

# Solution Force

Vol.8 March 2013


## Public Safety through ICT Helping cities stay safer

### Contents:

- Offering city-level business continuity ————— 2
  - Inter-agency Collaboration
  - Natural Disasters
  - Homeland Security
  - Identity Management
  - Critical Infrastructure
- Applying Lessons Learned From Catastrophic Events in the Decade Since 9/11 to Improve Your BCM Program ————— 7

## Solutions for Safer Cities

In an increasingly complex world, one company is ensuring public safety and enriching our everyday lives by providing the most innovative IT/network integrated solutions. NEC has developed the fastest and most accurate biometric authentication technologies available, enabling citizens to exercise rights and receive public services quickly and easily.

Make Public Safety A Reality  [nec.com/safety](http://nec.com/safety)

CITIZEN SERVICES & IMMIGRATION CONTROL • LAW ENFORCEMENT • PUBLIC ADMINISTRATION SERVICES • CRITICAL INFRASTRUCTURE MANAGEMENT  
INFORMATION MANAGEMENT • EMERGENCY & DISASTER MANAGEMENT • INTER-AGENCY COLLABORATION

© NEC Corporation 2013. NEC and the NEC logo are registered trademarks of NEC Corporation.  
Empowered by Innovation is a trademark of NEC Corporation.

Empowered by Innovation **NEC**

### NEC Corporation

7-1, Shiba 5-Chome, Minato-Ku, Tokyo 108-8001, Japan

Website: <http://www.nec.com/safety>

Contact: [info@publicsafety.jp.nec.com](mailto:info@publicsafety.jp.nec.com)

Companies and names of products and services shown are trademarks or registered trademarks of their respective companies. All rights reserved.  
"Solution Force" is published by NEC. Additional editorial material supplied by Gartner Inc. © 2013. Editorial supplied by NEC is independent of Gartner analysis and in no way should this information be construed as a Gartner endorsement of NEC products and services. Entire contents © 2013 by Gartner Inc. All rights reserved. Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.



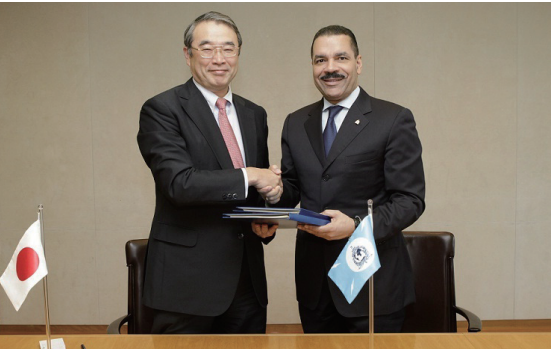
NEC offers city-level business continuity

Ensuring business continuity is a critical need for cities as numerous recent examples attest. Disasters, whether they are the result of terrorist attacks or natural calamities like earthquakes or tsunamis, have the potential to wreck havoc on cities -- destroying lives, infrastructure and economies.

Helping cities anticipate, prepare for, and recover from, disasters is something that NEC is uniquely qualified to do.

'Safer Cities' is an integral part of NEC's vision for Smart Cities, where people are able to live, work and play in safety and comfort, while co-existing in harmony with the environment. Through its Safer Cities suite of advanced technologies and solutions, NEC offers municipal authorities the ability to minimize the human and economic impact of disasters as well as to facilitate recovery.

NEC provides technology to Interpol



NEC President Nobuhiro Endo (left) and Interpol Secretary General Ronald K. Noble sealing the agreement in Tokyo.

NEC will be helping global law enforcement agency Interpol to develop core elements of the Digital Crime Centre which will be established at the Interpol Global Complex for Innovation in Singapore.

Under the three-year agreement signed in December 2012, NEC will provide technical and human resources worth some EUR 7.6 million to establish a Digital Forensic Lab and Cyber-Fusion Centre at Interpol's complex.

The Digital Forensic Lab will focus on identifying and test-bedding digital forensic technology and methodologies to help investigators better coordinate and conduct digital crime investigations.

The Cyber-Fusion Centre will provide a platform for law enforcement to collaborate with the Internet security industry to effectively combat digital crime. It will also provide expertise to national cybercrime units during enquiries, coordinate cross-border investigations and deploy investigative support teams to assist national law enforcement agencies during investigations following a serious cybercrime incident.

Improve inter-agency collaboration

Business continuity planning must be a group effort. In the modern city, many agencies are involved in both preparing for a disaster and responding to it. These include the fire service, the police, hospitals, utilities, telecommunications companies and transport. In some cases, intelligence services as well as the military are involved as well. Because there are multiple agencies involved, a platform for sharing information, for discussion and for decision-making is critical.

Against such a backdrop, NEC has developed solutions aimed at inter-agency collaboration. This platform, through a command centre, enables effective sharing of information that allows cities to prepare for specific threats that they face.

For example, take homeland security threats. These are potentially catastrophic events that can be prevented if there is advance intelligence. Prevention consists of three parts – sensing, sense-making and sharing. NEC has solutions that enable agencies to gather data from various sensor systems located in different parts of the city or country, making sense of these data, and then disseminating the relevant data for appropriate actions by the relevant agencies.

NEC provides, among others, identity management systems, object recognition systems, access control systems and event-driven systems to gather data from diverse sources. These sensors allow security agencies to watch out for the entry of undesirable people and locate them. NEC also has sensors to detect dangerous objects or record significant changes in the environmental landscape that might indicate potential danger.

NEC to modernize infrastructure of criminal ID system in western US



NEC will be modernizing the multi-state criminal identification system run by the Western Identification Network (WIN) in the United States, which provides identification services to the law enforcement agencies and citizens of its member states.

The states involved are Alaska, Idaho, Montana, Nevada, Oregon, Utah, Washington, Wyoming, and California (as an interface member). This is a database of about 28 million fingerprint records.

