Gartner Research

Publication Date: 28 January 2009 ID Number: G00164903

Predicts 2009: Business Continuity Management Juggles Standardization, Cost and Outsourcing Risk

Roberta J. Witty, John P Morency, Dave Russell, Donna Scott, Robert P. Desisto

Our 2009 predictions are focused on these areas: (1) the growing interest in applying a standard approach to all recovery efforts through the use of organizational certification; (2) the need to make sound investments for recovery by using a layered recovery architecture approach; and (3) the disconnect between the desire to outsource operations through software as a service (SaaS) and cloud computing and the organization's ability to ensure it can recover from a service provider's outage.

Key Findings

- Few organizations are seriously pursuing organizational business continuity management (BCM) certification.
- More than 50% of large enterprises already implement layered recovery practices today, while less than a third of midsize organizations, according to our estimates, do the same.
- SaaS and cloud computing service providers are not addressing their customers' disaster recovery and availability needs.

Recommendations

- Decide if organizational certification is appropriate for your organization. Review requests received from customers and trading partners during the past three years to see if the need is sufficient to make the investment.
- Evaluate recovery strategies to meet service-level agreements (SLAs), and layer them accordingly to meet recovery time objectives (RTOs) and recovery point objectives (RPOs) for disasters and other incidents such as data corruption. Consider not only the capital costs but also the people costs in managing the solutions. Ultimately, there are trade-offs between risk and cost, so be prepared to negotiate with business process and application owners. In some cases, they may accept more risk and a lower-cost recovery, and in other cases, they will not.
- If a SaaS application is considered highly mission-critical, then consider adding contractual incentives and/or financial penalties to ensure that the provider is duly motivated to support your required service levels.

WHAT YOU NEED TO KNOW

Enterprises are having to juggle multiple requirements, such as standardization of process, cost optimization and increased risk due to the growing use of outsourcing, to ensure that organizational resilience is cost-effective and sustainable.

ANALYSIS

Strategic Planning Assumptions

Strategic Planning Assumption: By 2012, less than 10% of organizations will have received external certification of their business continuity management and IT disaster recovery programs. Those that do are either regulated to do so, or will be mandated to do so by their supply chain partners.

Analysis By: Roberta J. Witty

Key Findings: The growing visibility of BCM in boardrooms around the world is putting considerable attention on the development of a best-practice model for BCM methodologies, terminology and so forth. Another outgrowth of this focus is the notion of organizational certification of their BCM and IT disaster recovery management (DRM) capabilities — from response to recovery to restoration of business and IT operations, as well as program management and governance. The United States has started a certification effort through Title IX of "Implementing Recommendations of the 9/11 Commission Act of 2007" (aka H.R. 1 and Public Law 110-53) report, which tasked the Department of Homeland Security (DHS) to develop a voluntary certification program for private enterprises on emergency preparedness and business resiliency. British Standard (BS) 25999 also has an organizational certification component that has gotten more attention during the past few years, primarily in the U.K.

However, there is much controversy about organizational certification for these reasons:

1. It is an expensive proposition requiring an initial investment and then regular updates to the certification received for every product, service and location involved.
2. Some industries are already required through regulation to provide recovery capabilities for certain parts of their operations — for example, commercial and investment banking, healthcare, utilities, and the nuclear industry. Therefore, obtaining yet another assessment is a duplication of work and a needless expense.
3. No one set of criteria can be used to demonstrate adequate preparedness and recovery program capabilities across the globe. This point is especially important for multinational organizations that may be dealing with recovery standards from many jurisdictions in which they operate (see "Hype Cycle for Business Continuity Management, 2008" for a list of international recovery standards).
4. Small and midsize organizations can least afford to make the investment in recovery planning and management programs and solutions on their own. Thereby, this potentially skews the supply chain to larger providers and removes the entrepreneurial ethos in the worldwide free market, unless governments and the largest supply chain partners provide financial assistance.

5. Some firms are concerned that, if they expose their recovery and availability deficiencies, they might be subject to legal recourse for loss of life and limb, as well as commercial losses incurred by trading partners and customers.

Market Implications: The area on which organizational certification will have the most impact is the supply chain: A larger organization, such as a multinational retailer, a national security provider or a multinational financial services provider, requires its outsourced business partners to provide evidence that they can meet the recovery requirements of the larger organization. There are several reasons why the larger organization has a need to acquire this evidence:

1. Many are required by regulation or contract to provide a certain level of service to their customers, and a breach in these agreements can mean financial penalties.
2. The reputation of the organization is at stake for many (but not all). Customers can change to another service provider if a service is not available when the customer needs it.
3. The larger organization has a stake in being in business for the long term and, therefore, wants to ensure its viability.

