April 3, 2008

Building The Business Case For Disaster Recovery Spending

by Stephanie Balaouras
for IT Infrastructure & Operations Professionals

FORRESTER® Making Leaders Successful Every Day

April 3, 2008

Building The Business Case For Disaster Recovery Spending

by Stephanie Balaouras
with Galen Schreck and Rachel Batiancila

EXECUTIVE SUMMARY

Your bill for disaster recovery preparedness can run into the millions of dollars depending on the level of continuity and the size of your environment. Since these investments are about cost avoidance and don't typically reduce the total cost of IT ownership, management is typically reluctant to fund these efforts. However, IT operations professionals constantly worry about their preparedness for threats like power outages, IT failures, and disasters. How do you persuade your management to approve the funding necessary to improve disaster recovery preparedness? To successfully secure funding, IT must work with business owners to calculate the cost of downtime, define recovery objectives, identify the likeliest risks, and select the most cost-effective technologies and services. Management is much more likely to approve funding when IT leads with a business case and business metrics.

TABLE OF CONTENTS

NOTES & RESOURCES

Forrester conducted a joint research study with *Disaster Recovery Journal* to get a snapshot of current DR planning, spending, and preparedness efforts, as well as to understand the most common causes of downtime.

Related Research Documents

"IT Consolidation Drives Active-Active Data Center Configurations"
December 7, 2007

"Maximizing Data Center Investments For Disaster Recovery And Business Resiliency"
October 5, 2007

"Six Years After 9/11, Most Firms Are Not Ready For Another Disaster"
September 11, 2007

SEVEN KEY STEPS TO BUILDING THE BUSINESS CASE FOR DISASTER RECOVERY SPENDING

Your management may balk at a purely financial case for justifying investments in disaster recovery (DR). These investments don't increase top-line revenue, though they will likely let you retain more of your profits through cost avoidance and corporate viability. Building the business case requires a different approach that calculates the cost of downtime, defines specific requirements, identifies realistic risks, selects cost-effective technologies and services, and shows a commitment to disaster recovery planning and preparedness as an ongoing program. Forrester recommends the following seven steps for securing new, additional, or ongoing funding of DR-related efforts:

- **Implement a continuity management process.** Technology supports disaster recovery preparedness; it does not constitute a strategy or plan. Before you can request funding for technology and services, you need to have a framework in place to manage disaster recovery preparedness as a continuous process, not a one-time event.

- **Conduct a business impact analysis (BIA) and risk assessment.** Before IT can request any funding, IT professionals must sit down with business owners to identify the company's most critical processes, map dependent IT resources, and calculate the cost of downtime. You then must perform a risk assessment in order to determine the probability and frequency of specific risks.

- **Calculate the cost of downtime.** It's critical to understand the cost of downtime because this will help business owners and IT determine acceptable downtime and data loss for each business process and guide future investment in technologies and services.

- **Develop impact scenarios that address all risks, not just "disasters."** Business owners and IT must also work with risk management professionals to assess the risks from credible disruptive events, such as power failures, IT failures, human errors, facility failures, natural disasters, and manmade disasters. When management thinks of disaster recovery preparedness, they often think of preparing for freak events, such as hurricanes, earthquakes, and terrorist acts. The reality is that the most common causes of declared disasters and major business disruptions are much more mundane events, such as power outages and IT failures. Disaster recovery planners and IT operations professionals must help management understand that disaster recovery prepares for not only "disasters" but all potential causes of downtime.

- **Position DR as a competitive necessity.** Downtime creates an opportunity for competitors to seize market share. Likewise, uptime creates the parallel opportunity to seize market share from competitors. This helps reframe the discussion from disaster recovery as an insurance policy to disaster recovery (or disaster resiliency) as a competitive necessity. Most companies, not just financial services companies, have alternate sites and use advanced replication techniques to protect data. Companies need to keep up with peers and competitors.

- **Develop a DR services catalog.** As you work with the business to identify requirements, start planning a DR services catalog. This catalog will be defined by business-process criticality, the expected recovery time and recovery-point objectives, the supporting technologies and services, and the cost to deliver this level of DR preparedness. IT must still develop formal DR plans, but to estimate funding requirements it's necessary to identify the DR technology and services IT will need.

- **Align DR technology investments with other IT initiatives.** Many of the technologies that facilitate rapid recovery and data currency also facilitate other IT initiatives such as server, storage, and data center consolidation. IT consolidation is critical to reducing costs and improving operational efficiencies, so it's a strategic initiative at many companies.

IMPLEMENT A CONTINUITY MANAGEMENT PROCESS

Before you can request funding and implement technology and services for disaster recovery, you must have a continuity management process in place. Technology is important, but it doesn't constitute a DR plan or an ongoing program to manage and measure continuity. To be certain that you are truly prepared, you should have documented plans for all risk scenarios, a strategy for continuously updating plans as a part of change and configuration management, and a testing strategy. The most advanced technology in the world is useless if you don't test. In addition, you need a set of key performance indicators so that you can measure the effectiveness of the overall process as well as individual plans.

As more companies adopt IT infrastructure library (ITIL) as a framework for the management, measurement, and delivery of IT services, IT infrastructure and operations professionals should look to IT service continuity management as a framework for institutionalizing disaster recovery preparedness.

Implementing a continuity management process is necessary to ensure the success of your efforts, but it will also help to secure funding. Management is much more likely to approve funding when these investments support an ongoing, measurable IT service — not just some ad hoc request.

CONDUCT A BUSINESS IMPACT ANALYSIS (BIA) AND RISK ASSESSMENT

Technology supports disaster recovery preparedness; technology investments alone can't provide an effective disaster recovery strategy and plan. Selling management on business metrics such as, "The business demands that we provide less than 4-hour recovery of our customer care system with less than a minute loss in transactional data," is much more compelling to an executive than, "We need $3.2 million for hardware and $300,000 per year in telecommunications expenses for a data replication solution." This is why conducting the BIA is so important and why IT can't just start with technology.

Companies don't always have the luxury of completing all three disaster recovery planning phases (BIA, risk assessment, and plan development) and often skip the BIA and risk assessment. We believe it's worthwhile to take a step back to conduct a BIA and risk assessment because it provides an opportunity to ask business owners for input into recovery time and recovery-point objectives.

It's also an opportunity to map critical IT dependencies by business process, not by individual application. IT systems are highly interdependent, so it's important to understand what groups of applications and data sets need to be recovered together in a specific sequence to enable the business process and ensure consistency. Restoring an individual application is no longer very useful in today's complex IT environment. For example, the process of financial accounting and reporting is likely dependent on multiple applications — all of which must be brought online to recover the entire business process.

To determine the appropriate recovery time and recovery-point objective during a BIA, you should collect the following types of information from business owners:

- **What are my company's most essential business processes?** Examples might be order-to-cash, supply chain management, and financial accounting and reporting.
- **What are the dependent IT systems for each business process?** This dependency mapping is probably one of the hardest steps to accomplish because basic business processes often rely on multiple integrated IT systems, and the sequence of recovery is critical in a disaster recovery scenario. There are some technologies, such as a configuration management database, that can assist with this dependency mapping and even automate the mapping.[1]
- **How quickly do I need to restore these critical processes?** What is the business' sensitivity to downtime of the dependent IT systems? Do I have any manual workarounds?
- **How much data can I afford to lose for each of these critical processes?** Is there some data that can be rekeyed? How often should the data be backed up locally, and how often should the data be transmitted off-site?
- **What would be the cost of downtime and data loss?** What would be the impact on company revenues, profitability, customer service, worker productivity, and compliance if the business process was unavailable and some data was lost?

CALCULATE THE COST OF DOWNTIME

Calculating the cost of downtime and data loss is not a simple exercise: Some effects are more easily quantifiable than others. Still, the exercise is essential because it's the cornerstone of the business case. To calculate the cost of downtime and data loss, determine the following for each business process:

- **Revenue losses.** How much revenue is lost as a direct result of downtime? If you're a company that processes business through a Web site, every hour of system unavailability represents lost revenue. Some revenue is deferred, but some of it is permanently lost because a certain number of customers will never come back to the site.

- **Impact to cash flow.** What would it cost the company if it could not recognize revenue and process accounts receivable?

- **Productivity losses.** During downtime, you continue to pay employees their full salaries and benefits (unless you pay them hourly) even while their productivity is halted or severely limited. What would be the productivity loss if your salaried workers were unable to work at their full capacity?[2]

- **Compliance and/or reporting penalties.** What would be the impact if IT systems that support financial accounting and reporting were unavailable at a critical fiscal close such as month-end, quarter-end, and year-end? In addition, what would be the impact if the company was unable to comply with a regulatory audit as a result of system unavailability or data loss? Regulatory agencies expect their rules to be met, regardless of the conditions. Regulations such as the Sarbanes-Oxley Act, Securities and Exchange Commission (SEC) rules 17a-3 and 17a-4, HIPAA, and the FDA's 21 CFR Part 11 mandate that businesses retain, archive, and ensure the authenticity of key corporate information. Determining your loss threshold against these regulations can help determine recovery time and recovery-point objectives.

- **Penalties and loss of discounts.** What would be the expected penalties or late fees as a result of an inability to process payments to suppliers, technology vendors, and strategic partners? What potential discounts would the company lose if it were unable to process early payments and to take advantage of discount terms?

- **Impact to customers and strategic partners.** Would the company be forced to pay penalties on unmet service-level agreements (SLAs) to customers or strategic partners?

Other, more difficult to quantify impacts that should also be taken into consideration:

- **Employee morale and employee confidence in IT.** Over time, as employees experience delays and loss of work due to major outages, productivity is affected as well as the relationship between IT and end users.

- **Damage to reputation and goodwill.** What would be the impact to the company's reputation and goodwill if its critical IT systems were unavailable for more than a few hours? A few days?

DEVELOP IMPACT SCENARIOS THAT ADDRESS ALL RISKS, NOT JUST "DISASTERS"

Management often views disaster recovery as preparing for such extreme events as 9/11, Hurricane Katrina, or the European floods of 2005. They further view the likelihood of these events affecting their business operations as so low that it doesn't warrant the investment in technology and services for disaster recovery preparedness. But when they understand that it's not just disasters but events such as power outages, IT failures, and human error that cause most downtime, and that declared disasters and business disruptions are much more frequent than they would suspect, they are more likely to take action.

More Than A Quarter Of Companies Have Declared A Disaster

According to the Forrester/*Disaster Recovery Journal* October 2007 Global Disaster Recovery Preparedness Online Survey, 27% of companies have declared at least one disaster in the past five years (see Figure 1). Note that a disaster declaration doesn't require the occurrence of a natural or manmade disaster: A disaster is any event that causes a business disruption that meets the activation criteria in a disaster recovery plan. An activation criterion could be, "Critical IT systems have been unavailable for more than 4 hours." Declaring a disaster is not a trivial event; it requires a series of predetermined steps and may result in increased costs from:

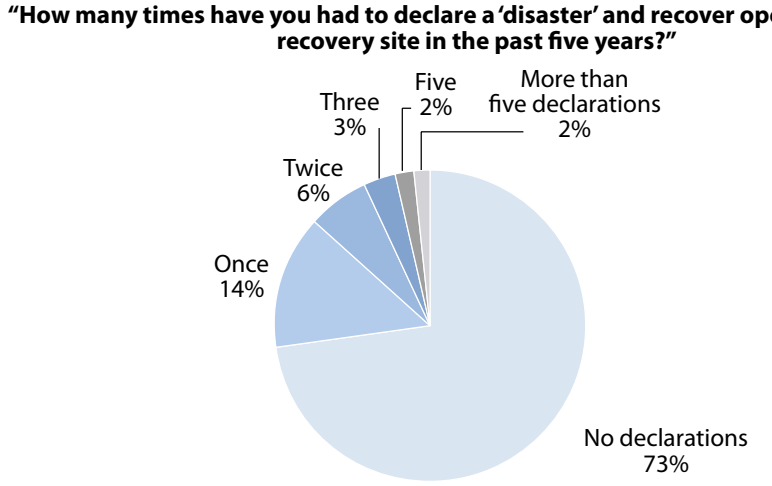
- **Notification of key parties.** Upon activating the DR plan, notification goes out to key teams that will cooperate with one another and execute their own part of the DR plan. These parties will likely include facilities, IT, and business operations, and the notification of employees, partners, customers, and stakeholders.

- **Failover of critical applications.** A DR plan requires that IT successfully failover or restart potentially hundreds of interdependent IT systems. In addition to the risk of an unsuccessful failover, you may have to pay staff overtime for working around the clock to get IT systems back up and running.

- **Activation of service provider resources.** The DR plan may also require that the company pay declaration fees and occupancy charges to a service provider or outsourced staff that is responsible for getting applications online at your hosted DR site.

Because executing a disaster recovery plan is complex, risky, and expensive, companies will avoid having to declare a disaster unless it's absolutely necessary. Given the consequences, it's very significant that 27% of companies have been forced to take this step in the past five years.

Figure 1 More Than A Quarter Of Companies Have Declared A Disaster In The Past Five Years



Base: 250 disaster recovery decision-makers and influencers at businesses globally (percentages may not total 100 because of rounding)

Source: Forrester/*Disaster Recovery Journal* October 2007 Global Disaster Recovery Preparedness Online Survey

42949 Source: Forrester Research, Inc.

Three-Quarters Of Companies Have Experienced A Disaster Or Major Business Disruption

Some events significantly disrupt business operations but don't trigger an actual disaster declaration. For example, there may be an IT failure that requires the recovery of a specific IT system at an alternate site but not the entire data center. It's not unusual for a company to failover a mission-critical application to an alternate site as a result of various failures. According our survey respondents, 76% of companies have declared a disaster or experienced a major business disruption.

Most companies don't realize that the most common cause of a declared disaster or major business disruption is a power failure. Forty-two percent of respondents indicated that a power failure was the cause of their most significant disaster declaration or major business disruption, followed by IT hardware failures and network failures (see Figure 2). Companies that operate in geographies with a low risk for natural disasters or a low risk for manmade events have a false sense of security when it comes to disaster recovery preparedness.

Use Risk Probability And Cost Of Downtime To Guide Investment Decisions

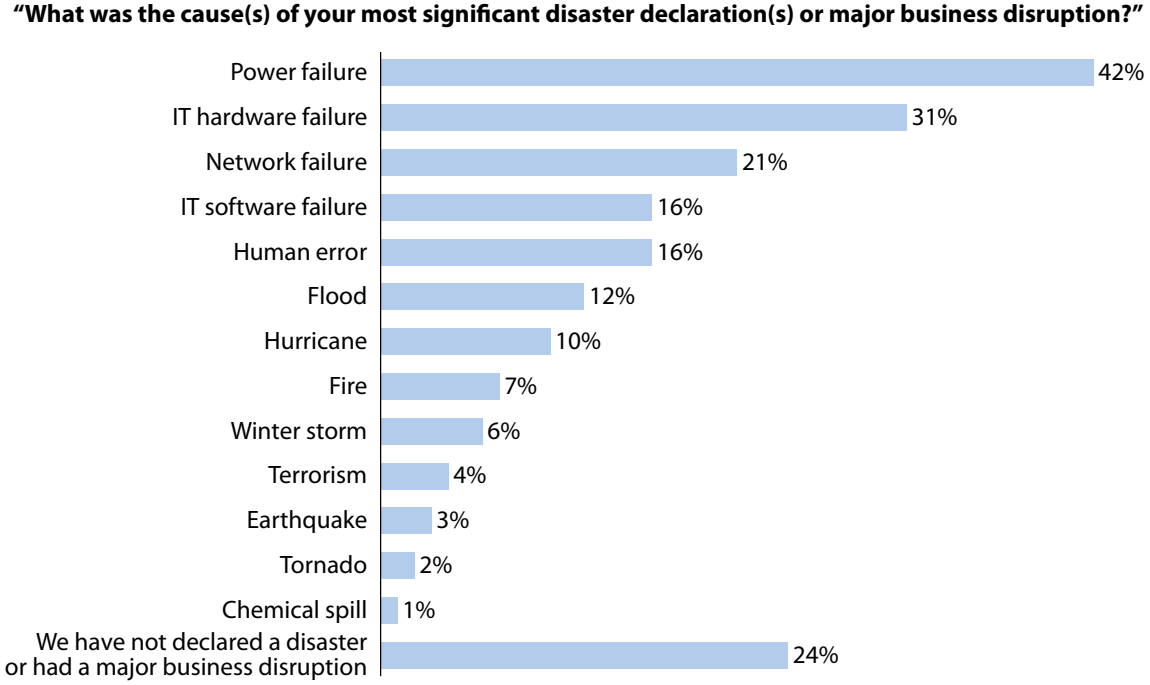
Spending on disaster recovery should be commensurate with the probability of risk and cost of downtime. Once you have identified the most probable risks, use previous cost of downtime calculations to determine the impact of each risk. We'll use severe winter storms as an example of a risk that a company based in the Northeast United States might need to examine. This company would need to take into consideration the:

- **Identified risk.** Winter storms with more than six feet of snow accumulation will likely force the closure of corporate offices for a business day.

- **Frequency of risk.** Due to the physical location of the corporate office in the Northeast United States, the frequency of such winter storms averages three times per year.

- **Vulnerability to risk.** All of sales, sales support, and senior management have laptops and remote access procedures. These employees can work fully from home and will be unaffected by an office closure. However, 400 employees in business-supporting functions (e.g., finance and HR) have desktops and no means to work from home. These are all salaried employees; the company will need to continue to pay these employees even while they can't work.

Figure 2 Power Failures Are The Most Common Cause Of Declared Disasters And Downtime



Base: 250 disaster recovery decision-makers and influencers at businesses worldwide (multiple responses accepted) (Does not include those who answered "Other" or "Don't know")

Source: Forrester/*Disaster Recovery Journal* October 2007 Global Disaster Recovery Preparedness Online Survey

42949 Source: Forrester Research, Inc.

With those risk factors, the company could calculate:

- **Impact.** The main impact of this risk is productivity loss, as these employees support revenue-generating activities; however, a one-day absence wouldn't have an immediate impact on revenue. Productivity loss is calculated as follows: 400 employees x $30 per hour (burdened hourly rate for these employees) x 8 hours = $96,000.

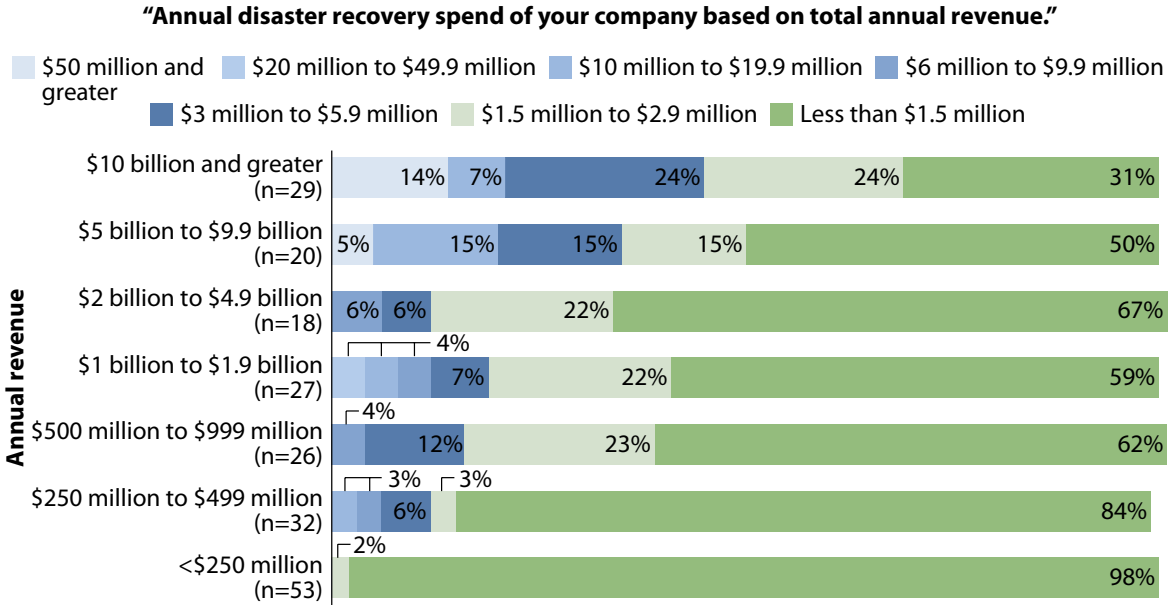
- **Annualized risk cost.** On an annual basis, the risk cost of this event is calculated as follows: 3 (frequency of the winter storms) x $96,000 (productivity loss for each event) = $288,000.

Our example company would use the annualized risk cost of $288,000 to guide investment in potential remote-access procedures such as SSL VPN, remote application presentation, and remote desktop access solutions.

POSITION DISASTER RECOVERY PREPAREDNESS AS A COMPETITIVE NECESSITY

Not surprisingly, DR spending increases with company revenue. The more revenue a company generates, the more it's willing to spend on people, technology, and services to protect its revenue, market share, and corporate reputation from downtime (see Figure 3). To protect your market share, it's important that your recovery capabilities match or exceed your competitors' capabilities.

Figure 3 DR Spending Increases With Company Revenue



Base: disaster recovery decision-makers and influencers at businesses globally
(does not include those who answered "Don't know" to the question, "How much does your company spend annually on disaster recovery?") (percentages may not total 100 because of rounding)

Source: Forrester/*Disaster Recovery Journal* October 2007 Global Disaster Recovery Preparedness Online Survey

42949 Source: Forrester Research, Inc.

More Companies Use Advanced Disaster Recovery Techniques

In the early to mid-1990s, only the wealthiest Fortune 500 companies could afford advanced disaster recovery techniques such as replication between production and recovery data centers. Adoption of advanced recovery strategies and techniques is much more common today. According to our survey, 85% of companies now have recovery sites. In addition, more companies are using dedicated IT infrastructure at the recovery site. According to our survey, 57% of respondents use dedicated IT infrastructure, whether that's at an internal site (34%), collocation site (11%), or service provider site (12%) (see Figure 4).

With dedicated infrastructure, companies can achieve a much better time-to-recovery and improve their recovery point using replication. According to our survey, 61% of companies use replication to protect mission-critical applications. Forty-three percent of companies extend the use of replication to protect business-critical applications.

Companies Now Measure Recovery Time In Hours

With investment in alternate sites, dedicated infrastructure, and replication, expected recovery time and recovery points are now measured in hours instead of days. According to our survey, 46% of companies expect to recover mission-critical applications in 10 hours or less, and 28% of companies expect to recover business-critical applications in 10 hours or less (see Figure 5-1). When it comes to limiting data loss, the news is even better; 65% of companies expect to limit data loss for mission-critical applications to 10 hours or less, and 51% of companies expect to limit data loss for business-critical applications to 10 hours or less (see Figure 5-2).

DEVELOP A DR SERVICES CATALOG

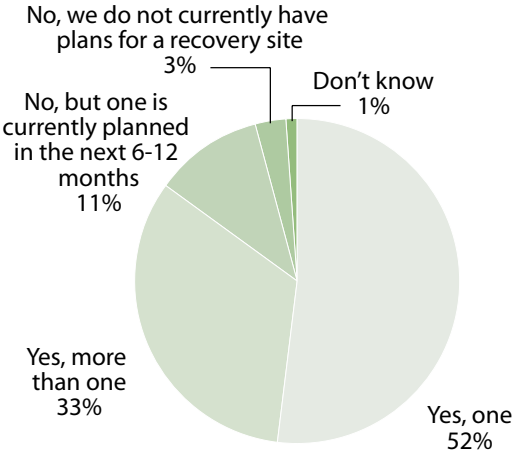
Once a company has calculated its cost of downtime, defined its recovery objectives, and identified the likeliest risks, it's ready to identify and estimate the costs of disaster recovery technologies and services that meet expected recovery objectives. When selecting services, you'll need to strike a balance between providing a range of DR services for applications with different criticalities and avoiding too many point products that could complicate recovery (see Figure 6).

Develop a disaster recovery services menu that contains recovery technologies and services with expected SLAs and costs mapped to business process criticality. If you can standardize tiers and SLAs, you'll be able to reduce the number of point products, minimize requests for nonstandard configurations, and provide a basis for memoback or chargeback. Since application owners are likely to classify all their applications as mission-critical, providing cost reporting or actually implementing chargeback will encourage business owners to make judicious selection of application criticality. Definitions of criticality will vary by company, but here is an example of a DR services catalog with four tiers:

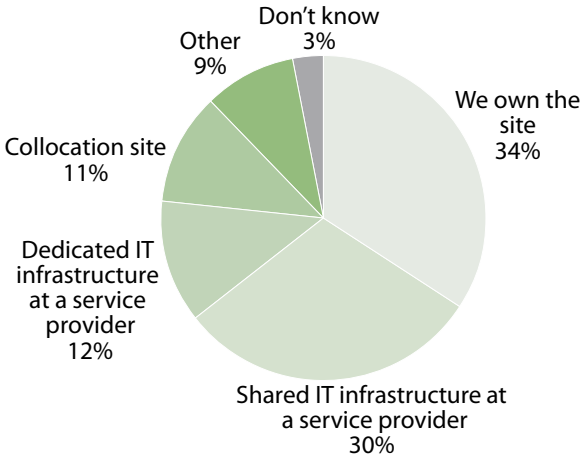
Figure 4 Adoption Of Advanced Disaster Recovery Techniques

4-1 Disaster recovery sites

"Do you have a recovery site for your data center and IT operations in the event of a disaster or other primary site failure?"



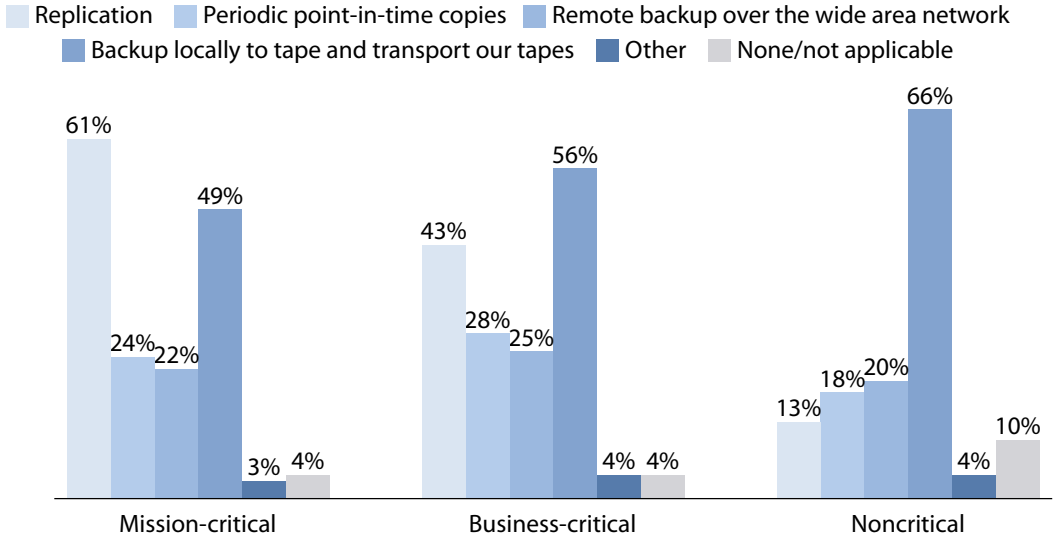
"How do you provision your recovery site?"



Base: 250 disaster recovery decision-makers and influencers at businesses globally
(percentages may not total 100 because of rounding)

4-2 Adoption of replication

"How do you copy data between your primary and recovery site(s)?"

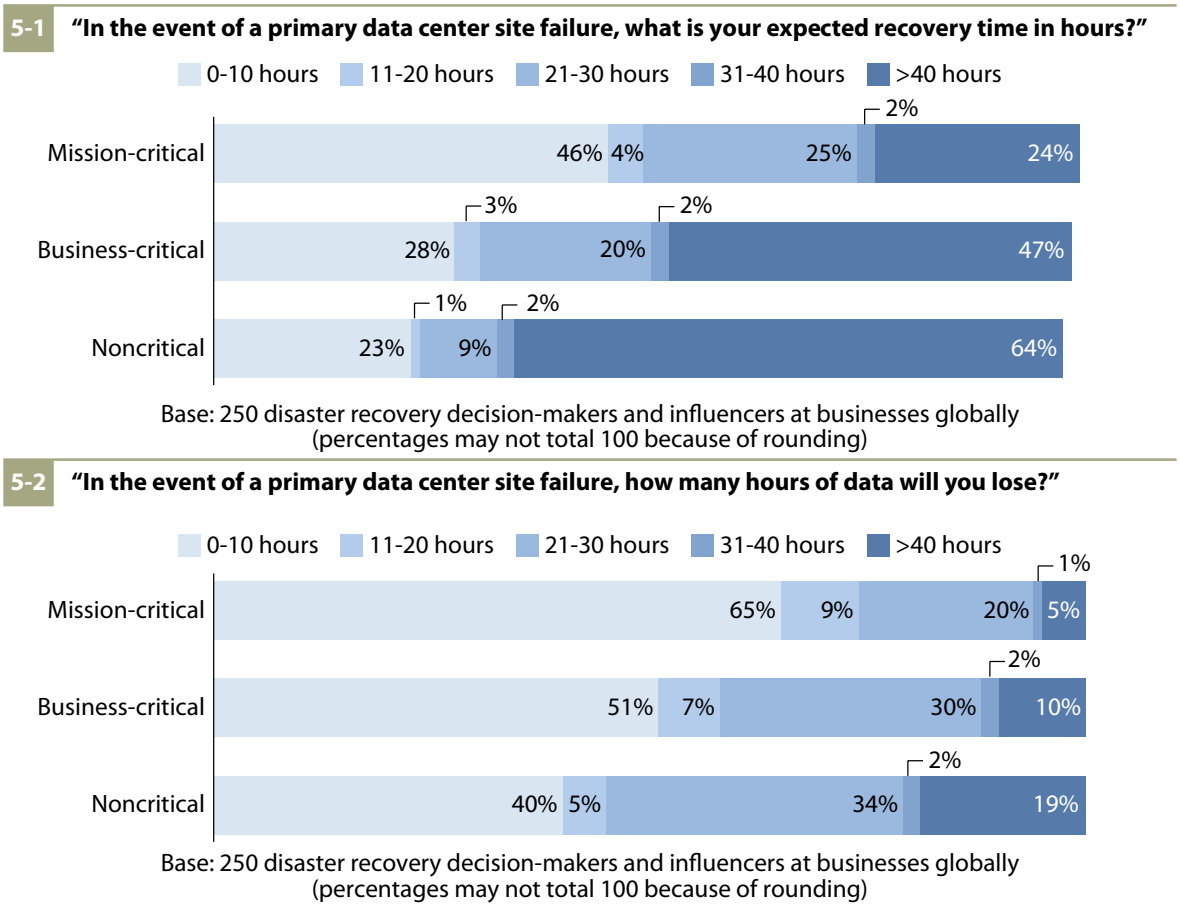


Base: 250 disaster recovery decision-makers and influencers at businesses globally
(multiple responses accepted)

Source: Forrester/*Disaster Recovery Journal* October 2007 Global Disaster Recovery Preparedness Online Survey

42949 Source: Forrester Research, Inc.

Figure 5 Expected Recovery Objectives By Application Criticality

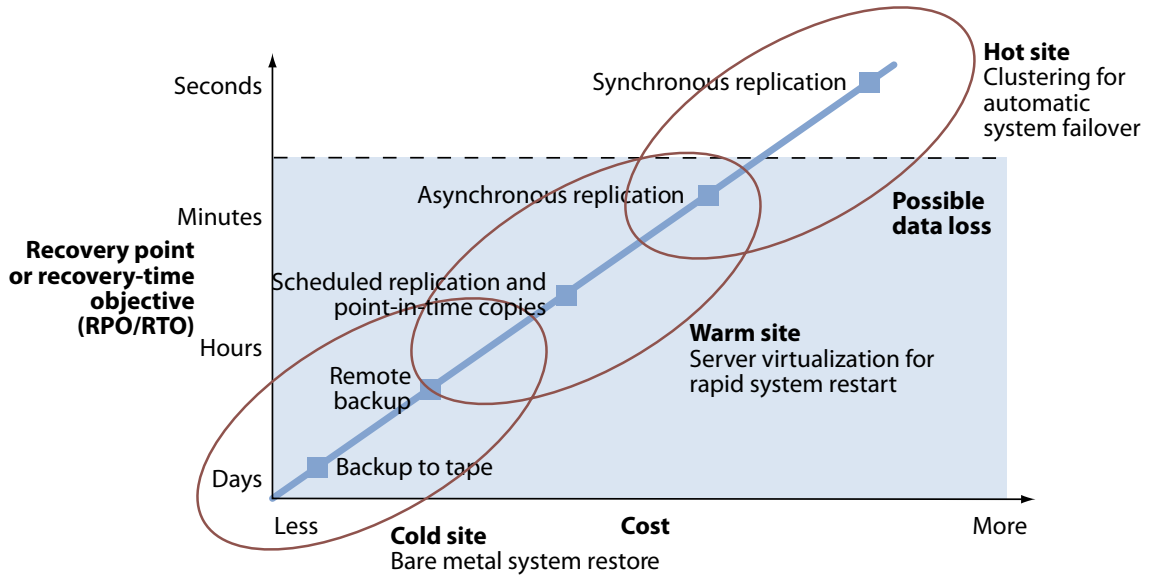


Source: Forrester/*Disaster Recovery Journal* October 2007 Global Disaster Recovery Preparedness Online Survey

42949 Source: Forrester Research, Inc.

- **Tier one: mission-critical applications.** A business process and its dependent IT systems that are vital to running day-to-day business operations are considered mission-critical. Without these systems, you can't conduct business, and you are losing revenue. Because they're the most sensitive to downtime and data loss, these systems must be restored within a few hours of a disruption, and the recovery point is zero data loss to a few minutes of data loss. This service level would be supported by synchronous or asynchronous data replication to an alternate site in conjunction with an application failover technology like clustering. The cost of this solution could run into the millions of dollars depending on the size of the IT environment because of the investment required in duplicate IT hardware and software licenses, software licenses for replication and clustering, and the bandwidth to support replication.

Figure 6 Recovery Continuum



42949 Source: Forrester Research, Inc.

- **Tier two: business-critical applications.** This is a business process and its dependent IT systems that are critical to ongoing business operations. In comparison to mission-critical applications, you can function (albeit in a diminished state) without these IT systems for a short time. These systems typically must be restored within a few hours to a day at most, and a few minutes to a few hours of data loss is acceptable. This tier would be supported by asynchronous or scheduled replication to an alternate site and would potentially take advantage of server virtualization for a quick application restart at the alternate site. Like tier one, these solutions are also expensive because they require the investment in duplicate IT at the alternate site. You may be able to support tier two service levels with less-expensive replication technology (perhaps server-based replication), less bandwidth, and no application clustering. It's also possible to reuse the investment in server hardware at the alternate site to run nonproduction workloads such as application development and testing.[3]

- **Tier three: business-important applications**. This is a business process and its dependent IT systems that are important to the business but not critical to running day-to-day business operations. Examples might be reporting, data warehouses, and department file shares. These IT systems must be restored within several days. A few hours to a day of data loss is acceptable. These types of applications might be supported by remote backup or even a third-party remote backup service to an alternate site. This service level would require much less bandwidth and no standby IT infrastructure at the alternate site. Infrastructure could be rapidly replaced through quick-shipment arrangements with vendors. System configurations and data would be restored from backups.

- **Tier four: business-supporting applications.** This is a business process and its dependent IT systems that support the business but are noncustomer-facing and nonrevenue-generating. Examples might be an employee expense submission application. These IT systems must be restored in several days to a week. Several days of data loss is acceptable, as there are manual workarounds to rekey the data. These IT systems might also be protected with remote backup, but backups are less frequent.

ALIGN DR TECHNOLOGY INVESTMENTS WITH STRATEGIC IT INITIATIVES

Disaster recovery preparedness is sometimes an afterthought. It's much easier to design availability and continuity into applications and infrastructure than it is to "bolt on" technologies after the fact. This is reason alone to be involved early with architectural decisions, but aligning with these decisions will also help justify any additional disaster recovery investments.

In addition to application and infrastructure decisions, DR technology investments should be included in discussions regarding IT consolidation efforts such as server, storage, and data center consolidation. Many of the technologies that facilitate application recovery and limit data loss for disaster recovery also enable these key initiatives. The strongest example is server virtualization. Server virtualization not only facilitates server consolidation and the deployment of networked storage, but it also facilitates the rapid restart of applications at a recovery site when used in conjunction with replication. Another example is storage consolidation. Storage consolidation not only has the benefit of increasing capacity utilization, but it can also reduce the complexity of disaster recovery. When more applications and data sets are networked to the same shared storage, you can use a single replication offering to protect all of them.

The key, then, is to not only ensure that availability and continuity are critical considerations in any IT decision or initiative, but to use the importance of the success of these projects to reinforce any additional investments.

RECOMMENDATIONS

DON'T LEAD WITH TECHNOLOGY

The cardinal mistake when developing disaster recovery strategies and justifying investments is to lead with technology. It might seem burdensome and complicated to conduct a business impact analysis and risk assessment with a cross-function team of business owners, risk management professionals, facilities, and IT, but it's critical; with the results you can identify business requirements, risks, and impacts to create quantitative justifications for investment and get the entire business onboard. It's also not necessary for these phases to take months to complete or require outside consultants to facilitate. It's possible with a targeted list of individuals and good project planning to complete these phases in a few weeks.

It's important to follow through with the other four steps outlined in this report because in many cases you're still trying to persuade a reluctant management to make these investments. You need to help them understand that they are potentially falling behind their peers and competitors in terms of readiness, that other parts of IT and the business would benefit from these investments, and that IT is serious about its request for funding and you can prove it.

SUPPLEMENTAL MATERIAL

Methodology

In October 2007, Forrester Research and the *Disaster Recovery Journal* (*DRJ*) conducted an online survey of 250 *DRJ* members. In this survey:

- Thirty-three percent of respondents were from companies that had 0 to 999 employees; 25% had 1,000 to 4,999 employees; 20% had 5,000 to 19,999 employees; and 22% had 20,000 or more employees.
- Eighty-three percent of respondents were from North America; 3% were from South America; 8% were from Europe, the Middle East and Africa; and 6% were from Asia.
- All respondents were decision-makers or influencers in regards to planning and purchasing technology and services related to disaster recovery.
- Respondents were from a variety of industries.

This survey used a self-selected group of respondents (*DRJ* members) and is therefore not random. These respondents are more sophisticated than the average. They read business continuity (BC) and disaster recovery publications and participate in online discussions. They have above-average knowledge of best practices and technology in BC/DR. While nonrandom, the survey is still a valuable tool in understanding where advanced users are today and where the industry is headed.

ENDNOTES

[1] Forrester evaluated the strengths and weaknesses of the eight vendors that have brought an original technology for automated application to infrastructure dependency mapping to market across 63 criteria. See the February 27, 2006, "The Forrester Wave™: Application Mapping For The CMDB, Q1 2006" report.

[2] New threats, such as bird flu, are forcing firms to realize that while they have taken extraordinary measures to protect and continue data center operations in the event of major disaster or serious business disruption, they have not taken the necessary steps to ensure that their people can continue to have access to their applications, data, and communication (email, messaging, voicemail, fax, etc.) in order to remain productive. See the December 27, 2006, "Workforce Continuity Is A Critical Strategy In Your Business Continuity Plan" report.

[3] Building a data center is a massive investment. It requires investment in real estate, reinforced facilities, raised floors, state-of-the art power and cooling, and IT infrastructure such as networks, servers, and storage — not to mention the experienced data center staff to manage it all. Firms build new data centers for a variety of reasons: capacity limitations, modernization, consolidation, and many others. But firms also need an alternate data center that's an appropriate distance away so they can failover critical business operations in the event of a primary site failure. Given the necessary investment, an alternate data center simply can't remain idle waiting for some disaster to occur. Firms must determine ways to maximize this investment to improve business operations, accelerate growth, or elevate availability. See the October 5, 2007, "Maximizing Data Center Investments For Disaster Recovery And Business Resiliency" report

FORRESTER®

Making Leaders Successful Every Day

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Australia
Brazil
Canada
Denmark
France
Germany
Hong Kong
India
Israel
Japan
Korea
The Netherlands
Switzerland
United Kingdom
United States

For a complete list of worldwide locations, visit www.forrester.com/about.

Forrester Research, Inc. (Nasdaq: FORR) is an independent technology and market research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. For more than 24 years, Forrester has been making leaders successful every day through its proprietary research, consulting, events, and peer-to-peer executive programs. For more information, visit www.forrester.com.

FORRESTER®