MAYER
BROWN
ROWE
& MAW

Disaster Recovery and Business Continuity

www.mayerbrownrowe.com

Introduction

This article is presented in three parts. Part I is an overview of the steps businesses should take in preparing, rehearsing and testing an effective business continuity and disaster recovery plan. Part II discusses the effect of 9/11 on business continuity and disaster recovery, and some practical suggestions for addressing the challenges that have recently emerged in this area. Part III discusses the decision to use outsourced business continuity and disaster recovery services, sets forth some general factors in evaluating a service provider, and suggests certain elements to be included in a business continuity and disaster recovery services agreement.

Disaster Recovery and Business Continuity

Context

For the purposes of this article:

Disaster recovery or DR means the process whereby, following a disaster or other disruptive event causing a company to lose, or lose access to, some or all of its data or resources, the company recovers, or gains access to, its lost data and resources through backed-up, redundant or duplicative systems;

Business continuity or BC means the process whereby, following a disaster or other disruptive event impeding or suspending a company's operations, the company restores operations through disaster recovery, failover, backup or mirrored procedures such that the company and the company's customers experience little or no disruption of service;

Service provider refers to a third party providing business continuity and disaster recovery services;

Company refers to a company or other organization providing business continuity and disaster recovery services or procuring such services from a service provider; and

Customers refers to the clients of either a company or a service provider.

While businesses have "backed-up" data since the advent of non-operational storage devices, the use of disaster recovery as a means of bringing a business back online is a recent development. Business continuity is a much broader concept, of which DR is a part, and is reflective of a shift in the corporate environment from mere protection of critical data to constant availability of a company's services. As the term suggests, DR deals with recovery but not continuity; while off-site storage of backup tapes may help a company to insure against a fire at the head office, storage and recovery alone do not provide a solution for resuming business the following day. As businesses are forced to recover from disasters with increasing speed, their focus has begun to shift from DR alone to BC, with DR merely a significant first step. Service providers are quick to point out that in today's marketplace, businesses must remain online, all the time, everywhere, with absolutely no data loss. Living up to such a

standard requires more than reliable safeguarding of data; it requires the development of plans that provide contingencies for disruptions to all business components and contemplate types of disasters that, prior to the events of 9/11, would not have been imagined.

I. REQUIREMENTS FOR AN EFFECTIVE BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

A. THE BUSINESS IMPACT ANALYSIS

An important first step in the development of a successful BC plan (BCP) or DR plan (DRP) is the performance by the company of a thorough Business Impact Analysis (BIA). A BIA entails identifying a company's critical business processes and IT systems, determining what may fail in the event of a disaster, and assessing the potential impact of such failures on the business of the company. As we shall see, a good BIA combines elements of a business overview, an inventory process, a cost/benefit analysis, triage, and even prophesy.

The initial stage of a BIA is the creation of a detailed and up-to-date documentation of the company's entire network and IT system configurations. A company should engage in an in-depth inquiry and conduct a detailed inventory in order to produce an accurate record or "blueprint" of all of the company's servers, applications, networks, routers, platforms, switches and individual desktop stations. This blueprint should include information regarding which aspect of the business or which corporate division is served by each IT component and which personnel bear responsibility for individual components. Once collected, this data should be documented with specificity and stored off-site and made accessible online. This ensures that in the aftermath of a catastrophic event disaster recovery personnel can access the information, from a remote location if necessary, and use it to quickly and efficiently grasp the company's IT infrastructure and network systems in the event that the company's own IT personnel are missing or unreachable (as was the case with many individuals during 9/11). The inclusion of information linking IT components to certain corporate divisions or company personnel facilitates the identification of the appropriate IT personnel or division managers to assist with disaster recovery efforts.

Once a company has documented and mapped out the various components of its IT infrastructure, including which business division is served by each, the company needs to use this information to identify those business processes and IT systems or components that are critical to the company's operations and corporate activities. The

company should take special precautions to identify and safeguard those processes, systems and components it deems critical. It should also ascertain the vulnerability of these systems and components with regard to potentially disastrous events. For instance, are some particularly vulnerable to hacking? Are others exposed to the elements? While it is impossible to foresee every possible scenario – no one, for example, could have predicted the events of 9/11 – it is useful for a company to envisage a variety of catastrophic events, from the mundane (weather related power outages or flooding, computer viruses) to the extraordinary (cyber-terrorism, military attacks) in conducting its BIA. A company must anticipate a host of possible disasters, and then attempt to predict the effect of each on the company's IT systems and functions, and assess the impact that a given disaster related IT failure would have on each business division and on the company's operations as a whole. A company should also try to identify and assess the various legal, regulatory and financial risks associated with various types of system failures. The predictions and assessments made during this stage of the BIA should inform the strategies and procedures developed for the company's overall BCP and DRP.