The updated system will include advanced identification capabilities such as high-resolution palm and fingerprint matching and other emerging biometric functions, disaster recovery facilities, and enhanced system performance.

The existing WIN system will be moved to a highly fault-tolerant architecture supporting advanced biometrics technology. It will also incorporate key elements of NEC's cloud-based offerings – such as FBI-compliant data centers, Network Operations Centre, remote-managed services, and server virtualization – that will be used to increase system security, reliability, and maintainability.

The idea of a networked, shared AFIS system was conceived in January 1988, with the first ever multi-state AFIS network going live in 1989. The enhanced WIN system is expected to be rolled out in 2013.

Typically, all this data are collected by different agencies, who have different access to primary sources. However, data from one agency alone is incomplete unless combined with other data from elsewhere to provide a full picture of the situation. NEC has developed an information sharing framework that pulls data together from different sources, thus allowing different agencies to pool their information. NEC is also able to provide analytics solutions to process and analyze the huge amounts of data created by sensors.

Social media has become a valuable source of information about the general tenor of society and their reaction to events. It can also be a communications platform for people organizing mass movements. The media is thus becoming a valuable source of intelligence, and the ability of agencies or business to develop the

capability to analyze sentiments from the content posted on social media streams has become more critical.

Homeland security threats are very real and potentially catastrophic. While they can be devastating, they are also sometimes preventable. Modern terror attacks require the efforts of multiple people, all of whom leave traces that a system with elaborate and effective sensors can pick up and interpret. NEC's inter-agency collaboration tools enable governments to capture data, and turn it into useful, actionable information.

Preparing for natural disasters

Disasters, especially, natural disasters, are typically not preventable. For business continuity as it relates to natural disasters, the strategy is to prepare before the disaster, to try to gather as much advance warning as possible and to warn people ahead of time.

Early warning requires gathering data from different sensors to predict incidents such as floods. To gather the data, NEC has sensors such as surveillance cameras, water level gauges, rain gauges and seismometers. A command centre then acquires and analyses the data to ascertain the likelihood of an event. If the data suggests that an event is imminent, the command centre can issue an evacuation order using different channels to reach the affected population.

To detect earthquakes and tsunamis, NEC also has ocean bottom observation systems, earthquake observation systems, land (river, coast, dam) observation systems and land observing satellite systems that are able to notice and alert the authorities to impending events. These systems use various types of seismometers, tsunami sensors, precipitation and water level sensors and surveillance cameras to detect changes in the environment that are preludes to earthquakes and tsunamis.

Thanks to NEC's more than a century experience in quake-prone Japan, the company is particularly strong in earthquake detection. NEC's earthquake early warning systems detect the initial tremors to calculate the scale and epicentre. This allows it to calculate when the secondary waves, the ones that cause the most damage, are likely to hit. NEC's system can also determine the risk of a tsunami.

NEC has a well-developed disaster emergency response

centre solution. The centre takes in meteorological reports, raw data from sensors and also consolidates video footage, as well as information and first-hand reports from police and first responders. This then allows the relevant agencies to determine the most appropriate response. The centre can also communicate and broadcast information to households, individuals and evacuation centers.

An extensive, redundant communications network underpins disaster management. It is vital as these networks carry the raw data that is needed for analysis. These networks also subsequently carry communications to first responders or to the civilian population.

Working closely with its partners, NEC provides satellite communication systems, terrestrial radio systems and fibre-optic networks to handle communication. Satellite communication systems are less reliant on infrastructure on the ground, which means they are less likely to be affected by earthquake. Terrestrial radio systems and fibre-optic cables can supplement satellite transmissions. These networks can be used for broadcasting alerts to the civilian population via radio and mobile phones.

Securing borders to enhance homeland security

An important part of preventing incidents like terrorist attacks is a country's ability to secure its borders. By being able to control access into its territory, countries are able to reduce the risk of terrorism-related events happening within its boundary.

However, in the face of globalization, it is not viable to simply put up steeper barriers to make entry more difficult. In today's economy, commerce and business would grind to a halt if cities and countries made entry and exit overly onerous.

That is why countries need to have a solution for managing traffic at the border that allows fast passage for legitimate, aboveboard travelers while at the same time, stopping undesirables from entering.

To address this, NEC has developed various manual and automated border control solutions leveraging on its proprietary leading-edge biometric technologies. These solutions allow the vast majority of legitimate travelers to breeze through immigration, thus allowing resources to be directed to persons who are more questionable.

Automated Immigration Clearance in Singapore



In 2006, Singapore moved to biometric passports so that it could get a visa waiver for its citizens to enter the United States. NEC developed the e-passports that allow Singapore citizens to clear immigration via an enhanced immigration automated clearance system using their normal passports as well as their biometric passports.

Today, eligible travellers may seek immigration clearance through the automated gates that are deployed at the key Singapore checkpoints. He or she would be allowed entry into Singapore upon successful verification.

Apart from speed of service, this system also reduces manpower costs, allowing Singapore's immigration officers to do more with less. Most people are able to clear immigration via the automated lane, thus freeing up officers to focus on other tasks.

Focus on identity management

The basic technology underlying NEC's various biometric solutions for immigration control is its automated fingerprint identification system (AFIS). To-date, there are some 500 customers in more than 30 countries around the world who are using NEC's AFIS solutions. This system, combined with another of its highly ranked facial recognition system, allows countries to safeguard their border checkpoints, airports, seaports and other entry points.

Besides border control, NEC's biometric solutions have been used for other applications such as national identification and law enforcement. In law enforcement, officials have been able to make use of AFIS to solve crimes. The technology is also used in prisons. It can record attendance, incorporate scars and tattoos, and be used for clocking in and out. Combined with a facility management system, it tracks the movement of inmates, assets and visitors.

