

MBA NewsLink

Disaster Preparedness/Business Continuity Planning: Readiness in the Face

MBA (6/12/2007) Mouhalis, Jeff

(Jeff Mouhalis is CIO and executive vice president of product delivery with Fidelity National Information Services, Jacksonville, Fla.)

(Part I of a four-part series.)

It's an unfortunate fact that today's world is fraught with potential perils, whether of the natural or human-made variety. As the aftermaths of the attacks of September 11th and Hurricane Katrina have shown, the ramifications of any disaster can be substantial and far-reaching, affecting individuals, localities, governments and private businesses. While there are many possibly disastrous threats, there are also concrete steps businesses can take now to establish plans for preparedness and business continuity.



Jeff Mouhalis

There is no way to sidestep calamitous events, but preparedness can mean the difference between successfully weathering the storm presented by the event or succumbing to its force. Companies must be better prepared than ever before to deal with a wide range of possible disasters that could disrupt their businesses. Unfortunately, many have yet to develop adequate disaster preparedness and business continuity plans, while others admit their current plans are simply not adequate.

One thing is certain: the interconnected and interdependent nature of business and world economies suggest that any major natural disaster, pandemic outbreak or terrorist attack will impact the world at large, far beyond the geographic boundaries of the event itself. This four-part series will examine potential threats to business continuity, the planning process for meeting these threats, specific steps to take and gauging your own and your vendor-partners' preparedness and viability, all to minimize the impact of any potential disaster.

Destruction Shows No Preference

In addition to the familiar—hurricanes, earthquakes, tornadoes and the like—businesses must now contend with new, but equally disruptive, threats as well. Terrorist attacks and global instability are becoming increasingly more probable, and like natural disasters, the global nature of 21st century business translates into a greater field of impact of their effects.

The trend of overseas business process outsourcing and international vendor relationships mean that a disaster or instability on the other side of the globe can have just as disastrous effects here at home. And while every disaster is different in terms of areas affected, amount of forewarning, and length of recov-

ery and reconstruction, in many ways business continuity planning is similar across the board.

For instance, hurricanes and typhoons are often forecast days, if not weeks in advance, but an explosion demands instant reaction, as would an earthquake, tsunami or other sudden catastrophes. Depending on the severity of an attack or industrial accident, recovery can be a matter of shifting operations to an unaffected area, whereas a natural disaster can place entire locales or nations into a tailspin that takes months or years to overcome.

The growing risk of a global pandemic such as Avian flu or other disease presents a unique dilemma. Not merely a matter of increased scope, a pandemic can impact a company's entire workforce and operations, whether all individuals are infected or not. In fact, a global avian flu outbreak—a scenario most experts consider an all but foregone conclusion at this point—will impact nearly every business, wherever they operate worldwide.

Any pandemic would bring about a substantial level of economic disruption whatever its effect on workforce and business activity. However, businesses can plan for threats such as avian flu perhaps better than other, more sudden, disasters, since many contingency plans take advantage of IT to keep businesses running. Even given the worst case scenario—pervasive travel restrictions, quarantines, vendor or employee unavailability and so on, technology will play a large role in keeping businesses up and running.

Preparation Begins Now

Organizations must begin planning today, at all levels of the organization, to prepare for a multitude of threats whose time of occurrence, course of development, and consequences are all wholly unpredictable. The only thing that can be addressed in advance is the contingency plan. The next part of this series will drill down and take a look at what specifically organizations can do today to ensure they are well prepared for the possibility of a future disaster.

(The views expressed do not necessarily reflect the views or policies of the Mortgage Bankers Association. MBA NewsLink welcomes your contributions. Articles and inquiries should be submitted to Mike Sorohan, editor, at msorohan@mortgagebankers.org.)

MBA NewsLink

Disaster Preparedness/Business Continuity Planning: Readiness in the Face

MBA (6/13/2007) Mouhalis, Jeff

(Jeff Mouhalis is CIO and executive vice president of product delivery with Fidelity National Information Services, Jacksonville, Fla.)

(Part II of a four-part series.)

In Part I of this series, we discussed some of the many possible threats to business continuity that organizations face today. The one action that can be undertaken in the face of these threats is concrete contingency planning to ensure that businesses can continue to meet their legal and fiduciary responsibilities even in the worst-case scenario. In this segment of our four-part series, we'll take a look at the business continuity planning process itself.



Jeff Mouhalis

Start at the Top

When determining who should be involved in business continuity planning, it's essential to start at the top of the organizational chart. For any disaster preparedness contingency plan to succeed, executive buy-in at the most senior level is essential. CEO-level endorsement is necessary to achieve maximum participation and funding for the effort, as well as to send the message throughout the organization that the program is crucially important.