The next step of the BIA is to perform a cost/benefit analysis and risk assessment based on the projected impact that IT failures caused by a disaster will have on each part of a company. This analysis is founded on a simple premise: if a disaster-related failure in a particular system, component or process affects a critical business unit or has a significant detrimental impact on the company's overall operations, the company will be willing to devote greater resources to the repair and recovery of that system, function or process. A thorough BIA not only identifies possible outcomes of a disaster and the effects on various divisions of a corporate enterprise, but also entails a cost/benefit and risk assessment analysis to determine which of those outcomes is tolerable and which warrant the costs of disaster recovery efforts to repair or restore the particular IT system or function at issue.

Based on the results of the cost/benefit analysis, it should be fairly simple for the company to establish a scheme in which certain IT systems and business processes are prioritized over others with respect to disaster recovery efforts. As the final step in its BIA, a company must therefore consider, taking into account all of the factors outlined thus far, how quickly and in what order it wants its various IT systems and business processes to be recovered. Having set forth a fixed sequence to govern the restoration of IT systems, functions and processes that have been damaged or disrupted due to a catastrophic event, a company may then allocate disaster recovery resources and personnel accordingly. These determinations should be formally documented and stored off-site and made available online, together with the "blueprint" of the company's network and IT system configurations, to ensure that the information can be accessed and referred to by disaster recovery workers. These documents will form the foundation of a company's final BCP and DRP.

B. NON-IT ASPECTS OF BCPs AND DRPs

It is crucial to note that while IT is an important aspect of any BCP and DRP, it is not the only aspect of a company that is affected by a catastrophic event. "From public relations to supply chain management to human resources, effective disaster recovery plans need to take in parts of a business that IT managers aren't always able to reach…"[1]

1. The Role of Individuals in a Business Impact Analysis and Disaster Recovery Plan

The identification of those personnel who bear responsibility for specific IT components, or whose corporate area of supervision is significantly impacted by a system failure, is a vital element of a BIA and, as discussed earlier, such information should be included as part of the formal documentation of a company's network and IT system configurations. Those personnel, whether business division managers or IT staff members, have a significant role to play in BC and DR procedures.

Both company managers and IT staffers should be actively involved from the outset in the formulation and oversight of their company's BCP and DRP. A division manager will be better acquainted with the specific infrastructure support and business processes necessary to resume business operations and may be better equipped than an IT manager to anticipate the impact of disaster related delays and failures on, and oversee recovery of, his or her business unit. A company should therefore seek the input of company managers when performing BIAs and developing a DRP, and secure the commitment of company executives at every level and in every department to the development and maintenance of a comprehensive BCP. Steps should be taken to ensure that IT and division managers are well-informed regarding the company's DR procedures, aware of the various "decision points" in the DR effort, familiar with the specific duties expected of them in the event of a disaster (including contacting staff members and communicating with customers, vendors and suppliers) and notified of the time frame and sequence in which these issues should be dealt with.[2] A BIA should provide information regarding the interrelationship between IT systems and corporate divisions that a company can then use to develop procedures for disaster recovery coordination among division managers. A BCP and DRP should also specify precisely which individuals bear responsibility for which tasks and decisions, where they can be

[1] Adam Lincoln: Thinking the Unthinkable; CFO Europe, March 2002; <http://www.cfoeurope.com/200203h.html>
[2] Id.

located, and how they can be contacted. However, in a catastrophic event of the type experienced on 9/11, or even in scenarios caused by more "mundane" disasters such as severe weather, many personnel necessary for a disaster recovery effort may be unavailable or inaccessible. A company should refer to its BIA to determine which recovery procedures rely on human participation, and insure that appropriate back-up is provided in its DRP and BCP.

Just as a BIA identifies critical business processes and IT systems which should receive priority in DR efforts, a BIA should similarly categorize employees, identify which must get back to work the soonest, and arrange for them to have first access to DR facilities and resources. A BCP and DRP should establish a procedure to locate and communicate with employees following a catastrophic event. This will reassure potentially panicky employees, enable individuals to regroup, and speed up the initiation of the recovery process.

