public cloud services for disaster recovery outsourcing (due to security issues, as well as the maturity of the external solutions).

Figure 2. Progress on IT DRM Modernization



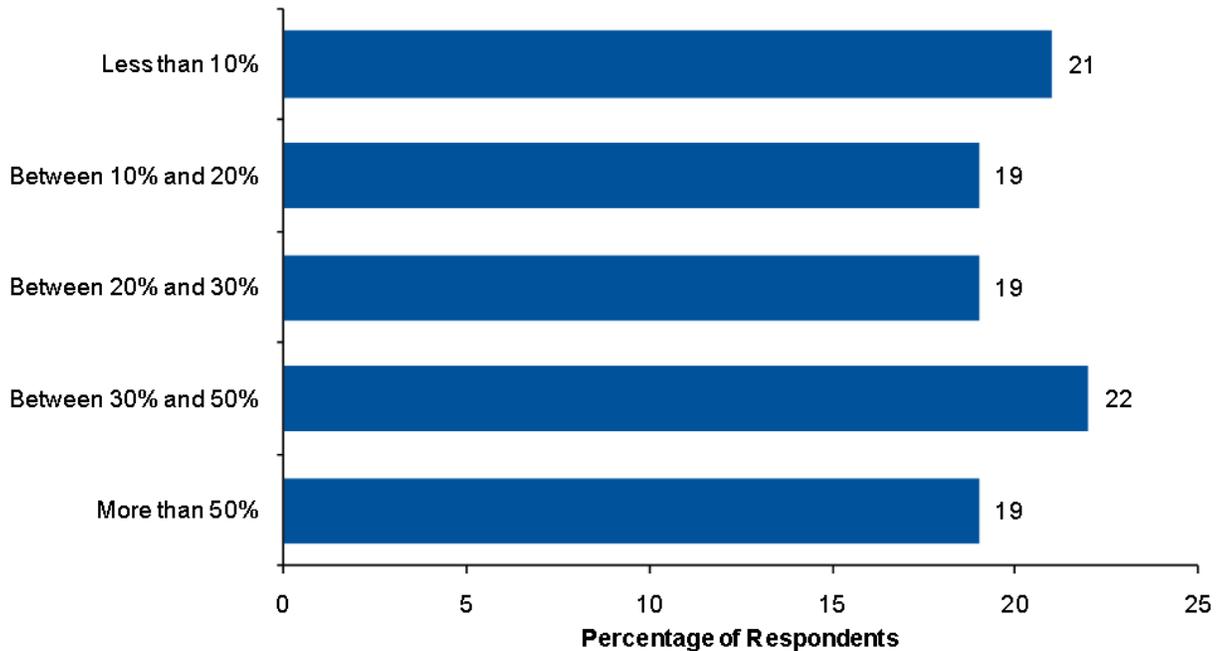
Source: Gartner (August 2011)

Proportion of Applications That Are Mission-Critical

Historically, the proportion of an organization's applications that it deems mission-critical has been between 10% and 20% of the overall portfolio. By categorizing and better understanding how applications are used in business processes, and how critical they are to the revenue, safety, operations, regulatory requirements and productivity of the business and staff, an enterprise can better prioritize its spending on IT resilience (to meet disaster recovery and IT service availability requirements). Best practice points to spending more money on the 20% that is mission-critical and less on the 80% that isn't, to reduce or eliminate the impact of an outage on the business.

As shown in Figure 3, however, the proportion of applications and services deemed mission-critical has risen for many enterprises. A plurality of 40% of enterprises in our most recent survey indicates that 20% or fewer of their applications/services are mission-critical. Of the audience, 60% has more than 20% of their applications/services categorized at the highest level of criticality, split fairly evenly between 20% and 30%, 30% and 50%, and more than 50%.

