



# *Surviving a Disaster*

**Emergency Response and Business Continuation  
Planning for Managers of Financial Institutions**

**From Chubb's Department of Financial Institutions**





---

**SURVIVING A DISASTER**

**EMERGENCY RESPONSE AND BUSINESS  
CONTINUATION PLANNING  
FOR MANAGERS OF FINANCIAL INSTITUTIONS**

---



---

## **CONTENTS**

Introduction: Lessons of September 11 .....	3
Risk Management Considerations.....	4
Key Elements of Disaster Planning .....	6
Conclusion .....	14



---

## INTRODUCTION: LESSONS OF SEPTEMBER 11

Before September 11, 2001, no one could have envisioned the devastating events that were to transpire, nor their far-reaching consequences. In many ways, the world became a different place, and the companies most affected by the terrorist attacks learned a number of valuable lessons.

In the wake of September 11, financial institutions and other organizations are reexamining their risk management plans, including emergency response, and business recovery and continuation planning. Effective risk management enhances the overall performance of an institution by reducing the likelihood and impact of loss events. Risk management today is more than sound business practice; it can be a marketable competitive advantage.

Good corporate governance requires directors and officers to act in good faith and in the best interest of the organization. With respect to managing corporate risks, this means providing direction and supervision to ensure that management:

- Understands the inherent financial risks, physical threats, and information security vulnerabilities and their potential impact on the organization.
- Dedicates staff and resources and assigns responsibilities to ensure ownership for and coordination of all emergency response and business continuity initiatives throughout the company.

When companies disclose their emergency response initiatives to shareholders, creditors, and other stakeholders, the public can be confident that the board has made informed risk management decisions.

---

## RISK MANAGEMENT CONSIDERATIONS

To be comprehensive, risk management planning should involve numerous key business management areas, including corporate security, information technology, compliance, counsel, finance, and auditing. A good risk management plan encompasses the following activities:

- Defining the risk appetite (risk tolerance) of the institution.
- Identifying risks to the organization.
- Evaluating and prioritizing those risks according to the relative likelihood of an event, the potential severity of the event's impact on the organization, and the organization's risk tolerance.
- Setting response goals for possible disaster events. These will drive the emergency preparedness and business continuation planning activities.
- Monitoring and updating strategies to incorporate changes to the firm and its environment.
- Implementing risk mitigation strategies, including the use of insurance to transfer those risks that pose a significant threat to the company's bottom line.

In every activity, the protection of human life and health must be an organizational priority.

### *Don't Overlook Business Continuation Planning*

One critical but frequently overlooked component of risk management is planning for continuity and restoration of business in the aftermath of a disaster.

Financial institutions, particularly banks and brokerages, have long recognized the need to protect vital information and be able to restore

---

business operations in the immediate aftermath of an event. In fact, bank regulators require such capabilities to ensure stability in the banking and finance sectors.

The purpose of a business continuity plan is to maximize the ability of the business to maintain outputs and services, as well as establish confidence in the ability of the business to survive a disaster. As part of an overall risk management plan, good business continuity planning will:

- Minimize losses.
- Control recovery costs.
- Maximize productivity during the recovery period.
- Minimize lost customers and revenues.
- Minimize regulatory impacts.
- Shorten overall time needed to resume normal business activities.

Some companies affected by the World Trade Center disaster did not have comprehensive contingency programs and backup recovery systems, and they struggled to recover. Most of those that did have emergency response and business continuation plans were able to quickly recover. The prepared companies not only designed contingency plans, but also kept the plans up to date so they could immediately be implemented should a disaster occur.

Given the importance of risk management, including emergency response and business continuity planning, it should have the support of the board and the highest levels of management in the organization.

---

## KEY ELEMENTS OF DISASTER PLANNING

In traditional risk management, risk identification has typically focused on natural, foreseeable hazards. But September 11 proved that organizations also need to consider formerly “unthinkable” hazards in the context of the organization’s unique operations and premises. Managers must now prepare for business interruptions caused by cyber- or bioterrorism, bomb threats, physical facility destruction, loss of key employees and suppliers, limited access to financial markets, communication failure, civil unrest, and every conceivable natural and man-made threat.

