Disaster planning

A Crawford & Company (Canada) Inc. Insurance Industry Update Fall 2007

Despite being host to nine of the world's 10 most costly disasters in the past two decades, North America's business community seems to be ill-equipped to deal with such events.

In 2007, AT&T's annual study on business continuity and disaster recovery preparedness for large U.S. private-sector businesses showed that 72 per cent have a business continuity plan in place, down from 73 per cent in 2006.

However, the picture is very different for small firms. A recent survey of such companies, conducted by TNS NFO for Office Depot in the U.S., found that only 29 per cent have a disaster recovery plan.

In a 2006 study commissioned by SunGard Availability Services and conducted by Harris Interactive, 46 per cent of the American senior executives surveyed said their companies' ability to deliver continuous information availability during a disaster is improving, but 39 per cent graded their firms' capabilities at C or lower, citing deficiencies such as inconsistent practices, lack of preparedness and competing priorities.

CANSTOCKPHOTO

Two years earlier, only 24 per cent of respondents gave their organizations such a low grade, leading to the disturbing conclusion that U.S. businesses are getting worse at disaster preparedness, not better.

Forty-two per cent of respondents said their disaster recovery plans would not work if there should be a flu pandemic. In fact, only 26 per cent of companies have a formal flu pandemic preparedness plan in place to protect their workforce and business.

In Canada, the situation is worse. A September 2006 survey conducted for Fusepoint Managed Services by Leger Marketing found that 72 per cent of business executives had no disaster recovery or business continuity plan in place, despite the fact that 75 per cent of them felt personally responsible for their company's preparedness and 36 per cent feared losing their job if they failed to protect their business in a disaster.

Less than half of those companies with a program actually had a full-blown plan. Twelve per cent admitted that their disaster plan was a phone tree and another 12 per cent didn't even know what kind of program they had.

This lack of preparedness is especially shocking when contrasted with the fact that the same Canadian executives thought disasters were on the rise. Forty-four per cent said their businesses had been affected by a power outage, information technology (IT) disaster or terrorist threat, and 21 per cent said they were more likely to have a disaster hit their workplace than five years earlier.

In the U.S., a similarly alarming disconnect existed between the downtime allowed in plans and the downtime senior executives felt that customers would accept.

Thirty-five per cent of the executives said their organizations could withstand eight to 24 hours of unplanned downtime before their business would be affected through lost revenue, customer satisfaction or productivity. However, 51 per cent of them said customers and partners would tolerate only two hours—or less—of unplanned downtime.

Business continuity—the new gold standard

Although often used interchangeably, the terms "disaster recovery" and "business continuity" are quite distinct points on the continuum of dealing with an event that could shut down a business.

Image Source Black/Getty Images

According to Public Safety Canada's *Keeping Canadians Safe* document, a disaster recovery plan deals with recovering IT assets after a disastrous interruption and is reactive. A business continuity plan, on the other hand, enables critical services or products to be continuously delivered to clients and is proactive.

While many smaller firms are more likely to think in terms of recovering after a disruption, larger companies feel great pressure to provide continuous service even in the face of a disaster.

According to Aon's *Global Risk Management Survey 2007*, injury to reputation is number one in the top 10 threats perceived by multinational companies. The second was business interruption, the fourth was distribution or supply chain failure, and the 10th was failure of a disaster recovery plan.

As if these weren't sufficiently menacing concerns, publicly traded multinational firms fall under American and Canadian legislation that requires financial disclosure within specified time frames.

The U.S. Congress passed the Sarbanes-Oxley Act (SOX) in July 2002 as an attempt to halt the spread of corporate fraud, to direct management attention to reliable financial reporting and to restore confidence in the capital markets. In Canada, the response to these same crises was Bill 198, which was passed in the Ontario Legislature in December 2002.

Foreign affiliates or subsidiaries of U.S. parent companies, or publicly traded Canadian firms, are subject to SOX or similar Canadian legislation.

