# 3. Business continuity: a systematic approach

**Yossi Sheffi**

Company operations can be disrupted in multiple and unexpected ways. Some disruptions are routine and can easily be overcome with available safety stock, expediting shipments, or well-rehearsed processes. Others, however, can be fatal to an enterprise, leading to tainting of the brand, loss of customers and even unplanned exit from the business, as the examples below demonstrate:

- Following an unsuccessful implementation of SAP's enterprise requirement planning system, coupled with the installation of a flawed automated warehouse management system, Foxmeyer, a $5 billion distributor of drugs, had to file for bankruptcy. Its main operating division was sold to McKesson, its largest rival, for only $80 million.
- As a result of a fire in an Albuquerque Philips plant in 2001, one of the plant's main customers, the Swedish electronic giant Ericsson, was driven out of the cellphone handset business, due to its slow response. This was in contrast to Nokia, also a major customer of the same Philips plant, which reacted quickly and was able to increase its market share.
- In 2002, Arthur Andersen & Co was basically liquidated after two of its partners were convicted of shredding documents related to the company's audit of Enron. In 2005, the US Supreme Court overturned the conviction unanimously but it was too late for Andersen.

Numerous other examples abound.[1]

## DICHOTOMY OF DISRUPTIONS

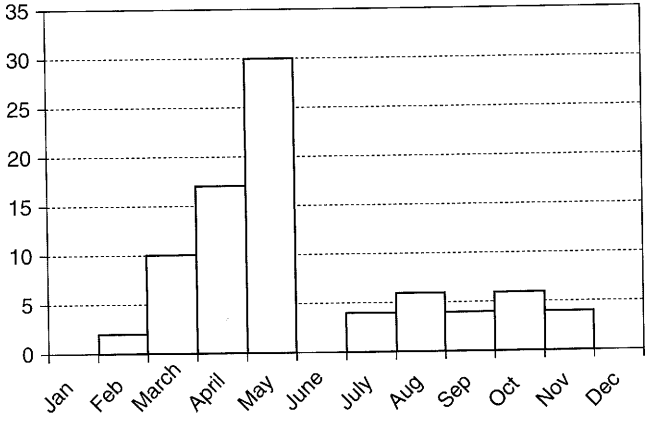
Disruptions can be classified into four categories: natural disasters, accidents, negligence and intentional attacks. These categories differ in the relative roles that human beings and random factors play in their cause.

**Natural Disasters**

Because many natural disasters are frequent, statistical models can be used to estimate the likelihood of their occurrence and their magnitude. Insurance companies have well-developed models of the likelihood of earthquakes, floods, hurricanes and lightning strikes for various areas of the United States as well as for other countries. Insurance premiums can even serve as a proxy for the likelihood of the relevant risk.

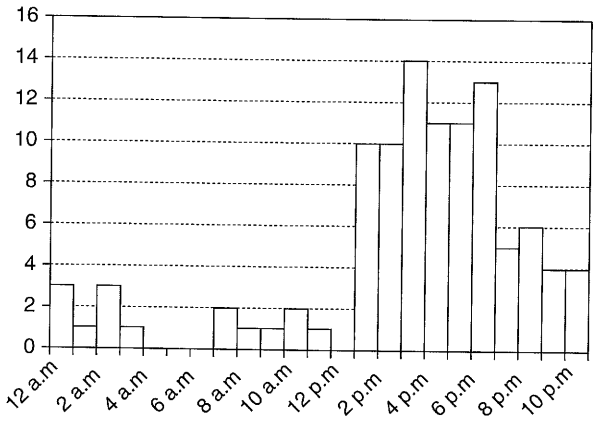
The statistics underlying these models are based on government data. Thus, the US Geological Survey (USGS) estimates that the areas most susceptible to earthquakes in the United States include the western US, the New Madrid zone in Missouri, and a few isolated locations on the United States East Coast. The US National Oceanic and Atmospheric Administration (NOAA) publishes statistics about severe weather. For example, the frequency of tornadoes in Oklahoma City is shown in Figure 3.1. Figure 3.2 depicts the time of day of tornadoes in Oklahoma City, indicating that they take place mostly in the afternoon and early evening hours. By knowing the increased likelihood of tornadoes at these times, organizations can train the right work shift at a plant in emergency evacuation.

Such preparations proved life-saving when a tornado hit the GM plant in Oklahoma on 8 May 2003, at 5.30 p.m. None of the more than 1000 employees who were at the plant was hurt because they all took shelter in the plant's fortified safe room when the tornado sirens sounded at 5 p.m. The tornado hit during the most likely month and at the most likely time of day.