Again, the experiences of September 11 offer important guidelines for anticipating once-unimaginable hazards and what businesses can do to better prepare for them. Based on these experiences, we offer 12 suggestions for sound emergency response and business continuation planning.

### *1. Dedicate resources to planning.*

Disaster preparedness requires dedicated resources. It is vital for the board to authorize management to dedicate financial and personnel resources to developing, maintaining, and implementing contingency plans.

### *2. Make saving lives a top priority.*

The loss of people is not only the most painful of losses, but also the costliest to the enterprise and its ability to continue in the aftermath of a disaster. Therefore, emergency response and business recovery plans should focus first on protecting lives.

Critical automatic fire suppression equipment and stair towers intended as areas of safe refuge were rendered inoperable at the World Trade Center towers. Emergency response plans that counted on these

---

features to protect life and property were immediately obsolete. Preselected safe assembly locations for the purpose of accounting for employees were inaccessible due to the widespread nature of the disaster. Many people who entered the towers daily were not employees (delivery people, contractors, tourists, etc.), yet there was no way to account for them. Reports of tower occupants in the process of safely evacuating only to be instructed to return to their workplaces are particularly troubling. These experiences suggest the need for more comprehensive planning for protecting lives. At the very least, create an emergency contact list for all employees to facilitate accounting for every individual. Keep the list up-to-date, off-site, and accessible to staff from several areas to improve the likelihood that it will be available when needed.

### *3. Rethink worst-case scenarios.*

Business managers once contemplated worst-case scenarios such as loss of a building or part of a building due to fire or explosion. Never did they imagine massive loss of life and structural failures impacting numerous buildings and an entire city neighborhood's communications, power, and transportation infrastructure. Nor did disaster preparedness planners consider the liabilities arising out of such an event. Many organizations are now rethinking the concentration of corporate assets in one location, especially since today's "wired" world makes it feasible to conduct business from multiple locations.

### *4. Include terrorism in disaster planning.*

Aside from businesses located in London's financial district where Irish Republican Army terrorist activity forced them to plan for bomb threats/incidents, few businesses had contemplated terrorism in their plans before September 11. The September 11 attacks illustrate that the scope of risk management protocols and procedures must include preparing for disasters caused by terrorists and other destructive

---

elements on a scale that few imagined. Corporations are being challenged to deal with terrorist threats in every conceivable form. Now we have experience with commercial airliners turned into flying bombs, anthrax, and cyberterrorism as real scenarios.

Resources to assist in your planning efforts include the Federal Emergency Management Agency (FEMA) and the Office of Homeland Security. At the local level, explore your state's commitment to disaster coalitions designed to ensure public-private sector cooperation, and encourage such activities in trade organizations.

### *5. Effective communication is vital in an emergency.*

Having a crisis communications plan in place allows management to concentrate on the specific messages that need to be conveyed, the audiences that need to be reached, and the distribution channels that will be most effective. On September 11, the abundant flow of information that was disseminated significantly helped restore calm and reduce confusion.

Communication spans a broad range of issues, from the initial declaration of an emergency situation to relaying evacuation procedures to providing critical information as an event unfolds. Employees and their families, emergency services, contractors and other visitors on the premises, key customers and vendors, shareholders, regulators, government authorities, and the news media will each require different information during and after the event. The ability to effectively manage these various information needs directly affects one of the company's most valuable assets: its reputation, the loss of which can seriously affect the firm's ability to survive.

September 11 teaches that crisis communication planning must also take into account the possible unavailability of traditional communication methods. Land-based communication lines were knocked out by the September 11 attacks, and cellular phones were

---

rendered useless when traffic volume overwhelmed the airways. Firms not physically affected nonetheless had their operations disrupted. Even emergency services discovered that their radios were rendered inoperable by interference from building structural elements, contributing to the large loss of firefighters. Furthermore, as firms tried to replace damaged systems, the local utility was swamped with those orders as well as critical repair work.

