Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
9.1 Introduction

Building an integrated straight through processing environment, both inside a firm and throughout the industry, demands an infrastructure that is resilient to unforeseen disasters. A disaster can be anything from a power disruption to an earthquake to a terrorist attack. Business continuity and disaster recovery, or the ability to recover and continue critical business functions soon after the occurrence of a disaster, are crucial aspects of an STP infrastructure. After the terrorist attack of September 11, 2001 in New York, financial services firms have been focusing on building business continuity plans. They are encouraged by the government, which is keenly aware of
the impact of a disruption in financial markets on the general economy. This chapter provides a detailed overview of the importance of *business continuity planning (BCP)* and provides a framework for planning quick recovery from unexpected disasters in an STP environment.

In Section 9.2, the impact of the September 11, 2001 terrorist attack in New York is discussed as an example of a disaster that exposed deep vulnerabilities in financial markets. Section 9.3 outlines how a particular firm can devise a business continuity and disaster recovery strategy for itself. While planning should be done in all departments in the firm, this chapter will focus on financial technology systems in particular. All the major milestones of creating and maintaining a business continuity plan are discussed in this section, including business impact analysis, audit checklists, service-level agreements, and testing.

While it is crucial for each firm to have its own business continuity plan, it is just as important for the industry as a whole to protect its infrastructure, since systems of each firm are intricately linked together in an STP environment. Section 9.4 examines the steps being taken by the industry as a whole to build a robust financial technology infrastructure, and how market interlinking is increasing exponentially around the world. Finally, continual testing and reevaluation of systems and plans are necessary to any business continuity plan.

### 9.2 Impact of Disasters on Business

After the terrorist attacks of September 11, 2001, the US equity markets were closed for four days; bond trading, including government securities trading, was disrupted for two days; and there were breakdowns and issues in the clearing and settlement mechanisms for government securities, repurchase agreements, and commercial paper. Operational failures such as these can cause liquidity bottlenecks and severely undermine confidence in financial markets. They are the result of telecommunications breakdowns, infrastructure meltdown, loss of crucial data and connectivity, and lack of a solid plan for quick disaster recovery. More than anything else, they point to the increasing interconnectivity between all participants in the marketplace, and the need for an industry-level business continuity plan as well as a firm specific plan. The SEC conducted a thorough analysis of the impact of the attacks of September 11, 2001 on the financial sector, and published a discussion note called *Summary of “Lessons Learned” from Events of September 11 and Implications for Business Continuity*. This section presents some of the findings in this

---

1US Securities & Exchange Commission, *Summary of “Lessons Learned” from Events of September 11 and Implications for Business Continuity*, February 13, 2002.
and other reports regarding the impact of disasters on critical business functioning.

Given the importance of the financial services sector in New York and for the economy in general, it was considered imperative that vulnerabilities be identified and mitigated. Both the SEC discussion note and a report by consulting firm McKinsey & Co\(^2\) point to several vulnerabilities in the current infrastructure, which were exposed in the September 11 disaster. The prominent breakdowns are briefly described below:

1. **Breakdown in payments systems**—Clearing and payments are vital to smooth running of financial markets. Overall, the payment systems worked fairly well. However, the clearinghouses suffered major disruptions, and this resulted in liquidity bottlenecks for many days, especially in the clearing of Treasury securities, which had to be suspended briefly. The Federal Reserve, along with other payment systems, stayed open for longer than usual to help facilitate the exchange of funds, allowing banks to borrow from the central bank discount window to maintain liquidity. In fact, according to the SEC, the Federal Reserve pumped $80 billion of liquidity into the market to prevent a market failure. Commercial

\(^{2}\)McKinsey & Co., *Impact of Attack on New York Financial Services*, November 2001.
paper, a fundamental pillar of corporate credit markets, also suffered breakdowns in clearing, and the fear of illiquidity made some corporations keep high cash balances for precautionary reasons, and this, of course, further exacerbated the bottlenecks in the market.