NEC identity management solutions have also been used in national identification projects to manage the identity of citizens, which in turn has led to the development of a slew of citizen services solutions. These can be deployed for use for general identification needs, verification of voter identity and the provision of social security benefits. The same solutions are at work in the management of foreign workers and professionals.

Through effective identity management solutions, NEC is able to help countries to better manage their borders to improve homeland security.

Worldwide NEC AFIS installations



Bringing South Africa's national ID system into the digital age

South Africa's national identification (ID) system provides an identity booklet to all citizens over the age of 16 which is used for access to public services and daily transactions. It used to be a paper-based system of recording thumbprints and over time, South Africa amassed some 45 million paper records, making checking fingerprints a nightmare.

In 2001, South Africa turned to NEC to create a digital database of existing and new fingerprints that could be processed, verified and authenticated in real time. The Home Affairs National Identification System (HANIS) leveraged on NEC's award-winning Automated Fingerprint Identification System (AFIS) to handle the more than 30 million digital records. Today, the system can handle as many as 70,000 searches in a single day.

With the system in place, queues are now shorter, delays have been reduced, and the accuracy of the system has dramatically reduced the possibility of fraud and identity theft.

Registering voters in Bolivia using biometrics

In just 75 days, NEC helped to create an electoral voter roll for Bolivia using biometric data that enfranchised Bolivians and enabled them to vote in the presidential elections of 2009.

Working with the National Electoral Court of Bolivia (Corte Nacional Electoral - CNE), NEC managed to create an electoral roll registering the voters living in Bolivia and abroad that was both accurate and reliable.

The logistics were challenging given that Bolivia covers 1 million sq km with a capital high in the Andes. In addition, there was also a desire to enfranchise Bolivians overseas.

The solution consisted of NEC's AFIS (Automated Fingerprint Identification System) and facial recognition technology, hardware, software, and staff training and support. To capture the necessary data, some 3,000 enrolment terminals were installed with biometric data gathering capabilities. The system used fingerprint, signature, and facial recognition technologies and also involved the construction of two data centers.

As a result of their efforts, the previous electoral voter list was purged of more than 3,000 duplicate and otherwise illegal voters, Bolivians living overseas were able to vote for the first time, and the voter list swelled from 3.5 to 5.2 million voters, allowing truly democratic elections for the first time in many years.

Given the scope, time frame and the results, NEC's project in Bolivia was an unprecedented success.

Protecting critical infrastructure

Cities have weak points in their physical infrastructure. Strike at a city's power or water supply, or disrupt its telecommunications and the entire city comes to a standstill. These are obvious, high-value targets and that is why it is vital to protect these places.

To enhance physical security at sensitive installations, NEC has high sensitivity cameras to capture video images, even in low light. NEC's behavior detection systems can analyze the data and automatically detect suspicious behavior.

NEC's biometric recognition solutions can also be used to manage the movement of people through sensitive facilities to ensure that only legitimate workers and visitors can enter. Within the facility, access to rooms and places



can be further restricted based on security clearance.

To handle vehicles, NEC's vehicle clearance system records license plates and allows the undercarriages of vehicles to be scanned for security purposes.

Public transportation networks such as trains are also vulnerable. To enable on-train security, NEC has a train-borne security and communications system that allows authorities to improve security and communications on mass transit systems.

NEC helps cities stay safer

NEC's suite of solutions is aimed at helping municipal governments keep their cities safe from natural or man-made disasters. Through early detection, counter-measures can be taken and lives saved. In the case of terrorism-related plots, good intelligence can actually prevent the event from happening.

Apart from early detection, preventive measures, better sharing of information, better physical security and multiple communications channels will allow governments to reduce the window of opportunity available to disrupt lives and economies. The business of government and enterprise can then go on un-interrupted.

Tops in Biometrics

NEC is a world leader in biometric solutions. NEC's biometrics algorithms have been tested by the United States National Institute of Standards and Technology (NIST) and found to be among the best in the world. NEC was ranked most accurate in both single and multi-finger tests.

NEC's algorithms were ranked among the top three in the one-to-one fingerprint matching tests and the two-finger matching tests. It consistently achieved top rankings in the lowest false accept and the lowest false reject rates tests. In the automated latent print identification, NEC ranked first in all accuracy text categories.

NEC's Face Recognition technology was also number one in the latest Biometric Grand Challenge's (MBGC) "Still Face Challenge", carried out by NIST in 2009. It also ranked highly in other related face recognition tests conducted by NIST.



About NEC Public Safety

NEC has a proven track record in public safety and continually aims to bring its best-of-breed cutting-edge security technologies and total solutions to help public and private institutions safeguard lives and property in both the real and virtual worlds.

The company has established Regional Competency Centers for public safety around the world, with the mission of helping government and safety agencies build necessary human capacity and technological knowhow to deal with modern-day challenges.

With a strong presence in Asia Pacific, Greater China, Latin America, Europe and the United States, NEC possesses the uniquely powerful platform for best practices to be shared meaningfully globally. More importantly, it enables NEC to leverage across regions to keep cities safer.

Applying Lessons Learned From Catastrophic Events in the Decade Since 9/11 to Improve Your BCM Program

Published: 3 August 2012  
Analyst(s): Roberta Witty

In the decade since the 9/11 attacks against the U.S., business continuity management has come of age as a professional discipline. A review of eight "trigger event" disasters in that time shows what BCM professionals have learned.

Key Findings

- Disasters — natural and manmade — have increased dramatically in frequency and impact in the past decade, making business continuity management (BCM) a mission-critical issue for virtually every enterprise.
- The unexpected nature of recent events, from a volcanic eruption to recent cloud and data outages, shows that the BCM professional must prepare for unpredictable, even wildly improbable events and their impact on the enterprise.
- BCM professionals must work with many internal and external stakeholders to develop appropriate responses for handling most large-scale disasters, which are beyond the enterprise's capacity to manage.
- BCM lessons learned since 9/11 can be grouped into four categories: planning and execution, crisis management, workforce resilience, and business operations resilience.

