

A New Paradigm for
**Business
Continuity
Management**

Lessons from September 11th

“Never again

do these global companies want to see themselves knocked out of business for days and weeks, or even hours, by a single cataclysmic event.”

The New York Times, January 29, 2002, in an article reporting on the decision of Wall Street firms to move various operations and thousands of employees to New York suburbs.

The terrorist attacks on the World Trade Center on September 11, 2001 were a dramatic test of the business continuity management programs of New York's financial services firms. Most business continuity strategies had simply never envisioned a disruptive event of the nature, scope, and duration of those on September 11th.

Deloitte & Touche was one of the firms affected directly by the attacks—our New York office was located directly across the street from the World Trade Center. That office is now closed, and more than 3,000 of our people have been displaced and are working out of temporary facilities around the New York region.

As a service to clients and the New York financial community, our New York financial services professionals hosted an online conference on November 7, 2001 to assess the changed environment and explore ways to respond. Our firm has advised major global financial services organizations for many years on strategies to maintain the continuous availability of their operations. The November 7th conference provided an opportunity for us to revisit the contingency planning process and gain the perspectives of financial services clients and colleagues.

In this document we distill some of the lessons learned from September 11th and other economic, social, technological, and geo-centric events that have been converging over the past decade, all of which pose threats to the continuity of business operations.

Perhaps the most important lesson from these experiences is that today's business environment is riskier and less predictable than ever before. It requires a new approach focused on *optimizing the availability of all mission-critical assets* – people, processes, data, technology, and facilities – whether addressing disaster situations or limiting downtime in the normal course of business. The elements for this new approach to business continuity management are outlined in this report.

March 2002

The World is Riskier. And It's Not Just Terrorism.

The September 11th terrorist attacks put business continuity management on the top of the senior management agenda. While most financial services firms already had contingency plans in place to respond to disruptive events such as fires, telecommunications breakdowns, and computer viruses, September 11th changed everyone's perception of the probability and impact of formerly unimaginable events and the requirements for effective business continuity strategies.

Lessons from New York's Ground Zero

Considering the unprecedented events of September 11th, the financial services industry responded well. Employees moved to contingency sites or to newly leased facilities. Data processing was switched to backup data centers. Firms allowed competitors to share their facilities. After closing for four days to allow its member firms to reestablish operations, the New York Stock Exchange (NYSE) reopened.

September 11th was certainly not the first time that major financial centers have been subjected to serious disruptions. London has endured politically motivated bombings; the Credit Lyonnais headquarters in Paris suffered a major fire in 1995; Tokyo's subway system was the site of a lethal gas attack. These events had led financial services firms to reexamine the quality of their business continuity strategies.

The destruction caused by the attacks on September 11th, however, was of an entirely new order of magnitude. In all, 30 million square feet of office space in downtown Manhattan were either destroyed or damaged, equivalent to 30 Empire State Buildings. Insurance claims are expected to range from \$30 billion to \$60 billion, far higher than the record of

\$16.8 billion from Hurricane Andrew in 1992. The concentration of securities processing firms in lower Manhattan raised concerns about the potential impact on the US financial system.

September 11th demonstrated that financial services firms need to revisit their business continuity strategies and 'think the unthinkable.' The financial services industry learned several important lessons on September 11th.

People Issues are Paramount

Many firms found that they were not adequately prepared to provide alternative offices, telephone lines, and computers to displaced employees. Employers quickly learned that while they might have had redundant data systems, the people who ran the systems, made business decisions, or maintained customer relationships could not be duplicated.

Given this experience, a number of banks in the UK have decided to lease contingency office space located outside central cities and separate from their back up data centers.

The emotional impact on individuals of a tragedy of the scale of September 11th also cannot be overemphasized. Some employees were unable to return to work immediately, and many needed support and counseling.

Geographical Concentration Increases Risk

Firms with operations concentrated in lower Manhattan were affected more severely than those with more widely dispersed operations.

The Bank of New York was displaced from four locations in downtown Manhattan that housed its primary data center, foreign exchange and treasury operations, and a securities processing center.

Soon after September 11th, Morgan Stanley decided to sell its new 32-story one-million square-foot office tower, which was located near its headquarters in midtown Manhattan, and instead will purchase a corporate campus north of New York City, citing "business continuity planning requirements."

