AT&T Newsletter 5 – Business Continuity

Sponsor's introduction

Alex Parker - Vice President, Global Service Management AT&T

A survey of Gartner Symposium/ ITxpo 2011 attendees found that business continuity is one of the top two priorities for enterprise decision makers in 2012. (Source Schindler Technology, October 2011) Business and financial decision makers recognize that the consequences of any failure in business continuity can be disastrous in terms of customer service and satisfaction, reputation damage and financial cost. That makes continuity a strategic business issue, not a technical one, and involves all senior decision makers.

Major natural disasters such as floods, pandemics, civil unrest or other major events are becoming more and more frequent; in fact, 2011 was a record year, increasing the risk to business. However, many business failures result from problems in the supply chain, product recalls, compliance issues or day-to-day incidents and small disruptions such as data corruption, computer viruses, network problem or workplace inaccessibility. The causes are less dramatic, but the consequences can still be extremely serious.

The first six months of 2011 saw $265 billion in economic losses due to natural disasters, well above the previous record of $220 billion. (Source msnbc.com) That's why it pays to be prepared, with a business continuity plan that ensures the availability of critical services, processes and operations. The aim of a business continuity plan is to reduce risk and ensure continued financial and competitive success by supporting strategic and tactical resilience across an organization. With the right plan in place, your organization can continue working in the event of a disaster and make an orderly recovery and resumption of normal working.

Multinational organizations can spread the risk by implementing business continuity on a global scale. Technologies such as mobility and virtualization enable global operations to continue, regardless of a disaster in a specific location. With a global business continuity plan, your organization becomes less dependent on local facilities.

Organizations that have survived a disaster and recovered quickly demonstrate their strengths to stakeholders. As a result, many have seen their stock value increase by 15-20 percent compared to what it was before the disaster. (Source Business Continuity Institute)

The level of threats is increasing and risk, vulnerabilities and consequences increase. The risks are just too high to ignore. To ensure survival, I would urge our customers to act now to put a strategy in place and embed continuity in business processes. If you look at the time, money and effort invested in business continuity by AT&T, customers of our network and IT services should be able to sleep a lot better than their competitors.

Alex Parker, Vice President, Global Service Management, AT&T

Why business continuity matters

Business continuity is significantly different from disaster recovery. Business continuity is a proactive strategy that aims to protect your organization by identifying, anticipating and minimizing risks, rather than responding to incidents after the event.

A proactive strategy is essential because your organization faces threats or events from many different sources – direct and indirect. The business continuity landscape highlights four areas of risk - major events, business issues, data problems and location dependency.

Incidents take many different forms

Major events that affect business continuity include external factors such as the impact of terrorism, civil unrest, natural disasters or pandemics, as well as internal problems such as power failures, data center loss or building fires. Japan, already badly hit by the explosion at a nuclear plant in 2011, faces the risk of a major earthquake hitting the key business centre of Tokyo in the next few years. Although major events of this type are relatively infrequent, the financial consequences are extremely high.

Business issues resulting from poor management can also pose a serious threat to continuity. A lack of governance, failure to meet industry standards or comply with regulatory compliance can impact your organization's ability to continue trading, while an inaccessible workplace, product recalls or problems in the supply chain can cause severe disruption to production and customer relationships.

Protecting your data and your information systems is key to business continuity. The increasingly frequent and sophisticated threats from viruses and worms together with network problems, server failures and application outages can disrupt your operations with consequent impact on organizational efficiency, productivity and competitiveness, as well as business continuity.

Organizations with multiple sites face the risk of location dependency if they only develop local continuity plans. Without a global strategy, major disruptions at one site can impact the whole organization if the plan does not support access to resources in other sites, for example.

The wide-ranging risks mean that a company-wide business continuity strategy is essential. Failure to protect the business against even minor disruptions can have serious consequences. Estimates from IBM indicate that problems with data can incur direct financial costs up to $100,000 per incident, while a single business-related issue could cost up to $10 million. Major events have the potential to inflict consequential costs in excess of $100 million in extreme circumstances. (Source IBM) Disasters also have serious potential consequences through loss of income, damage to reputation and customer confidence and, ultimately, an inability to continue business.