Recommendations

- Work with key enterprise stakeholders to identify all risks to business operations, not only those related to traditional BCM thinking. Do not focus on what's likely; focus on what is possible — that will expand your list of planning scenarios and have everyone thinking outside the box.
- Select an appropriate BCM framework or set of standards, and develop a road map for BCM maturity improvement based on the framework.
- Engage with external stakeholders — including supply chain and other business partners, customers and clients, and government authorities — to develop effective BCM plans.
- Improve planning and execution processes, including extended outage planning; the complete loss of facilities, physical assets, IT infrastructure, vital records and workforce; and working with external partners, such as government agencies and suppliers.
- Improve crisis management processes, including crisis management execution, crisis communications and the use of social media.
- Improve workforce resilience processes, including succession planning, long-term absenteeism, shelter in place, workforce identification and tracking, and challenges to privacy policy requirements.
- Improve business operations resilience processes, including supply chain availability, loss of transportation infrastructure, loss of telecommunications infrastructure, cultural and language coverage, remote/telework arrangements, the use of collaboration tools and social media, and production work reassignment to other locations.

LIST OF FIGURES

Figure 1. 2010 AMR Research Survey: Supply Chain Failures..... 8  
Figure 2. Relative Impact of Disasters on Global Business ..... 9  
Figure 3. BCM Key Lessons Learned (by Event) ..... 10

Strategic Planning Assumption

By 2015, 75% of organizations with BCM programs will have integrated public social media services with their crisis communication strategies.

Analysis

The Decade When BCM Came of Age — Because There Was No Choice

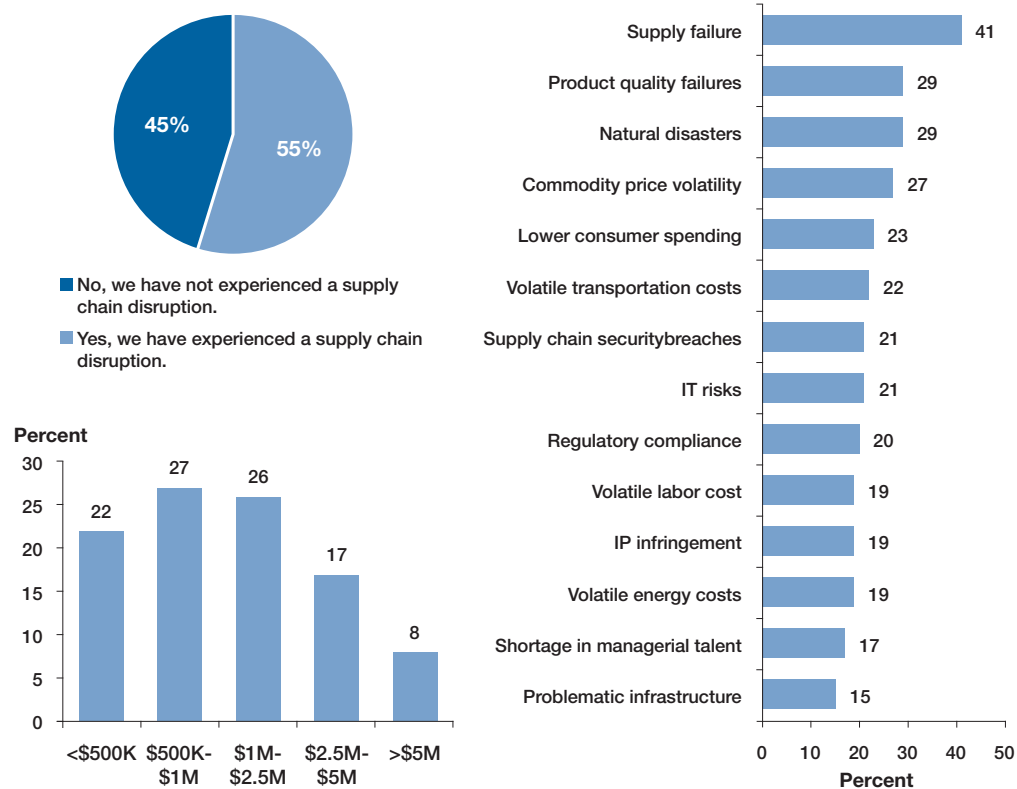
In the decade since the devastating 9/11 terrorist attacks against the U.S., a long series of large-scale disasters, natural and manmade, has focused the world's attention on the critical need for improved BCM processes and practices. During this period, enterprise BCM programs have been tested as never before, and BCM as a professional discipline has risen from a marginal function — largely within the IT organization — to a board-level concern.

Research clearly shows that natural and manmade disasters are increasing in frequency<sup>1</sup> and cost.<sup>2</sup> In 2010

alone, natural disasters claimed more than 304,000 lives,<sup>3</sup> cost insurers \$43 billion and caused total economic losses of \$218 billion. The economic losses from manmade disasters for the same period were \$24 billion, mostly from the 2010 oil spill in the Gulf of Mexico. These incidents and many others — including IT outages such as cloud disruptions, service provider failures and less mature change management practices — have resulted in customers being unable to access their own data, and have also strained enterprises' workforce continuity plans, damaged their supply chains and stretched their IT capabilities to the breaking point.

In the 2010 AMR Research Supply Chain survey (see Figure 1), almost half of the respondents reported that their enterprises had experienced supply chain disruptions in the previous year, most with damage in the \$500,000 to \$2.5 million range. The types of disruption were extremely wide-ranging — supply failure was the single most significant type of disruption, followed most closely by product quality failures, natural disasters and commodity price volatility.