2. Reconciliation issues—Reconciliation, as discussed in Chapter 7, is a crucial factor in building trust, reliability, and automation in the financial market. Some transaction records were lost; others could not be confirmed, causing distortions in balance sheets and credit disruptions across institutions in the market. Often, transactions had to be reconstructed because of the physical damage to the computers holding the information, leading to a laborious and sometimes inaccurate process.

3. Markets closed—Several markets remained closed for days due to the physical damage to the buildings that housed the exchanges. These included commodities and foreign exchange markets, and equity markets, all of which were closed for four days. The fact that the foreign exchange market was closed meant that foreign banks were unable to borrow US dollars from US banks, causing ripple effects in the country’s balance sheet. The Federal Reserve Bank arranged for $90 billion in foreign exchange to meet this shortfall.

The three major breakdowns discussed above caused severe problems in the normal workings of financial markets in the US, with effects echoing around the world. They exposed the financial system’s vulnerability to unexpected disasters. In particular, it showed that the areas below were weak spots in the way business was conducted in the market currently.

■ Lack of business continuity planning (BCP)—The lack of sound business continuity and disaster recovery planning was painfully obvious in the aftermath of September 11, 2001. Financial firms had quite clearly never imagined a wide-area disaster, severe physical damage to their infrastructure, and loss or inaccessibility of critical staff members. More often than not, BCP was done for breakdowns in individual systems and disasters such as fires in buildings. In fact, many firms had backups to their primary systems in nearby buildings, or even when they were located in faraway sites, the firms depended on the ability of staff to quickly travel to the backup site. With rows upon rows of buildings destroyed, all transportation systems shut down, and the whole city in a state of emergency, these BCP steps were not a feasible solution for a disaster of the magnitude of September 11. The result was that several firms were unable to get their backup systems up and running, because the backups were also destroyed, or due to the disruption in transportation, it was impossible for staff to get to alternate sites.
■ **Concentrated operations**—The concentration of operations geographically was one of the major reasons that financial systems failed after September 11. Here, the reference is to primary sites, where the majority of critical business functions were being conducted by a staff on systems in close proximity to each other. This proximity, clearly leading to efficiencies before technological advancements in telecommunications, now is not only unnecessary but also results in hazard zones. This was not only true in individual banks, but also in clearing-houses and settlement houses. Finally, as discussed in the last section, this is especially problematic when backup sites are also close to the primary sites.

■ **Interlinked and interdependent systems**—The third most important feature of the financial system that made it vulnerable to disasters was the increasing interlinking and interdependence of financial systems. Connectivity between banks, broker-dealers, exchanges, custodians, clearinghouses, and other market participants is becoming more and more common, especially as the entire industry moves towards a more STP environment. But the very fact that an STP infrastructure is being built demands attention to the vulnerability it is allowing to seep into the system with its deep interlinking and connectivity. This was obvious in the aftermath of September 11 when many financial participants suffered even when their own systems were all right, because their critical business functions depended on other systems that they were connected to in the industry.

■ **Special choke points**—The McKinsey report very appropriately pointed out that a few critical links in the financial system, special choke points, needed to be given special consideration when planning for business continuity and disaster recovery. Given the increasing interdependence of the different systems in the lifecycle of securities trading and settlement, these choke points include exchanges, clearing firms, and inter-dealer brokers. The spillover effects of a disruption in the normal workings of these links is particularly devastating for the health of the system overall.

The first step to addressing the vulnerabilities and weaknesses in the financial system is to build both an internal and an industrywide BCP, which is the subject of Sections 9.3 and 9.4 that follow. See Figure 9-2.