2. The Human Factor

Unfortunately, it is often simpler to predict how a catastrophic event will impact technological systems than to guess how individuals might react following a disaster. When a disaster of the scale and magnitude of 9/11 occurs, it is difficult to predict how effectively a BCP and DRP can be implemented. It is also difficult to formulate a BIA that takes into account all of the effects of a disaster of that proportion. Even if a company's BIA successfully predicts and addresses the effects of such a disaster on its IT functions and systems, it is difficult to foresee the effects on the company's employees and staff. While no BIA can predict all of the effects of a large scale 9/11-type disaster on a company's employees and staff, the human elements and tendencies discussed above should nevertheless be addressed in the BIA. The BIA can then be used to configure a plan that not only provides for IT network and systems support, but also for necessary humanitarian support, while providing solutions to address human errors and delay.

3. Third Parties

In the current interconnected and highly specialized business environment, the majority of companies are dependent on a plethora of supply chain partners, vendors and service providers. "Any interruption in the flow of information in a business process, whether internally self-contained or extended throughout the supply chain, has ripple effects across the companies involved."[3] Companies therefore need to work together

[3] Charles King; After September 11: Lessons on Planning and Implementing Business Continuity; The Sageza Group, Inc. 2002; <http://www.sageza.com/available/White%20Paper/After%209-11.pdf>

with their strategic business and supply chain partners to develop BCPs and DRPs that "reduce the risk of significant down time by establishing specific, demonstrable performance guidelines for all involved parties."[4]

A company's BIA should reflect which strategic partners, suppliers, vendors and customers are critical to the company's business operations, and how the company's relationships with those third parties might be impacted by a disaster. The company then needs to incorporate specific procedures for dealing with such third parties into its DRP and BCP. It sounds basic, but if a company's business recovery plan includes a role for a third party supplier or a key customer, the company must ensure that this third party is aware of its role by providing them with the details of the company's plans.

Of course, 9/11 illustrated in graphic detail that a disaster may not be isolated to one company or even to one immediate geographic area. To the extent that a company's third party partner, supplier or customer might be affected by the same disruptive event, a company should also make an effort to become aware of the third party's own BCP and meet to discuss and coordinate overlapping responsibilities.

4. External Factors

Even if a company's BCP and DRP provide for effective back-up for all of the company's IT systems and successfully protect its business data, the company cannot set its BCP and DRP into motion and resume its business operations unless it is physically able to access its information systems and backed-up data. In performing a BIA, a company should anticipate that essential services and physical infrastructure may be severely impacted as well, hampering attempted disaster recovery efforts. Anyone who tried to travel into Manhattan or use a phone in New York on 9/11 knows that such failures can create disrupt business processes and need to be considered when developing a BCP or DRP. When formulating its BCP procedures, a company should consider whether access to its backup data or off-site recovery facility depends on physical infrastructure such as roads, tunnels, bridges, or phone lines that might be affected by the same disaster. If a company's recovery plans require the transportation of equipment or personnel to an off-site location, but roads are blocked due to a large-scale disaster, the company's plans should provide for alternatives.

When developing such alternatives, it is in a company's best interests to be innovative. For example, after the 9/11 attack destroyed the phone lines of one downtown Manhattan firm, it had customer calls forwarded to an answering service, which then sent emails about the calls to company employees, who were then able to

[4] Id.

call the customers back on cell phones.[5] A company should propose and test alternative telecommunications or transportation routes before incorporating them as part of its disaster recovery or business continuity plans. Which brings us to the next subject: the testing and maintenance of DRPs and BCPs.

C. TESTING AND MAINTENANCE OF BCPs AND DRPs

It vital that a company set up formal procedures for the periodic testing and updating of its BIA, BCP and DRP. A company might consider establishing a DR team to rehearse the BCP and DRP, handle ongoing disaster planning and update recovery plans on a regular basis. This team can develop hypothetical scenarios and rehearse plans based on the company's BIA, applying them across all divisions of the business. Following a rehearsal, the group should identify the plan's shortcomings and improve the DR procedures where necessary. Improvements to the plans should not just focus on IT recovery, but on meeting the needs of the company's employees, customers and supply chain partners as well.

The company must remember to update and retest their plans whenever it adds another critical application or system to its IT network. IT system configurations should be regularly updated, documented and archived. In addition, as new technologies develop, they should be tested and incorporated into the company's BCP and DRP. For example, Blackberry devices and satellite phones are two relatively new technologies that proved highly useful to companies who used them in their disaster recovery efforts on 9/11. Other new technologies are discussed further in the next section.

It behooves a company to place a priority on completion of a BIA and the development and upkeep of an effective BCP and DRP. How well a company's management can handle the aftermath of a disruptive event reflects on the overall corporate governance mechanisms and capabilities of a business enterprise. The presence of a comprehensive BCP and DRP will give the company's investors, customers, and supply chain partners confidence in the management's abilities and in the business's capability to withstand and recover from a disaster.

[5] Joel Snyder: Lessons on Disaster Recovery; Network World Fusion 2001; <http://www.nwfusion.com/cgi-bin/mailto/x.cgi>

II. EFFECT OF 9/11 ON DISASTER RECOVERY AND BUSINESS CONTINUITY

A. NEW CONCERNS IN THE AFTERMATH OF DISASTER

An effective BCP and DRP needs to address the possibility of any or all of a company's crucial IT systems and business units, key partners and necessary personnel, identified through a thorough BIA, suddenly becoming unavailable. The fundamental lesson arising from the experience of those companies most affected by 9/11 is that achieving business continuity is a function of a company's ability to replicate and disperse its critical data, resources and personnel. In other words, the best way to ensure that critical data are not lost, and personnel not rendered ineffective, in a disaster is to store multiple backups of all such data at several dispersed locations, and have multiple sets of recovery personnel who can each handle the crucial recovery processes if the others are prevented from doing so. Maintaining active data centers (ACD) in multiple locations both across the country and overseas is the most effective way to ensure that critical data and personnel are never lost, even if one such ACD is destroyed or disabled.

A related best practice for preserving critical data is to use disk-based replication rather than tape backup. Not only is disk-based replication more reliable, but in the event of a disaster, tape data can require several days to restore while remote disk data can be restored in a matter of hours or even minutes. Tape recovery is resource intensive, often depending on the ability of ground transportation to deliver the tapes to the recovery center after a disaster and requiring several people to complete the restoration process. In New York, some companies were still restoring tapes months after 9/11.[6] Tapes are more cumbersome to store and transport and are also more vulnerable to physical damage. Remote disk-based replication enables more rapid restoration of business processes in an automated, synchronized and timely manner, and does not require nearly as many resources to complete the restoration process. The process of backing up data remotely to disk is called mirroring.

The two main choices for remote disk mirroring are synchronous and asynchronous. Synchronous remote mirroring ensures that the remote site fully reflects all data additions, modifications and transactions, but in distances over 400 miles, this method begins to create some amount of latency (a gap between the time at which the

[6] Charles King; After September 11: Lessons on Planning and Implementing Business Continuity; The Sageza Group, Inc. 2002; <http://www.sageza.com/available/White%20Paper/After%209-11.pdf>

data leaves the company and arrives at the remote site). Asynchronous remote mirroring mitigates this latency, but data backed up using this method will not leave the company until anywhere between two to fifteen minutes after the transaction has occurred.[7] In other words, synchronous mirroring ensures that no data is lost, but may require some time before the mirrored data can be accessed, while asynchronous data is available the moment the data leaves the company, but such transfer will only take place two to fifteen minutes after the transaction occurs, such that some data will be lost during the few minutes following a disaster. Therefore, a combination of both methods is preferable for companies that cannot afford any data loss whatsoever and have sufficient resources to maintain both close and distant remote storage sites

After conducting its BIA and identifying all key partners and external dependencies, it is important for a company to work with those partners to ensure that the company's BCP minimizes any possible downtime by providing clear, detailed and rehearsed guidelines for such partners to follow in case of a disruption in business. For example, many companies have implemented electronic supply chain management (SCM) platforms to automate and streamline their supply partner relationships, or have rolled out enterprise resource planning (ERP) systems to make certain critical business processes (such as inventory maintenance, customer service and order tracking) more efficient. Both platforms require constant communication and cooperation with key third parties. In the event that one such platform becomes disabled, it is imperative that the company have pre-established recovery procedures for quickly identifying the collection of key third parties and implementing alternative measures for preserving the relationships while the platforms are restored. In addition, companies will want to work with their telecommunication providers, Internet service providers and other utility providers to ensure that each has their own contingency plans to deal with disruptions on their own ends and that each is aware of the role they are to play in the company's own BCP and DRP.

An effective BCP and DRP must also address the human factors and dependencies identified in the BIA. One important lesson learned in the wake of 9/11 is that employees may be unable to perform their duties during and after a serious disaster. The emotional stress caused by such events can be enough to impair even the most reliable staff members. Even those employees with the ability to put emotions aside and work toward restoring regular operations may be prevented from doing so by closed buildings and roads and other safety considerations. Similarly, employees at a company's service providers, suppliers and other key partners may be unable to work during and after certain serious disruptions. An effective BCP and DRP can address these issues in several ways. First of all, companies can explore ways of automating critical recovery tasks for rapid and reliable recovery. Automated recovery procedures

[7] Id.

that can be launched remotely are likely to recover critical processes more rapidly and reliably than systems dependant on people. Second, after identifying the critical recovery personnel, an effective BCP and DRP will provide mechanisms for contacting those people (who, as mentioned above, should be located at dispersed locations) and communicating their responsibilities to them. In addition, the BCP should contain provisions empowering staff with the authority to make certain key decisions outside the traditional bureaucracy when those processes impede rather than enable effective solutions. This may involve granting staff temporary authority to order new equipment, confirm configurations and allocate additional personnel.

Finally, and perhaps most importantly, an effective BCP should also provide senior executives with guidance on how to handle the trauma suffered by employees following a serious disaster such as the disasters of 9/11. Before employees can return to work or even begin implementing disaster recovery procedures, they may need to talk about what has happened to them, and to their friends, family and customers. Executives must let their employees know how much they matter to the company and give them a chance to deal with what has happened before asking them to act.

B. NEW SOLUTIONS AND TECHNOLOGIES

While the standards for general business performance have greatly increased, so have BC and DR technologies emerged enabling companies to maintain such standards, even after the occurrence of a disaster. Such new BC and DR technologies include virtual private networks (VPN), storage area networks (SAN), voice over Internet protocol (VoIP) and satellite links. New solutions employing these technologies include synchronous remote data replication to a data center and asynchronous data replication to a hot standby, as mentioned previously; remote virtual tape; fiber channel SAN tape/disk extensions; and iSCSI tape backup. According to the Meta Group, networked storage through SAN and networked attached storage (NAS) will account for about 70 percent of all storage by 2007 or 2008.[8] Also emerging are storage resource management (SRM) tools which identify critical applications and data dependencies (such as IBM's upcoming intelligent device discovery tool designed to automate the asset inventory and tracking process within an enterprise).

One area where these new technologies can be most useful is voice services. While the Department of Defense designed the Internet to withstand a nuclear attack, voice services are far more easily disrupted, as evidenced by the 200,000 Verizon

[8] Jacqueline Emigh; Your Disaster Recovery Plan: How Newer Technologies Will Help; May 17, 2002 <http://www.enterprisestorageforum.com/technology/features/article/0,,10564_1140551,00.html>

Communication lines knocked out by network failures on 9/11.[9] Public telephone and shared packet networks may require weeks or even months to reestablish following such a disaster. VPNs, which are deployed on an IP network, can provide unlimited virtual circuits, unlike the circuit-based public telephone and shared packet networks, and can be deployed in hours. VPNs also support multimodal access technologies, including analog, ISDN, DSL and cable, provide end-to-end security, and are less expensive to support and maintain. Voice services also lend themselves to IP networks, which are infinitely more reliable than any single telecom carrier. VoIP exploits many of the advantages of VPNs such as universal IP addressing, multicast communications and integrated support for voice, data and multimedia. Through universal IP addressing, a lost connection can automatically be switched to a new connection from any remote location without any disruption to the communication. In addition, public switched telephone networks provide little or no security while VoIP can offer various levels of security and encryption. Satellite services, in turn, provide an excellent method for backup communications. With many companies relying on backup sites located more than 100 miles away for data recovery, satellite services offer a reliable backup method that is not dependent on physical lines and, when provided as a utility, can be very cost effective.

Another emerging technological trend in DR and BC is the use of Web-based recovery and continuity services. DR and data centers can be expensive to maintain, especially when disasters triggering their need will most likely be rare. New products that exploit Internet capabilities can help companies offset this added cost. Maintaining critical data and applications on the Internet can enable employees to resume work from any location with a computer and an Internet connection, such as temporary offices or even their own homes. For example, the Anyware RealTime WebSheet™ from VistaSource and RIMES Online™ from RIMES Technologies Corporation enable dealers and traders to create a mobile or virtual trading desk. According to one industry expert, such solutions would have enabled firms whose dealers and traders were affected by the events of 9/11 to simply have staff continue working from home locations in the weeks and months after the disaster.[10] The DR site itself would have needed only to implement a new server and install the firm's analytics and models created with the Anyware™ software, eliminating the need to reconnect the plethora of data feeds and trading stations that such firms depend on. The process of setting up such a solution requires a great deal of server and software configuration (e.g. routing backups of all of the firm's data feeds to the backup server and the virtual trading platform) but disaster recovery planners can perform this work in advance, and going

---

[9] *Disaster Recovery and Business Continuity Planning, Post 9/11; PWC, April 2002; <http://www.pwcglobal.com/servlet/printFormat?url=http://www.pwcglobal.com/extweb/manissue.nsf/DocID/AB49D633F32BF73C85256BA800577B49>*

[10] Dave Shore; Web-Based Solutions Can Ensure Business Continuity; May 28, 2002; <http://www.zdnet.com.au/newstech/enterprise/story/0,2000025001,20265544,00.htm>

forward they would need to focus solely on maintaining the ready availability of a reliable server. Other Web-based solutions such as online data storage and Web-based SCM and ERP platforms also help ensure that a company can recover quickly, and with minimal resources, from the temporary or permanent impairment of its physical plants or offices. Combining Web-based solutions with data mirroring, replication and dispersal measures will do much to ensure that at least one set of all critical data and applications is up and running at all times.

III. OUTSOURCED DISASTER RECOVERY SERVICES AND BUSINESS CONTINUITY

A. DECISION TO OUTSOURCE DR AND BC SERVICES

1. Benefits of Outsourcing

Most companies simply do not have the staff, the resources, or the infrastructure to carry out all aspects of the BC and DR services they require. Maintaining DR centers and multiple, redundant office space for the few periods and again when they suddenly become necessary is costly and inefficient. Supporting and keeping DR systems up to date requires ongoing investment and attention to evolving trends and technologies. Clustering and mirroring requires constant monitoring and testing. Most companies do not want to spend large sums on infrastructure and personnel solely to strengthen and update their contingency plans. Outsourcing BC and DR services offers a viable solution to these challenges.

Outsourced solutions can offer the redundancy and security required at significantly lower costs than in-house services. Technology upgrades and system maintenance are a standard part of any hosted service and most BC service providers will commit to constantly improving the quality of their service over the term of the outsourcing agreement. Outsourcing also offers companies a wide range of BC and DR solutions; remote data storage, Web-based hosting, network security and DR centers can all be offered on a hosted basis. BC and DR service providers' own storage facilities and equipment are both redundant and specifically designed to withstand disasters in order to protect both them and their customers.

2. Selecting an BC and DR Service Provider

After the events of 9/11, many service providers have begun to offer BC and DR services and solutions. Such services may range from consulting and assistance with the development of BCPs and DRPs, to providing hardware and software solutions for DR and BC, to maintaining multiple alternative facilities equipped with office equipment and systems for IT operations, call centers or other critical business processes. The particular nature of a company's critical business processes, and the particular recovery requirements of those processes, largely will dictate the choice of service provider.

Despite their often differing needs, most companies will need to consider a few fundamental factors in evaluating a potential BC and DR service provider. Specifically, service providers must be able to understand how a company's IT architecture relates to its overall business strategy and the role of various systems within the larger framework of the company's operations. They must have a clear focus on BC and not merely DR alone, and understand the business-critical requirements and dependencies of the company. They must have a complete picture of the company's key third party relationships and offer solutions to recover from disruptions to those relationships. Service providers must have the resources and expertise to manage complex continuity and recovery systems and keep these systems up to date. An added benefit is experience across companies' range of industries, geographic regions and types of disaster situations, increasing the service providers' ability to think for the company and make intelligent and quick decisions.

For their most critical business processes, companies should seek the utmost protection and commitment from service providers. Service providers must be able to guarantee that they have the resources to accommodate and protect such critical processes, even in the event of simultaneous disasters with several of their customers. This factor requires sufficient physical space, sufficient workstations and other hardware, and sufficient human resources to run the services for several customers at once. It also requires the ability to support multiple platforms and IT environments (they should at least be able to support all of the platforms and environments used by the evaluating company). With respect to less critical processes, or for companies unable to afford the cost of such a high level of service, many service providers operate on a first-come / first-served basis. In the event of disasters like 9/11 where many companies in a small geographic are affected all at once, such service providers will likely be unable to handle the needs of all of their customers. Therefore, the best practice for companies choosing to take this latter route is to have maintain some BC and DR procedures in-house and/or use a second BC and DR service provider in a limited fashion (e.g. for the more critical data and processes).

3. Offshore Outsourcing After 9/11

The benefits of outsourcing offshore have not diminished as a result of 9/11. If anything, because the attacks caused damage on American soil rather than abroad, offshore outsourcing of DR services might be more appealing than ever. Enterprises with manufacturing facilities, data storage facilities, and DR centers abroad may be better placed to withstand disasters in the United States, and outsourcing these functions to an offshore service provider may further achieve the advantages of outsourcing discussed above.

Companies deciding to pursue offshore outsourcing options for DR and BC services or other services should nonetheless consider certain recommendations to deal with the possibility of disasters occurring at the service provider's location. Companies should consider the political, social and economic risk of the offshore location, including whether political unrest is likely to disrupt business activities, whether the social climate is such that offshore employees can be relied upon to remain committed to a foreign customer, and whether the economic situation adequately protects the fiscal side of the outsourcing arrangement. As well, companies should consider the language skills of the offshore staff, especially with regard to telecommunication and satellite access. Communication with the offshore provider will be key in times of disaster and disruption; both the company and its customers will rely on easy communication with and via the service provider and companies should ensure that the provider has the language skills to solidify this communication.

On an operational level, companies should consider selecting offshore service providers that have a local development facility that can handle maintenance and development operations in the short term while the offshore disruption is resolved, and the applicable outsourcing agreements should specify the number of local resources that the service provider will commit in the event of a disaster at the offshore service center. Second, companies should ensure that all disaster recovery systems and processes are thoroughly documented so that local staff or another service provider can temporarily take over for a disabled service provider, and should have a local project manager or service provider liaison that can step in and handle this process. Finally, outsourcing customers should evaluate the offshore service provider's own disaster recovery plans and security policies, which should include maintaining multiple communication links, remote hot sites and redundant systems that can be used in case of a disaster.

B. KEY PROVISIONS IN A DR AND BC SERVICES OUTSOURCING AGREEMENT

1. Scope of Services to be Provided

Clarity as to exactly what the service provider will do once a disaster is declared should be the company's primary focus. The service provider may be asked to participate in the design of the actual BCP and DRP and then perform any or all of the tasks described therein such as carrying out the remote disk mirroring, maintaining business recovery centers, setting up a VPN or a wireless network and rerouting voice and data networks to restore connectivity, as well as (with the help of the company) regularly rehearsing, testing and updating the two plans. From the company's perspective, the scope of services set forth in the agreement would ideally be all-inclusive. Specifically, the customer could request that the services performed by the service provider include those set forth in the BCP and DRP plus all incidental services not described which are necessary to fully restore all critical operations of the company. However, there is clearly a cost trade-off to such a provision. The service provider will resist such breadth of responsibility or else may price it at a significant premium. Ultimately the costs of the various levels of protection available will need to be evaluated against the potential business impacts. Whatever scope of services is chosen, those services should be tested and rehearsed to ensure that they meet the desired objectives in the event of a disaster.

2. Defining A Disaster

Before a service provider takes action to grapple with a disaster, a determination must be made that a disaster has occurred. Broadly speaking, a disaster can be defined as any unplanned event which prevents a company from conducting its business and servicing its clients. But such a definition does not clearly state when the service provider should begin providing DR services or deal with the specifics of the company's business and operations. One solution is to both (a) have the services begin automatically upon the occurrence of one of the pre-determined events enumerated in the services agreement, and (b) allow the company, in its sole discretion, to declare a disaster. The service provider is in the best position to monitor and determine whether one of the enumerated events has occurred. Automatic activation of the DR services is important if the disaster is such that the company is unable to notify the service provider on its own, and if the company is willing to pay the additional fees needed to invoke a disaster recovery plan then it should be entitled to make a disaster declaration at will.

3. Priority

Service providers have numerous customers. If a disaster occurs, when will a particular customer receive the service provider's attention? First-come first-served priority systems are not always the most beneficial because they create a scenario whereby companies race to declare a disaster, thereby ensuring that they will have their needs addressed by the service provider before the service provider's other customers.[11] In a disaster recovery services agreement companies should try to negotiate to receive at least the same priority as the service provider's other customers. Such a guarantee may be of limited effect if the service provider has only limited space and is forced to make a choice between which companies to service. With new storage technologies emerging every day, it may not be unreasonable to require the service provide to warrant that it has sufficient capacity to handle all (or some high percentage) of its clients in a given geographic in the event they all suffer simultaneous disasters. DR service providers also typically do not count on having to provide continuity services to their customers for long continuous periods of time. Companies should therefore require the service provider to warrant that it is able to provide continuous services to the company for as long as is necessary for the company to resume normal operations.

4. Service Level Agreements

Every outsourcing agreement should contain service level agreements (SLAs) against which the service provider will be measured. In the case of a BC and DR services agreement, the core SLAs should cover all of the service providers primary responsibilities, such as the maintenance of the DR centers, recovery equipment and facilities to ensure that they remain updated to reflect any changes in the company's IT architecture and operational environment. In particular, the SLAs should set minimum standards for time and effectiveness of failover, failback, mirroring and clustering processes, and should require the service provider to restore such critical processes as bandwidth, IT processing speed and telecommunication services at the same speeds and levels at which the company normally operates. The SLAs should set forth target service levels for the main DR processes, often expressed as percentages (e.g., 99.95% of data will be backed up within 5 minutes of each transaction), and credits should be issued to the company if the service provider misses the target levels (e.g., 5% of the fees allocated to data backups will be credited for every 5% difference between the target level and the service provider's actual backup performance). The good news is that with most BC and DR arrangements there now exists sufficient experience and available data to enable companies to make informed decisions about their SLA needs and requirements.

[11] See Tari Schreider, US Hot Site Market Analysis & Forecast, available at www.drj.com.

5. Force Majeure

Another important consideration in negotiating a BC and DR services agreement is whether and to what extent the service provider will be entitled to avoid or cease performing the services due to force majeure events. This is important given that a typical force majeure provision may end up relieving the service provider of responsibility at precisely the time when the company needs the provider's DR services. Ideally from the customer's perspective the occurrence of force majeure should not impact the provision of disaster recovery services. For example, war with the Taliban in Afghanistan would not prevent most service providers within the United States from providing their services. However, if the service provider in question had resources requisitioned by the United States government to assist in the war effort then it may become difficult or impossible for the service provider to perform its duties. In that instance, the service provider would want to be able to be excused from performing (at least temporarily) under the theory of force majeure. Given the nature of BC and DR services, the force majeure events enumerated to excuse non-performance by a service provider should be extremely limited and carefully drafted to include only those events against which the service provider is truly incapable of protecting itself. Since BC and DR service providers are paid precisely to defend against such things as fires, flood, labor disputes, and the like, they are in the best position to ensure that such events do not impact their services (e.g., by employing rooms that purge all oxygen to prevent fires; by paying their staff enough to avoid labor disputes; or by suspending equipment off the ground to avoid flood damage), and therefore such predictable disasters should not be set forth as force majeure events. Other occurrences, such as acts of war, rebellions or revolutions may be more appropriate events upon which to excuse performance.

6. Insurance

One way of addressing the force majeure issue and the potential exposure faced by the service provider is to require the service provider to carry insurance that is triggered in the case the service provider is rendered unable to provide the needed services to the company, or where the service provider simply fails to provide the recovery and continuity services for which the company contracted. Such a provision would aim at compensating the company for damages it sustains as a result of the service provider's failure to perform. Although certain force majeure events, such as terrorism, are typically carved out of many insurance policies, the ISO's current standard form allows for terrorism coverage up to $25,000,000, and some carriers will offer increased amounts, albeit at increased premiums.

Conclusion

The risks of not having a BCP and DRP are potentially enormous and may result in loss of data, business interruption, loss of goodwill and impact on stock price, and liabilities (for example, negligence claims for failure to maintain sufficient disaster recovery arrangements; breaches of contractual obligations due to interruption of services; and failure to comply with regulatory obligations of the business). The results could even entail bankruptcy for the company[12] and potential personal liability for its officers and board of directors. An effective BCP and DRP requires careful analysis and evaluation of the entire enterprise, and a commitment to make business continuity a priority and business-wide focus. Although some companies may have the resources and expertise to handle business continuity and disaster recovery in-house, many companies will want to take advantage of the cost savings and technology expertise of BC and DR service providers. And perhaps the most important thing to keep in mind in the aftermath of 9/11 is that disasters such as fire, power failure, work stoppage, phone failure, denial-of-service attacks and the like are no longer the only types of concerns facing BC and DR planners, even if they will doubtless affect more companies sooner than the next act of terrorism or act of war. Careful planning for all types of disasters is key if companies are to keep up with the stringent availability and recovery standards facing businesses today.

For further information contact David Hudanish (212-506-2524) dhudanish@mayerbrownrowe.com or Nigel Howard (212-506-2121) nhoward@mayerbrownrowe.com.

[12] Roberta Witty & Dona Scott, Commentary: Firms Need Recovery Pans, CNET News.com, September 13, 2001 ("Gartner estimates that two out of five businesses that experience a major disaster go out of business within five years").

MAYER BROWN ROWE & MAW