Figure 1. 2010 AMR Research Survey: Supply Chain Failures



2010 AMR Research Supply Chain Management User Wants and Needs Survey  
Source: Gartner (August 2012)

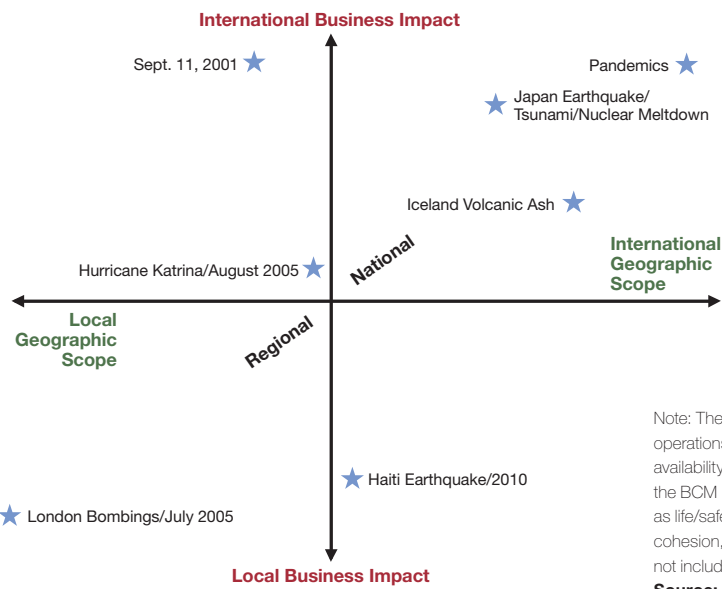
It is important to note that calculations of probability are meaningless when you're talking about events reported on this research. Organizations that are prepared for such events are thinking about what's possible, not what's likely. No terrorist attack (or volcanic eruption) is ever "likely," at least not in terms of a specific attack vector directed at a specific target. Ask yourself whether there's something you can do at a reasonable cost to prevent dreadful outcomes — and if so, do it.

Effective BCM Requires Thinking Beyond Your Own Four Walls

A broad range of factors — including worldwide political and economic instability, volatility in the price of energy

supplies and other commodities, and global climate change — is likely to make the future even more uncertain and risk-intensive than it is today, with more and more large-scale, highly disruptive events occurring. Nonetheless, most enterprises are still planning only for short-term business disruptions and "predictable," localized events, and most are not prepared to conduct the sophisticated risk management that a highly uncertain business and operational environment requires. Gartner believes this failure to address the real risks and uncertainties of a changing world represents an unacceptable level of risk for most enterprises. Figure 2 shows the impact of various disasters from a geographic-scope perspective.

Figure 2. Relative Impact of Disasters on Global Business



Note: The figure shows the relative impact on business operations, such as raw materials availability, workforce availability, the shipment of goods and the impact on the BCM profession. There are other impacts — such as life/safety, community and international humanitarian cohesion, government response and reputation — that are not included.  
Source: Gartner (August 2012)

A localized event can be characterized as one in which: (1) The impact is small — by geographic area, workforce count, product impact and organizational event; and (2) business operations can continue at some level, because: (1) The public infrastructure is working and responsive; (2) there are a small number of government agencies involved; or (3) available internal and external resources are strained (but not broken) due to the reassignment of production resources to recovery efforts. You will also manage via incident response plans instead of full-blown recovery plans. Crisis communications will be at a team level as well as on a one-to-one basis.

By contrast, a regional, national and international event can be characterized as one in which: (1) The geographic impact is large, and the workforces of many organizations are impacted — and is likely to include the public as well; and (2) business operations are disrupted, sometimes severely, because: (1) The public infrastructure is no longer reliable; (2) many government agencies are involved and coordination between them and the organization is mandatory; or (3) the impact of the event exceeds all available resources — internal and external. You will be activating a full set of recovery plans. Crisis communications requires an "all hands" approach with ongoing, interleaved communications demands by internal and external parties.

Eight Events That Changed BCM Planning

BCM success is ultimately determined by the ability of the enterprise, government agencies, utilities and transportation services, and other partners to respond effectively to the unexpected and maintain critical business operations. For this reason, Gartner has considered eight major disruptive events from the past decade — all very different, but all with important, and sometimes common, triggering events for improved preparedness, response, recovery and continuity practices — and developed a set of BCM lessons learned from them. See Note 1 for a more detailed review of each disaster:

- 1. The 9/11 Terrorist Attacks: The Event Heard Round the World
- 2. Severe Acute Respiratory Syndrome (SARS), "Bird Flu," "Swine Flu" and Other Pandemics: World Travel Has Its Disadvantages
- 3. The London Transit System Bombings: A Prisoner at Work
- 4. Hurricane Katrina: When Supply Chain Risk Management Became a Recovery Practice
- 5. The Iceland Volcano Eruptions: How Relatively No Physical Damage Stopped the World
- 6 & 7. 2010 Haiti Earthquake and Queensland Flooding: Social Media Became an Essential Recovery Tool
- 8. The Japanese Earthquake and Tsunami: Culture and Language Matter

BCM Lessons Learned Since 9/11

Figure 3 summarizes the key lessons learned from each event. Many of the key lessons learned from the above events can be applied to almost all of them. However, in Figure 3, we indicate where a lesson was most important to the management of the event, or when the lesson first occurred. For example, crisis management applies in every event, but we highlight it below only where something new came out of the event that altered the scope of the process.