### 9.3 Firm-Level Business Continuity Planning

BCP is a methodology for planning how to deal with unforeseen disruptions in financial business processes. These disruptions are expected to be of a large scale, such as the disaster of September 11, only 5% of the time; more often than not, disruptions are minor and on a much smaller scale. These smaller disruptions may
be due to short-term power outages, fires, disk drive failures, or computer viruses. Regardless, the firm must make a plan based on a thorough analysis of all scenarios that may affect its normal working, and create and test contingency and recovery measures for such situations. This section discusses what constitutes BCP for a financial services firm, focusing on financial technology systems in an STP environment. Barring concern for personnel safety and physical infrastructure, the two most important assets in an STP environment are **business workflows** and **data**. Systems throughout an organization are interconnected, constantly updating and processing information that is stored in databases. A breakdown in any process or loss of any vital data can result in loss of revenue and profits at a minimum.

There are three main dimensions to a business that are vulnerable to disasters: connectivity, data, and expertise. Businesses cannot afford to have any downtime in these three aspects of providing services to their clients. In fact, in a world where businesses need to operate 24 hours a day, the disruption of services can be fatal to a business. The goal is to provide seamless business-as-usual processing even when, behind the scenes, unforeseen circumstances have caused the regular infrastructure to break down. Solutions are therefore needed for data protection and high availability at all times, which means organized disaster recovery and graceful transition to backup systems if disaster occurs.

### 9.3.1 BUSINESS CONTINUITY MODELS

Traditionally, business continuity models depended on an active operating site with an associated backup site. This includes technological backup for both data
processing and business operations. Because it was focused on hardware and software, it required staff to be able to move from the active to the backup site easily in order to operate from the backup servers. It limited geographic separation to allow staff to quickly access the backup sites for recovery of business-as-usual processes. As September 11 showed, this kind of geographic concentration of active/backup sites can be problematic in the case of a wide area disaster, especially if transportation systems are affected negatively. Thus, while this model is the most cost-effective, it is not appropriate for the kind of disasters firms now find themselves facing.

A business model that has recently been emerging as the model of choice is the split operations model. This involves nationwide or global operations, where both the technology and the staff are dispersed over a wide area, and are equally equipped real-time to pick up process functionality. It is also known as an active/active model because each site can absorb the operational responsibility for a department or for the entire firm. After September 11, a number of firms separated their technology staff to different buildings across New York and New Jersey to reduce the impact of concentrated vulnerabilities. Again, data is continually updated in real time as are software updates, and testing is done on a regular basis to make sure that both sites are always current.

Even as firms have improved their ability to have IT systems and staff dispersed over a wide area, the business staff is still usually concentrated in one area. This is true of senior management, which often all sits in one building, and also of front-office trading staff, which usually sits close to each other.

### 9.3.2 MAKING A BUSINESS CONTINUITY PLAN

Making a BCP for a firm can be divided into ten steps as shown below, based on the framework provided by the Business Continuity Institute. Each of these steps is discussed in detail in this section. See Figure 9-3.

1. Initiation and management
2. Business impact analysis
3. Risk evaluation and control
4. Developing business continuity management strategies
5. Emergency response and operations
6. Developing and implementing business continuity plans

---

3The Business Continuity Institute, *10 Standards of Professional Competence*, August 2003.
7. Awareness and training programs
8. Maintaining and exercising business continuity plans
9. Crisis communications
10. Coordination with external agencies

BCP is essentially a written collection of procedures that are developed through thorough analysis, development, and extensive testing, to prepare a firm for emergencies or disasters. It is also sometimes referred to as a disaster recovery plan (DRP). Once a BCP has been developed and published, both employees and shareholders have confidence in the firm’s ability to continue business with a safe and orderly recovery with an emergency management team in the face of unexpected disasters. This means that there will be minimal potential economic loss, legal liability, and loss of leadership if critical staff members are cut off from the rest of the firm. It is also important for satisfying regulatory compliance requirements for such circumstances, and in doing so, lowers insurance premiums for the firm.