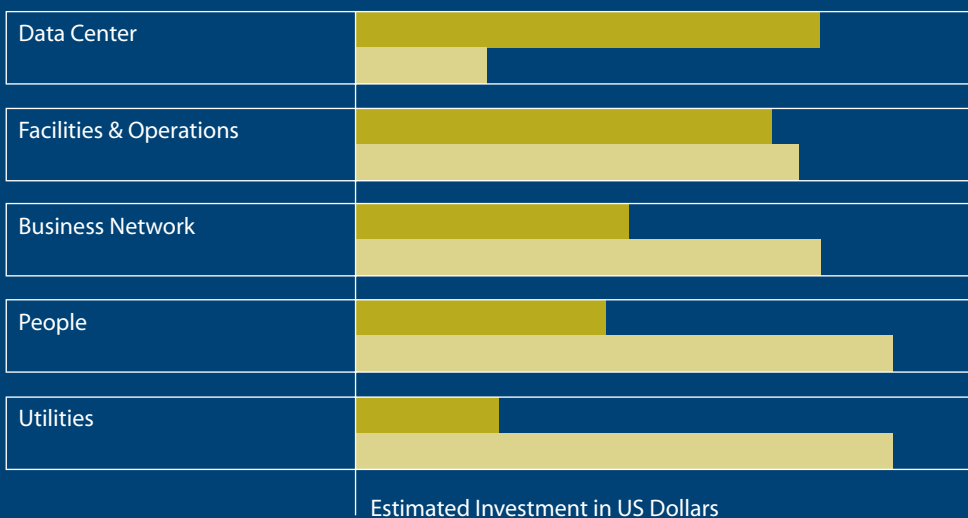
Planning Must Include Desktop Technology

While encryption, firewalls, and backup sites protected data centers, the companies displaced from the World Trade Center and nearby buildings found that much of the information residing on desktop computers and local area networks was lost or inaccessible. The TowerGroup estimates that securities firms affected by the attacks will have to spend \$3.2 billion simply to replace damaged computer hardware including 50,000 workstations, 16,000 trading desks, and 34,000 personal computers.

Transportation Systems are Vulnerable

Business continuity plans had assumed that transportation systems would continue to operate. For example, many plans

BCM Investment vs. September 11th Impacts



With the singular exception of rapid data recovery, both the government and many businesses experienced unacceptable business disruption that challenged current Business Continuity Management thinking.

■ Investment
■ Impact

Source: Deloitte Consulting

called for executives to fly to backup facilities. On September 11th, however, the nation's airports were closed, aircraft were grounded, and all bridges and tunnels into and out of Manhattan were shut down. Executives couldn't travel to backup facilities, and businesses were unable to ship documents or deliver paychecks.

"Many financial services firms found that they were unable to maintain operations on September 11th in the face of simultaneous disruptions to people, facilities, communications systems, and the transportation network. September 11th demonstrated that firms need to reexamine the business continuity strategy for every aspect of their operations."

Ted DeZabala, Partner, Deloitte & Touche, New York

Don't Neglect Vendors

Many companies found they had not paid enough attention to the business continuity prospects of their vendors. For example, the Bank of New York processes half the government securities traded in the United States and 12 percent of the nation's money transfers. When the bank was displaced from several locations and telecommunications systems were disrupted, many trades were delayed in settling and clients were unable to learn the status of trades.

Going forward, firms will need to be certain that their vendors for critical functions such as market data, IT infrastructure, telecommunications service, and call centers have adequate business continuity management.

Safeguard Communications

Despite efforts to obtain redundant service from multiple carriers, many firms were left without telecommunications service when two telephone central offices in lower Manhattan were damaged. One of these central offices was 140 West Street, whose 32 floors of equipment handled 30 percent of the voice and data traffic for lower Manhattan. Firms had difficulty communicating with their employees, other locations around the world, and their clients. Wireless cell phone and pager systems were also affected. The task was complicated further by the Internet becoming overloaded by the rush of people seeking news updates.

Testing is Essential

Some firms found that their backup data centers lacked real-time data and had problems communicating smoothly with the backup data centers of other firms. Frequent testing of business continuity plans is essential and needs to include the other firms and exchanges with which the company needs to communicate. In the summer, Merrill Lynch carried out an extensive, two-day disaster-management exercise that in retrospect helped prepare the firm's people and technology to respond well to September 11th.

Re-Evaluate Insurance Coverage

As a consequence of record claims stemming from September 11th, property and casualty insurance premiums have skyrocketed by up to 400 percent, deductibles are higher, and coverage restrictions are being included in policies (e.g., on terrorism, bio-hazards, or cyber-risks). Increasing costs and the difficulty in obtaining coverage will shift the ROI for alternative risk management strategies.