"Both SOX and Bill 198 are focused on internal control over financial reporting in accordance with generally accepted accounting principles," explains Robert Krische, Crawford & Company (Canada) Inc.'s vice president, Finance and Accounting. "Accordingly, manage-

ment is required to evaluate the effectiveness of internal controls, provide evidence to support the evaluation, report on material weaknesses and, in the case of SOX, subject their internal control review and assertions to outside audit."

These laws offer little or no leeway in the event of a disaster or other event that causes the loss of data. Firms must be able to file their reports on time and have the data to back them up, or harsh consequences apply. The prospect of such punishment provides a further incentive for companies governed by the legislation to make sure that their operations suffer no downtime.

In the public and financial services sectors, many Canadian organizations—such as governments, banks, investment advisers and insurers—are specifically mandated by law and/or industry requirements to document, test and audit their business continuity plans. In the event of a disaster, governments must be able to protect and assist the public, and financial institutions must be able to provide customers with access to their assets.

The Personal Information Protection and Electronic Documents Act (PIPEDA), an extension of the Privacy Act, applies to the private, public and not-for-profit sectors in Canada. It requires organizations to obtain consent from individuals, including employees, to collect, use or disclose personal information. Organizations must also disclose why the information is being collected, collect only what is required, and retain it only as long as necessary to fulfil the initial task. Like SOX, Bill 198 and other laws, this legislation has increased the requirement for effective long-term storage of data.

Even small companies should prepare

Every organization is at risk from:

- Natural disasters such as tornadoes, floods, blizzards, earthquakes and fire
- Accidents
- Sabotage
- Power and energy disruptions
- Communications, transportation, safety and service sector failure
- Environmental disasters such as pollution and hazardous materials spills
- Cyber attacks and hacker activity.

While the pressures on large organizations—whether from the marketplace or governing bodies—force them to institute business continuity plans, enterprises of all sizes benefit from making such preparations:

- Being operational during or within a few hours of a disaster could mean business survival. According to the National Archives and Records Administration in Washington, 80 per cent of companies without well-conceived data protection and recovery strate-

Jim Reed/Digital Vision/Getty Images

gies go out of business within two years of a catastrophe.

- Having a plan in place and being able to implement it successfully when disaster strikes keeps financial losses down. Quickly restoring IT and telecommunications infrastructures minimizes interruptions for personnel, suppliers, vendors, partners, investors and customers—and likely enhances the company's reputation and professional standing in the business community. In fact, some organizations require their business partners to prove that they have an effective business continuity plan in place, making firms with such programs more competitive.

- Developing a plan requires an in-depth analysis of all aspects of a business, from IT equipment to human resource requirements to business procedures. Such an examination often reveals gaps, redundancies or special needs. Addressing these problems leads to greater efficiency on a day-to-day basis, again enhancing competitiveness.
- The assessment process can also sometimes identify risk exposures that can be reduced or eliminated, leading to lower insurance premiums.

Protecting data is crucial

Companies of all sizes have become highly dependent on electronic storage and manipulation of data, so protecting that information is a fundamental part of any plan.

For a small office with a handful of people, this aspect of the plan might include:

- Using firewalls and up-to-date anti-virus software and exercising caution with passwords and e-mail attachments
- Backing up data files every evening and taking the CD, DVD or tape to someone's home
- Making sure that key employees have home computers that can access the data and are equipped with all relevant software.

Some firms, like Crawford & Company (Canada) Inc., have decided that they will tolerate almost no downtime for their computer systems.

"It's not just our claims information, it's our customers' as well," says Ken Lloyd, Crawford's assistant vice president, Compliance and Best Practices. "Even back in August of 2003, when the power went out all over Ontario and several U.S. states, we didn't lose even a second of computer time or any data. Our backup battery system kicked in, then our generators went on, and people outside of the affected area would have had no idea that the power was out here."

How to set up a plan

Good business continuity plans go well beyond the protection of computer systems and electronic data and can range from quite simple to very sophisticated.