The exercise of developing the BCP is headed by a team put together specifically for this purpose. The process itself involves a number of participants headed by the project management office (PMO), including IT managers who manage IT operations, system administrators who are responsible for maintaining daily IT operations, the staff (Information System Security Officers) responsible for maintaining the firm’s IT security activities, and the users who need the systems to conduct their job functions. In addition, one of the results of BCP will be the assignment of an emer-
gency team that will coordinate contingency operations to remedy disruptions due to unforeseen circumstances.

### 9.3.2.1 Initiation and Management

A policy statement forces the planners to clearly state their vision, goals, and objectives in making a BCP. It also establishes stakeholders and sets out responsibilities among staff members for developing, implementing, and testing the plan. A BCP must really be approached the same as any financial technology project, which requires a vision statement with scope specifics, analysis, implementation, testing, and maintenance. This statement can range from one to a few pages and is really a lighthouse to make sure the project is implemented on time and on budget.

### 9.3.2.2 Business Impact Analysis

*Business impact analysis* or BIA is essential for putting a dollar value on how much it would cost a business if processes were disrupted or shut down for an hour, or a day, or a week due to any of the risks identified in the last section. It identifies the processes that are most essential and costly to lose, and in doing so, gives them highest priority when determining level of protection in a BCP. Many consider this to be the most important step of the entire business continuity exercise, as it determines all the focus of the plan.

Usually, the risk assessment stage consists of the following eight steps:

1. Establish and agree on terms of reference and scope of work with stakeholders.
2. Identify and describe key critical business processes in the firm.
3. Determine, through interviews and analysis, how the impact of disruption of business critical processes could negatively affect the firm’s assets, reputation, or financial position.
4. Determine the *minimum service level (MSL)*, that is, the level to which a process must be recovered for service expectations to be met, and the resources required to achieve this level of performance.
5. Determine the *recovery time objective (RTO)* for each process, that is, the time by which the process must be recovered to its minimum service level.
6. Determine *recovery point objective (RPO)*, that is, the point to which information must be restored for business objectives to be met for each process.
7. Identify the dependencies between these business processes.
8. Summarize and present findings to senior management in a business impact analysis report.
9.3.2.3 Risk Evaluation and Control

The first step in any business continuity exercise is to do a risk analysis study, which means identifying the range of threats that the business faces. For each of these threats, a business impact analysis is conducted that calculates the cost to the business of losing operational functionality due to the realization of risk. Risk assessment not only documents all the threats that a business faces, but also does an assessment of the likelihood of each threat occurring. BCP falls under the general rubric of risk management, along the lines of credit, market, and operational risk in terms of importance. However, unlike operational risk, which is the result of systemic errors in the process flows or systems, business continuity is for disruption risk management. The controls instituted as part of BCP can be thought to be protection against three classifications of threats:

1. **Natural**—This includes natural disasters such as floods, fires, hurricanes, and earthquakes.
2. **Human**—This includes malicious computer viruses, terrorist attacks, and sabotage.
3. **Environmental**—This includes hardware and other related infrastructure problems, such as telecommunications outage, power failures, and equipment failures.

Usually, the risk assessment stage consists of the following five steps:

1. Establish and agree on terms of reference and scope of work with stakeholders.
2. Identify, through interviews and analysis, all potential internal and external threats to the firm.
3. Estimate the probability of each of these threats occurring.
4. Identify risk reduction and mitigation alternatives.
5. Summarize and present findings to senior management in a risk assessment report.

9.3.2.4 Developing Business Continuity Strategies

After the initial analysis on critical business functions and threats to these functions, the most important and extensive part of BCP begins. This is the stage where the strategies for disaster recovery are developed and documented. There are six main steps in this stage.

1. Understand the available recovery strategies and the advantages, disadvantages, and cost of each alternative.
2. Identify the recovery strategy for each business functional area.
3. Consolidate all the strategies into one document.
4. Identify off-site and alternative facilities.
5. Develop business unit strategies.
6. Obtain sign-off and commitment from management for suggested and developed strategies.