Event Observations

Business Continuity Plans

- Plans did not provide for the occurrence of successive interruptions in different forms and places
- Communications plans and strategies had limited success or failed altogether
- Non-integrated business unit and business partner plans were insufficient
- Continuity plan, testing and maintenance were inadequately performed

Crisis Management

- People issues were not adequately addressed
- Resource concentration was a significant vulnerability
- Crisis management organizations (e.g., command centers) were inadequate and often redundant
- Technology and network connectivity, both vital to survival, were shown to be unacceptably vulnerable
- Critical service providers, affected by the disaster, performed poorly and invoked *force majeure* clauses

Other

- Public services (e.g. transportation, telecommunication, emergency services) had limited or delayed availability
- Geography was critical to recovery
- Security of vital records was compromised

A View from New York's

New York Financial Services Executives Assess the Impact of September 11th on Business Continuity

The New York office of Deloitte & Touche convened an online and live conference on November 7, 2001 for senior financial services executives to assess the changed environment for business continuity management in light of September 11th and to explore how best to respond. The conference gave participants the opportunity to reconsider the framework for business continuity strategy and learn from the experiences of executives who had lived through the ultimate test on September 11th. The shared insights of clients and colleagues at the conference provided a deeper understanding of the refinements to business continuity strategy required to meet today's new profile of risks.

In opening the conference, Bill Freda, leader of the firm's Financial Services Industry practice, said that while firms were getting back to business as usual, it was a redefined version. The panelists all noted the existence of new, less predictable risks and the difficulties that this more uncertain environment posed for modeling risk scenarios. The consensus was that going forward, business continuity strategies must have the flexibility to respond to a broad range of unexpected events.

Survey Results Show New Focus on BCM

The financial services executives attending the conference were surveyed regarding their approach to business continuity management in the wake of September 11th. Notable survey results included the following:

- Respondents rated people as their highest priority for business continuity management, rating it an average of 4.4 in importance on a scale of 1 to 5
- 83% of respondents said they plan to report periodically on business continuity preparedness to their respective boards of directors
- 74% of the respondents said their contingency plans would include continuous availability strategies in the future; another 11% already had redundant facilities

- 53% of respondents said their firm now planned a geographical realignment
- 64% of respondents said their firm expects to see increased costs of risk mitigation programs
- 68% of respondents indicated that the company plans to also validate their suppliers' and service providers' potential for business continuity

Speakers with First Hand Experience

The conference was chaired by Ted DeZabala, a partner in Deloitte & Touche's Enterprise Risk Services group and a leader in business continuity and security services. The panelists were senior financial services professionals who played key roles in business recovery efforts after September 11th.

Bill Freda

Managing Partner, Financial Services Industry Practice
Deloitte & Touche

Roger Burkhardt

Chief Technology Officer
The New York Stock Exchange

Richard W. Closs

Senior Vice President
Fidelity (National Financial Services Corporation)

Michael J. Lesser

Deputy Superintendent of Banks
State of New York Banking Department

Christopher M. Treanor

Managing Director
Marsh & McLennan

Ground Zero

Fidelity Investments and the New York Stock Exchange were two of the companies affected by the attacks on the World Trade Center. Here are the stories of that day, as told by their executives during Deloitte & Touche's Web conference.

Fidelity Investments

Approximately 1,000 Fidelity employees were located at 200 Liberty Street in lower Manhattan when the World Trade Center was attacked. All employees were evacuated safely — but then the firm faced major challenges.

- A breakdown in telephone and cell phone service cut the firm off from clients and the markets, which had not yet announced that they would remain closed.
- Fidelity tried to contact each employee, but it took four days before all employees could be contacted. Now, the firm has made it each employee's responsibility to contact the firm in an emergency.
- The firm decided to transfer displaced employees to its other facilities in New Jersey, Massachusetts, and New Hampshire. This plan, however, required employees to spend five days each week away from home. Even though they were lodged at nice hotels, after two weeks most employees wanted to be back with their families. Fidelity responded by instituting four-day weeks, providing transportation, and hiring additional people.
- While most data functions were adequately backed up, the firm's risk-management system based in New York was down. The firm quickly bought a server, debugged it, and installed it in their New Hampshire facility by Friday, September 15th, only to be shut down by the Nimda virus a few days later.

Fidelity found that, with a few minor adjustments, its business continuity plans stood the test. All of its operations and business lines were operating when the New York financial markets reopened on Monday, September 17th.

New York Stock Exchange

While its main facilities were not damaged and it was fully operational on September 11th, the New York Stock Exchange (NYSE), had 130 employees on the 29th and 30th floors of the South Tower of the World Trade Center. The Exchange safely evacuated all of its employees, having learned valuable lessons from the 1993 World Trade Center bombing. Still a joint decision was taken by the industry and regulators to close the exchange until September 17th. Several reasons were cited.

- Many NYSE member firms were displaced from their offices and communications links were damaged.
- Increased security and limited transportation options in the area made it difficult for employees to travel to the trading floor.
- Opening could have hampered the rescue effort.