In certain industry sectors,

> *Risk = Threat x Vulnerability x Consequence*

regulators have recognized the critical importance of business continuity and have made it mandatory for organizations to develop robust business

Figure 1: Crisis/Incident Management Program Scope: Event Types

Direct
Accident
Power Outage
Fire
Explosion
Terrorism
IT Outage
Natural Disaster
Pandemic
Supply Chain Disruption
Workplace Violence

Indirect
Product Recall
Product Poisoning
Financial Fraud
Customer Dispute
Executive Fraud
Government Investigation
Kidnapping

Source Gartner: Crisis/Incident Management Defined, 2012, Roberta J. Witty, January 2012

continuity plans. These include Sarbanes-Oxley across all sectors, HIPAA in the healthcare sector and Basel II in financial services. Insurers too are demanding that clients prepare business continuity plans; those who don't face major increases in insurance premiums.

Disasters caused by major external events

Major events like floods or a pandemic can lead to travel restrictions, absenteeism, supply chain disruption, infrastructure damage and other logistical problems that put severe pressure on business continuity.

When organizations suffer a disaster that affects an entire region, effective communication and collaboration are vital elements of a business continuity plan. By maintaining continuity of communication, organizations can keep employees, customers, suppliers and other stakeholders informed and up to date with changing circumstances. A global infrastructure solution is also vital for maintaining continuity. Access to globally-distributed services means that infrastructure and support teams are more resilient against events that impact an entire region.

Telepresence solutions – the latest HD videoconferencing technology – are starting to play a key role in this type of scenario by enabling executive teams to maintain continuity of operations during a disaster or when travel is restricted. Participants from various locations participate and behave in virtual meetings as if they were present. This improves the quality of the meeting and the decisions that are made. Telepresence supports executive-level meetings with customers, suppliers, partners, colleagues and business partners, regardless of any disaster or other major problem.

High-quality collaboration with strategically-important stakeholders ensures continuity of critical external, as well as internal operations. It is particularly important, for instance, for maintaining supply chain operations in a business environment that is increasingly interconnected and interdependent.

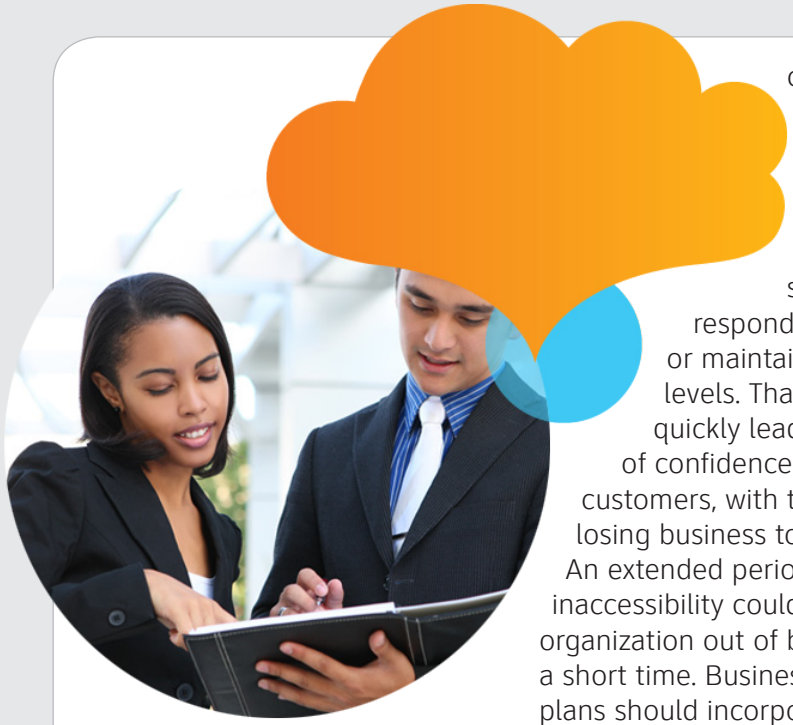
When a major disaster strikes, it's also essential to enable managers and employees to continue working and collaborating to maintain project continuity and effective decision making. Travel restrictions and other logistical disruptions make it difficult for employees to access the normal workplace. However, increasing levels of mobilization and the growing sophistication of mobile devices mean that employees can continue to work remotely regardless of location, improving business continuity. Smaller telepresence units, for example, enable home-based employees to collaborate with the same level of efficiency

Web conferencing also plays an important role in maintaining productivity and collaboration. In the event of a disaster, a CEO could follow up a crisis meeting by telepresence with text messages to all employees to check that everyone is okay. The CEO could then update employees with a message broadcast via web conferencing. While recovery was underway, employees could continue working via web conferencing.