For a small organization, the plan could include:

- Making sure that computer operations can resume in homes on a temporary basis

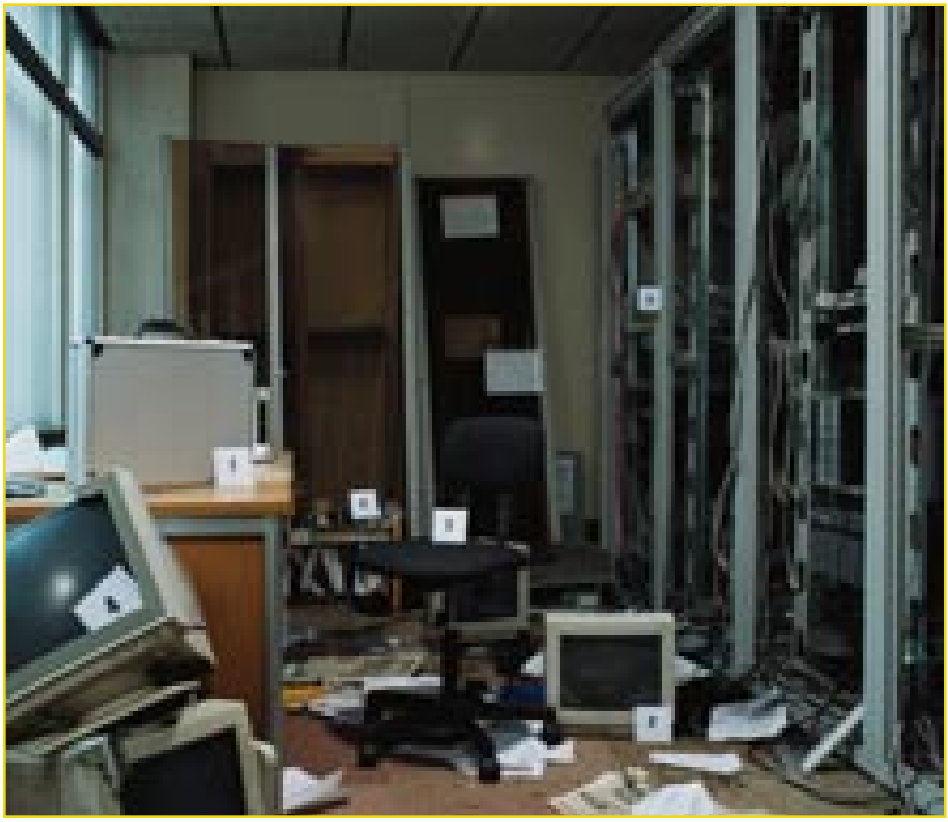

Image Source Pink/Getty Images

- Selecting a phone system that allows remote access to retrieve messages and have calls forwarded
- Providing employees with up-to-date lists of contact information for other staff, customers and suppliers—one for the office and another to be kept at home
- Keeping copies of important documents and banking information at a secondary location
- Maintaining a website to communicate with customers.

For larger firms, such as Crawford, the plan might be highly complex, involving a detailed, fully documented plan available to participants over the internet; teams of people responsible for various tasks; highly sophisticated computer and telephone backup systems; and fully equipped alternative commercial spaces.

According to Public Safety Canada, no matter what the size of the firm, effective plans have certain features in common:

- Governance
- Business impact analysis (BIA)
- Plans, measures and arrangements for business continuity
- Readiness procedures
- Quality assurance techniques (exercises, maintenance and auditing).

Governance

Senior managers or a business continuity planning committee would normally:

- Approve the governance structure.
- Clarify the roles of all participants in the program.

- Oversee the creation of a list of appropriate committees, working groups and teams to develop and execute the plan.
- Provide strategic direction and communicate essential messages.
- Approve the results of the business impact analysis.
- Review the critical services and products that have been identified.
- Approve continuity plans and arrangements
- Monitor quality assurance activities.
- Resolve conflicting interests and priorities.