NYSE also helped the American Stock Exchange (AMEX), which had to vacate its main facility and trading floor due to water and power problems. The NYSE invited the AMEX to relocate to its Blue Room. The change of location was invisible to AMEX clients, who continued to send their trades to the Securities Industry Automation Corporation (SIAC), which handles processing for the AMEX and the NYSE. SIAC simply rerouted AMEX trades to their computers at the NYSE Blue Room.

The NYSE knew that public confidence in the financial system was at risk, and that it would have to be prepared to handle exceptionally high volume when the markets reopened. On Monday, September 17th, NYSE systems smoothly handled a record of \$2.3 billion in shares traded on Monday, and \$10 billion for the week, twice the average volume.

The NYSE is taking no chances for the future, and plans to build an alternative trading floor at an undisclosed location.

Unpredictable Risks on the Rise

September 11th was the most destructive instance to date of a new reality—increasing threats of business interruption from a growing list of less predictable, often man-made, risks. Several long-term trends that have generated important benefits have also made business operations more complex and vulnerable to disruption.

- Globalization has allowed firms to enter new markets, but exposed them to terrorist threats in more locations.
- Consolidation offers economies of scale, but mergers often lead to more geographic concentration as operations are combined to achieve efficiencies.

“There are some potential systemic vulnerabilities now due to geographic concentration of the major exchanges and payment systems operations centers. . . . It is the possible coordinated strategic attack on physical operations centers, and on the complex of ‘systems of systems’ which enables this industry to function world-wide, that is of rising concern . . .”

Robert T. Marsh, Chairman of the President’s Commission on Critical Infrastructure Protection, September 11, 1997

- Outsourcing allows firms to concentrate on core competencies, but leaves them more dependent on the business continuity management of their vendors.

The greatest risks, however, may come from the increasing dependence on complex information systems and the Internet. Information technologies have allowed financial services firms to handle ever larger trading volumes, operate seamlessly in multiple locations around the world, enhance customer service, and increase efficiency. Along with these benefits, however, firms now face substantially increased risks from network failures, computer viruses, hackers, and cyber-terrorism.

These threats are not hypothetical. Just one week after the World Trade Center attacks, the Nimda virus infected tens of thousands of computers around the world. Although the cost is not yet clear, computer industry analysts expect that the damage could exceed the \$2 billion to \$3 billion that the Code Red virus cost companies just a few months earlier.

The 2001 Crime and Security Survey by the Computer Security Institute and the US Federal Bureau of Investigation found that in 2000:

- 65 percent of large institutions suffered security breaches resulting in financial losses of \$380 million, up from \$265 million in the prior year
- 94 percent of firms detected viruses, up from 85 percent
- 40 percent of firms experienced external attacks, up from 25 percent
- 38 percent were the target of denial-of-service attacks, up from 27 percent.

The US FBI has warned corporations to be on guard against hacking and other electronic assaults on their information systems. In October, US President George W. Bush established a new federal government office to combat cyber-terrorism.

Not only are threats to information systems becoming more common, the increasing size and velocity of financial flows has dramatically increased their potential impact. And today’s customers, both institutional and individual, expect around-the-clock service and real-time access to market and account information.

With any interruption in business operations potentially crippling, traditional approaches to business continuity management are no longer sufficient. Financial services firms need to adopt a new approach that seeks to ensure continuous operation when unanticipated events occur.

Other Factors Before and Since September 11th

As macro economic, political, and technology trends converge, a paradigm shift in business continuity occurs, from which financial institutions consider the protection of people, assets, and systems under multiple world scenarios.

| | |
|--------------------------------|---|
| Weather | Hurricanes, tropical storms, ice storms, severe weather, floods, blizzards... Weather-related incidents have become a significant influence on business availability, and have increased dramatically over the past decade. |
| Cyber Terrorism | Security incidents are increasing — particularly denial of service incidents, unauthorized penetration, and theft of enterprise data. |
| Explosion of Data | More data will be created in the next three years than in the entire history of the human race. 75% of this data will be rich media – text, image, video, audio, fingerprints, Internet – requiring extensive redundancy and Near Real Time Recovery. |
| Mobile Workforce | An increase in telecommuting helps reduce real estate costs but increases dependence on cell phones, pda's, computer networks, and telecommunications. |
| Cost of Down Time | The average cost of down time has soared to over US\$ 1 million per hour, with dramatic escalation for companies and processes that are increasingly dependent upon the Internet for e-commerce. |
| Enterprise Applications | The rapid adoption of enterprise-wide applications, and an expanding definition of what defines "mission critical", is increasing the demand for more extensive business continuity management. |
| IT Infrastructure | Many institutions have grown their IT infrastructures so rapidly that they are faced with environments that are costly to manage, difficult to leverage, almost impossible to control, and risky to recover. |
| Regulations | Industry regulators are adding their perspective on business continuity, disaster recovery, and security. |
| Economy | All of the above factors are converging in an uncertain economy that has placed pressure on earnings and investment capacity. |

New Risks Require a New Approach

The increasing number of less predictable risks, coupled with the increasing velocity of financial markets, requires firms to adopt a new paradigm for ensuring business continuity.