Figure 3. BCM Key Lessons Learned (by Event)

Event/Lesson Learned	Planning and Execution				Crisis Management				Workforce Resilience					Business Operations Resilience							
	Extended Day Outage Planning	Loss of Control	Loss of Facilities, Assets, Vital Records and Workforce	Heavy External Party Reliance and Collaboration	Crisis Command Center	Crisis Communications	Social Media	Organization Reputation	Succession Planning	Large-Scale Absenteeism	Privacy/HR Policy Challenges	Personal Recovery Training	Public Health Concerns	Shelter in Place	Culture/Language	Large-Scale Telecommunications	Loss of Air Transportation	Remote Work/Collaboration	Product/Service Demand Changes	Supply Chain Disruptions	Emergency IT Change Management
2001: Sept. 11	X	X	X	X	X	X		X	X		X					X	X	X	X		
2002 and Ongoing: Pandemics	X			X						X	X	X	X					X	X		X
2005: London Transit Bombings					X	X								X							
2005: Hurricane Katrina		X	X	X	X	X		X		X	X	X	X		X	X				X	X
2010: Iceland Volcanic Ash																X	X	X	X	X	
2010: Haiti Earthquake/ Queensland Floods			X		X		X						X								
2011: Japan Earthquake/ Tsunami/Nuclear Meltown	X		X		X	X	X	X					X		X						

Source: Gartner (August 2012)

Planning and Execution

- **Prepare for disruptions that could last for extended periods.** A pandemic may persist, and even get worse, over a period of several months, and this makes long-term planning crucial. Under these conditions, just-in-time supply chain and inventory management simply will not work, so critical supplies and raw materials must be stockpiled and alternative sources identified. The loss of the most basic supplies and services — including food supplies, water and transportation — must also be expected and planned for (such as by rationing). In general, BCM professionals must determine that their pandemic plans are viable, and ensure that they can be used effectively not just for days, but also for weeks and months. (pandemics)
- **Recognize that the enterprise is not the primary authority in charge of the recovery from a regional event.** An effective response to a large-scale disaster will require coordination and collaboration by a large number of external parties. In most cases, overall recovery activities will be managed by government authorities, so establish relationships with local, county, regional, state and federal/national government-based emergency management agencies. Previously cultivated relationships with utility providers and IT vendors will also play a critical role in ensuring operational resiliency. For this reason, critical external parties should be actively involved in the enterprise's BCM program, primarily in planning and exercising activities. (9/11)

Develop ongoing, working BCM relationships with public health authorities, as well as with business partners. Public health departments, such as the U.S. Centers for Disease Control and Prevention (CDC), have a critical stake in containing, managing and mitigating any major disease outbreak. They are also the most reliable and credible sources of information about health issues, and for this reason, ongoing relationships with them are crucial to developing an effective enterprise response. Third parties — for example, supply chain partners — will also be crucial to effective continuity efforts, and the enterprise should develop coordinated response capabilities with them. (pandemics)

- **Start recovery execution early.** Hurricanes and other such storms normally present themselves long

before they strike. Hurricanes typically have a five-day warning, which is called a "cone." Follow government weather-tracking services for a storm impacting your area and start the execution of your recovery procedures before the storm strikes. (Hurricane Katrina)

- **Plan for the startup of business operations after power is restored.** Recovery follows power restoration; therefore, have enough generators and fuel supplies to last for a few days to one week, if feasible. This point is especially important if your recovery sites are also impacted by the disaster. Work with your power utilities to ensure that they understand your recovery needs, and that you understand their procedures and capabilities to get power back in your business locations. Plan for gaps in both programs. (Hurricane Katrina)

One particular problem in Japan is that different parts of the country use different electrical standards, which added another layer of complexity to the task of replacing computers, telephones and other mission-critical equipments. This may not be a problem in other regions, but it is a consideration that BCM professionals should take into account. (Japan earthquake/tsunami/ nuclear disaster)

In the months after the disaster, Japanese enterprises also faced the possibility of energy-conserving "rolling brownouts." BCM plans should allow for scheduled or unscheduled shutdowns of their facilities and processes if brownouts occur after a disaster. Recovery procedures should also be prepared for shortages of even the most basic supplies, including food and water — existing supplies of which may be contaminated — and medical equipment, such as bandages and other first-aid supplies. (Japan earthquake/tsunami/nuclear disaster)

- **Plan for the complete loss of personnel, facilities and vital records, as well as long-lasting damage to affected areas that make them uninhabitable and unusable for residential and business operations.** The 9/11 attacks showed that enterprises must prepare for massive events that can destroy or fundamentally disrupt every aspect of their operations. Many of the enterprises located in the World Trade Center lost large amounts of their entire operational capabilities — people, facilities and information — when the buildings were destroyed. (9/11)



Have site maps, drawings and inventories of all equipment and replacement options in case of complete asset destruction. Due to the vast water destruction incurred after Hurricane Katrina, many paper-based documents were destroyed. Ensure that copies are kept at off-site locations that are far enough away from a risk-assessed impact area. (Hurricane Katrina)

The almost unimaginable chain of events in Japan — and their ongoing "ripple effects" on enterprises worldwide — make it clear that the unthinkable is no longer unthinkable. BCM professionals must plan for the complete loss of people, facilities and resources for extended periods. More than a year after this event, large areas of Northeastern Japan remain profoundly damaged and effectively unusable for business operations. Organizations need to plan for the long-term transition of work to other locations, if possible. Data centers located in Japan in particular should be reviewed for their risk exposure, and alternative arrangements should be made if the risk is too high for the business being performed in them. (Japan earthquake/tsunami/nuclear disaster)

Crisis Management

- **Establish a command center to handle workforce needs.** 9/11 forced us to think about tracking all workforce members as well as visitors in our facilities. It also required us to set up programs and communication methods to help the emotional and logistical needs of the families of its victims. In addition, it is important to set up an internal BCM website to which employees can turn to find up-to-date information regarding an incident. Finally, leverage TV and radio outlets for large-scale events. (9/11)
- **Recognize that information communicated in the immediate aftermath of a disruptive event is likely to be highly inaccurate.** Confusion and rumormongering inevitably follow any disaster — particularly one as frightening as a terrorist attack. Witness and media reports are likely to be inaccurate and incomplete. Also, due to the availability of news through many outlets today, people will likely have access to information as quickly as, if not faster than, the enterprise will, so enterprises must act quickly and efficiently. The BCM professional should be careful to make decisions based only on the most reliable

information available. (London bombing)

- **Communicate with the workforce often, even if you have nothing new to tell them.** The information communicated to the workforce must be as accurate and complete as possible, and it should be regularly sent. If there is no update on current conditions, for example, then the enterprise should say that to show it is actively concerned with employees' well-being and is also a trusted source of information. Use multiple media outlets for that communication — do not rely on one or two standard, corporate communication mechanisms. (London bombing)
  - **Establish a social media monitoring program with defined roles and responsibilities for a public information/digital information officer for outlets such as Facebook and Twitter.** Most people communicate through one or both of these social media outlets. During a crisis, much will be said about the event, as well as your organization (if impacted), from the minute it occurs. You need to follow all that is said about your organization to manage your reputation, as well as to control rumors, errors and panic about what your organization is or isn't doing to manage the event. (Haiti/Queensland)
- Gartner predicts that, by 2015, 75% of organizations with BCM programs will have integrated public social media services with their crisis communication strategies. Social media holds the potential to transform enterprise BCM and crisis/incident management practices worldwide. In many cases, social media may represent the only available means of: (1) locating and contacting personnel when external or internal enterprise communications are either partially or completely lost; (2) providing stakeholders with the information and assistance they need; (3) informing citizens, customers and partners of product/service availability; and (4) taking other business-critical actions following a disruptive event. The use of social media enables enterprises and BCM professionals to: (1) identify the scale of a disaster; (2) determine the well-being, location and status of their personnel; (3) receive requests for assistance/service; (4) monitor the disaster's impact on the organization's reputation; and (5) develop the situational awareness necessary to optimize response coordination.

- **Create presence and organization-level accounts for social media outlets, such as Facebook and Twitter.** Communications about your organization must come from official accounts, not individual people within the firm. Multiple people need access to these accounts in case someone is unavailable to post an update when it is most needed. (Haiti/Queensland)
- **Establish official crisis management websites — one for the internal workforce and one for external parties.** All interested parties of your organization — internal and external — need to be communicated with during a crisis. Set up these "black sites" before an event occurs. Often, during a disaster, your call centers will be overwhelmed with inquiries; therefore, these websites are a requirement to handle the call volume. The internal website should be part of your intranet and contain links to internal HR and BCM policies and procedures, as well as external links to resources such as weather tracking, financial aid and employee assistance programs. The external website should be one you switch to only when there is a crisis large enough to have a moderate to severe impact on the organization. It should report critical information about the event, provide regular updates as to how the organization is managing it, and report how customers, partners and other interested external parties should contact your organization during this critical time. Do not host crisis management websites in only one production data center. Host them with a third party that is out of your geographic area, or at multiple data centers under your control so that they can be immediately activated after an incident. (Haiti/Queensland)
- **Work with local authorities to assist in public recovery efforts, thereby improving the organization's reputation as a community leader.** Not every business may be impacted by the disaster. In the aftermath of Hurricane Katrina, because there was no power, ice and water were in very short supply. The public needed information about where to find food, shelter, fuel, emergency medical services, financial aid, and so on. Establish relationships with local authorities so that your organization can become an information distribution point for critical survival information. (Hurricane Katrina)

Workforce Resilience

- **Identify which employees are likely to be affected by a disruptive event (location by location).** Terrorist attacks, by their very nature, are difficult to predict, but certain locations are identifiable as potential targets. (For example, central London and the World Trade Center had been targeted previously.) This makes it possible to identify — at least in broad, locational terms — which employees might be affected by an attack, and then develop BCM plans based on their potential unavailability. Update your calling trees regularly — at least every quarter, or more often if your organization has a high turnover rate. The nexus of mobile devices, emergency notification, big data and cloud computing is making it much easier to track employees under crisis conditions. However, there may be privacy issues that need to be addressed before using this nascent capability. These lessons can also apply when violence comes from within a business (that is, workplace violence). (London bombing)
- **Develop and communicate a personnel succession plan.** The most devastating losses on 9/11 were, of course, human, with key enterprise personnel — from CEOs to IT professionals — killed or injured. A clearly defined and communicated succession plan is crucial to maintaining business resiliency under the most disruptive conditions. Cross-train personnel for all critical production and recovery roles within the enterprise, and have at least tertiary support for recovery and executive management. (9/11)
- **Plan for large-scale absenteeism (30% to 40% of the workforce).** Many personnel will be unable or unwilling to come to the workplace for extended periods, or travel to locations that are under threat of a pandemic. The reasons are likely to be wide-ranging, including fear of contagion and the need to care for sick family members. Cross-train the workforce so that available workers can perform critical roles and responsibilities, and create a shift system that will enable round-the-clock coverage when necessary. Where appropriate, make advance arrangements with external parties to provide necessary skills. Implement expanded work-at-home options, including remote network access, teleconferencing and remote videoconferencing. Use more online systems, including order-taking systems, knowledge bases and FAQs. (pandemics)