*Source:* Branick (2000)

*Figure 3.1 Tornado frequency in Oklahoma*




*Source:* Branick (2000)

*Figure 3.2 Time of day for tornados in Oklahoma*

## Accidents

Accidental disruptions are unexpected detrimental events resulting from human errors. In many cases accidents result in investigations using root cause analyses aimed to improve procedures, designs, organization or some other contributing aspect. Furthermore, as it turns out, safety experts have documented the fact that when a system experiences hundreds of small accidents (with no injury), one can expect dozens of accidents resulting in one or more injuries and one major accident involving loss of life or serious injuries (Heinrich, 1959). Consequently, many safety efforts are focused on the 'Safety Pyramid' shown in Figure 3.3 – working to eliminate unsafe and/or hazardous conditions, reducing the number of small mishaps, leading to a reduced likelihood of more serious accidents.

To this end, air traffic control systems, the nuclear energy industry and the chemical industry have all developed processes of 'near miss'. Such processes involve the reporting, investigation and dissemination of lessons learned from unsafe occurrences, even when no accident took place. In addition, many companies dealing with hazardous conditions have implemented process safety management (PSM)[2] systems aimed at reducing the number of incidents, since that should lead to a reduced accident rate and the elimination of severe accidents. PSM systems include audit programs that verify the compliance with and safe implementation of procedures. For example, Figure 3.4 depicts the marked reduction of incidents as a function of the audit process at Du Pont; a process which is part of the manufacturer's PSM.

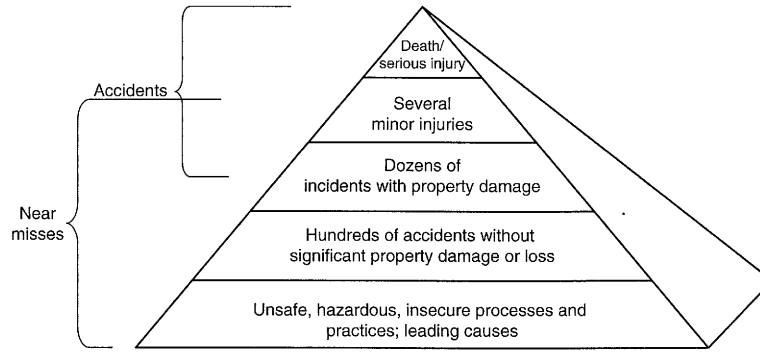
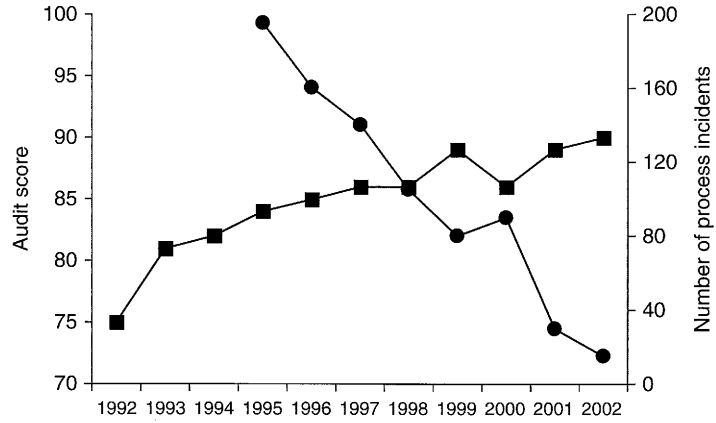



*Figure 3.3 The safety pyramid*




*Source:* E.I. Du Pont de Nemours & Co. (2004)

*Figure 3.4 Incidents versus audit scores at DuPont*

## Negligence

Disruptions based on negligence are, in some sense, close in nature to disruptions resulting from accidents. The root causes, however, are somewhat different and the avoidance mechanisms are different.

Negligence disruptions are of two main types: (1) non-compliance with regulations; and (2) disconnection from (changing) societal norms and expectations.

Non-compliance with regulations can result in the confiscation of shipments, but also the closure of plants. In 2004 the UK government

suspended the license of Chiron Inc. to manufacture Fluvirin, an influenza virus vaccine, at its plant in Liverpool because of contamination at the plant. This suspension took the Liverpool plant offline for five months, resulting in severe shortages of flu vaccine in the US since Chiron was supposed to supply about half of the US's 100 million annual doses. Chiron's non-compliance with the UK government's pharmaceutical manufacturing procedures caused the company to lose a large volume of sales, as well as tainting its brand. It also created significant difficulties for US consumers; during the 2004–05 flu season flu vaccines had to be rationed and the health givers had to manage a priority scheme for consumers. In 2006 Chiron was acquired by Novartis.

But negligence on the part of an enterprise does not result only from non-compliance with regulations. In many cases, companies can suffer significant losses, including tainting of their brand, due to not keeping up with changing consumer and media expectations.