Business continuity management has traditionally been reactive and tactical. A financial institution typically plans its operations, facilities, and infrastructure to support its business goals, such as enhancing customer service, maximizing revenues, and minimizing costs. Decisions on where to locate facilities, for example, are based on such factors as accessibility to labor force, cost, and quality of transportation systems and other public services.

“In the UK, a number of banks have revisited their business continuity management arrangements. As a result of the events of September 11th, they have decided there is a need to separate staff from IT operations in a crisis situation. Thus they are looking to provide cheaper out-of-town contingency centres for their people, whilst the IT contingency arrangements may remain in the major centres.”

Bernard Kenny, Partner, Deloitte & Touche, London

Only after facilities are installed or infrastructure is built do most firms address the risks inherent in these business decisions. Planning focuses on preventing or recovering quickly from events that could damage facilities or information systems through such measures as data and physical security, monitoring systems, backup and restoration procedures, emergency procedures, and insurance coverage. The emphasis is on foreseeable events, such as natural disasters, criminal activities, or service disruptions. The likelihood of an event, based on past experience, drives

the level of commitment, management resources, and funding devoted to preparing for it. The goal is to recover from any business interruption in a few minutes or hours.

The traditional approach to business continuity, however, is unable to address today's greater, and less predictable, risks. Man-made risks ranging from physical terrorist attacks to computer hackers are on the rise and difficult to foresee. Long-term business trends such as globalization, industry consolidation, outsourcing, and reliance on information technologies and the Internet have made firms more vulnerable to breakdowns.

Developing a New Approach

The new approach to business continuity assumes that facilities and systems will fail eventually, no matter how many precautions are taken. September 11th dramatically demonstrated that formerly unanticipated events can occur. The goal is to design a firm's human, physical, and technical resources to maintain continuous operations when disaster inevitably strikes.

The new paradigm for business continuity differs from the traditional approach by the following key characteristics:

Top Management Priority. Instead of being conducted after business decisions have been made, planning for disruptive events should be integrated from the outset into the firmwide planning process for human resources, information systems, real estate, telecommunications, and vendor selection. Senior management should take an active leadership role in business continuity management, rather than delegating it to middle management and forgetting it.

Continuous Availability. Recovering from a disaster in minutes or hours is no longer adequate. The goal is to ensure continuous availability of operations around the clock, 365 days a year by anticipating and mitigating disruptive events.

Expect the Unexpected. Rather than basing plans on the frequency of past events, business continuity strategies need to encompass events that are rare or have never occurred, including terrorism and other man-made events that could have a severe impact on operations.

Broad Scope. Business continuity strategies should go beyond technology systems to include any potential point of failure in the organization that could

disrupt operations. Planning should cover risks to employees, exchanges, telecommunications and energy providers, and the public transportation system among others.

Cover Service Providers. Given the importance of outside vendors and industry-wide exchanges and utilities, the ability to withstand a potential interruption to such third-party providers of critical services must be part of any business continuity strategy going forward.

Developing a strategy that meets these stringent criteria will require identifying and planning for a wide range of potential disruptive scenarios.

Business Continuity Management—New Paradigm

| | Traditional Approach | New Reality |
|----------------------------|-----------------------------------|--|
| Management Disposition | Due diligence | Active commitment |
| Organizational Positioning | Middle management | Senior executive |
| Basis for measurement | Historical, experience-based | Unknown potential and frequency |
| Requirements | Recovery in minutes, hours, days | Continuous availability |
| Priority | Low—an afterthought | High—consideration early in all planning processes |
| Focus | Technology | People, processes, and technology |
| Plans | Reactive | Anticipatory |
| Cost | Distinguishable, minimized | Embedded into business plans |
| Vendors | Inherent trust | Seeks multiple providers; verification of preparedness where single providers are required |
| Insurance | Open-ended policies, low premiums | Coverage restrictions, higher premiums and deductibles |

Questions Each Firm

| Should Ask

- **Do plans exist** for all areas of recovery? Are they regularly maintained and tested?
- **Does your plan adequately consider** the impact of man-made threats such as cyber-terrorism, bio-terrorism, or coordinated attacks?
- **What would you do if** you could never return to your offices or data centers? Could your employees work from home?
- **How quickly could you contact** each of your employees, vendors, and key customers? Would you be prepared to contact them if telecommunications service broke down?
- **Can decisions be made** if communications are unreliable or key decision makers cannot be located or are not available?
- **How concentrated are your people** and assets? In the same facility or facilities that are in close proximity?
- **Have all facilities** and single points of failure been considered?
- **Are third-party service providers prepared** in case of disaster?
- **Is there an effective program** to prevent and detect threats?
- **Is business continuity planning included** at the outset of all business planning or only performed after the fact?