Business impact analysis

The purpose of the business impact analysis is to:

- Decide what goods or services must be delivered.
- Establish the minimum acceptable delivery levels and the maximum period of time the service can be down before severe damage to the organization results.
- Assess how long the organization could function without the service or product and how long clients would accept its unavailability.
- Determine which processes and functions are required for the creation of revenue; how much revenue is lost if they are not performed, and for how long; whether clients would go to another provider, resulting in further loss of revenue.
- Assess how long it would take before additional expenses would start to add up; when extra personnel would have to be hired; whether fines or penalties from breaches of legal responsibilities, agreements or governmental regulations would be an issue, and if so, what the penalties are.
- Estimate the approximate cost of the loss of consumer and investor confidence, damage to reputation, loss of competitiveness, reduced market share and violation of laws and regulations.
- Use the business impact analysis to help decide what needs insurance coverage and how much; examine the existing policy for uninsured and underinsured areas and non-specified levels of coverage.
- Rank the critical business services or products, based on the potential loss of revenue, time of recovery and severity of impact; then determine minimum service levels and maximum allowable downtimes.

- Identify dependencies—Internal dependencies include employee availability; corporate assets such as equipment, facilities, computer applications, data, tools, vehicles; and support services such as finance, human resources, security and information technology support. External dependencies include suppliers; any external corporate assets such as equipment, facilities, computer applications, data, tools, vehicles; and any external support services such as facility management, utilities, communications, transportation, finance institutions, insurance providers, government services, legal services, and health and safety services.

- For computer systems, determine the minimal acceptable data loss guidelines and build the necessary redundancy and backup infrastructure to fulfil the guidelines' objectives.

Plans, measures and arrangements

This step consists of the preparation of detailed response/recovery plans and arrangements to ensure continuity, and outlining how to ensure that critical services and products are delivered at minimum service levels within tolerable downtimes. Continuity plans should be made for each critical service or product and include:

- Mitigating threats and risks—Moderating risk is an ongoing process that should be performed at all times. An organization that requires electricity for production could install stand-by generators to minimize the risk from a short-term power outage. An organization that relies on internal and external telecommunications to function effectively could use alternative communications networks or install redundant systems to mitigate the risk from communications failures. All reasonable measures that can be taken to safeguard property should be instituted before a disaster occurs.

CANSTOCKPHOTO

- Analysing current recovery capabilities—Assess recovery arrangements already in place and include them in the business continuity plan if relevant.

- Creating continuity plans—Ensure that plans are made for increasing levels of severity of impact from a disruption. One company might use paper forms to keep track of inventory until computers or servers are repaired or electrical service is restored. A large financial firm might find any computer disruptions unacceptable, so an alternative site and data replication technology must be used, as well as redundant backup systems. Keeping cost, flexibility and probable disruption scenarios in mind, choose the most realistic and effective options for each critical service or product.

- Response preparation—Teams of trained and experienced personnel who are knowledgeable about their responsibilities must lead and support recovery and response operations. The number and scope of teams will depend upon the organization's size, function and structure.

- Internal communications—Make sure that staff have secure phone and/or internet access and multiple contact information for emergency authorities, employees, customers, essential vendors, business partners and insurance companies.

- External communications—Publish emergency contact information on the company website so that customers, suppliers and media will know how to get in touch, where backup locations will be, what to expect from the company in the event of a prolonged disruption, and how to place orders or make and receive payments.

- Maintain access to critical company information—The business continuity plan and any banking resources, insurance policies, digital photos of premises, contracts and payroll files that can be kept electronically should be backed up along with other data; paper files or other hard materials like access cards can be duplicated and stored remotely.

- Alternative facilities—If an organization's main location or information technology assets, networks and applications are lost, one of three types of facility should be available:

  - A cold site is not furnished or equipped for operation. Proper equipment and furnishings must be installed before operations can begin, and substantial time and effort are required to make a cold site fully operational. This the least expensive option.

  - A warm site is electronically prepared and almost completely equipped and furnished for operation. It can be fully operational within several hours. This more expensive than a cold site.

  - A hot site is completely equipped and furnished, and often even fully staffed. It can be activated within minutes or seconds. This is the most expensive option.

  For security reasons, some organizations employ "hardened" alternative sites, which may have backup generators, physical security, and protection from electronic surveillance or intrusion.