The June 1996 issue of *Life* magazine carried an article about child labor in Pakistan. The article was accompanied by a photograph of 12-year-old Tariq surrounded by parts of Nike soccer balls he was stitching for 60 cents a day. The article generated a public outcry, including demonstrations of activists in front of Nike outlets. In an effort to pre-empt legislation by politicians responding to their constituents, the soccer ball industry came up with a self-monitoring Partnership Agreement, which it co-signed with UNICEF and the International Labour Organization. Nike's brand, however, was tarnished by the episode.

Thus, child labor, environmental protection, global warming, retail diversity, executives' morals, and other causes can make a company the target of well-funded and well-organized consumer groups as well as a media target. Despite the fact that the underlying activities are not illegal, dealing with such incidents can, at the very least, divert management attention from the business; but these incidents can also cause permanent damage to companies in terms of brand equity and actual sales.

**Intentional Disruptions**

Intentional disruptions constitute 'adaptable threats' in which the perpetrators attempt to maximize their likelihood of success. Consequently, such attacks are likely to take place at the worst time and in the worst place – when the organization is most unprepared and vulnerable.

In the summer of 2002, for example, the International Longshore and Warehouse Union (ILWU) staged a work slowdown in the Pacific coast ports of the USA. To maximize the effect of its action, the union timed it to October, planning to choke the ports just as the volume of shipments

from Southeast Asia increased before the holiday shopping season in the United States.

On 28 November 1995, French workers participated in their second nationwide strike in five days to protest against austerity measures proposed by the government of Prime Minister Alain Juppe. In Paris, 85 bus drivers employed by the Parisian transportation authority, the Régie Autonome des Transports Parisiens (RATP), decided to create a disruption in support of the general strike. They knew exactly what to do. The 85 buses blocked the main RATP garage and within hours the entire bus and subway system ground to a halt throughout Paris.[3]

After the United States imposed tariffs on steel imports in March 2002, the World Trade Organization (WTO) ruled that the tariffs were a violation of international trade rules. The WTO decision gave the European Union (EU) and several other countries the right to impose retaliatory tariffs on billions of dollars' worth of American exports. Rather than retaliate by imposing steel tariffs, the EU decided to hit the Bush administration where the tariffs would hurt the most. It published a list of products targeted for tariffs that included citrus fruit, textiles, motorcycles, farm machinery, shoes and other products. The common denominator for these products was that they were all made primarily in political 'battleground states' that the Bush administration would need to win in the November 2004 US presidential elections (Allen, 2003).

These examples demonstrate the non-random, adaptive nature of purposeful disruptions. Terrorism, of course, is the ultimate form of intentional attack. The 11 March 2004 Madrid bombers did not blow up an airliner or attack an airport because, after 9/11, airports around the world had enhanced security measures. Instead, the bombers struck an undefended target – trains in the heart of Madrid. The March 2004 attack took place at the height of the rush hour when the packed trains ensured maximum carnage.

Clearly, labor actions and political maneuvering have nothing to do with terrorism; managers have only to remember that intentional disruptions will strike at the least-defended place at the most inconvenient time. The adaptive nature of intentional disruptions is also the reason that insurance companies find it difficult to calculate premiums in these cases.

## Summary of Disruption Types

Since high-impact disruptions make headlines, and in many cases involve court battles, such disruptions are well documented. Examining hundreds of disruptions, one can conclude the following.

Disruptions should be thought of as supply chain issues, rather than company issues. They can be caused by problems with a company's

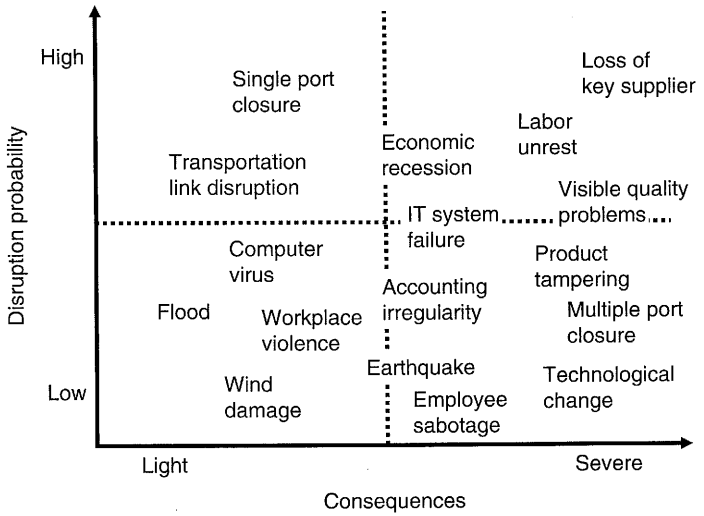



*Figure 3.5 Incident priority chart*

suppliers, transportation routes, distribution network or customers. They can also be caused by the environment (physical, legal or cultural) the company is in. Thus, detection requires a focused and sustained effort throughout an enterprise's ecosystem.