Crafting a Business Continuity Strategy

A business continuity strategy must be tailored to the specific requirements of a firm's business operations.

The first step is to identify the potential events that could interrupt business operations and then develop mitigation alternatives that will avoid or minimize any disruption. By evaluating costs and benefits, firms can prioritize these mitigation alternatives and design a coordinated business continuity strategy. Each of these steps is described in more detail below.

Identify Potential Scenarios

While financial services firms have traditionally based their business continuity strategies on their best prediction of what disruptive events will occur, this approach is increasingly untenable in today's highly uncertain environment. Instead, they should identify a range of potential scenarios, then take steps to be prepared no matter what may happen. The range of business-disruption scenarios will depend on each firm's particular configuration of facilities, technology, and operations. However, the scenarios for most financial institutions will include the following:

Geo-Centric Scenarios

- An event affecting both buildings and people in one location, e.g., New York
- Events affecting both buildings and people in multiple locations, e.g., New York and London

People Scenarios

- Inability for employees to access facilities
- Workforce unable to work due to emotional trauma or other impacts
- Loss of workforce
- Loss of key members of management team

Infrastructure Scenarios

- Telecommunications outage
- Internet outage
- Loss of transportation service or access

Market Scenarios

- Failure of a market utility or exchange
- Business interruption to a critical vendor
- Counterparty failure

For each scenario, the likely impact on business operations must be assessed. This assessment should also consider the possibility that more than one of these scenarios will occur simultaneously.

This is exactly what happened on September 11th, when several extremely unlikely events occurred at once—the destruction or damage to 30 million square feet of office space in downtown Manhattan, loss of telecommunications service, overload of the Internet, breakdown in the transportation system, and extensive loss of life, among other impacts.

Assess Mitigation Alternatives

The next step is to develop mitigation alternatives for each scenario to avoid or minimize any business interruption. The goal is to avoid single points of failure—where possible, duplicate people, facilities, technology, and vendors. Of course, a firm can't afford to mitigate every risk. Mitigation alternatives must be evaluated using criteria such as cost, potential impact, time required to implement, human resources required, regulatory requirements, and level of insurance coverage available.

Business continuity management is an ongoing process, not a single event. Business continuity strategies must be continually reassessed in light of evolving

business developments and new risk scenarios. In addition, business continuity should be integrated into the planning processes throughout the year for every aspect of the firm.

Although each situation is unique, financial services firms should consider five key areas.