It is apparent that firms must provide for backup communications and, when choosing providers, must consider the peak capacities of those providers. One possible solution may be to set up Web-based and wireless communications as a way to keep many stakeholders informed; even at the height of the World Trade Center disaster, most people continued to have Web and wireless communications access.

Perhaps the greatest communication attribute to have is experience. Often an outside advisor, such as a public relations agency with crisis management know-how, can help. Skilled crisis practitioners understand how crises develop and know what other companies in crisis situations have done. By taking on some of the burden of crisis communication, outside public relations counsel can free management to do what it does best— restore the business's full operational capacity.

By keeping key audiences—both internal and external—well-informed, organizations can save lives, maintain credibility, minimize damage to reputation, protect their ability to do business, and generally lessen the negative effects of a catastrophe.

#### *6. Establish clear lines of authority.*

One of the first decisions to be made at the time of an event is to declare it a disaster and thus set the disaster plan in motion. The emergency response plan should direct that critical decisions be made by those in a position to have the relevant information and only after a

---

comprehensive review and evaluation of the situation to determine the suitability of those decisions. The plan should include chains of command and communication that anticipate the unavailability of key decision-makers during an emergency as well as afterward, when critical business continuation decisions must be made and implemented. Appropriate staff should be cross-trained to ensure redundancy in emergency management and authorized to make critical decisions when necessary. Finally, a succession plan should be developed, not only for senior managers, but for all key employees. Maintaining leadership and decision-making capabilities can determine whether the business will survive the disaster.

### *7. Anticipate the loss of backup facilities.*

On September 11, even those businesses with seemingly complete, up-to-date disaster plans faced surprises when it came time to implement them. Plans requiring “hot sites” or alternate backup facilities for resuming operations did not account for demands on the backup providers that would overwhelm their ability to meet their contractual obligations. Backup providers never imagined an event that would have all of their clients needing the facility at the same time. Contracts for use of backup facilities typically assumed a need of relatively short duration—not an event that would displace clients for months. Plans assumed that electronic backup files would provide the information necessary to resume operations quickly, but many companies discovered they were more dependent on paper than they realized, and document reconstruction became an additional task.

Frequency of backup was also an issue on September 11. The loss of electronic information was immediate, total, and unexpected. Records of some trades completed just before the World Trade Center attack were lost entirely and took days to reconstruct using counterparties’ records. For an institution that conducts backups nightly but conducts \$25 million in trades daily, a loss of one day of trading records is

---

significant. Therefore, real-time backup of critical financial records should be an institution's goal.

Technology can create other impediments. If a business changes platforms or software, but the changes are not mirrored at its backup facilities, recovery efforts may be delayed while technical staff solve the problem.

For financial market intermediaries, trading activities can be the lifeblood of their businesses. Great technical strides have been made in recent years to speed trading, such as direct electronic hookups and Internet trading. New legal developments also recognize and accommodate electronic trading. These developments also bring new risks, such as systems failures and hacking.

In addition, many World Trade Center firms were located in close proximity to their backup facilities. What was presumed to be a safe, efficient post-loss location instead became unavailable when the disaster enveloped a large geographic area. Similarly, many organizations found critical vendors and clients caught up in the same event due to their proximity. What happens if, at the same time you are trying to restore critical operations, business stops because a key client is also down, or a critical business partner cannot function? Suppose your recovery plan included the use of air transportation, but airlines were grounded and airports were closed or key employees refused to travel by air out of fear of another attack?

### *8. Anticipate cyber disasters.*

Financial institutions are leaders in the use of technology to transact and process business. Unfortunately, the efficiencies offered by technology are accompanied by a host of business risks and legal liabilities, including viruses, cyber extortion, Web site hijacking, and electronic theft of funds or data. All have the potential to shut down an institution's e-business. Furthermore, because of the open and

---

anonymous nature of the Internet, cyberattacks may become attractive for disrupting corporate activities and could be the next front where terrorists wage a devastating attack.