Some disruptions can be specified and measures can be taken to avoid them or minimize their consequences. These include industrial actions, computer viruses, financial irregularities and so on. Many companies plot such disruptions on two axes – disruption likelihood and disruption severity – in order to prioritize avoidance and resilience measures aimed at these disruptions. A stylized example of such a priority map is depicted in Figure 3.5.

In many cases, however, disruptions cannot be reasonably anticipated or their nature is so different from past experience that standard measures are insufficient. Examples include 9/11, SARS (Severe Acute Respiratory Syndrome), Chernobyl, Bhopal, Ford/Firestone and many others. Furthermore, while the probability of a particular disruption hitting at a particular site at a given time is very small, the probability that some disruption will hit somewhere in the company's ecosystem is likely to be significant. This is particularly relevant for large multinationals operating throughout the globe, such as General Motors or Procter & Gamble (P&G). This means that in addition to trying to identify specific risks, companies should build general resilience – the ability to bounce back from any type of disruption, regardless of its nature.

Risk management involves two components: prevention and recovery. The focus of prevention is on avoiding disruption, and the avoidance methods depend on the type of disruption. Recovery and business continuity are concerned with activities after a disruption has taken place. The question at that point is how resilient the business is – how quickly can it recover and get back to the prior level of production, service or any other relevant metric.

Like any other business function, business continuity involves planning and execution. In the context of business continuity, planning is about creating options for the emergency management team which has to respond to an unfolding disruption. (Note that this chapter does not focus on disaster recovery, DR, which in most companies is focused on information technology. Information Technology or IT disaster recovery is based on building in redundancy, including backups and shadow operations. DR is a relatively mature function with many suppliers offering services in this area.)

## EMERGENCY MANAGEMENT

In order to understand the options that emergency management planners have to be ready for, one has to examine the process of emergency response. What will the team responding to a disruption need in order to be effective? At the outset, it should be mentioned that this chapter is not concerned with 'small disruptions' for which normal safety stock (of parts or products), expediting items, or overtime at certain facilities will suffice. The focus of this chapter is on those significant yet rare disruptions that pose a danger to the continuation of the business.

Managing such high-impact, low-probability disruptions involves certain elements which are described in this section.

### The Emergency Management Center

A central emergency management center (EMC) is essential to a timely and coordinated response to major disruptions. The main functions of the EMC include information dissemination and response coordination.

In order to be able to disseminate accurate information, the EMC should be able to get accurate information, process it and then assess it, and decide which channels of information dissemination to use and how to use them.

The information collected should include both the present and the expected future status of employees, plants, orders, deliveries and any other aspect of the disruption affecting the company's eco-systems. To be

able to disseminate such information the EMC needs to have a clear list of priorities and execution levers – to be able to change suppliers, prioritize customers and communicate to Wall Street and shareholders estimates of the extent of the disruption, the ongoing efforts and estimates of future status, including timing to recovery.

Many companies run such centers. For example, Wal-Mart's Emergency Operation Center was instrumental in the company's response to Hurricane Katrina in 2005. Wal-Mart was able to recognize the magnitude of the oncoming storm early, and to prepare the supplies and equipment that would be needed as well as to stage them around Louisiana and Mississippi well before the hurricane hit. Immediately after the hurricane hit, it was instrumental in helping the devastated communities with 1500 truckloads of free merchandise, including food for 100,000 meals.

Most states, cities and towns around the US have some type of emergency management center. For example, the city of New York operates an independent agency, the Office of Emergency Management, whose nerve center is New York's Emergency Operations Center. The center includes representatives from some 130 city, state, federal and non-profit agencies and is staffed around the clock, monitoring emergencies around the city. It serves as a central information and decision-making clearing-house, assessing emergency situations and coordinating the response.[4]

**Taking Care of Employees**

Most companies understand that their most important assets are their employees. Furthermore, implicitly or explicitly they create the expectation that they will help their employees in case they are in need as a result of a high-impact event. Indeed, Wal-Mart, BP and other large companies operating in the areas hit by Hurricane Katrina made special efforts to locate employees and take care of their needs in the hours and days after the hurricane devastated parts of Louisiana and Mississippi on 28 August 2005.

BP philosophy in their makeshift emergency operation center was to 'overwhelm employees with support'.[5] BP had 1064 employees in the affected areas, with 450 of them in the hardest-hit areas. They also were dealing with employees' families and contractors. In dealing with each case, BP provided salary continuation, supplies and equipment, interest-free loans, temporary housing, car rentals, child, elder and pet care, Federal Emergency Management Agency (FEMA) insurance advice and other assistance. Many of these policies were developed 'on the fly' but were then quickly codified and used immediately in the aftermath of hurricanes Rita on 23 September and Wilma on 21 October of 2005.