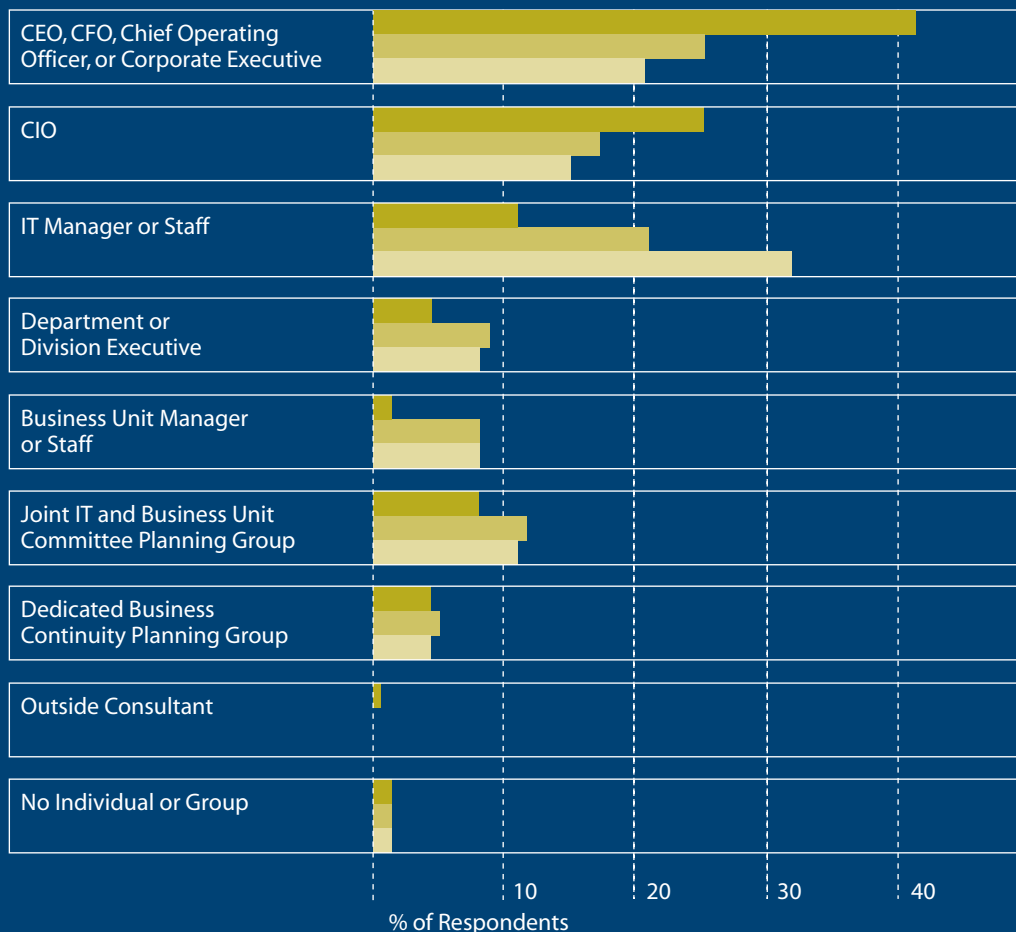
People

As September 11th demonstrated, a disaster can result in extensive loss of life, key leadership positions being vacant, workers

emotionally unable to return to work, and loss of intellectual capital. To be prepared in the face of such impacts, consider a variety of mitigation alternatives:

- Cross-train so that several employees possess critical knowledge and skills
- Improve knowledge management
- Conduct succession planning to ensure an orderly transition of management responsibilities
- Disperse business functions geographically

Who Owns, Creates and Maintains Your Business Continuity Plan?



The continuity and security of the business is now recognized by most leading companies as being an absolute responsibility at the highest levels of the organization.

- Owns
- Creates
- Maintains

Base: 250 companies with business continuity plans

Data: InformationWeek research business continuity survey of 350 business technology managers

Source: Deloitte Consulting

Facilities

Damage to facilities can destroy trading floors, headquarters, or other facilities and result in inadequate office space for employees. To ensure that operations continue, consider the following strategies:

- Decentralize facilities to minimize the likelihood that more than one facility will be damaged
- Establish a redundant trading floor
- Lease emergency office space in less expensive locations but within driving distance from the firm's primary facilities (in case flights are suspended)
- Employ telecommuting or a virtual office so that employees can function from anywhere
- Enhance evacuation plans
- Provide emergency transportation

Network

A loss of service in telecommunications, the Internet, or private networks would leave firms unable to communicate in real time with clients, exchanges, industry utilities, and vendors.

To ensure that communications networks continue to function:

- Review network topology to identify and eliminate single points of failure, e.g., by receiving telecommunications service from multiple offices

- Reexamine the capabilities of telecommunications vendors and the vendor selection process
- Employ a mix of communications technologies such as wireless, satellite, and browser-based technologies
- Increase resiliency through such strategies as dark fiber, hot cut-over, and end-to-end network management capability

Information Systems

Terrorist attacks, viruses, and computer hackers can threaten the integrity of information systems and data. Mitigation strategies include:

- Distributing computing functions and data
- Computing mobility
- Fault tolerance, thin client
- On-demand computing, load balancing

Vendors

Financial services firms rely on outside vendors and other industry players for functions such as market data, back-office processing, and clearing trades. To ensure continuous service:

- Use multiple vendors for the same service, where possible
- Where firms must rely on a single vendor, require a third-party attestation that the vendor's business continuity plans are adequate.

By challenging assumptions about the potential depth and breadth of disruptive events, the terrorist attacks of September 11th posed a severe test of business continuity strategies. Financial institutions learned important lessons about what is required to maintain continuous operations. By sharing what was learned by firms that lived through these extraordinary events, we trust that this document will contribute to the new paradigm for business continuity management now emerging in response to today's riskier, less predictable, business environment.

How We Can Help

At Deloitte Touche Tohmatsu, we have a global team of senior professionals who together have decades of experience assisting large financial institutions with the development and implementation of their business continuity plans.

Our global Business Continuity Management team provides integrated services to meet each client's specific needs. They draw on the firm's Enterprise Risk Services, Human Capital Advisory Services, Real Estate Consulting, and Tax Advisory Services, as well as other areas as needed.

Our business continuity management professionals are members of Deloitte Touche Tohmatsu's Global Financial Services Industry practice, (GFSI) which supports this team through a worldwide network of financial services practices in 40 countries around the world.

GFSI enables us to bring the resources of our global organization to clients, wherever they do business, as well as the in-depth knowledge of local markets provided by our country practices.

Our services include:

Analysis & Diagnostic Services

- Business Impact Analysis
- Operational Resiliency and Recoverability
- Information Technology Resiliency and Recoverability
- Network and Systems Security
- Systems Development Quality
- Crisis Management
- Extended Enterprise

Strategy & Planning Services

- Operations and Technology Recovery Strategies
- High-Availability Technology Architecture
- Secure IT Architecture
- Information Security Management Programs
- Crisis Management Programs
- Cyber-Incident Response Programs

- Systems Development Quality Assurance Programs
- Business Continuity/Disaster Recovery Planning Programs

Testing & Certification Services

- Business Continuity/Disaster Recovery Plan Testing
- Network and Systems Penetration Testing
- Systems Quality Assurance Testing
- WebTrust
- SysTrust
- SAS-70

Human Capital Advisory Services

- Crisis Communications Strategy
- Employee Communications Feedback Mechanisms
- Executive and Staff Safety Programs

- Workforce Skills Assessment and Deployment
- Workforce Recruiting, Orientation and Training
- Travel Safety Policies
- Workplace Transition/Relocation Strategies

Real Estate Services

- Facility Risk Assessment
- Infrastructure Reliability Assessment
- Facilities Geo-Strategies
- Vendor Network Interruption Strategies
- Transportation/Accessibility Assessment
- Real Estate Portfolio Assessment
- Financial Commitment Analysis
- Exit Strategies (voluntary or involuntary)

Global Business Continuity Contacts

For additional information, contact one of our business continuity management leaders or visit our website at www.deloitte.com/gfsi.

AMERICAS

Ted DeZabala
New York
+1 212 436 2957
tdezabala@deloitte.com

John Gimpert
Chicago
+1 312 946 2591
jgimpert@deloitte.com

Steven Ross
New York
+1 212 436 2226
stross@deloitte.com

Dave McCrory
Atlanta
+1 404 220 1493
dmccrory@deloitte.com

Debra Phelps
Houston
+1 713 982 2677
dphelps@deloitte.com

Neville Morcom
San Francisco
+1 415 783 4064
nmorcom@deloitte.com

Mark Steinhoff
Boston
+1 617 437 2614
msteinhoff@deloitte.com

Marcel Labelle
Montréal
+514 393 5472
marlabelle@deloitte.ca

Osmar Lujan
São Paulo
+55 11 3150 1913
olujan@deloitte.com.br

EUROPE

Han Roest
Amsterdam
+31 20 5824400
hroest@deloitte.nl

Oktay Aktolun
Istanbul
+90 21 22 83 1585
oaktolun@deloitte.com

Giacomo Galli
Milan
+39 02 88 01 254
ggalli@deloitte.it

Caroline Veris
Antwerp
+32 3 800 86 76
cveris@deloitte.com

Roger Verster
Johannesburg
+27 11 806 5216
rverster@deloitte.co.za

Dmitry Smirnov
Moscow
+7 (095) 933 7300
dsmirnov@deloitte.ru

Chris Verdonck
Brussels
+32 2 800 24 20
cverdonck@deloitte.com

Bernard Kenny
London
+44 20 7303 5471
bekenny@deloitte.co.uk

Damien Leurent
Paris
+33 1 40 88 29 69
dleurent@deloitte.fr

Joachim Schauff
Duesseldorf
+49 0 211-8772-255
jschauff@deloitte.de

Benoit Schaus
Luxembourg
+ 352 451 452 493
bschaus@deloitte.lu

Pierre Poulain
Paris
+ 33 01 40 88 84 14
ppoulain@deloitte.fr

Henri Ahrens
Madrid
+34 91 582 1011
timaloney@deloitte.es

Martin Heystek
Zurich
+ 41 1 421 6426
mheystek@deloitte.com

ASIA/PACIFIC

Gregory Lo
Hong Kong
852-2852-5892
greglo@deloitte.com.hk

Darryl Butler
Melbourne
61-3-9208-7200
dbutler@deloitte.com.au

Mike Gelormino
Tokyo
81-3-6400-5595
michael.gelormino@
tohmatsumi.co.jp

Alan Nisbet
Singapore
65-530-5509
anisbet@deloitte.com

Deloitte Touche Tohmatsu is one of the world's leading professional services organizations, delivering world-class assurance and advisory, tax, and consulting services through its national practices. More than 95,000 people in 140 countries serve over one-quarter of the world's largest companies, as well as large national enterprises, public institutions, and successful, fast-growing global growth companies. Our internationally experienced professionals strive to deliver seamless, consistent services wherever our clients operate. Our mission is to help our clients and our people excel.

Deloitte Touche Tohmatsu serves financial services firms globally through our Global Financial Services Industry practice. GFSI's industry specialists represent every major financial center in the world and bring decades of experience and leadership in banking, securities, insurance, and investment management to each client assignment.

For more information about our practice visit our website at www.deloitte.com/gfsi.