System failure, service disruption, or a catastrophic loss of proprietary data can severely damage a business, eroding its reputation and customer and shareholder confidence in its ability to safeguard customer assets and information, as well as affecting shareholder value, corporate stability, and financial performance. Regulatory guidelines such as the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act should be adopted to prevent loss and limit liability.

It is the board's responsibility to ensure that a chief information security officer and an effective risk management program are in place to protect the safety and soundness of the institution.

*9. Determine the preparedness of key service providers.*

It is important to determine whether key counterparties, information processors, and vendors have conducted similar emergency response and business recovery planning exercises. Information outsourcing and transaction processing involve operational risks similar to those that arise when those functions are performed internally. These risks include threats to the availability of systems used to support transactions, to the integrity of customer information security, and to the integrity of risk management systems.

It is management's responsibility to exercise appropriate due diligence in creating, managing, and monitoring outsourcing arrangements and determining that contracted service providers have developed crisis plans, including security programs to protect customer information.

---

*10. Determine the preparedness of financial market intermediaries.*

The effectiveness of financial intermediaries' contingency plans is an important aspect of the risk profile of the corporations relying on them for market transactions. The sudden failure of a market intermediary can raise unique liquidity concerns for financial institutions.

Intermediaries—whether traditional exchanges, ECNs, interdealer brokers, or simply large OTC traders—must take steps to ensure that, in the event of a disaster, they can provide both historical records to their customers and an alternative way to continue to conduct business.

*11. Test, practice, and update your disaster plans regularly.*

Routine emergency response and business continuation plan testing improves the chances of an organization surviving a disaster. It is vital to conduct a live worst case test at principal locations at least annually.

Untested plans could prove to be ineffective at the time of an event.

When business functions or the business environment change, or test results indicate a need for adjustment, update the plans accordingly. A plan is only as good as its currency.

*12. Transfer risks that can financially devastate your business.*

When losses cannot be avoided but have potentially severe financial consequences, most businesses purchase insurance to help mitigate them. However, one of the most prevalent mistakes is to undervalue business income, extra expense, and dependent business premises insurance needs. Financial resources at the time of a loss can mean the difference between survival and failure. Management should establish a realistic picture of the organization's financial needs, determine how much of that can and should be funded out of operating cash, and purchase sufficient insurance to cover the remainder. The events of September 11 placed unanticipated demands on the insurance industry, too, so make sure your insurer will be there to respond; deal with highly rated companies with strong balance sheets.

---

## CONCLUSION

September 11, 2001, sharply defined the need for corporations to place a high priority on comprehensive, enterprise-wide crisis planning. Directors, officers, and managers need to consider the lessons of that day in order to take steps to manage the organization's risks and instill a sense of confidence in employees and stakeholders before a disaster occurs.

Prudent corporate governance requires corporate management to prepare for events that were unimaginable prior to September 11. To be successful, crisis planning requires strong leadership from senior management. Directors and officers have a duty to lead the way and to participate in crisis planning that includes business continuity and contingency plans. By defining crisis roles and responsibilities, corporate leaders can minimize the risk to their organization.

The better a company's disaster planning, the less confusion and delay that will occur during an actual emergency—and the better it can protect its employees, its customers, and itself.









**Chubb Group of Insurance Companies**

Warren, NJ 07059  
[www.chubb.com](http://www.chubb.com)

For promotional purposes, Chubb refers to member insurers of the Chubb Group of Insurance Companies underwriting coverage. This guide is advisory in nature. It is offered as a resource to be used together with your professional insurance advisor in maintaining a loss prevention program. This guide is necessarily general in content and intended to give an overview of certain aspects of liability in the United States. It should not be relied on as legal advice or a definitive statement of the law in any jurisdiction. For such advice, an applicant, insured, or other reader should consult their own legal counsel. No liability is assumed by reason of the information this document contains.