  Whatever the type of facility, staff will need to have timely access to computers, software, data files, telephones, radios and/or televisions, office equipment, office supplies, first aid and sanitary supplies, water and food.

- Staff accommodation—the plan should include a contingency for housing employees, and sometimes their families, if they must move to another area; personnel co-ordinating this relocation should have access to corporate credit cards to deal with immediate expenses.

Readiness procedures

Training is crucial to the smooth implementation of business continuity plans. All staff should be briefed on the contents of the plan and their individual responsibilities, trained for tasks they will need to perform, and aware of other teams' and team members' functions. Employees at all levels should know how they will be notified of developments.

After training, exercises or tests should be held in order to achieve high levels of competence and readiness. Although exercises consume a lot of time and resources, they are the best way of validating a plan and should include:

- Goal—the aspect of the plan to be tested
- Objectives—challenging, specific, measurable, achievable, realistic and timely
- Scope—departments or organizations, geographical area, and test conditions and presentation
- Artificial aspects and assumptions—which aspects are artificial or assumed, such as background information, procedures and equipment availability
- Exercise narrative—gives participants the necessary background information; sets the environ-

Keith Brofsky/Digital Vision/Getty Images

ment; prepares participants for action; and specifies time, location, method of discovery and sequence of events, whether events are finished or still in progress, initial damage reports and any external conditions
- Communications for participants—enhances realism by giving participants access to emergency contact personnel who share in the exercise; messages can also be passed to participants to alter or create new conditions
- Testing and post-exercise evaluation—impartial monitoring determines whether objectives were achieved and assesses participants' attitude, decisiveness, command, coordination and communication; debriefing should examine what did and did not work, emphasizing successes and opportunities for improvement.

Exercises are often done on a "desktop" basis, without actually shutting down buildings and relocating staff. Various scenarios are put forth, and to the extent possible, staff act as though the situation were real as they go about fulfilling the roles they're assigned in the business continuity plan.

Actual testing of computer systems is more often done at scheduled times, usually annually. The system is actually shut down and then restarted to make sure that the redundant systems and backup technology work as they should and that no data is lost.

"We do this once a year at Crawford, and it's a big undertaking, involving notification of all staff and customers," says Dale Avis, vice president of Information Technology for Crawford & Company (Canada) Inc. "Although it's a seamless rollover to the secondary system, we don't want anyone to try to use it while the IT department conducts tests on it and the backup system."

Quality assurance techniques

Reviewing the business continuity plan should assess its accuracy, relevance and effectiveness, and show what needs improvement. Continuous appraisal, essential to maintaining the plan's effectiveness, can be performed by an internal review or external audit.

Internally, organizations should review their plan:
- On an annual or bi-annual scheduled basis
- When changes to the threat environment occur
- When substantive changes to the organization take place
- After an exercise, to incorporate findings.

If external consultants are used, they verify the procedures used to determine critical services and processes, as well as the methodology, accuracy and comprehensiveness of the plan.

"Business continuity planning is an ongoing process, not an endpoint," Avis says. "Once the plan is developed, it must be constantly maintained to ensure that it remains valid and effective."

Pandemic planning

Planning for an influenza or other disease pandemic shares many features with business continuity planning for damage to premises, but there are a few key differences.

In the event that a quarantine is declared in a particular location but employees are not sick, a flu pandemic plan would likely include arranging for people to work from home rather than an alternative office location, to avoid the risk of spreading infection or to abide by a more general quarantine order.

Because illnesses usually take some time to become widespread, there is likely to be more lead time than with other types of disasters, so implementing plans could take place over a period of days or sometimes weeks. However, a pandemic

CANSTOCKPHOTO

is expected to last for quite some time, with two or three waves lasting six to eight weeks each, coming at intervals of three to nine months.

It is likely that key staff will be unavailable in a pandemic. The Public Health Agency of Canada estimates that minimum absenteeism rates will be 20 to 25 per cent for two weeks at the height of a severe wave, compared to eight per cent in a normal winter. The agency also warns that there could be a higher-than-average number of illnesses and deaths among people under 65.