Figure 3. Proportion of Applications or Services That Are Mission-Critical (n=91)



Source: Gartner (August 2011)

When we see the proportion of applications/services rising toward the 50% level (or more), the reasons include:

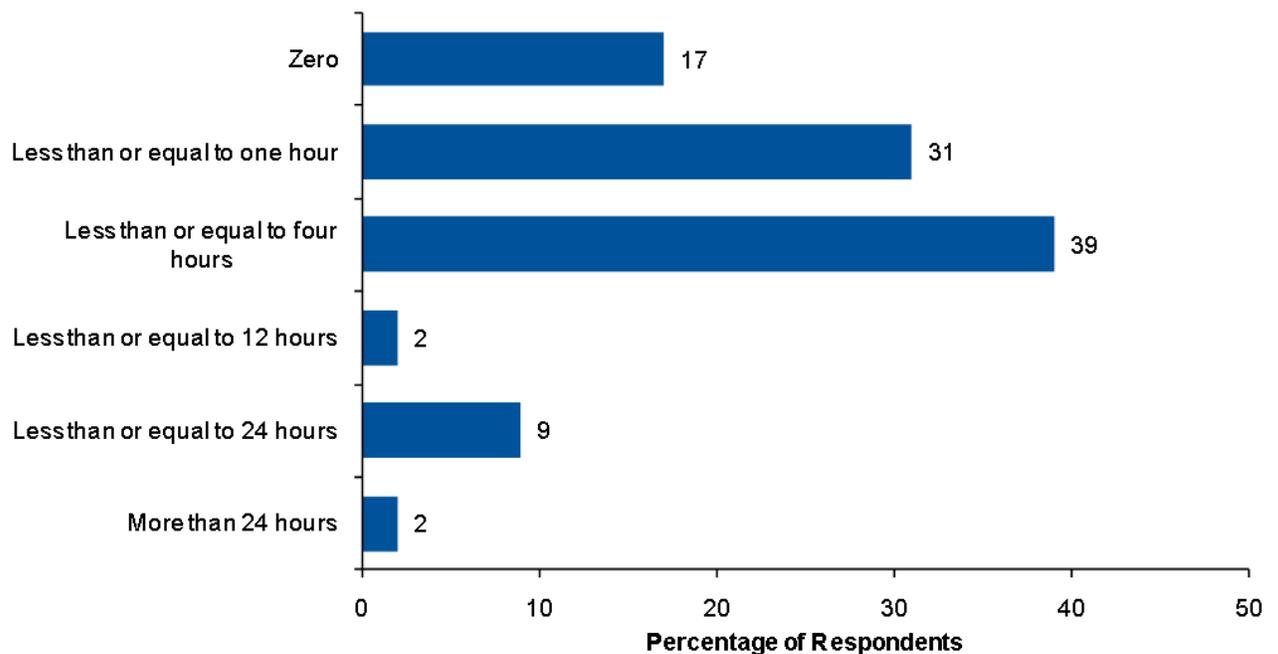
1. The enterprise has consolidated and rationalized business processes, and has integrated or retired a greater number of applications/services to meet business requirements, and, therefore, has fewer "stragglers" or legacy applications that are non-mission-critical.
2. The enterprise has not consolidated and rationalized applications, but has otherwise integrated mission-critical with non-mission-critical applications/services in a way that requires them all to be operating, lest they impact the business in an outage.
3. The IT organization does not know what is mission-critical; the business tells it that nearly all applications/services are vital to operations, and the IT organization manages based on those assumptions.

The main implication for rising mission criticality is the additional cost associated with resilience. If an enterprise deems all its applications/services as mission-critical, then it may not be able to afford to protect them against the impact of an outage. This is especially true for organizations that fall into the category of No. 2 and No. 3 above (that is, they have not consolidated and rationalized their applications/services, and, therefore, they are spending too much money protecting non-mission-critical applications/services, and likely not enough on those that are truly mission-critical).

RTOs of Top-Tier Applications/Services Are Shortening

RTOs have been reduced for many years, as a result of the integral nature of IT in many business processes. In our most recent survey (and as shown in Figure 4), 87% of the enterprises surveyed have RTO for their most mission-critical applications/services as four hours or less. This is up from 73% in the survey we conducted just one year earlier, in December 2009. The cost implications are significant, especially for the 48% of enterprises that have an RTO of between zero and one hour. Very short recovery times of one hour or less require not just fully redundant alternative environments (to which to failover in the event of an outage or disaster), but also require that they be active or standby — meaning that they cannot be used for other purposes during normal operations.

Figure 4. RTOs of Mission-Critical Applications (n=93)



Source: Gartner (August 2011)

Enterprises that optimize on cost and reduce their RTOs to two to four hours can generally share their disaster recovery environments with another purpose, and, therefore reduce their overall capital investment requirements. In the case of an outage or disaster, the less critical work would be shut down (often, this is in development and test environments), and a reconfiguration would make the environment look like the production applications and services.