Another supply chain area where organization certification is a high probability is the IT service provider market. Information security services; hosting, co-location and cloud computing services; and application SaaS services are leading areas where a prospect or customer should require evidence that the vendor can meet recovery requirements.

Albeit national security is the professed goal of the U.S. initiative, the DHS initiative has seen missed deadlines in the assignment of the oversight body, controversy from industries that are already regulated and have mature recovery programs in place, and conflicts between industry players that are already providing expert content. An additional complicating factor is the transition of government administration to President Barack Obama's administration. Many DHS officials will be leaving their posts due to the administration change, and therefore, the new officials may have a different set of priorities.

Obtaining certification will require consulting services and the resulting external financial expenditure, for the initial certification, as well as in the ongoing maintenance of that certification. Spending this money may be a challenge for many organizations in today's economic climate, thereby reducing the number of organizations that can make the business case for obtaining certification. To date, few consultancies have been certified to conduct an organizational certification. For example, BS 25999 certification in the U.K. can be obtained only through BSI and Lloyd's. In the U.S., a handful of consultancies (Perry Johnson Registrars of Detroit is one) have this certification from BSI. NFPA 1600, the Standard on Disaster/Emergency Management and Business Continuity Programs (2007 edition, U.S.), does not yet have a certification component. However, the Title IX initiative may become that vehicle for NFPA 1600.

Recommendations:

- Decide if organizational certification is appropriate for your organization. Review requests received from customers and trading partners during the past three years to see if the need is sufficient to make the investment.
- Determine what and where within your organization would require organizational certification — for example, which products, services and locations will need to be certified.
- Prioritize the organization certification schedule, based on the largest revenue provider or regulatory requirement.

- If your organization has already been reviewed for disaster preparedness and that review has been used successfully by a customer or trading partner to assess your organization's ability to meet its recovery requirements, then ask future customers, trading partners and prospects to use the same review. There is no reason to waste money in getting a review every time you are asked for one if you have already proven your capabilities. In the new Title IX process, this reuse process is referred to as an "attestation."

- Small or midsize businesses (SMBs): Ask your supply chain partner how it can support your organization's ability to meet the recovery requirements you are being asked to comply with. This support can come in several forms: direct recovery financial support or angel funding to company operations as a whole (which is likely available only for SMBs that are providing a unique product or service to the partner); expert guidance through the transfer of knowledge between the partner's recovery staff and the SMB; or a combination of both.

- There is no emerging leader from the long list of BCM standards and frameworks, and Gartner does not predict that one will predominate worldwide. There will be pockets of acceptance by organizations, depending on the industry and the geographic location. Because no single model has been agreed on (although ISO plans to issue a final BCM document within the next 12 to 14 months), no single set of audit standards can be used for business continuity in the same way that specific auditing standards such as Public Company Accounting Oversight Board's (PCAOB's) Auditing Standard No. 5 has been defined for regulations such as the Sarbanes-Oxley Act's Section 404, Health Insurance Portability and Accountability Act (HIPAA), and PCI Security Standards Council. Therefore, organizations should take the following actions to develop their own recovery framework:

    - Review several existing models, and develop your own BCM model, based on appropriate industry and country regulations and standards. Using multiple references will provide a broader view of BCM to assist in developing a program that is applicable to your organization's business needs.

    - Find out which models your external auditors are using for audit work. Auditor alignment should be a consideration when selecting an enterprise framework.

    - Nonregulated U.S.-based organizations: Follow the work being done in relation to U.S. Title IX to understand how it might influence your models.

    - Due to the lack of a single model and a supporting audit framework, the only means by which organizations can assess the effectiveness of recovery and continuity controls is through the use of tabletop and live testing that best supports the operation's risk mitigation objectives.

    - Use the Gartner BCM Activity Cycle and maturity self-assessment tool to help manage your own BCM programs, as well as assess the current level of recovery or preparedness maturity. Build a road map to improve maturity during the next five years.

Related Research:

"Hype Cycle for Business Continuity Management, 2008"

"Activity Cycle Overview: Business Continuity Manager Role"

"Toolkit: Risk Program Maturity Assessment 1.2"

Strategic Planning Assumption: By 2013, more than 50% of midsize organizations and more than 75% of large enterprises will implement layered recovery architectures.