Similarly, Wal-Mart not only worked to locate and help all its associates in the devastated communities in the wake of Hurricane Katrina, but also guaranteed a job for every one of its displaced workers.

**Taking Care of Business**

Naturally, after the initial 'first response' of taking care of employees and helping the devastated communities, businesses have to turn to business. In some cases business can rely on operational redundancies, such as safety stock, redundant capacity, and stand by suppliers and can continue operations relatively quickly. Immediately following the 9/11 attack, Merrill Lynch was able to move its operations and manage its business from backup locations which were complete with backup IT infrastructure in New Jersey (Ballman, 2001). Deutsche Bank was able, on the very same day, to clear more than $300 billion with the Fed (the Federal Reserve System), even though its US operations center was located in the South Tower of the World Trade Center. Redundant ('just in case') IT systems in Ireland took over when the New York systems were destroyed.

In other cases, businesses adjust quickly, using Herculean efforts by employees to get the business going again. Hurricane Katrina left 195,000 Mississippi Power customers without electricity. The company hired nearly 11,000 outside workers to complement its 1250 employees, and within 12 days was able to restore power to all its customers who could safely take electricity. And this feat was accomplished in the harshest conditions, with its corporate headquarters destroyed and its disaster management center flooded.

Within four days of the storm, all but 15 of Wal-Mart's 126 stores in the devastated region were reopened, using field generators and dry ice where power was not available. This quick action helped not only the business, but also employees and the communities where Wal-Mart operates.

Procter & Gamble's Folgers coffee plant in New Orleans is the largest of its kind in the US and it produces more than half of all Folgers coffee. Not only was the plant flooded during Hurricane Katrina, but it lost its water source (the plant requires 300 gallons per second to process the coffee beans) and most employees lost their homes and had to take care of their families. Through preplanning (for generators and emergency processes) and improvisation (digging a special well and housing employees in trailers), P&G was able to restore the plant to full production within a few weeks. By 17 September 2005 the first production batch left the New Orleans plant and by 16 October all plant operations resumed.

## PLANNING: CREATING THE OPTIONS

A growing body of legal opinions suggests that courts are likely to hold that most events are foreseeable and that there is a responsibility to undertake reasonable efforts to prepare for and mitigate disruptions. The risks of low-probability events are, however, difficult to assess since there are not 'enough of them' to develop their estimated likelihood.

Any planning effort is about preparing the largest number of options for the team responsible for their execution in the aftermath of a disruption. Having safety stock, secondary supply sources, alternative transportation routes, and other such ready alternatives gives the execution team options for responding to the disruption. It also gives them time to develop new, long term options while the redundant capacity is being utilized.

Planning for disruptions can be divided into two clear categories:

1. preparing for specific disruptions; and
2. preparing for the unknown (and in many cases unknowable) disruptions.

As mentioned above (see also Figure 3.5), preparations for specific disruptions can be prioritized and specific measures can be taken. Preparations for unknown disruptions, especially high-impact ones, require building general resilience throughout the enterprise's supply chain.

The following sections outline several aspects of business continuity planning, from the perspective of creating options for the emergency management team. One should remember, however, the old military adage that no battle plan survives the first shot. This is also true about business continuity plans when significant disruptions take place – especially low-probability disruptions. The corollary is that business continuity plans should be understood only as creating options for the emergency managers, not dictating specific actions. It also means that in some cases emergency managers will have to fall back on corporate values and culture to guide their actions. This is discussed below in the section on 'Beyond Contingency Planning'.

### Mitigating Financial Fallout

Naturally, every disruption involves a potential financial loss. The short-term financial impact of any disruption can be protected against with insurance and other financial engineering tools. For example, Southwest Airlines' hedging of fuel prices in 2001 helped it maintain profitability in the aftermath of the airline industry slump following 9/11 and the sharp

increases in oil prices following the Iraq War and Hurricane Katrina. Naturally, insurance instruments are designed specifically to compensate enterprises for certain specific disruptions. Typically, insurance covers disruptions rooted either in natural phenomenon, such as earthquakes, or in accidents, such as plant fire.

Some high-impact, low-probability disruptions, however, are difficult to insure against. The reasons are that they either cannot be specified, are rooted in phenomena outside the enterprise (a supplier's failure), or involve terror or war acts. Many insurers exclude such risks from their coverage because the probability of the underlying phenomenon cannot be calculated and therefore there is little basis for setting the premium. In cases such as a terror act or war the damage can be so great that spreading the risk is not sufficient to ensure the viability of the insurance carriers. For example, in Israel, the government is the 'insurer of first resort' for war-related damage. It has a formula for compensating individuals and businesses for war- and terror-related losses of property.