There is an additional implication for the 17% of enterprises that indicated their RTO as zero — that they build their applications for multisite continuous availability (see "How to Calculate the Cost of Continuously Available IT Services"). Because packaged applications generally do not allow for active/active operations in two or more sites simultaneously, enterprises that require this level of resilience write their own applications and architect them from the beginning of the application life cycle, with full knowledge upfront of the applications, infrastructure and operational requirements.

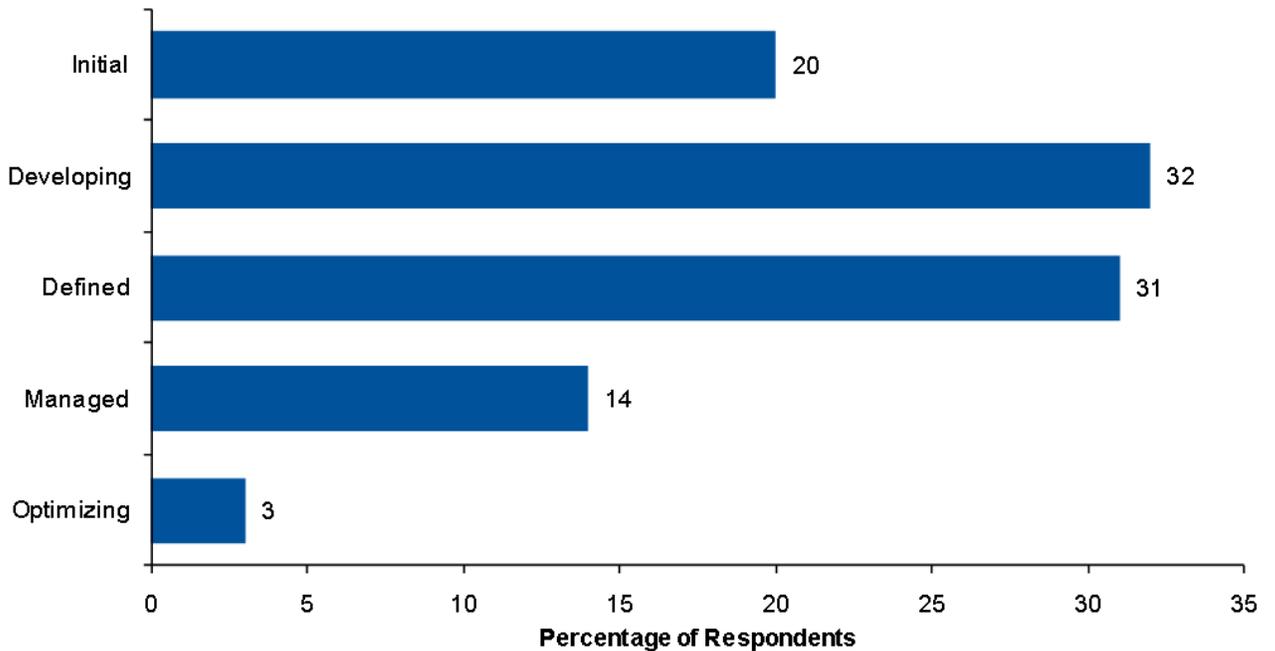
Maturity Level of BCM

For many of the reasons discussed previously, almost every enterprise needs to make a serious, sustained effort to advance recovery and continuity maturity levels. Maturing programs will move the enterprise beyond a traditional, narrow, IT-centric focus, and eventually beyond the IT organization itself. As these programs mature, they will embrace business recovery, contingency planning, crisis/incident planning, pandemic planning and emergency response, along with IT DRM. This is a long-term undertaking that requires serious commitment from senior executives and line-of-business leaders, and also from other internal stakeholders, ranging from the legal department to the HR organization and external partners.

Gartner has identified five BCM, backup and IT DRM maturity levels — aligned with our established maturity levels — that represent increasing capabilities. They range from Level 1 to Level 5, but it is not until Level 3 where there is formal responsibility for BCM, and repeatable recovery plan management and testing processes are in place (see "ITScore for Business Continuity Management"). For many IT organizations, Level 3 represents the minimum "good enough" level of maturity.

During the same operations resilience session in which the IT DRM modernization polling questions were asked, we asked attendees to rate the current maturity of their BCM/IT DRM program. Client maturity results from the ITScore database that is internally maintained by Gartner are shown in Figure 5, with the average maturity score being 2.38 (a result that is reasonably consistent with the 2.55 scoring average BCM/IT DRM maturity score, as well as with the overall maturity distribution). These scores point to the need to improve IT DRM maturity to a minimum of Level 3, which turns IT DRM into a set of repeatable processes instead of projects.

Figure 5. Current BCM/IT DRM Maturity Levels (n=35)



Source: Gartner (August 2011)

IT DRM Action Items:

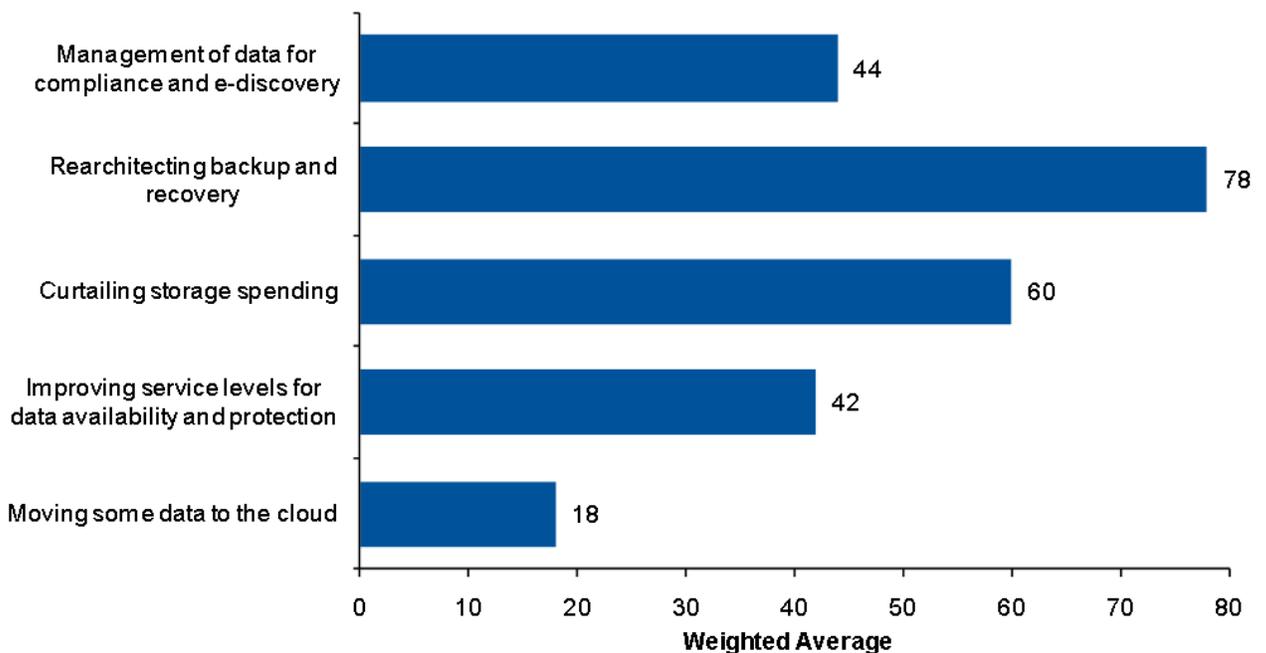
- Use Gartner's ITScore for BCM to assess your maturity levels. Improve your IT DRM maturity levels to a minimum of Level 3, which implements processes instead of projects, for long-term sustainability.
- To reduce IT DRM costs, do a realistic assessment of your IT service/application criticality levels. Invest more on higher levels of criticality and less on lower levels. Moreover, if your RTO is two to four hours, then look to share and repurpose infrastructure at the disaster recovery site to save capital costs.

Backup and Recovery Modernization

Backup and recovery is one of the oldest and most frequently performed operations in the data center. Nearly every organization is protecting its data with backup and disaster recovery technology and plans. In many cases, these plans and solutions have been in place for years, and they are no longer adequate to meet the required, much less the desired, availability levels.

At Gartner's December 2010 Data Center Conference, a session on data management was held. Audience polling in Figure 6 shows that, of all the data management options, rearchitecting backup and recovery was viewed as the top priority. Note that participants were allowed to choose their top three responses, in priority order, which yielded a weighted result. While cost containment is always top of mind, and compliance and the cloud have received a lot of press, backup improvements garnered the most first- and second-priority votes.