Analysis By: Donna Scott and Dave Russell

Key Findings: Layered recovery architectures define methodical strategies for meeting IT service recovery requirements based on service levels. More than 50% of large enterprises already implement layered recovery practices today, while less than a third of midsize organizations, according to our estimates, do the same. We are predicting a 50% increase in growth of these architectures due to the following reasons:

- Dependency on business systems has increased, with business costs of downtime escalating across all industries.
- Many organizations cannot afford a "one size fits all" recovery strategy tied to the requirements of their most critical applications, especially because an increasing number of applications are becoming Tier 1. As a result, companies implement a layered recovery strategy to contain costs and match the quality of service to the criticality of the IT service.
- The length of time to recover data from tape often takes 24 hours or more, and does not meet escalating business requirements for business system availability.
- The increasing trend toward more-granular application or business system recovery (versus a complete site failover for disaster) enables a more custom and selective approach toward the recovery of critical business systems.
- The implementation of recovery SLAs or targets is driving more-systematic analysis of and implementation of an architecture that matches appropriate recovery solutions with the criticality of business systems.

Market Implications: Enterprises will become more systematic about designing recovery architectures to meet specific recovery objectives that are based on the tiering of mission criticality associated with business systems (which is usually determined during a business impact analysis). Recovery architectures will often consist of between three and five levels. An example of a recovery architecture's levels is shown below:

1. Real-time replication (synchronous or asynchronous). Note that sometimes this is broken up into two tiers — one for synchronous replication and one for asynchronous replication.
2. Snapshot-based replication, or point-in-time replicas.
3. Disk-based backup.
4. Tape-based backup.

Matching recovery architectures to IT service criticality (and the associated service levels) allows enterprises to better match service delivery costs to the service levels required. For example, using real-time replication with its higher cost of service delivery for non-mission-critical IT services will increase the cost of recovery over alternative methods. As a result, enterprises following this approach will better be able to balance risks versus costs and to optimize the costs spent on recovery services.

Contrary to market hype, tape-based backup solutions will remain nearly ubiquitous — but they will be used for catastrophic recovery only in the upper tiers of business criticality (for example, when the other recovery methods do not work), or they may be used as the primary means of

recovery for the lower tiers of business system criticality. Disk-based recovery is faster and will typically be used as the primary means of recovery for lower tiers of business system recovery, while real-time replication or snapshot-based replication will be used for the most critical business systems requiring shorter recovery times (generally, less than 12 hours). Note that these recovery strategies are not mutually exclusive. For example, an enterprise may use real-time replication as its primary method of recovery, but also use point-in-time replicas in case of data corruption and tape-based backup for catastrophic recovery requirements.

The increased focus on recovery and the fact that every enterprise needs recovery solutions will keep investment and products flowing in the replication and recovery markets. There will continue to be intense competition from replication and backup suppliers, in both the software and hardware businesses. We do not see consolidation occurring and, in fact, expect even more market fragmentation to occur as database and application system vendors give market preference to their solutions over that of more generic storage-based solutions.

Recommendations:

- Perform a business impact analysis (BIA), and review it annually to determine the criticality of your business systems. Tier them into three to five categories, and associate recovery service levels to each tier (that is, RTO, RPO, availability and mean time to repair).
- Evaluate recovery strategies to meet SLAs, and layer them accordingly to meet RTO and RPO for disasters and other incidents such as data corruption. Consider not only capital costs but also the people costs in managing the solutions. Ultimately, there are trade-offs between risk and cost, so be prepared to negotiate with business process and application owners. In some cases, they may accept more risk and a lower-cost recovery, and in other cases, they will not.
- Expect that many vendors will begin to offer layered recovery and unified recovery management solutions. We advise clients to engage with a competitive RFP and bid process and possibly even review current products if running older versions to determine if there is the opportunity to leverage the competitive market to obtain a better deal by switching to a new vendor.
- Don't give into the hype on the demise of tape. Although disk-based backup is widely used and growing, enterprises need an off-network storage medium to protect against sabotage and multiple points of failure or disaster.

Related Research:

"Rabobank Group Benefits From Strategic Data Center Planning"

"Recovery Will Move to Disk-Based, Manager of Managers Approach by 2011"

"Best Practices for Conducting a Business Impact Analysis"

Strategic Planning Assumption: By 2012, less than 20% of today's SaaS and cloud computing vendors will offer customers a combination of disaster recovery service-level guarantees.

