Avoiding the pitfalls of outdated disaster recovery plans

Evolving business expectations and threats may require new disaster recovery approaches

IBM

Contents

The evolving threat landscape

When Superstorm Sandy hit the New York City area in late 2012, the New York Stock Exchange closed for two days. In one sense, the NYSE was fortunate: many businesses in the region went without power for weeks. Eighteen hundred flights were cancelled. The New York City transit authority suspended public transportation and closed Manhattan bridges and tunnels. Twenty-five percent of cell towers were damaged, affecting service from virtually every mobile telecommunications carrier.

Superstorm Sandy wasn't the worst storm to ever hit the northeastern United States. But because enterprises now depend on technology, including the technology that makes information and applications continuously available, Sandy tested many businesses' disaster recovery plans. It challenged organizations to think about the availability of key resources—including people, technology, data and space—in ways they had not before.

According to Forrester Research, enterprises today spend an average of 6.2 percent of their IT budgets on business continuity and disaster recovery—a jump of one full percentage point over the amount spent in 2010.[1] However, most of these funds are spent on in-house disaster recovery operations. Considering a less-than-robust economy and the decreasing cost of hardware, in-house disaster recovery once seemed like a logical choice. But, as Forrester notes, internal disaster recovery operations are plagued by a number of problems, including insufficient skills, insufficient testing and a general lack of focus.[2] This situation was evident in the aftermath of Superstorm Sandy, when many disaster recovery plans did not work well. Many IT and business executives decided to re-evaluate their disaster recovery strategies in light of lessons learned from this storm.

This is a bad time for out-of-date disaster recovery plans. The threat landscape has been evolving. Weather events—including hurricanes, tsunamis, tornadoes, floods and earthquakes—now have a more significant impact on businesses: as organizations become more technology dependent, any outage can prove crippling. In addition, businesses are increasing investments—especially IT investments—in emerging areas of the world. This trend requires organizations to focus more strongly on their disaster recovery operations, because investment in emerging nations often outstrips those countries' ability to support sophisticated disaster response.

Disruptions and disasters are also negatively impacting organizations beyond the realm of operational continuity. Along with contractual liability and loss of sales, organizations now face regulatory penalties for failing to meet data availability and recovery standards. In the age

of social media, information about any corporate failing—including the inability to operate during disaster—can be immediately disseminated. Negative blogs, tweets or posts can potentially damage an organization's reputation. That's why, according to the 2013 IBM global reputational risk and IT study[3], an increasing number of organizations are delineating reputational risk as a distinct category in their risk management frameworks.

How well will your disaster recovery plan work when the time comes? It's a hard determination for any organization to make. Most organizations are not in the business of disaster recovery. They are in the finance business, or the manufacturing business, or the transportation business. Without the experience that comes from operating through disaster after disaster, in-house business continuity and disaster recovery teams may face challenges in developing, implementing, testing and maintaining disaster recovery strategies. It is difficult, in times of calm and order, to foresee the myriad things that can go wrong in times of chaos, then plan for them accordingly.

How well will your current disaster recovery plan work when the time comes? It's a hard determination for any organization to make.

IBM, however, *is* in the disaster recovery business. From experience gleaned supporting thousands of clients' recovery operations worldwide, IBM has identified seven faulty assumptions on which many organizations base their disaster recovery plans. These assumptions may have been sound as little as 5 or 10 years ago, but IBM believes that they are often no longer valid. Pressures such as the need to accommodate data growth, increasing business demand for access to IT functions, the management of growing data center footprints and the demand for 24x7 application availability have both spawned a need for a sharper focus on disaster recovery and left IT professionals with little time to worry about disaster recovery. This paper will discuss those faulty assumptions, along with IBM offerings designed to help organizations modernize disaster recovery efforts.

Common faulty disaster recovery assumptions

In IBM's experience, too many organizations erroneously believe the following seven statements.

1 We'll be able to keep the business running during a disaster because we've developed a work-from-home strategy.

To restore business as quickly as possible after a disaster, organizations need to find ways to keep their key employees working. Some recovery plans are dependent on IT staff working from their homes.

Work-from-home strategies often don't perform as expected. Employee homes may be damaged during the same disaster that affected the business. Some employees may have to evacuate. Even those employees who can stay at home may not have access to the same information and applications as they do in the office, a situation that limits productivity.

Cloud-based disaster recovery solutions can give organizations more flexibility to recover from any location. They accomplish this by using web-based portals for cloud control. Nevertheless, to recover business operations rather than just infrastructure, it is crucial to have qualified IT and business personnel present at the recovery site. Since organizations should expect to have only a fraction of their staffs able to work during a disaster, many businesses may have to consider contracting with a technology provider that employs personnel specializing in disaster recovery.

Communications with our employees, customers and supply chain will continue. We have wireless capabilities for phone calls, emails and texts.

If an enterprise cannot communicate with its employees, customers, members of its supply chain, and, in certain circumstances, the media, it may not be able to restore business after a disaster. It is therefore crucial to develop plans for communicating during times of disaster. These plans should include directives on who is authorized to speak on behalf of the company, the type of information to be communicated under which scenarios, when and to whom. Communications strategies will vary by audience. For example, the type of information the organization wants to communicate to its key employees will likely vary substantially from the information it imparts to the media. Employees' need to communicate with the organization itself must also be accommodated.

As important as determining a communications plan is determining the channels through which the organization will communicate during times of disaster. Organizations are typically comfortable using emails, phone calls and texts for internal communications; print, television and radio for communications with the broader community. However, many organizations still need to refine their social media strategies for communications with the public in times of disaster. Other organizations have yet to devise any type of social media strategy at all. In IBM's view, this is a mistake. If an organization does not take the lead in communicating via Twitter, Facebook, LinkedIn, YouTube and other sites, outside posters and bloggers may frame the conversation. IBM suggests developing and implementing a social media strategy for disaster communications that includes reporting on business activities during disaster, engaging members of the community and responding to their concerns.

If an enterprise cannot communicate with its employees, customers, members of its supply chain, and, in certain circumstances, the media, it may not be able to restore business after a disaster.

We'll be able to restore our key business applications because we've backed up our data.

Tapes are a good choice for secondary backup. However, with recovery time objectives frequently running less than 24 hours, tapes may no longer be the best choice for primary backup. In addition, tapes can be vandalized, sometimes by disgruntled people working inside the organization. Worse, a single missing or damaged tape can jeopardize an entire disaster recovery operation.

Organizations that rely solely on tape also often face challenges transporting those tapes to disaster recovery sites. In times of disaster, roads may be impassable and regional and national transportation systems may shut down, making it impossible to transport tapes, a situation that negatively impacts disaster

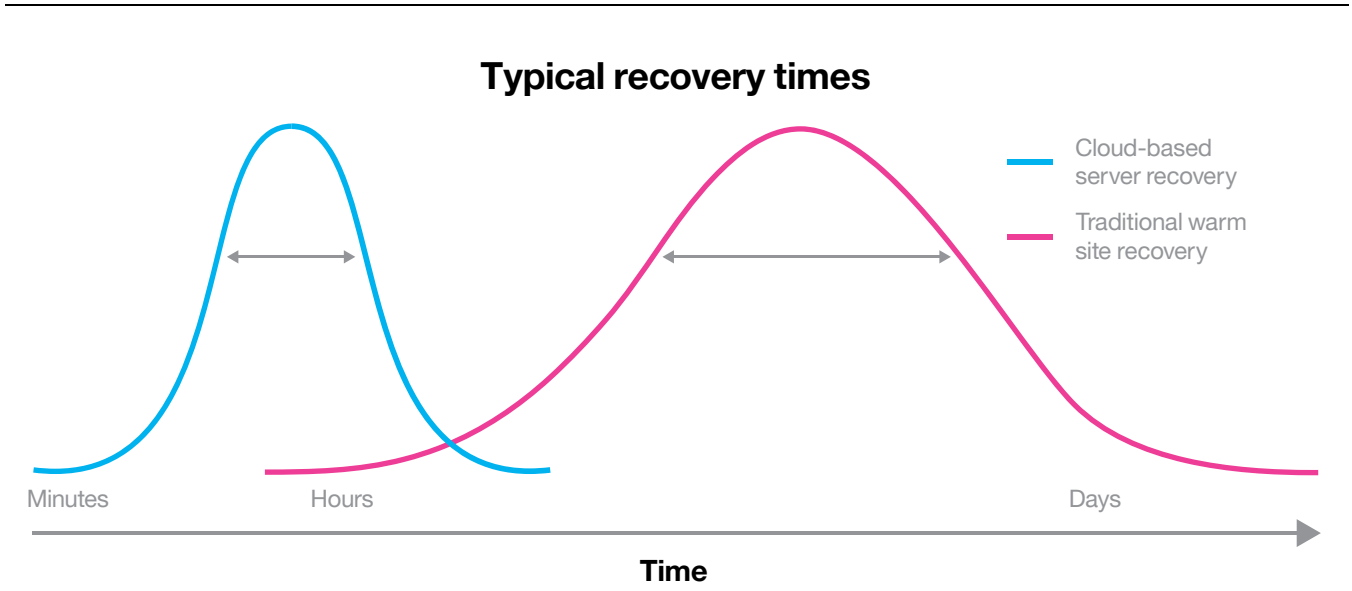

Figure 1. In IBM's experience, it typically takes between 2,000 and 3,000 minutes—33 to 50 hours—to recover applications via traditional disaster recovery approaches. (See the bell curve to the left.) With cloud-based disaster recovery, that time can sometimes be shortened to just a few minutes, depending on the number of servers being recovered.

recovery plans. At the very least, transportation may take longer than expected, making recovery times unacceptable.

Even if tapes can be transported to a secondary site within a reasonable period, many organizations find that restoring operations from tape backups simply takes too long. In IBM's experience supporting clients in recent years, best case time for full recovery from tape backup typically runs about 20 hours. In worst case scenarios, backup can take about 80 hours. (See Figure 1.)

In an around-the-clock business world, organizations need their most critical applications available within minutes or hours, not days. One way to achieve such high availability is to employ cloud-based disaster recovery services with very short recovery time objectives. As with all technologies, cloud computing has limitations and risks which organizations should carefully consider before implementing cloud technologies into their disaster recovery plans.

We know our disaster recovery plans for IT work. We test them every year.

Despite the changing risk landscape, many organizations cling to disaster recovery standards set long ago. Annual disaster recovery testing is a prime example. Many organizations continue to believe that once-a-year testing proves the efficacy of their disaster recovery plans. However, this standard was set when data center operations were much more stable. Today, applications change frequently, greater volumes of data are constantly being generated, a variety of operating systems are used and infrastructures frequently combine both physical and virtual resources. A successful test completed months ago doesn't necessarily prove an organization's ability to recover today's data center operations. Instead, disaster recovery testing performed only periodically disconnects disaster recovery efforts from the change-management process. Also, organizations too often only test a subset of their applications and IT environments, further limiting their ability to determine how their recovery plans would work during a disaster. Full-scale tests of all applications and environments are needed to determine if disaster recovery plans will work as expected.

Furthermore, too many organizations fail to take process skills into account when testing their disaster recovery plans. During times of disaster, IT operations may require additional process skills because many IT resources may not be immediately available. Therefore, it is vitally important to have on hand professionals with the hardware, software and applications process skills necessary to perform the manual tasks required until IT resources are again running. Again, employing a provider of cloud-based disaster recovery services—one that offers easy testing and virtually seamless replication of data and applications—can help. It keeps an organization's disaster recovery efforts in the hands of experienced specialists.

We'll be able to continue data center operations from our secondary data center site.

Opting to run recovery operations from a secondary data center site removed from the corporate campus is a good idea. But too often, alternate sites are too close to the organization to escape the effects of disaster. Weather events and acts of terrorism can effect an entire region. In the case of Superstorm Sandy, for example, power outages, public transportation shutdowns and communications problems affected not only New York City, but parts of Long Island, New Jersey and Connecticut—hindering the ability to restore operations from secondary data centers in those areas. Conversely, secondary sites are sometimes placed so far away from an organization's primary campus that it becomes impractical to transport tapes and staff to the secondary location, particularly when the disaster disrupts air travel.

To overcome these obstacles, data replication and synching between primary and secondary sites should be implemented, eliminating the need for the transportation of backup media. Those attempting synchronous replication will find distance-related network latency issues a concern. For "real time" recovery point objectives, organizations should use two sites close enough for synchronous data replication. However, as noted above, if sites are too close together they may be susceptible to the same disruption that affected the organization's primary site. Conversely, if a secondary site is placed too far away from the organization's primary site, performance may be impacted by latency. Therefore, organizations that operate under regulatory requirements for data availability or who cannot afford to lose access to information may want to consider employing a tertiary site where data is replicated asynchronously. The third site should be far enough away from primary and secondary sites that it is unlikely to be impacted by the same disruptive event.

Figure 2: Organizations often base their disaster recovery plans on faulty assumptions covering everything from employee work plans to projected speed of IT recovery.

Given the need for two or three sites, contracting with an experienced disaster recovery provider may be beneficial. Such a provider should offer a large network of resiliency centers that can provide the secondary (synchronous) or tertiary (asynchronous) site, or both, without generating the costs associated with acquiring additional data center space.

Successful failovers during testing validate our business continuity capabilities. It's one thing to recover operations; quite another to get back to business as usual. Failback, the process of returning operations to production data centers, is the first step in resuming normal data center operations.

Any data that was created at the disaster recovery site while in disaster recovery failover mode needs to be replicated back to the original production site during the failback process. It is easy to neglect the failback procedure in business continuity and disaster recovery planning. With a virtualized recovery solution, failback is typically quicker and less complex than in traditional recovery operations. The need for less manual intervention significantly reduces the time and effort required to get back to normal operations.

7 We'll be able to quickly recover from disaster because we've made provisions for our organization's employees, communications, data and applications.

An organization's recovery from disaster does not just depend on its own recovery operations, but on those of its supply chain constituents. A web retailer may modernize its disaster recovery plans, test them regularly, and be able to resume operations quickly after a catastrophe. However, if its suppliers have no way to deliver merchandise to the retailer's warehouse, the business cannot be fully restored. It is important, therefore, that organizations develop a strategy to test not just their own recovery operations but those of their upstream and downstream supply chain linkages. IBM recommends that organizations take into consideration the risks to all critical supply chain linkages, then develop, document and test appropriate mitigation responses.

How IBM can help

With an evolving threat landscape and concern about the true costs and capabilities of their current disaster recovery plans, many organizations now consider the value of modernizing disaster recovery operations by contracting with a partner to provide these functions. In fact, Forrester reports that more than half of the organizations surveyed in its "Risks of 'Do It Yourself' Disaster Recovery" report would consider outsourcing part or all of their disaster recovery operations if such a move would also lower these functions' total cost of ownership.[4]

IBM strongly believes that disaster recovery approaches need to evolve to keep pace with changing risk dynamics. Businesses can start slowly, increasing disaster recovery testing frequency; finding safe, secure and fully functional emergency work areas for their key employees; and migrating to the cloud both their most critical data and those applications with the lowest tolerance for downtime. IBM offers services to help in these efforts, including:

- IBM Resiliency Consulting Services
- IBM Infrastructure Recovery Services
- IBM Managed Resiliency Services
- IBM SmartCloud Resilience.

IBM Resiliency Consulting Services provide a comprehensive suite of services that help organizations determine how to develop a successful resilience program. Services help organizations design, plan and implement resilience plans and test infrastructure resiliency.

IBM Infrastructure Recovery Services cover both work area recovery and IT recovery. IBM's **work area recovery services** allow organizations to secure alternate work environments in IBM's worldwide network of 150 business resiliency centers during times of disruption or disaster. These highly secure facilities offer ready-to-use workstations equipped with personal computers, phones and other work tools.

The facilities are equipped with redundant communications capabilities, multi-vendor IT equipment and uninterruptible power supplies and are staffed by IBM recovery experts. In some regions, IBM offers a mobile IT recovery option through which mobile units are delivered to a site of the organization's choosing for temporary use.

Disaster recovery approaches need to evolve to keep pace with changing risk dynamics. Businesses can start slowly, increasing disaster recovery testing frequency and deploying high availability, cloud-based recovery techniques for applications with the lowest tolerance for downtime.

IBM's comprehensive **IT recovery services** can be tailored to meet the user's specific business and technical requirements. Services covered range from simple hardware replacements to the provisioning of highly complex mirrored environments. Solutions encompass computing hardware, peripherals, communications equipment, operating systems and infrastructures. Comprehensive recovery operations can be performed from an IBM recovery site. IBM recovery sites offer the same features as those listed for work area recovery.

IBM Managed Resiliency Services can help organizations keep their critical business processes operational and business information accessible in the event of an outage. These services support integrated administration, monitoring, data protection and disaster recovery. The IBM Managed Resiliency Services portfolio helps organizations select capabilities based on the criticality of their data and processes. By managing and operating these services—either fully or partially—IBM can help businesses avoid downtime, improve staff productivity, manage operational expenses and comply with regulatory requirements. **IBM managed continuity** provides organizations with IT-ready, hardened and dedicated data center space and power for primary, secondary and tertiary data centers. Its purpose is to provide organizations with high-availability backup and recovery for IT infrastructure. Data room design and implementation and ongoing management services are all included.

Cloud computing is a growing component of disaster recovery. **IBM SmartCloud Resilience** offers two cloud services that can help organizations modernize their approach toward disaster recovery: IBM SmartCloud Managed Backup and IBM SmartCloud Virtualized Server Recovery.

IBM SmartCloud Managed Backup offers public, private and hybrid cloud-based data protection solutions for organizations that need cross-enterprise information resiliency and data recovery. This service helps organizations to simplify backup with automated and standardized tools and processes that consolidate dispersed information onto a single infrastructure. IBM SmartCloud Managed Backup is a security rich and highly scalable solution that allows organizations to choose and implement a plan tailored to meet backup priorities, retention and retrieval goals, and needs for data protection and scalability. This service helps reduce backup errors and the need for manual intervention. Tape protection and management services are also offered for those organizations that want to take a hybrid tape/cloud approach to data backup.

What IBM SmartCloud Managed Backup does for data, **IBM SmartCloud Virtualized Server Recovery** does for servers and applications. IBM SmartCloud Virtualized Server Recovery is a cloud service designed for organizations that need faster, more reliable and more affordable recovery of their IT infrastructures. It provides advanced failover/failback capabilities for virtually immediate recovery, and offers the ability to recover server environments that include a mix of physical and virtual servers. Tiered service levels allow organizations to differentiate applications based on their importance and their tolerance for downtime. IBM SmartCloud Virtualized Server Recovery can also be integrated with existing infrastructure recovery services for a comprehensive and holistic hot-site solution.

Getting started

Modernizing an outdated disaster recovery strategy is a challenging process. To begin, consider:

- Do you have the expertise in-house to run and maintain an effective disaster recovery program in a 24x7x365 world?
- Can you obtain ongoing funding for your disaster recovery program?
- Do you have a consistent and frequent testing and exercise regimen?
- If your organization experienced a disaster, would you be able to access backup data and systems quickly and effectively?
- Are your current business continuity solutions scalable to handle changing requirements?
- What will happen to your business if you lose a day's, a week's, or a month's worth of critical data?
- What will happen to your business if you have to go for a prolonged period without your critical applications?

Organizations should keep these considerations in mind as they begin modernizing disaster recovery plans. If an organization finds that it needs professional expertise, IBM Resiliency Consulting Services can help. For those organizations that wish to use cloud computing to better protect data and applications, IBM offers an orderly approach to cloud transition. This approach includes devising an end-to-end cloud strategy for business resilience, designing a plan for cloud transitioning and the transition itself—including migration, standardization and registration.

Conclusion

Disaster recovery has never been more important, but too many organizations are hampered by lack of focus, lack of funding and insufficient skills. In addition, many organizations simply do not have the knowledge gleaned from previous disaster recovery experience to anticipate the myriad things that can go wrong with their strategies. With more than 50 years of experience in business resilience and information protection, IBM is deeply qualified to help. We have a broad portfolio of services to accommodate a variety of recovery point objectives and recovery time objectives. (See Figure 3.) We offer 150 resiliency centers in 50 countries, staffed by more than 1,800 disaster professionals.

IBM is an acknowledged leader in the cloud-based data backup and server recovery market, offering organizations the ability to protect critical data and applications, then restore them in minutes. Our services allow us to customize solutions so they meet the recovery needs of our clients. Finally, IBM offers services to support employee productivity and help organizations avoid loss of revenue and reputation, often at a lower total cost of ownership than in-house plans. Together, these services help enterprises avoid the pitfalls of outdated disaster recovery practices.