Figure 6. Rearchitecting Backup Is the Top Data Management Priority (n= 44)

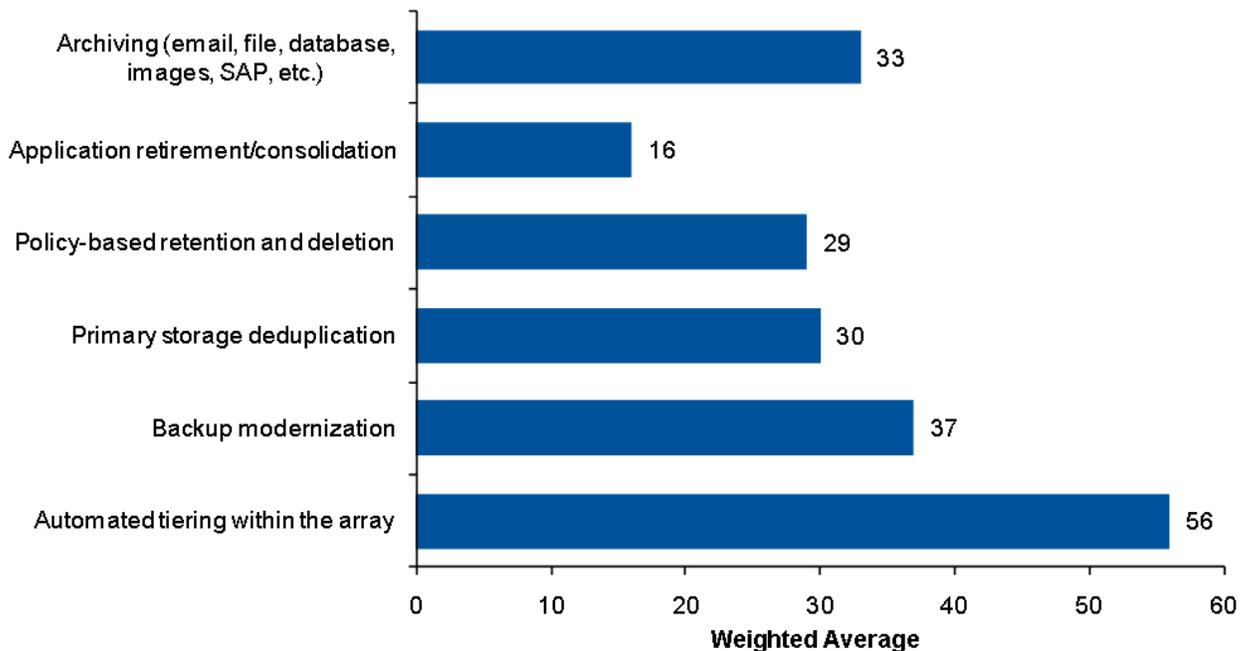


Source: Gartner (August 2011)

When the same audience was polled regarding which specific data management techniques and technologies were planned for implementation during the next year, only tiering in the storage array received more overall votes than backup modernization (see Figure 7). However, backup modernization was seen as a higher priority than archiving or primary storage deduplication. Note that the audience for the questions in Figure 6 and Figure 7 were not solely backup or even

disaster recovery management professionals; rather, they were storage managers and administrators who focus on a wide range of tasks, which further demonstrates that the need to modernize backup is being more broadly recognized as a top priority to ensure application and data availability.

Figure 7. Backup Ranks Near the Top for Data Management Implementation (n= 44)



Source: Gartner (August 2011)

Backup and Recovery Modernization Action Items:

- Charter a backup modernization initiative to assess current recovery capabilities, scope present and future recovery requirements, and prepare enhancement service options to be addressed. Most backup plans are aged and typically do not protect all critical servers and applications, and they may not meet the needed service-level agreement for the restore time.
- Look to deploy, or more fully deploy, recent proven backup products, such as incremental forever or synthetic full processing, deduplication, server virtualization improvements, and snapshot and replication integration. These features help to better protect the changed environment by shortening the backup window, reducing the capacity requirements for backup data and/or aiding in allowing for more recovery points.

RECOMMENDED READING

Some documents may not be available as part of your current Gartner subscription.

"Reimagining IT: The 2011 CIO Agenda"

"Best Practices for Addressing the Broken State of Backup"

"Use of Disk for Backup Accelerates at the Expense of Tape"

"Avoid the Grim Reaper Syndrome: Integrate Recovery and Resilience Into the Project Life Cycle"

"How to Calculate the Cost of Continuously Available IT Services"

"ITScore for Business Continuity Management"

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509