- **Prepare for challenges to privacy requirements and HR policy enforcement.** As the pandemic spreads, more tracking of and communication with impacted workforce members will be required. Some of these activities may break your organization's privacy policies and require a loosening of HR policy enforcement. (pandemics)
- **Train the workforce to be prepared at home if a disaster strikes.** If the workforce is impacted by the same disaster that impacts the organization, then their focus will be on their personal lives, not on the organization, thereby making the organization's recovery long and hard. Train the workforce using programs from the American Red Cross so that they are in a better position to manage their recovery needs and possibly return to work sooner so that organization-level recovery requirements can be met. (Hurricane Katrina)
- **Work with public health authorities to ensure that personal hygiene best practices are implemented in the workforce.** Washing hands, using masks, not shaking hands, not meeting in groups and so on are all personal hygiene best practices that must be implemented within the organization to reduce the risk of a contagion spreading within the work environment. Signs, posters and training are all required so that the workforce understands the why and how of these best practices. (pandemics)
- **Plan for shelter in place.** When an event occurs (for example, a dirty bomb, chemical spill or shooter) that results in conditions making it hazardous for people to go outside, or when transportation outlets are not working, thereby preventing people from getting home, you need to house your workforce and/or visitors in your own facilities, with multiple rooms predetermined for this effort. For example, when the July 2005 London bombings occurred, for a few hours, there was neither an explanation for the events nor a report as to how long they might go on. Therefore, organizations needed to think about housing their workforces for an extended period of time. Fortunately, that was not required, but organizations still need to be prepared for it. (London bombing)

Business Operations Resilience

- **Anticipate cultural and language differences.** Many enterprises with operations in Japan or working relationships with Japanese businesses encountered severe cultural and linguistic difficulties following the disaster. For example, enterprises that wanted to transfer their data to backup sites for safekeeping outside Japan found an acute shortage of non-Japanese-speaking personnel who could make the necessary prioritization decisions about the data due to the evacuation of almost all expatriates from the country during the first four days of the disaster. However, cultural differences presented themselves in other, subtler ways. Many Japanese enterprises were, for example, unprepared for the need to allow their personnel to work from home for extended periods, because this has not traditionally been a widespread business practice in Japan. BCM professionals must recognize and take into account cultural differences of this type, and adapt their plans to accommodate them. (Japan earthquake/tsunami/nuclear disaster)
- **Plan for the degradation and complete loss of telecommunications services.** 9/11, like many other large-scale disasters, acutely disrupted telecommunications networks for weeks after the event because of damage to basic infrastructure. In the immediacy of a disaster, government agencies will often use volunteer amateur radio operators to establish repeater systems that re-establish emergency communications. Any effective BCM program must include plans and supporting technologies for communicating with personnel when landline and even mobile communications are disrupted. Use emergency or mass notification tools and procedures to send messages to multiple endpoints, as well as a toll-free telephone number for employees to call to get updates. (9/11)

Have satellite phones on-site and train employees in their use. Some organizations had implemented satellite phones as part of their BCM programs, but recovery personnel were not well-trained in their use — you must be in a direct line-of-sight to the satellite for them to work properly. (Hurricane Katrina)

The Iceland volcano eruption damaged telecommunications capabilities (voice, radio and data) far beyond Iceland. To prepare for an event like this,

BCM professionals must ensure that alternative and redundant communications mechanisms (for example, videoconferencing facilities, which proved completely inadequate during this crisis, as well as social media services and Skype) are available. (Iceland volcano eruption)

- **Develop BCM plans that prepare for the complete loss of travel capabilities for at least one week.** The Iceland volcano eruption showed that unanticipated natural disasters can acutely disrupt land, sea and air travel across very wide areas. This means that enterprises must have the means to track their traveling personnel, and also provide them with alternative travel and accommodation arrangements where possible. Note: 9/11 also resulted in U.S. and Canadian airspace being shut down for three days. (Iceland volcano eruption)
- **Ensure that personnel can work from home or appropriate alternative locations following the event.** This will require employees to be provided with the necessary tools and technologies (for example, mobile phones, notebook computers and Internet services) in their homes or designated locations. (London bombing)
- **Train personnel, including senior executives, in the use of collaboration tools and social media.** One of the most striking impacts of the Iceland volcano eruption was that many senior executives of major enterprises were unable to return to their home locations, in some cases for weeks. Those who were comfortable with social media and collaboration tools, from instant messaging to videoconferencing, functioned extremely well during this difficult period, while those who habitually used only face-to-face contact did not. (Iceland volcano eruption)
- **Determine which parts of the business will experience demand changes, and reallocate excess capacity to other areas.** A pandemic, like many other types of disaster, will likely reduce demand for some of the enterprise's products or services, while potentially increasing demand for others. It is important to have a plan in place to ensure that excess capacity is not wasted and can be used where it is needed. (pandemics)

- **Prepare unaffected facilities/workers for increased work volume.** Large-scale disasters mean that large groups of citizens will be temporarily moving away from the impacted area into nonimpacted areas. Organizations catering to the citizenry, such as banks and retail outlets, will likely experience a jump in business volume as a result of the shifting population. Staff and prepare your workforce in close proximity to the impacted areas for this increased volume of work. Also, many business processes require collaboration across a number of workgroups — some co-located, some not. When documenting the business process for recovery purposes, identify these on-site and off-site dependencies so that work can be conducted from alternative facilities. (Hurricane Katrina)
- **Prepare for severe supply chain disruptions.** Due to the complete destruction of the operations of the Port of New Orleans after Hurricane Katrina, shipments in and out of the area disrupted many supply chains in the U.S. This was the first time in recent history in which organizations had to scramble to realign shipments with other transportation outlets, warehouses and distribution centers. The recovery practice of supply chain risk management grew up and out as a result of these challenges. (Hurricane Katrina)

The effects of the Japanese disaster are still being felt by enterprises worldwide. The production of many Japanese goods — notably high-end semiconductors — was severely impacted. Identifying and locating alternative means of procuring and transporting critical components is crucial to any effective BCM plan. This was also a side effect of the 2011 Thailand flooding, which caused the pricing of some hard drives to double in a matter of weeks (if one could even get the drives at all). (Japan earthquake/tsunami/nuclear disaster)

- **Establish emergency IT change control procedures.** Insurance and medical practices change in the immediacy of large-scale disasters. However, those practices, which often have multiple layers of control, need to be relaxed during those times. Ensure that you implement emergency IT change control procedures so that such restrictions can be easily lifted, thereby reducing delays in handling insurance and medical claims. (Hurricane Katrina)