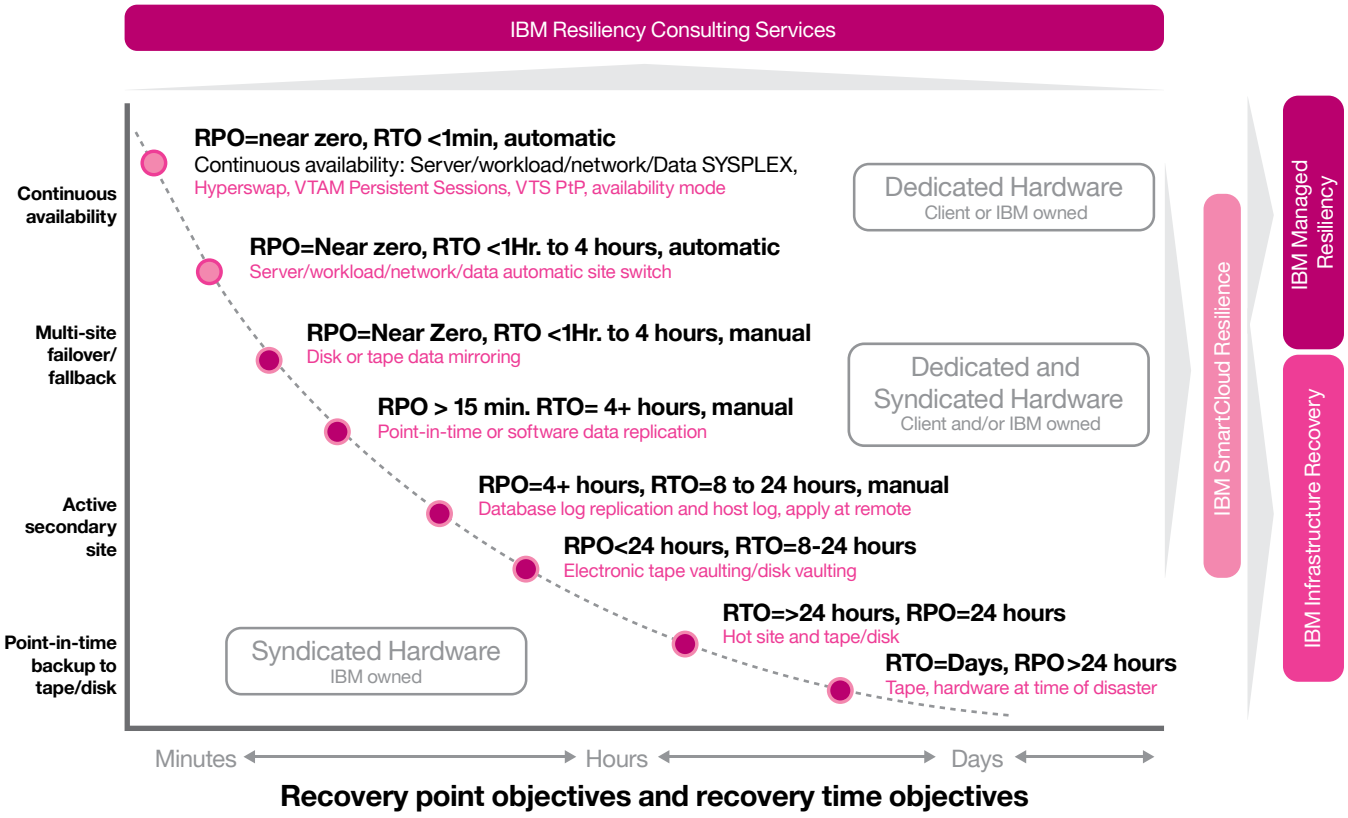

Figure 3. IBM Resiliency Consulting Services offers numerous approaches for supporting different recovery time objectives and recovery point objectives. Organizations may choose a continuous availability approach for their most business-critical applications, and longer recovery times for applications deemed less vital.

For more information

To learn more about IBM disaster recovery services, talk to your IBM representative or your IBM business partner, or visit:

ibm.com/services/continuity

IBM Corporation
IBM Global Technology Services
Route 100
Somers, NY 10504

Produced in the United States of America
August 2013

[1, 2, 4] *The Risks of "Do It Yourself" Disaster Recovery*, a commissioned study conducted by Forrester Consulting on behalf of IBM, January 2013.

[3] *Six keys to effective reputational and IT risk management*, IBM, 2013.

Please Recycle

BUW03031-USEN-03