By using global managed services to deliver unified communication and collaboration tools, organizations can quickly scale levels of home working and virtual team meetings. Employees working remotely can also access globally-consistent infrastructure and services to maintain their productivity.

When Japan suffered the double disaster of a tsunami and earthquake, a number of major corporations were forced to take emergency measures to maintain business continuity. AT&T worked with a global IT company based in Tokyo to relocate its mail servers and wireless facilities to a safer location so that it could restore services and set up conferencing and remote working facilities for employees. AT&T also helped a global consumer products company to quickly scale its existing remote access service so that more employees could work from home during the duration of the transport problems.

Cloud-based services and applications are playing an increasingly-important part in enabling home-based employees to continue working effectively. They provide the rapid scalability that is essential in the event of a disaster and give organisations the flexibility to set up effective, productive working arrangements without major infrastructure investment. Cloud-based collaboration tools, for example, support virtual team meetings with audio, video or web conferencing. Teams can share documents and applications cost effectively using Internet connections and standard USB web cams.



Although natural disasters or other major problems such as terrorism or civil unrest make the headlines, serious incidents at an organization's own sites can have equally damaging consequences. A major fire, power failure or serious damage to a data center also requires a response that includes high levels of remote working, virtual collaboration and communication.

Disasters caused by business management problems

Organizations are also at risk from a variety of business management or data-related problems that require a wide-ranging response to maintain continuity. The problems can be caused by direct events, such as an accident, power outage, fire and supply chain disruption or by indirect events such as product recalls, product tampering, financial or executive fraud, customer disputes, government investigations or data theft.

If all or part of the workplace is inaccessible, for example, because of fire, local flooding or other damage, an organization could find it impossible to deliver normal standards of customer service, respond to requests or maintain production levels. That can quickly lead to a loss of confidence among customers, with the risk of losing business to competitors. An extended period of inaccessibility could put an organization out of business in a short time. Business continuity plans should incorporate collaboration and remote access solutions to reduce the risk of damage from inaccessibility.

Problems in the supply chain can threaten customer confidence. Organizations can reduce the risk to supply chain continuity by making use of global communications to access a globally-distributed supply chain. IP networks and cloud services provide a flexible infrastructure to integrate new suppliers quickly and smoothly.

Compliance or legal issues also pose a serious threat to business continuity. Lack of governance or failure to meet regulatory compliance or industry standards could lead to regulatory fines and loss of business. Poor data backup, for example, could lead to data breaches or data losses that contravene industry standards, particularly in heavily-regulated industries. It could also lead to loss of business if compliance is part of the contractual agreement with clients. An organization could be liable for the consequences to third parties when its systems crash, for example.

The business continuity plan should therefore include solutions that protect the security and integrity of data that affects compliance or industry accreditation. Remote vault services or offsite data backup, for example, can reduce risk by managing the process externally.

Disasters caused by data problems

Risks relating to data are the most frequent threat to business continuity, and they also attract the wrong sort of headlines. Dropbox, the file sharing service, faced a Federal Trade Commission (FTC) inquiry in 2011 alleging that it had misled customers about the security and privacy of their file. The company's service description had stated that all customer files stored on their servers were encrypted and inaccessible without a customer's password. This claim was disputed by a member of a research institute, leading to the FTC inquiry and subsequent negative publicity for Dropbox. As well as damaging corporate reputations, serious data problems can impact an organization's productivity, decision making, responsiveness and ability to operate key business processes.