Executive commitment and visibility are important first steps, but must go hand-in-hand with a clear vision for business continuity that is centered on identifying, measuring and mitigating risk associated with disastrous events. With clear vision, BCP becomes mainly a procedural affair, and as such, a goal every company can successfully achieve.

To approve funding and other resources for the planning process itself and plan execution in the event of disaster, companies should establish a cross-functional oversight group composed of executives who are authorized to drive the program at all levels. They should also ensure that business continuity initiatives align with the company's overall business strategy. The group should meet regularly to review the progress of the planning process and direct or redirect priorities as necessary to achieve BCP goals.

Cover All the Bases

Taking the additional step of appointing a full-time, certified BCP manager to develop the program vision and to campaign for management support and funding for the BCP program adds an important dimension to the program. This manager sponsors and/or coordinates all major disaster preparedness initiatives and is responsible for crisis management logistics and coordination in the

unfortunate event of any disaster.

Another key to a successful BCP initiative is creating a planning process that includes every functional department in the organization and establishes participation and accountability across core processes and functional departments. Plans should be made for offsite continuance of essential business operations through the deployment of strategies such as site redundancy, telecommuting for critical employee roles, Web-based audio and video conferencing solutions and so on.

By their very nature, disasters are chaotic events fraught with confusion, and it's difficult to overstate the importance of pre-establishing well-defined roles and responsibilities throughout the company. Individual department managers, for example, must have their own clearly delineated functional plans to enact in cases of emergency. Given the potential for chaos and overall disruption, planning must also include measures for ensuring employee and client communications throughout the disruptive event. Critical teams must be assembled to address matters of onsite security and offsite command centers. It must also be understood by everyone involved that business continuity planning is not a simple 'one-off' effort and that continual testing, evaluation, and—when necessary—restructuring of the BCP is critical to success.

Up Next

As mentioned in the first part of this series, IT plays a critical role in disaster preparedness. Backup systems and communication channels should be established and continually tested for readiness and operational integrity. It cannot be overemphasized that steps must be taken today to ensure that critical systems will continue to operate, regardless of the circumstances of a particular disastrous event. We'll look specifically at IT contingency planning next.

(The views expressed do not necessarily reflect the views or policies of the Mortgage Bankers Association. MBA NewsLink welcomes your contributions. Articles and inquiries should be submitted to Mike Sorohan, editor, at msorohan@mortgagebankers.org.)

MBA NewsLink

Disaster Preparedness/Business Continuity Planning: Readiness in the Face

MBA (6/14/2007) Mouhalis, Jeff

(Jeff Mouhalis is CIO and executive vice president of product delivery with Fidelity National Information Services, Jacksonville, Fla.)

(Part III of a four-part series.)



Jeff Mouhalis

In the first half of this series, we discussed potential events that could create business disruption challenges and the foundational components of establishing a comprehensive business continuity plan. Certainly, resources and business processes attached to contingency planning must be designed to minimize the likelihood of an unplanned business interruption and to minimize the negative effect on critical services, should one occur.

Redundancy is Key

In many ways, IT preparation for disasters is not much different than established best-practices for service and technology providers across the board. Standards of redundancy for systems, communications channels, power supplies and data are all key components for ensuring minimal disruption to operations for the in-house organization as well as for vendors and/or clients.

Most companies deploy multiple electrical feeds to support critical environmental systems, central and distributed computer systems and office workspaces. Since municipal utilities may be compromised in the event of a disaster, electrical power should ideally be backed up by diesel generators with an onsite fuel supply. If one electrical feed fails, an uninterruptible power system should be employed to take over its functions, without disruption, until an alternate electrical power source is up and operational.

Maintenance contracts should be reexamined to ensure the constant viability of environmental and computer systems. Well-documented emergency response and recovery procedures are must-haves, but they should also be rehearsed and tested regularly in order to maintain mission-critical systems. On-site backup capabilities should exist for all hardware and telecommunications used to deliver contracted services, with hardware used for this purpose configured with fault tolerance and dependability in mind.

Disaster procedures for computer systems and business unit operations should spell out the business requirements, strategies, resources and procedures necessary to minimize the likelihood of all types of potential disasters. The plan should also provide for timely and complete business recovery if a disaster occurs. All key personnel

should be well trained on emergency response and recovery procedures.

Of course, daily backups of application data and programs are an excellent hedge against potential situations that cause primary systems to be compromised or destroyed. Backups should reside offsite in secure, environmentally controlled storage facilities located a significant distance from primary data centers. Dedicated disaster backup facilities can include recovery facilities owned by the company, or a contractual arrangement with proven commercial disaster recovery facility providers.

Communication

Formal network switching arrangements should be arranged with long-distance phone carriers. It may also make sense to invest in satellite phones for key executives, in the event that land and cellular lines are down in the wake of a disaster, as was the case after both 9/11 and Hurricane Katrina.

In the case of a pandemic emergency, travel restrictions, quarantines and fear may keep employees and executives from the workplace for extended periods. Therefore, ensuring that every key member of your staff has reliable, secure broadband access to necessary systems and data is important as well. In the case of critical staff, companies should oversee installation of redundant broadband at employee homes.

Working in tandem, off-site disaster recovery facilities and telecommunication recovery arrangements can enable quick recovery for data processing services. Backup facilities must possess sufficient computing and office equipment, telecommunications, computer/office supplies and other resources needed to deliver the service levels that are required.

When disaster strikes, clients should be notified of your operational status as quickly as possible via telephone, electronic mail, fax transmissions or other means. Regular updates should also be provided so clients understand what to expect and when, and how the company will address client-specific processing considerations during contingency operations.

Next Time

In the final installment of the series, we'll look at coordinating your company's efforts with those of your vendor partners, local governments and agencies, as well as the need for the continual updating and real-world testing of your BCP.

(The views expressed do not necessarily reflect the views or policies of the Mortgage Bankers Association. MBA NewsLink welcomes your contributions. Articles and inquiries should be submitted to Mike Sorohan, editor, at msorohan@mortgagebankers.org).

MBA NewsLink

Disaster Preparedness/Business Continuity Planning: Readiness in the Face

MBA (6/15/2007) Mouhalis, Jeff

(Jeff Mouhalis is CIO and executive vice president of product delivery with Fidelity National Information Services, Jacksonville, Fla.)

(Last of a four-part series.)



Jeff Mouhalis

In the first three parts of this series, we looked at the various disasters and events that could disrupt business operation, the steps companies can take to create a strong business continuity plan for their organization and some specific technological precautions that should be in place to help minimize the amount of time business operations are affected.

In this final installment, we will examine the necessity of coordination with others—clients, vendors and governmental and private organizations—to control the negative impact of a disaster on business continuity.

Partnership

Businesses should be thoroughly familiar with the BCP provisions their vendor partners have in place and ensure that all involved parties are working from the same playbook. In addition to determining if vendors have sufficiently robust contingency plan in place to minimize downtime and continue to provide services, it makes good strategic sense to compare plans before the fact and work to fill any operational gaps on either side.

Coordination between businesses and vendors can make all the difference between absorbing the shock of disaster with minimal harm to operations or having it permanently scar business relationships when processes and systems fail. Equally important is the need for companies to coordinate their own plans with those of local, state and federal government.

Private organizations and agencies such as the Red Cross also have plans for the aftermath of various disaster scenarios. The movement and actions of these, as well as governmental bodies, could help or hinder an individual company's plans for recovery within their locale. It makes sense, therefore, to examine these plans as well (as much as is possible), seeking areas of crossover and possible collaboration. In the chaos following a large-scale disaster, collaboration and coordination with all possible allies makes strategic sense.

Practice Makes Perfect

It's important to remember that disaster preparedness and contingency planning are an ongoing process that must continually adapt to changing realities and new devel-

opments. BCPs should be reviewed and updated frequently as part of normal business planning, introducing changes as need dictates. A comprehensive review should be conducted at least once a year, examining all critical plan points, strategies, team structure and responsibilities and contingency procedures.

Additionally, mock disasters and other 'live' tests of the plan are necessary to determine its real-world viability. Plans should be regularly exercised to provide ongoing validation of recovery resources and processes, training for recovery teams and to identify any weaknesses or improvement opportunities.

The crisis management team should test the recovery performance of central and distributed systems, LANs, WANs and critical applications to validate equipment and procedures. Client support and overall crisis management plans should be tested to validate integration and coordination of business functions during a crisis.

Departmental and functional disaster plans should also be thoroughly tested along with redundancy and recovery of technology assets. Testing methods could include facilitated plan reviews, table-top exercises involving mock disasters, emergency notification drills and business resumption testing conducted at designated recovery facilities.

Disasters do not occur in a vacuum, and neither should a good BCP. At least once annually clients should be invited to participate in disaster recovery tests to assist in validating recovery plans. Companies, clients and third-party vendors should work to coordinate test objectives and develop 'scripts' for the mock disaster and recovery. All test results should be documented and made available to clients. Lessons learned during these tests should direct appropriate plan improvements.

Conclusion

American businesses and their international partners have little say in global events, pandemics, natural disasters or the evil plans of terrorists. The only thing we can control is how prepared our organizations are for the possible disasters that may come our way. If your company does not yet have a comprehensive and well-documented plan for crisis management, disaster recovery, and business continuity, making this initiative a high priority could be the best move you ever make.

Nothing mitigates disaster better than aggressive business continuity planning, testing, training and maintenance. Still, to never need it would be best of all.

(The views expressed do not necessarily reflect the views or policies of the Mortgage Bankers Association. MBA NewsLink welcomes your contributions. Articles and inquiries should be submitted to Mike Sorohan, editor, at msorohan@mortgagebankers.org).