Most of the high-impact, low-probability disruptions, which are the focus of this chapter, are not insurable. They involve business continuity activities which have to be planned well in advance, even though the nature of the disruption is not known. There are several aspects of preparation, however, which are common to all high-impact disruptions. Many aspects of such planning can be gleaned from examining actual disasters and analyzing what was necessary to make the effort succeed.

## Building the Emergency Response Infrastructure

As mentioned earlier, an effective emergency management center (EMC) is necessary for effective disruption mitigation and recovery efforts. Thus, one of the first steps in business continuity planning is the organization of such a center. The most important function of the EMC is information collection, analysis and dissemination. To ensure the flow of information, Intel, for example, has a regional EMC in every region of the globe where it does business. These centers are equipped with every conceivable type of communication gear from land lines to cellular to satellite phones, as well as VHF, UHF, SSB[6] and even ham radio. These centers are also tuned to local television, radio and Internet sources of news. All the regional EMCs feed data and information to a central EMC.

Naturally, getting the information is only half the battle. Analyzing what is going on, taking actions and feeding information to executives is the other half. To this end, the EMC has to be staffed by trained professionals who become team leaders for manufacturing, procurement, logistics, human resources, public relations, legal and other relevant functions. The

structure of the EMC and the make-up and training of EMC personnel are some of the most important elements of business continuity planning. Just as important is the delegation of authority to the EMC. The EMC may operate in conditions of uncertainty and without constant communication with senior management. Yet decisions may have to be taken quickly. Thus the EMC needs clear guidelines regarding the actions it may (and may not) undertake. Some organizations put in place 'triggers' for delegation of authority, making certain types of decisions conditional on the nature and extent of a disruption.

**Planning to Take Care of Employees**

As mentioned earlier, most companies are committed to accounting for and helping their employees in the event of a high-impact disruption. In preparation for this, human resources policies have to be developed and communicated – how long can employees expect salary continuation? To what extent can they expect interest-free loans? What type of family assistance can they expect?

Some companies are reluctant to develop and communicate such policies, arguing that such policies will commit them to a level of care they may not be willing or able to provide their employees. However, this may be moot since prior behavior is likely to create a level of expectation which companies will be expected to provide – even if the standard was set by other companies in the same geographical area or the same industry. The level of employee support, as well as community assistance, offered by Wal-Mart in the aftermath of Katrina, the care shown by BP for its employees and their families, and the speed with which Mississippi Power restored electricity to its customers, all create a standard which other companies will be held to.

In addition, publishing certain emergency processes, including emergency phone numbers and information channels, will help the recovery and business continuity efforts themselves by creating a tactical 'playbook' for the recovery teams and a set of behavioral expectations for the employees. For example, the EMC may expect every employee household in the hurricane-prone Southeastern US to have food and water for a few days as part of the two-way expectation. Thus the provision of certain necessities will not be a top priority in the first few days.

But the most important element in preparing to take care of employees and their families is to have the data. To this end, BP developed a geographical information system which charts the location of every employee's home as well as family-related information, so that in a disaster, the EMC knows what it has to deal with.

## Building Redundancy

In the immediate aftermath of a disruption, business continuity is based primarily on redundancy: inventory of finished goods can be used to satisfy customer orders, safety stock of parts and materials can be used to keep factories going, manufacturing and other operations can be relocated from disrupted facilities to facilities that have extra capacity, and so on.

Keeping extra inventories or underutilized capacity just in case of a disruption is expensive. In particular, when preparing for high-impact, low-probability events, this approach will require a lot of extra inventory (and/or redundant capacity) held for long periods of time. Today's lean supply chain operations obviate such a business continuity strategy since the extra cost will render the business uncompetitive.

Some level of strategic redundancy is justified, however, since it will give the enterprise some 'breathing room' to plan the recovery.

## Building Flexibility

Since redundancy is expensive, the solution for business continuity and speedy recovery is the development of flexibility. Business and supply chains can be designed so that they can move to alternate suppliers, transportation routes or manufacturing sites with relative ease.

Flexibility is a company characteristic which is well beyond the charter of any business continuity planner – but it has the potential to provide most of the benefits for business continuity planning. The reason is that at its core, building flexibility into an enterprise and its supply chain is, in fact, a business continuity planning activity which is all-encompassing.

Flexibility is based on three principles: interchangeability, speed and process design.

Interchangeability is the capability to move from one supplier to another, from one manufacturing facility to another, and from one transportation route to another. Interchangeability requires that equipment be standard, like Southwest Airlines' exclusive use of Boeing 737 aircrafts or Intel's identical design of all its plants. It also requires standardization of parts, as well as use of commodity parts and materials which are commonly available, rather than special-purpose parts. Interchangeability also requires cross-training of employees so that they can perform tasks other than their day-to-day ones.

Speed means efficient internal communications links as well as the ability to work across functions and company 'silos' in order to accomplish tasks. Thus, companies which use cross-functional teams extensively in their day-to-day operations are, in fact, preparing for disruptions already.

Process design involves many aspects. For example, some companies use postponement strategies – adding specific value to certain products at the latest possible time. For example, Hewlett-Packard (HP) separates the manufacturing of its printers for the European market from the activities of putting in the right power supply, cable, decals and user manual which are specific to each country. If there is a disruption in a given country, HP is not stuck with too many printers in that language but can redirect the flow of printers elsewhere. In another example of process design, Helix used demand flow technology to break down its manufacturing process to small, standard subtasks that workers can learn quickly. This allows the company not only to cross-train employees easily but also, in case of a disruption in its plants, to move production to suppliers who can be quickly trained to manufacture its vacuum pumps.

As mentioned above, building in flexibility involves all corporate functions. For example:

- Engineering can specify standard parts.
- Procurement can ensure multiple sources.
- Manufacturing can use simple, standard processes.
- Distribution can use multiple channels.
- Supply chain management can use postponement strategies to push value addition back in time.
- Human resources can build incentives for cross-training.
- Legal management can develop procurement and sales contracts with built-in flexibility.

Having the flexibility gives the EMC many options to redirect products and materials, outsource manufacturing, change suppliers, and so on.

**Collaboration**

When a disruption hits, speed of communications is paramount. For example, imagine an executive calling the local chief of police at 1 a.m. and having to explain who she is, where she works and what the needs are. Clearly an unfolding disaster is not the time for first introductions.

To prepare for effective disruption management, executives who will be manning the EMC should develop ties with local, state and federal authorities in the regions where they do business. They should also develop contacts with other companies in the same industry and in the same geographical area.

Large-scale disasters will invariably involve government help – which is the reason for developing public–private contacts in preparation. But

banding together with other companies who may either have the same problem (and are thereby able to help each other by combining resources) or may just be able to help is also important. Such relationships can be developed through participation in chambers of commerce, professional associations and other industry and/or local groups.

## Detection

One of the most important preparations which any organization can take is building early detection mechanisms. Early warning allows organizations to prepare, thereby at best avoiding or mitigating the disruption, or at the very least making a more effective recovery effort.

In some cases, early detection is the most important factor in the response plan; as is the case with pandemic planning. This is why the World Health Organization and national authorities are watching for any sign of human-to-human transmission of the avian flu. Early detection will allow for effective quarantine, identification of specific strains and development of vaccines.

Companies operating in uncertain environments invest in early warning systems. For example, UPS operates its own meteorology department. The department issues detailed forecasts regarding key airports where UPS operates – routinely besting the US meteorological service in its forecast accuracy.

A tsunami detection system has been in place in the Pacific Ocean since 1948. It is based on signals from eight deep-ocean sensors mounted on buoys and about 100 coastal monitors, all tuned to detect wave patterns characteristic of a tsunami. In the United States the National Weather Service operates a program called TsunamiReady, promoting emergency awareness, and coastal communities at risk have installed warning systems and disseminate information about evacuation procedures. The system is credited with saving hundreds of lives when Crescent City in Hawaii was evacuated before the tsunami generated by the 1964 Alaska earthquake reached the island. The lack of a tsunami warning system around the Indian Ocean meant that the December 2004 Sumatra tsunami killed 175,000 people in Indonesia, Thailand, India, Sri Lanka, Bangladesh, the Maldives, Myanmar, and even Somalia on the east coast of Africa.

An early warning system for a company's supply chain requires continuous monitoring of its key suppliers for financial health, quality of parts and ethical treatment of employees. In the near future it may also mean monitoring suppliers for their environmental policies and carbon footprint, since the market may demand that companies not only comply with

government regulations but also lead in these areas. A failure may have negative consequences for the brand and sales.

## BEYOND CONTINGENCY PLANNING

Building in flexibility and redundancy, building the response infrastructure and revisiting insurance requirements, and building collaborative linkages with public and private organizations, go a long way towards increasing the number and quality of options that will be open to the people who will be executing recovery efforts.

High-impact disruptions, however, can go well beyond the 'normally unexpected' events. Predicting and preparing for the consequences of 9/11, SARS, Chernobyl, hurricanes Katrina, Wilma and Rita, Bhopal, or other past disruptions was difficult. Predicting and preparing effective responses for an avian flu pandemic, a possible Tiananmen Square II, jihadist control of Middle East oil, or 'intifada-like' patterns of suicide bombings in Europe and the US is difficult. In part, the difficulties arise from the fact that effective communications and therefore command and control will not be quickly established.

In any of these situations, organizations will have to rely on their local units, managers and employees, regardless of their level and training and preparation, to lead in the recovery efforts. For this purpose, as well as for dealing with smaller disruptions, companies and other organizations can build a culture of empowering lower levels in the organization to take the initiative. Such an 'asking for forgiveness rather than permission' culture is likely to encourage local units close to the problem to take action in a timely fashion.