One of the major external threats is the growing level and sophistication of network attacks. AT&T has seen a 700+% increase in the maximum size of Distributed Denial of Service attacks in gigabytes per second from 2004 – 2011. Symantec reported that the number of targeted cyber attacks increased by almost 400 percent during 2011. The Department of Homeland Security reported that, in 2011, security experts at the Idaho National Laboratory had

responded to more than 340 requests for support following cyber attacks, compared to 116 in 2010. Cybercriminals, intent on stealing intellectual property and other valuable corporate data, are using sophisticated techniques that are becoming increasingly difficult to detect.

The situation is becoming more complex as, for instance, supply chain collaboration moves organizational security control outside the traditional perimeter. The intranet is now much harder to define and secure because it extends wirelessly via wireless LANs, cellular networks and Bluetooth. As the network extends further, it becomes increasingly difficult to manage security consistently, with variations in collaboration partners' security policies.

Growing levels of mobility are also making network security more difficult to control. Mobile endpoints such as smart phones, laptops and tablet computers increasingly store high-value proprietary data, increasing the risk of losing data if the device is lost or stolen. The consumerization of IT, where employees use their own mobile devices for business tasks (BYOD), means that many mobile devices with corporate access may not have corporate security cover. This means that business applications and data are vulnerable.

The business continuity plan must therefore include solutions to improve network security so that organizations can meet emerging security challenges while supporting mobility, consumerization of IT and high levels of collaboration with customers, suppliers and partners.

End-to-end security solutions including intrusion detection and protection, network-based security platforms, mobile security and device management can help to reduce risk.

Data is also at risk from data center outages or internal problems such as disc or server failures, data corruption and network problems. To reduce the risk, organizations should deploy virtualization as an integral element of a business continuity strategy. Virtualization makes IT resources more resilient and less location dependent and allows a rapid, reliable, cost-effective recovery in the event of a disaster or attack

Cloud-based solutions offer a further layer of business resilience. Cloud-based hosting, for example, enables a data center to be located away from physical buildings so that a disaster such as a fire would have a minimal effect on IT systems, reducing risk and improving business continuity. Customers should also carry out their own due diligence on a cloud-based solution.

Global continuity

The increasing globalization of business operations means that multinational organizations must enable the same levels of business continuity and network security across all territories. That means managing business continuity on a global scale, with solutions that take account of local differences such as power supply problems in India or the likelihood of frequent floods in Eastern Europe.

In the event of a major disaster, domestic suppliers would be vulnerable to local problems. However, global service providers can offer back-up on a global scale, reducing the risk of business failure. With a global business continuity plan, your organization becomes less dependent on local facilities.

Network solutions from global service providers enable multinationals to deploy global business strategies without the complexity of managing multiple networks and service providers. Technologies such as virtualization enable global operations to continue, regardless

of a disaster in a specific location, for example by mirroring computing resources and data in multiple locations around the world.

AT&T and business continuity

> *The only thing harder than planning for an emergency is explaining why you didn't.*

AT&T recognizes the critical importance of business continuity to its own operations and has a comprehensive strategy in place. Every process has a back-up, ranging from power generation to web center resilience to ensure continuity. Portable equipment for core infrastructure is on standby for rapid deployment to a site that may need it, and the company even has empty offices with IT and communications equipment installed. AT&T uses its 38 data centers around the world to mirror information across all sites. A problem on any site can be resolved quickly because a copy of the same data is available in other locations.

Based on years of experience, AT&T can provide advice and guidance, as well as practical support through professional services, to help with strategy development and implementation of business continuity plans.

The company's portfolio of networking, communication and collaboration solutions support the essential remote working and virtual collaboration processes essential to maintaining continuity and confidence following a disaster. AT&T's cloud, hosting and virtualization solutions provide customers with alternative infrastructure solutions that can minimize risk in the event of a disaster.

As a global service provider, AT&T can act as a trusted adviser making recommendations on the most appropriate solutions for local conditions. Global players like AT&T enable multinational organizations to deploy global business continuity strategies without the complexity of managing multiple networks and service providers. The company has the resources to provide support that can scale to meet the needs of organizations affected by major regional disasters.

From the Gartner Files:

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

Many backup/recovery and disaster recovery processes are antiquated and not up to the task of meeting current business requirements. This research discusses how the modernization of backup and recovery is becoming a high-priority project for many client organizations.

Overview

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 (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.

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

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				
Ranking	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)

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).

Proportion of Applications That Are Mission-Critical

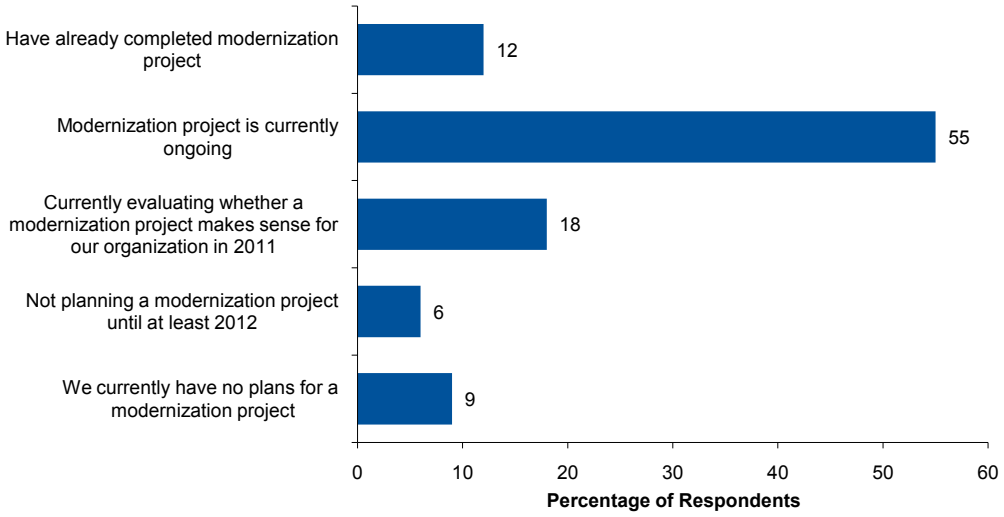
Historically, the proportion of an organization's applications that it deems mission-critical has been between 10% and 20% of the overall portfolio. By categorizing and better understanding how applications are used in business processes, and how critical they are to the revenue, safety, operations, 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%.

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

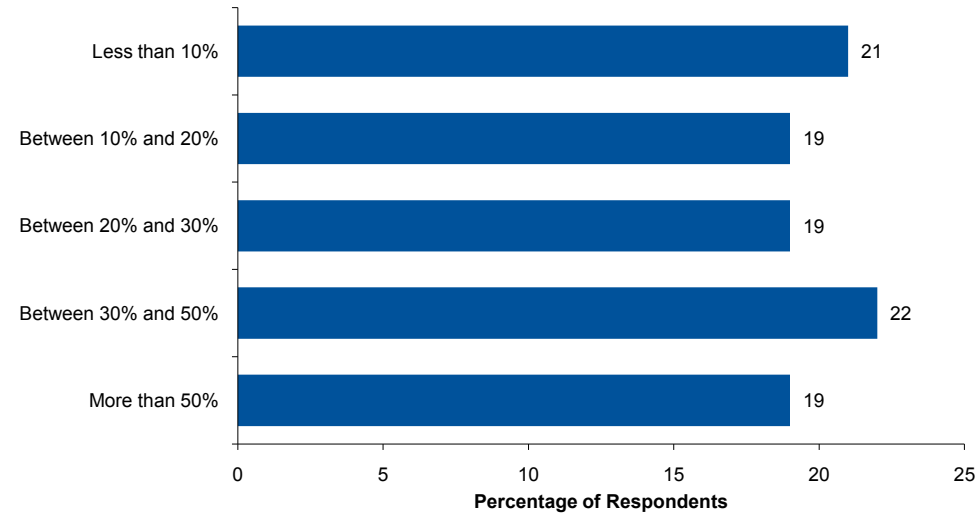
1 The enterprise has consolidated and rationalized business processes, and has integrated or retired a greater number of applications/services to meet business

Figure 2. Progress on IT DRM Modernization



Source: Gartner (August 2011)

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



Source: Gartner (August 2011)

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.

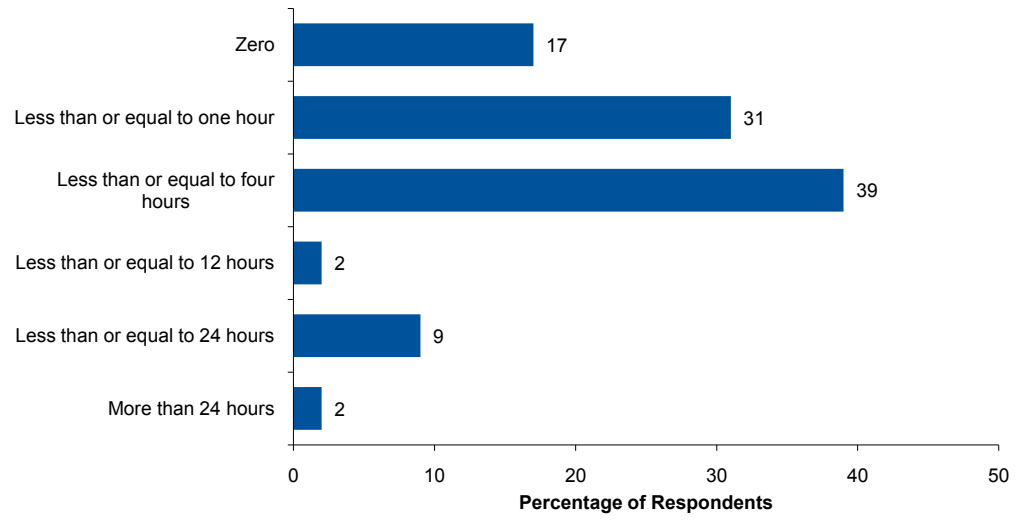
Enterprises that optimize on cost and reduce their RTOs to two to four hours can generally share their disaster recovery environments with another purpose, and, therefore reduce their overall capital investment requirements. In the case of an outage or disaster, the less critical work would be shut down (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. 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

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



Source: Gartner (August 2011)

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. 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.

IT DRM Action Items:

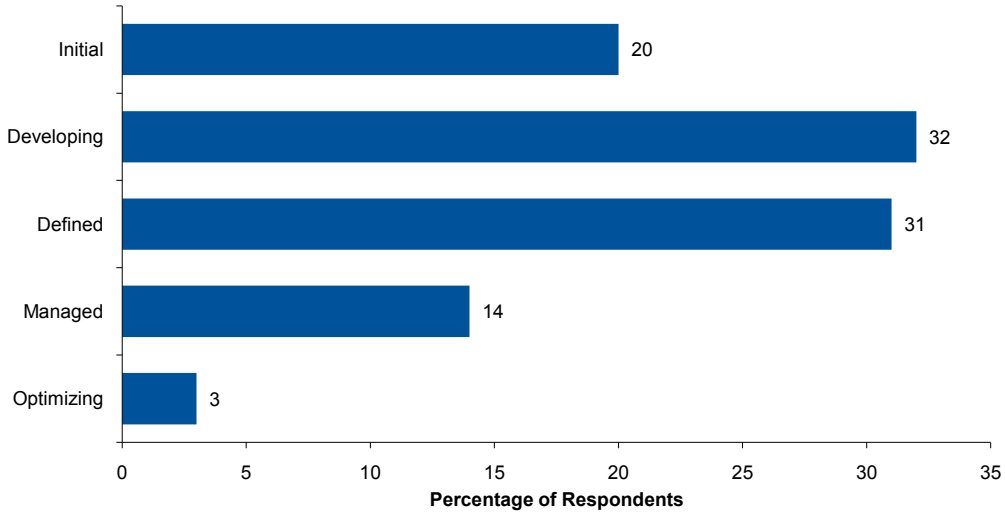
- Use Gartner's ITScore for BCM to assess your maturity levels. Improve your IT DRM maturity levels to a minimum of Level 3, which implements processes instead of projects, for long-term sustainability.
- To reduce IT DRM costs, do a realistic assessment of your IT service/application criticality levels. 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.