### 9.3.2.5 Emergency Operations and Response

Business continuity has to incorporate emergency response requirements as well. These are additional operations that will be incorporated into the BCP that are specifically responses to emergency situations, such as fire and hazardous materials leaks. These are more related to immediate threat to lives of personnel and not just mere disruption of business functions. Emergency actions can include evacuation, medical care, firefighting, and other such actions. Again, the BCP sets out clear roles and responsibilities for the individuals who will take over as Emergency Operations management and implement the procedures set out in the Emergency Response and Operation part of the BCP.

### 9.3.2.6 Implementing the Business Continuity Plan

Once the documentation of the plan has been completed, it must be implemented; that is, the analysis, strategies, and suggestions must now be organized into a clear set of action plans, checklists, procedures, and databases.

### 9.3.2.7 Awareness and Training Programs

A BCP is of little use if everyone is not made aware of it, and if the appropriate people responsible in case of emergency are not trained in their roles and responsibilities. Preparing a program to create and maintain corporate awareness is part of the BCP. There are several ways in which training can be given to employees, including computer based, classroom, scenario based, and instructional guides. Ideally, business continuity instruction would be a part of new employee orientation and current employee refresher programs.

### 9.3.2.8 Testing and Maintaining Business Continuity Plans

Once a plan has been completed, it must be tested, maintained, and updated with regular exercises that monitor its effectiveness and identify strengths and weaknesses. For exercises to be useful, exercise objectives and success criteria must be established. Types of exercises that would require a run-through of the BCP based on realistic scenarios include: walk-throughs, simulations, functional tests across
specific lines of business, planned tests, and unannounced tests. Regular testing is a key part of a BCP and should be scheduled throughout the year. Feedback and results should be documented and kept as part of audit and control.

It is very useful as the business expands that external threats and their business impact are also reevaluated. Whenever changes are made to the plan, change control procedures must be used to make sure that changes to the published criteria are done in a logical order and then announced to all relevant parties.

### 9.3.2.9 Crisis Communications

While often neglected, developing an efficient plan for communicating during a crisis with employees, management, customers, shareholders, and external agencies such as local government and the media, is crucial as part of reassuring all people and agencies affected about the status of the firm’s response to a crisis. Again, all essential crisis communication procedures must be clearly laid out in the BCP with members of the emergency team assigned as part of their task list.

### 9.3.2.10 Coordination with External Agencies

It is imperative that the BCP team also outline any procedures necessary for coordinating continuity activities with external agencies, whether government—local, state, national, or defense—or other participants in the network to which the firm is connected. The next section discusses in detail how the financial industry in the US and across the world is working on business continuity management tests and guidelines for the industry as a whole. As far as the government is concerned, this is especially relevant in large-scale disasters such as terrorist attacks and earthquakes, where the lives of citizens are at stake. In fact, there are many laws and regulations that are applicable to such situations, and the BCP team must be aware of and include these regulations in their plans. Finally, coordination with external agencies involves communication and exercises to test coordinated plans to counter disruptions in business continuity.

### 9.4 Industrywide Business Continuity Planning

The operations of all the participants in financial markets are now deeply intertwined. This will be particularly true as STP becomes more a reality not just internally in the firm, but also externally across all the participants in the market. Institutions coordinate everything from live data feeds to order routing, to trade matching and clearing, payment and settlement, to collateral and asset management. Such coordination means that the resilience of the entire financial system as a whole must be strengthened because failure or disruption at one link in the chain of events can adversely
affect the entire lifecycle of a transaction. With the realization that financial systems are more interlinked and interdependent, industry organizations across the world, including the US, England, and Singapore, have been conducting industrywide exercises to test business continuity planning for the entire financial market.

The aim of industrywide business continuity exercises is to answer the following questions:

■ How resilient is a country’s financial sector; that is, how quickly can the sector recover from major operation disruption?
■ Do firms across the industry plan and prepare effectively for disasters?
■ What are the dependencies between firms that make it more vulnerable to a domino effect of disruption in one area?
■ How can the sector improve its recovery capability overall?