Again, this chapter comes back to Katrina as an example in which several organizations did not perform as expected:

- The mayor of New Orleans was hesitant to issue evacuation orders until 36 hours before Katrina hit.
- The government of Louisiana was slow in marshalling its resources and asking for federal help.
- The federal government and its lead agency, the Federal Emergency Management Administration (FEMA), was assessing what was going on and worried about organization charts, while people were drowning.

Other organizations sprung into action. And it was another agency of the Department of Homeland Security (DHS) which demonstrated how

disaster recovery should be handled. Anticipating the disaster, the US Coast Guard (USCG) moved assets and personnel into the perimeter of the affected area and sprung into action first. The USCG is credited with saving 33,000 people in the aftermath of Katrina. To appreciate the magnitude of this effort, note that in an average year, the USCG saves about 4500 people around the entire country. Interestingly, the DHS has never issued a specific order for the USCG to deploy. The USCG and its units around the country just did so. Even more telling – several of the media sources and follow-up investigations cited the fact that the Coast Guard's Air Station New Orleans (ASNO) managed the operation despite complete loss of communication with the outside world and its own chain of command for extended periods. This was testament to the value of the USCG's 'Principles of Operations'[7] which include 'On Scene Initiative' among other principles such as flexibility, clear objective, unity of effort and effective presence.

Building such a culture in a commercial organization is not easy, but many resilient companies exhibit such corporate culture. At UPS, 'nobody goes home until all the packages are delivered', and at Toyota any line worker can stop the production line if they notice a defect moving on the production line. Gordon Bethune was able to move Continental Airlines within a short period from last to first in on-time performance among US airlines and from first to last in percentage of lost luggage, by empowering employees to take charge.

## SUMMARY

To have effective business continuity efforts, executives and managers facing a high-impact disruption need to have as many options open to them as possible. The development of these options is what business continuity planning is about.

The most important preparation is setting up the appropriate infrastructure for collecting and disseminating information. Such a facility should coincide with the analysis and decision-making function which we referred to as the emergency management center. To ensure the effectiveness of the EMC, a clear delegation of authority to the executive in charge and the team involved should be outlined in advance.

Building the options for effective recovery involves: building redundancy and flexibility into the supply chain of the organization; designing products and processes which have ready substitutes; building collaborative linkages with local, state and federal authorities, as well as with other industry and local organizations; and building an effective detection and

warning mechanism in order to allow emergency managers the maximum time to plan and organize specific recovery efforts.

One of the most important aspects of business continuity planning is recognizing that corporate culture, employee loyalty and corporate values are likely to play a very significant role in the success of recovery efforts. This is particularly relevant for extreme disruptions that may involve loss of communication for prolonged periods.

## NOTES

1. See, for example, Sheffi (2005). Also see *Supply Chain Digest* (2006).
2. The US Occupational Safety and Health Administration (OHSA) has issued PSM regulations and the Environmental Protection Agency has issued requirements for accident prevention. Many companies, such as Du Pont, go beyond the minimum required in the regulations in their processes and procedures.
3. A general report on the strike was retrieved 5 October 2004 from: http://www.cnn.com/WORLD/9511/france_strike/. The site of the *International Workers Bulletin* (retrieved 5 October 2004) mentions some of the tactics employed, http://www.wsws.org/public_html/prioriss/iwb12–4/france.htm.
4. See http://www.nyc.gov/html/oem/html/home/home.shtml.
5. Presentation by Mark Dice, BP at BP's 'Blue Chalk' Leadership Conference, San Francisco, 13 September 2006.
6. SSB = Single Side Band. It is a form of high frequency (HF) communication mechanism.
7. See, for example, http://www.uscg.mil/top/about/doc/Chapter_Four.pdf.

## REFERENCES

Allen, Mike (2003), 'President to drop tariffs on steel', *Washington Post*, 1 December.

Ballman, J. (2001), 'Merrill Lynch Resumes Business Critical Functions within Minutes of Attack', *Disaster Recovery Journal*, **4** (4), http://www.drj.com/special/wtc/1404–04.html, retrieved 12 October 2004.

Branick, Michael L. (2000), 'Tornadoes in the Oklahoma City, Oklahoma area since 1890', National Weather Service Forecast Office, Norman, Oklahoma, February, http://www.nwsnorman.noaa.gov/tornadodata/okc_main.html, downloaded 5 October 2004.

E.I. Du Pont de Nemours & Company (2004)

Heinrich, H.W. (1959), 'Industrial Accident Prevention: A Scientific Approach', New York: McGraw-Hill.

Sheffi, Y. (2005), *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*, Cambridge, MA: MIT Press.