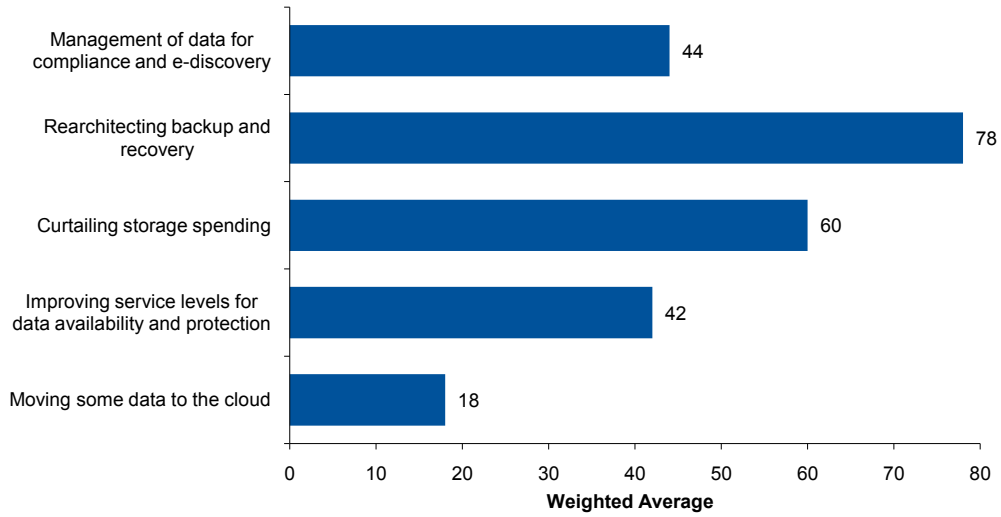
At Gartner's December 2010 Data Center Conference, a session on data management was held. Audience polling in Figure 6 shows that, of all the data management options, rearchitecting backup and recovery was viewed as the top priority. Note that participants were allowed to choose their top three responses, 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

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



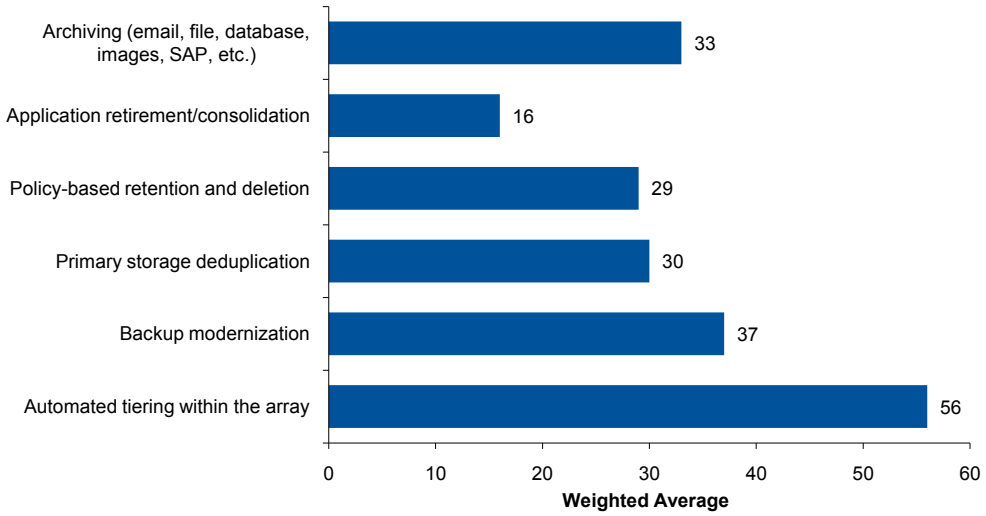
Source: Gartner (August 2011)

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



Source: Gartner (August 2011)

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



Source: Gartner (August 2011)

of press, backup improvements garnered the most first- and second-priority votes.

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.

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.

Gartner RAS Core Research Note G00215300, J. Morency, D. Scott, D. Russell, 11 August 2011

AT&T Newsletter - Issue 5, 2012 - Produced by the AT&T Global Field Marketing team in EMEA.

www.att.com/business
To contact us please visit: www.corp.att.com/worldwide