Usually, a scenario is provided to the market participants with a date and time, and then everyone goes into emergency response mode. The test results are evaluated, and a report created that documents answers to the questions listed above. This section will review the major industrywide business continuity tests conducted in Singapore, the United Kingdom, and the United States, and discuss the lessons learned. However, before going to the case studies, it is useful to discuss at an abstract level the key vulnerabilities in a financial sector that is deeply interconnected.

Just as internal business functions can be divided across three dimensions, across the industry there are also the same three dimensions to business-as-usual processing:

1. **Connectivity**—all major participants are connected via a myriad of connections which, as discussed in Chapter 5, require servers and networks.
2. **Data**—without data, processes cannot be recreated by reestablishing connectivity under expert staff.
3. **Staff**—although processes are increasingly automated, expert staff, both IT and business, is needed for emergency and extraordinary circumstances.

For each of these dimensions, the critical operational components of the entire financial system that uses them must be identified. Each institution contributes to the industry infrastructure and business continuity uniquely, and an industry organization with representatives from all market participants must examine and document the role of individual firms for disaster recovery coordination. Of course, expectations will be highest for institutions whose activity affects the highest number of processes. This includes major clearing and settlement entities, such as Depository Trust and Clearing Corporation (DTCC), and other utilities that provide payment
infrastructure across the industry, such as the SWIFT network. In addition, companies outside the financial services sector on which key business processes depend must also be consulted and included in an industrywide BCP. These are civil and commercial authorities such as those providing health care, telecommunications networks, and transport. Clearly, an industrywide plan is far more involved and requires more coordination and effort, but is ultimately the key to the entire sector functioning smoothly through an emergency.

Along with dividing the key dimensions of business processes among institutions, they must also be categorized according to business function. Operations that require the highest level of operational resilience because of their importance must be considered first when developing a line of defense against disasters. Thus trading, brokering, clearing, settlement, and custody will be placed higher than any other reporting communication between firms, for instance. See Figure 9-4.

Figure 9-4 shows that the trade lifecycle, as discussed in Chapter 2, touches many market participants including inter-broker dealers, exchanges, clearinghouses, and data vendors. Each of these participants is linked by a web of networks, and a collapse in any one of these due to viruses, fire, server destruction, and so forth, can break the business-as-usual processes. Data integrity and preservation is also extremely important, for this is what the connectivity is being used for in the first place. Data changes as it goes through processes, and at any given point, a snapshot of the data must be saved in case the data is lost due to any unexpected hazards.

| Industrywide business continuity vulnerabilities |
|-------------------------------------------------|
| **Connectivity**                               |
| Between                                          |
| Firms :                                         |
| Exchanges :                                     |
| Clearinghouses :                                |
| Custodians :                                    |
| Inter-broker dealers :                         |
| Data vendors :                                  |
| **Data Types**                                 |
| Trade details :                                 |
| Data feeds :                                    |
| Counterparty details :                         |
| Credit ratings :                                |
| Account details :                               |
| **Staff**                                       |
| Expertise :                                     |
| Business :                                      |
| Technology :                                    |
| Police :                                        |
| Systems :                                       |

Figure 9-4  Industrywide business continuity vulnerabilities.
This means that participants immediately switch to their backup data servers if needed. Information such as account details, counterparty details, and trade transaction details are all part of important data fields that are exchanged between market participants in a trade lifecycle. Finally, while automation is the mantra of STP, a staff that is expert in finance, technology, systems, and business continuity is necessary to the normal business functionality of any industry, mainly because unexpected extraordinary circumstances sometimes occur.

All these vulnerabilities were kept in mind, and the sector’s resilience to them in case of unexpected disasters was examined in the case studies discussed next.