Analysis By: Robert DeSisto and John Morency

Key Findings: Despite its obvious importance to service customers, Gartner believes that only a minority (less than 5%) of SaaS and cloud computing vendors will be positioned to support the

combination of disaster recovery service levels that will collectively define a worst-case application service outage duration that is independent of disaster event severity.

The primary reasons are the following:

- The lack of recovery-centric service levels offered by providers today (that is, RTOs and RPOs).
- The relatively immature stage of the server and storage virtualization management technology that is needed to support this class of customer-specific service-level granularity.
- The lack of an agreed-on business model for competitively pricing subscriber-specific recoverability guarantees.
- Methodologies that define systematic and repeatable disaster recovery test procedures that can be executed on a per-application and per-subscriber basis are virtually nonexistent at this time.
- Often, SaaS applications are not architected to support automated or semiautomated failover application and data recovery between a primary production data center and secondary recovery data center.

Market Implications: Today, most SaaS and cloud computing providers have well-defined, documented and tested business continuity plans in place for recovering their data center facilities and infrastructure. However, policies that govern the delivery of subscriber-specific RTO or RPO service levels often do not exist.

The lack of these policies is creating service subscribers' increased operations risk. For one thing, recoveries for mission-critical business processes that depend on Web-based applications and data often need to occur on the order of hours (or, in some cases, even in minutes) instead of days. This is true for internally developed Web applications, as well as those delivered as a service by external providers. Complicating support for this requirement is the fact that, unlike their mainframe- and minicomputer-based predecessors, Web-based applications are inherently more distributed, making both recovery testing and the recovery process itself far more challenging. Effective recovery testing for service-oriented-architecture-based applications is an even greater challenge. The result is that the enterprise IT organizations that can claim in-house support for this new generation of recovery-centric service levels are a very small minority.

This lack of support creates a new market differentiation opportunity for both SaaS and cloud computing vendors. For both large and small disaster recovery providers, however, supporting this requirement is more a matter of industry survival. As a result, the required provider policy, management software technology and provider operations procedure changes will happen because both large (for example, SunGard) and not-so-large (for example, IPR International) disaster recovery service providers are already addressing this survival issue head-on. In the case of SunGard, its Advanced Recovery services now include support for specific RTO-based service levels that range between four hours and 12 hours. IPR's Assured Recovery Services support five separate recovery tiers with RTO guarantees that range from a low of one hour to a high of 72-plus hours.

As a result, these and other providers are already offering or will soon begin to offer application-centric service-level guarantees as part of their next-generation service offerings. Because this will competitively impact the businesses of some (but not all) SaaS and cloud computing providers, these providers will need to support comparable service guarantees or risk losing customers to disaster recovery providers that also look to becoming SaaS or cloud computing

vendors to expand their service portfolios. Highly visible incidents such as the customer impact that resulted from the recent service outage of Google's enterprise e-mail services for several hours will also increase the market visibility of what can result when these service guarantees are not in place.

The provider management changes that are required will result in only a relatively small number of existing SaaS or cloud computing vendors offering support. However, these providers are far more likely to be the larger vendors (the 5% of the providers that have the majority of market share), which provide sustainable service-level support during the next 24 to 36 months.

Recommendations:

When considering the use of SaaS:

- Before making contractual commitments to any SaaS provider, ensure that you have a complete understanding of the provider's recovery management procedures and managed service levels that address the key questions contained in this research.
- Do not rely on the provider's claims that SAS 70 Type 2 certification is sufficient to address your specific recovery requirements. Take the extra time to learn whether the provider's recovery procedures and supporting operations management software will be sufficient to support the specific recovery objectives required by your business.
- Consider adding contractual incentives and/or financial penalties to ensure that the provider is duly motivated to support your required service levels, especially for mission-critical applications.

Related Research:

"Critical Recovery Questions to Ask SaaS Providers"

"Google E-Mail Outage Stresses SaaS/Cloud Services Vulnerability"

Note

Recently, Gartner conducted an independent survey of its clients. Your direct feedback is underpinning the activities we have under way to continually improve our research. This year's Predicts report is one example of those changes.

You told us to simplify the number of different terms we use. In the past, we used two different terms to identify our most important statements about the future. We have standardized on one term — Strategic Planning Assumption (SPA) and we continue to use this nomenclature.

You told us that you value our research most when we are direct. Your confidence in our advice comes from the facts and assumptions we provide in supporting our positions. The numerical probabilities we used with SPAs outlived their usefulness, and we will no longer use numerical probabilities.

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
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner