

Weather Can Make Or Break Your Business

Management needs to create and execute a business continuity (BC) plan that is capable of handling the vagaries of weather.

March, 2000

A lightning bolt in New Mexico literally caused Ericsson to cease being an independent supplier of cellular telephone handsets. According to The Wall Street Journal, the fire caused by the lightning at a Philips Plant "touched off a corporate crisis that shifted the balance of power between two of Europe's biggest electronics companies ... Philips needed weeks to get the plant back up to capacity. Nokia ... met the challenge with a textbook crisis management effort. Ericsson ... moved far more slowly."

MASS MEDIA SOURCES ARE NOT ABLE TO CONVEY THE SPECIFICITY THAT METEOROLOGICAL SCIENCE AND TECHNOLOGY IS NOW ABLE TO DELIVER.



Photos courtesy of Weather Data, Inc.

December, 2002

Kansas City Southern Railway (KCS) receives, as part of its business continuity (BC) plan a tornado warning specifically tailored to its right of way, as a tornado began forming southwest of its tracks through the city of Newton, MS. A KCS train approaching Newton was stopped by dispatchers and held outside of the projected path of the tornado. Maintenance crews were rounded up before the storm even reached Newton. Twenty-seven minutes after the warning was received by KCS, the tornado moves through the city, injures 70 at a Wal-Mart and damages a furniture factory. Kansas City Southern suffers no damage and its tracks are cleared of debris and reopened within two hours.

MICHAEL R. SMITH, WEATHERDATA, INC.

THESE INCIDENTS REPRESENT THE EXTREMES OF BUSINESS continuity (BC) as it pertains to weather:

- Ericsson ceased being an independent player in an important global industry.
- Nokia turned a potential business disaster into an opportunity.
- Kansas City Southern managed to avoid a loss altogether and quickly resumed normal operations.

Successful BC doesn't happen by chance. Successful management of the business crisis created by weather is a result of cohesive, comprehensive planning that combines thinking outside-the-box with the establishment of proactive procedures that include real-time information and execution.

Many of you are intimately familiar with the basic processes of business continuity planning (BCP), but you need to understand the importance of creating and executing a successful plan to handle the unforeseen contingencies of weather.

Mitigating Weather-Related Hazards

In many discussions with BC professionals, weather is "stereotyped." For example, "We're in the South, we don't have to worry about snow." Or "We aren't in Oklahoma, so tornadoes aren't a problem." This type of thinking is counterproductive. If you rely on trucks to deliver parts to or from Florida, two inches of snow along Interstate 75 in central Georgia will cause far more problems for your supply chain than 10 inches of snow along Interstate 75 in Detroit. Similarly, in the past five years, major tornadoes have occurred in Washington, D.C., Orlando and Salt Lake City — far from the traditional tornado belt.

Successful mitigation of weather-related hazards requires an assessment of vulnerabilities across the entire organization:

- How do we make decisions to suspend operations and shelter people when a tornado or major windstorm threatens — without costly false alarms and their attendant costs?
- How do we protect our systems from lightning?
- Can distant weather events disrupt operations even if the weather is clear at our facility? They can if you run a call center with calls related to weather (i.e. insurance claims) or have a geographically dispersed network or supply chain.

Once the vulnerabilities are assessed, procedures for mitigating

Hibernia National Bank Survives Hurricane Lili (October 3, 2002)

Q&A with Scott Hall, vice president of Hibernia National Bank, Technology Risk Management (New Orleans, LA)

How did the hurricane affect business?

The branch locations in the projected path of the storm started closing the day before the anticipated time of arrival. This was due in part because of employee security and safety concerns as well as ordered evacuations. Several roads in many of the lower-lying areas of Louisiana started flooding and subsequently were closed by state police. These locations were closed the day of the storm and remained closed the following day. Some locations were able to open on a limited basis to help with the financial needs of our customers. There was a dramatic decrease in the number of items processed because many customers made proper financial provisions ahead of time and many evacuated out of the area.

Can you review the losses and the effect of those losses on business?

Our losses were generally limited to minor structural damage. Obviously, expenses increased because of the pre-planning activities undertaken prior to the storm's arrival with the acquisition of generators, lodging and food arrangements for recovery team members, etc.

What was Hibernia's recovery time?

Our computer operations center never shut down. We ran 24 hours a day and were prepared even if we lost power. Emergency generators were standing by and diesel fuel was readily available from our suppliers who were on full alert. We made hotel and food accommodations for some of the recovery team members who remained in or near the computer center to provide support for critical services. Elsewhere, some recovery teams were sent out of the area to be pre-positioned at the recovery site. Some of the locations in the direct path of the storm had power failures, but were quickly opened with generator power.

What was your continuity plan in case of a natural disaster?

In order to properly plan for and recover from any disruption or potential disruption, all scenarios must be planned for and executed accordingly. Hibernia National Bank uses three distinct scenarios to be addressed in the disaster recovery (DR) plan: (1) technology disruption, (2) local disruption and (3) community-wide disruption.

Technology Disruption

Addresses the recovery of technology resources used to perform critical business functions for the business unit. Proper planning should address all potential impacts associated with the loss of technology infrastructure. This scenario assumes that the community is not experiencing a disruption and that the business unit's primary work location is intact and accessible.

Local Disruption

Takes into consideration the day-to-day issues that the business unit must plan for in the event that their primary work facility and information technology (IT) systems support are unavailable for an extended period of time. This scenario assumes the community as a whole is not experiencing a disruption.

Community-wide Disruption

Addresses the recovery of the business unit and its IT systems in the event a major disaster (usually natural disaster) occurs that severely impacts the community in which the business unit's primary work location is resident.

In addition to the three scenarios, we maintain a separate

| Weather |

each of the vulnerabilities must be established and personnel must be briefed and trained. Drills are strongly recommended so that the correct procedures become second nature.

The U.S. has the most volatile weather on earth — if your operation is geographically large or if weather disruptions can be mission-critical, then weather should be monitored 24/7 for your enterprise.

Getting the Right Information

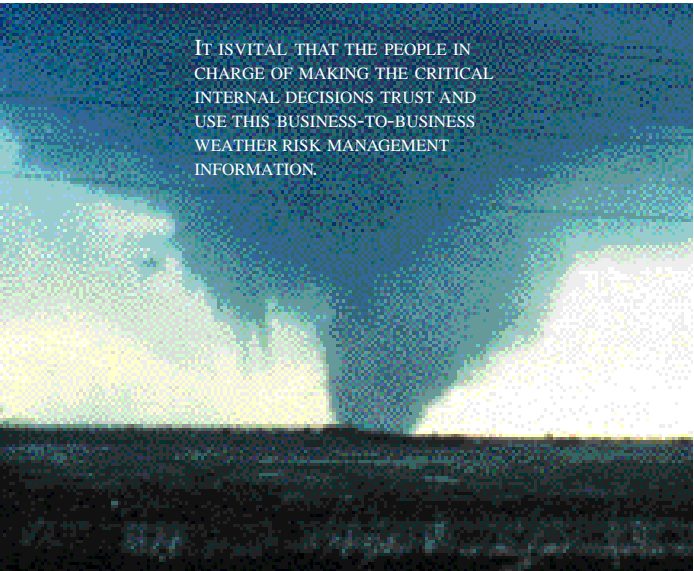
Unfortunately, the first two steps — assessment and procedures — can be for naught if the wrong decisions are made when a major weather event threatens. There are as many opportunities to make the wrong decision as there are sources of weather information — The Weather Channel®, local television, local radio, NOAA Weather Radio, the Internet, etc. While free, these information sources may prove quite costly in the long run because they provide information intended for the public at large rather than the requirements of a particular business.

Asking a security guard or another untrained person (who has other responsibilities besides monitoring the weather) to interpret a myriad of different information sources, to look at a highly technical radar display and come to the right decision in a matter of seconds is asking a great deal — and is a recipe for failure.

You must look for site-specific, business-to-business, mission-critical weather information that is tailored to the requirements of your individual business. This just-in-time (JIT) information is necessary when implementing emergency procedures. For example, knowing that a public storm warning for your county does not apply to your specific location helps.

It is vital that the people in charge of making the critical internal decisions find, trust and use site-specific, business-to-business, mission-critical weather information. After all, if the decision is going to be made to shut down every time a storm is within 30 miles of a plant, it defeats the purpose of both the meteorological information and the BC plan. Over the long run, avoiding false alarms (and their costs) is as important economically — and for the credibility of the warning system — as it is to detect and protect against genuine threats.

Of course, there must be a way to immediately convey a



IT IS VITAL THAT THE PEOPLE IN CHARGE OF MAKING THE CRITICAL INTERNAL DECISIONS TRUST AND USE THIS BUSINESS-TO-BUSINESS WEATHER RISK MANAGEMENT INFORMATION.

sheltering decision to those affected by it. Employees and visitors must be able to do an orderly shutdown of operations and reach shelters quickly. Because there is an inverse correlation between leadtime (the time from when a warning is issued to when the storm arrives) and accuracy, the warning should arrive in sufficient time to successfully implement the plan — but no sooner.

In some cases, a solution to weather-related risks does not involve focusing on storms or other extreme weather, but rather, on small-scale weather. For example, in a number of industries such as wind power production, wine making, agriculture, etc., it is vital to gather and tally weather information on a much more granular scale than is available from the federal meteorological network.

Increasingly, state governments, non-traditional federal agencies (U.S. Forest Service, for example), television stations and others are creating mesonetworks of weather observations. In meteorology, *meso* means small in scale. Meteorologists view an individual thunderstorm as a meso-scale phenomenon as opposed to a hurricane, which would be considered ordinary in scale. So, mesonetworks are established to better measure features like thunderstorms, snow bursts and other small meteorological features than the ordinary federal network can. In some cases, individual companies and cooperatives have established weather networks for their own use.

A meteorological services partner integrates data from all of the appropriate sources to achieve the desired results and can disseminate the data to headquarters and the field operations as required. Typically, this service will cost an organization less money than building its own meteorological infrastructure.

The same network of temperature sensors used in agriculture or to detect temperatures along highways is used by meteorologists downstream to better forecast what is approaching. With the proliferation of these meteorological observation networks, the National Lightning Detection Network™, increasingly high-resolution weather satellites and National Weather Service and private-sector weather radars, high resolution storm warnings and forecasts are becoming ever-more reliable. This is usually not apparent from watching television or using other mass-market sources of weather, which is understandable. The average television market covers tens of thousands of square miles and cannot focus on the specific square mile in which your facility is located. Mass media sources are not able to convey the specificity that meteorological science and technology is now able to deliver.

Most leading companies that have developed and implemented BC plans that proactively mitigate weather have found them to be extremely cost-effective. And, if you are unfortunate enough to have a dangerous storm threaten your facility, you — and your employees and stockholders — will be very glad that you planned for that contingency.

CI

Michael R. Smith is CEO and founder of and certified consulting meteorologist for WeatherData, Inc. (Wichita, KS). He can be reached at (316) 265-9127 or via e-mail at ceo@weatherdata.com.

Hurricane Plan that is published on our Intranet and updated annually. It contains specific information and instruction to properly plan for and execute the recovery effort. If we ever have to declare a disaster, we maintain a hot site agreement with a disaster recovery vendor as well as an internal work area recovery site that is completely out of the area of the risk being mitigated.

Did you test that plan prior to this event? How did you test and did the test(s) go well?

We conduct annual tests with our DR service provider. Because of the threat of hurricanes and other natural disasters, we attempt to perform our test prior to the beginning of the hurricane season. Our tests are very successful and become more robust and aggressive every year. Our end-user community participates in our tests and helps identify opportunities for improving not only its recovery, but the recovery of the technology.

Did the company's continuity plan prove successful after the hurricane?

Absolutely. We use an incident management team strategy, where there is representation from all functional, support and executive areas of the bank. The incident management team DR plan outlines the roles and responsibilities of each area to help facilitate a smooth and rapid recovery of a disaster or major disruption.

Has the hurricane changed the way that you approach business continuity (BC)?

The hurricane helped to reinforce the importance of a sound DR plan that includes training and awareness, maintenance and testing of the DR plan. It confirmed our belief that our current DR plan and practices will recover our bank.

What changes have you made to your BC plan as a result?

As a result of the hurricane, we implemented five guiding principles, which were created immediately following Tropical Storm Isidore and prior to Hurricane Lili:

1. We will err on the side of conservatism.
2. If a city (City Hall, etc.) closes in a market, our locations will close in that same city.
3. Communication lines updated hourly.
4. Our customers will understand.
5. Managerial autonomy is encouraged.

Any advice for other businesses in terms of preparing for and recovering from a natural disaster?

To have a successful recovery effort prior to, during and after a natural disaster, consider your employees and their needs. A company's greatest assets are its employees. Without their dedication and involvement in a recovery role, any recovery effort will fail no matter how well documented and robust a DR plan may be. It doesn't matter how many hot sites agreements you may have or the number of contracts in place for quick-ship hardware. If you don't have employees to carry out the DR procedures, you don't recover.

Any advice for other financial institutions?

Hibernia Bank has specific federal and state regulatory guidelines with which it must be in compliance; however, the greatest success in a BC program lies in the fact that BC must have buy-in from executive management in order to be successful. Executive management support has made our BC process a huge success. There's a lot to be said for a CEO who spends time in an incident command center to show his/her support and concern for the employees, customers and branch locations.

Scott Hall, CBCP is vice president of Hibernia National Bank, Technology Risk Management (New Orleans, LA). He can be reached at (504) 533-3342 or via e-mail at shall@hibernia.com.