**CASE STUDY: SINGAPORE**

On May 9, 2006, the Association of Banks in Singapore (ABS) conducted a large-scale real-time industrywide business continuity exercise. Singapore is considered by many to be the financial hub of East Asia and therefore a terrorist target. The scenario was as follows:

*On Tuesday 8th May, Singapore’s financial industry was rocked by a major terrorist attack. Reports of explosions began filtering through at around 2:15 pm. Evacuation and cordons were set up by police and transport was halted. Key financial indices plummeted in response.*

The exercise scenario was delivered in real time through news broadcast and websites as well as telephone injects simulating a broad range of customers, regulators, media, and security issues.

According to ABS, Exercise Raffles, as it was called, saw the participation of more than 170 major financial institutions in the financial sector of Singapore, including banks, the Singapore Exchange (SGX), the Monetary Authority of Singapore (MAS), as well as providers such as SWIFT and the Singapore Automated Clearinghouse. The exercise lasted from 2:00 pm to 5:30 pm and tested the resilience and coordination of participants in recovering business critical processes both internally and externally in conjunction with other firms, in the face of a terrorist attack. It was also an opportunity for firms to test their own internal BCPs.

Overall, the test was deemed successful, with the general market conditions restored to business-as-usual quickly. The Singapore Exchange Ltd., which operates the city’s securities and derivatives market, did not suspend stock trading, and the Monetary Authority of Singapore, which also took part in the drill, provided S$2.2 billion in response “to demand for liquidity by the banks.”

---

1Bloomberg, *Singapore Stages Anti-Terror Drill for Financial Industry*, May 10, 2006.
CASE STUDY: UNITED KINGDOM

The UK has three financial authorities, known as UK’s Tripartite Authorities: these are HM Treasury, the Bank of England, and the Financial Services Authority, and they work together to ensure the smooth, efficient, and effective running of the UK’s economy and the financial sector. Recently, they have been working to ensure that there are procedures in place that will facilitate the resilience of the financial sector against an industrywide operational disruption. Together, they have established the Financial Sector Continuity website (http://www.fsc.gov.uk/), which provides information on business continuity for the UK financial sector. While the Authorities had been conducting business continuity tests, the terrorist bombings of July 7, 2005 in London pushed the government and industry into a more proactive state vis-à-vis disaster recovery planning. In 2005, the Tripartite Authorities conducted the largest industrywide business continuity test in the world and published its findings. In November 2006, the Authorities conducted another six-week test; this time the scenario was that of a flu pandemic.

Large-Scale Disaster Scenario: Over 3,000 people from 70 organizations participated in the Marketwide Exercise of 2005. A major disruption due to a terrorist attack was simulated to test the response, communications, decision-making, and coordinated recovery of the sector. Every dimension from financial markets and systems to civil contingency responses and media was under examination in the test. Planning the scenario under the sponsorship of the Tripartite Authorities involved the consulting firms KPMG and Crisis Solutions Ltd., and representatives from all the key financial and civil organizations in the country. As in Singapore, which incidentally based its scenario on this exercise, the scenario was broadcast via websites and media to participants who then had to react to the situation in an organized manner. The Authorities deemed the test was a success in that the market was able to continue functioning, with participants putting all their business continuity plans into action and the civil authorities such as Transport for London also implementing their emergency strategies. In a post-test questionnaire, 90% of the participants stated that the exercise increased or validated their understanding of the marketwide response process. The exercise reinforced the importance of industrywide tests in strengthening the financial sector against unexpected disasters.

Flu Pandemic Scenario: Around 70 firms participated in the November 2006 test, including key infrastructure providers such as payments, clearing and settlement, and the main exchanges. The scenario simulated the first five months of a flu pandemic, and participants assessed how they would cope as the pandemic worsened. Of course,

KPMG LLP (UK), UK Financial Sector Market-wide Exercise 2005, 2006.
the most obvious disruption would be caused by rising levels of absenteeism among employees in this case. Early results indicated that overall, the financial sector had controls in place for such an event that would allow it to be able to sustain its core services. However, it was highlighted that considerations such as key staff members working from home needed to be incorporated into business continuity planning.

The Financial Services Authority, Resilience Benchmarking Project, Discussion Paper, December 2005.

HEDGE FUNDS

Studies estimate that the number of hedge funds in the US is over 9,000. Even though these hedge funds manage large sums of money, most of them lack the IT infrastructures of large securities firms. The question of who is managing the disaster recovery of the mission critical data and systems of hedge funds has traditionally been neglected.

However, large hedge funds have become aware of the importance of BCP and are paying more attention to their infrastructure and process resiliency. Of course, this applies to funds that have over $1 billion under management; note that most hedge funds are much smaller and will continue to pose a threat to industrywide business continuity unless they are pressed to make disaster recovery plans.

CASE STUDY: UNITED STATES

Large-Scale Disaster Scenario: Just as the UK has the Tripartite Authorities looking after the general safety and health of the financial sector, the four associations—The Securities Industry Association (SIA), the Bond Market Association (TBMA), the Futures Industry Association (FIA), and the Financial Information Forum (FIF)—have together been working on building the resilience of the US financial sector against disasters. On October 14, 2006, a second annual industrywide business continuity test was conducted, this time on a larger scale than the one the previous year, involving more participants and more business processes. Again, the aim of the test was to evaluate the ability of primary security market participants to operate during a significant emergency of some kind. It involved more than 250 firms, including buy-side and sell-side firms, exchanges, service bureaus, clearinghouses, and other industry utility providers, each of which demonstrated that it could continue functioning by switching to backup sites and using business continuity communication and recovery
Straight Through Processing for Financial Services

Procedures. Product groups and business processes covered included components for equities, fixed-income, options, futures, settlements, and money markets.

In the test, which simulated over 80% of normal market trading volume, all the firms and infrastructure providers were able to connect simultaneously when the emergency was announced by utilizing backup data centers, alternative trading sites, and emergency management teams. In doing so, they were able to continue business-as-usual and to place test orders, receive executions, and conduct settlement and payment interactions. According to the report published after the test, the test achieved a 95% overall success rate.

Pandemic Scenario: In March, 2007, the Government Accountability Office (GAO) released a report based on a year-long study of the resilience of financial markets in the US to disasters. The GAO study concluded that the country’s seven critical exchanges, clearing organizations, and payment processors had taken steps to improve their ability to recover from unexpected disasters. These included steps such as increasing the distance between primary and backup sites for operations and clearing. However, it found that these organizations were ill-equipped to handle a major pandemic in which there would be a great deal of pressure on telecommunications infrastructures. It urged financial services firms to increase their efforts to create business continuity plans and conduct disaster recovery tests particular to pandemic scenarios.

RECOMMENDATIONS

The development of a comprehensive BCP is important to ensure operations are not significantly disrupted in case of a disaster such as a terrorist attack or pandemic. As far as possible, operations—including staff, IT systems, and databases—should be dispersed over multiple sites covering a wide geographical area.

1. A solid BCP must be prepared based on:
   a. Estimation of probability of a disaster
   b. Business impact of the disaster
   c. Recovery strategy from the disaster
2. Staff must be educated and trained in BCP procedures.
3. Firms must participate in industrywide disaster recovery tests as systems in different organizations are interlinked.

United States Government Accountability Office (GAO), Financial Market Preparedness, March 2007.
9.5 Summary

This chapter discusses the salient parts of a BCP, which constitutes a strategy for recovering from sudden and unexpected disruption of critical business functionalities. Business continuity and disaster recovery became more important after the occurrence of the September 11, 2001 terrorist attacks in New York, which led to widespread failure in financial systems. Developing a business continuity and disaster recovery plan requires setting aside resources and treating the development of the plan as a project for the firm. Once the analysis has been conducted, and strategies have been formulated, the plan must be tested using simulated emergency scenarios. These scenarios are also important when it comes to industrywide testing, which has become more of a focus recently as firms in financial sectors across the world become more deeply interlinked.