Andreas Pollock/Digital Vision/Getty Images

Planning for this eventuality should include:

- Making provision for people to work from home—using compatible home computers or laptops that are able to access the company server, along with telephone services that can be redirected to home numbers
- Cross-training other people in key job functions
- Outlining clear chains of command for decision-making
- Researching contractual or legal implications for non-performance of business agreements
- Appointing an influenza manager to co-ordinate prevention efforts, keep track of staff and if possible, determine the health status of employees
- Making sure that key people have training in crisis communications and/or media relations
- Explaining the contents of the pandemic plan to all staff
- Checking that sick leave and absentee policies are up to date
- Anticipating increases or decreases to the volume of business, depending upon the type of product or service offered
- Outlining steps that can be taken to minimize risk of infection, such as using telephones and videoconferencing instead of meetings; installing protective barriers between staff and customers; raising cleaning standards in the office, both for furniture and equipment and for staff; delivering information electronically rather than by mail or courier.

What not to do

According to Mike Thompson, a managing partner with Linus Information Security Solutions in Australia, organizations often make serious mistakes in their business continuity planning:

- Focusing on scenarios—Planning should be based on the loss or unavailability of key resources, regardless of the circumstances. If planners concentrate on specific scenarios, the number of procedures increases proportionally until people realize that scenarios and their combinations are infinite.

- Lack of commitment—Some organizations are forced to implement business continuity plans because of regulatory requirements, media or vendor scare tactics, or internal reporting. They have no real understanding of the investment and process required.

- Using vendors with a vested interest—Outsourcing, hardware, software and backup site vendors attempt to use business continuity as a tool to generate more revenue.

- Allowing IT to drive planning—Business continuity is an issue for the entire organization, not just the IT department.

- Ignoring other benefits—Business continuity management is far more than a risk mitigation strategy—it can an improve business processes, organizational structure and strategic planning.

- Focusing on product, not process—Many consultants emphasize extracting information, not describing the process or educating. The client gets a report, but is left with no buy-in. Clients need only a small team to coach, mentor and guide them through the process so they can believe in the results and learn and repeat the process themselves as the business changes.

- Using poor industry standards—Although a standard must be generic enough that organizations across all industries can use it, planners must provide enough direction for its practical application.

- Not taking software into account—Businesses seem reluctant to adopt a software management tool for business continuity planning. Paper-based systems result in poor update cycles and distribution. Independent automatic offsite backup of business continuity material should be used to ensure access to plans if disaster strikes.

- Losing sight of the point—Too much background information can get in the way when a crisis occurs, so it should be easy to find the implementation information when needed.

Where to get help

The business continuity planning field has grown tremendously since 9/11, with a variety of consultants offering services that range from helping organizations to develop and test plans to supplying them with sophisticated electronic backup technology and fully equipped alternative locations. A quick search of the internet will provide the websites of these firms, but it is important to choose the right one.

"Finding a consultant with 'real world' business continuity and crisis management experience, especially in your industry, can be extremely helpful and is likely to result in a more meaningful work product," says Joseph DesPlaines, director of business continuity and emergency management for Frontier Airlines. "Therefore, I recommend that consultants provide examples of actual experience and references from the clients who engaged them for this work."

It's also important for the consultant to understand regulatory requirements. "Some industries, like commercial aviation, banking, utilities, etc., have significant government regulation for how they must handle a crisis and what needs to be considered in business continuity programs," he explains. "Interviewing a consultant and asking their view of your industry regulations will reveal whether or not that consultant understands your environment."

DesPlaines' other recommendations include:

- Identify the parameters of the project and the timeline, specifying clear performance expectations.

- Include financial performance incentives and penalties in the agreement, as well as an arrangement to pay in installments over a specified period of time, tied to the achievement of performance objectives.

- Use your own lawyer to develop the contract, with special attention to non-compliance consequences and ownership of the work product.

- Make sure that the consultant's values and communication style are a good match with your organization's.

Not all firms can or want to use a consultant to come up with a business continuity plan. For these companies, many resources are available:

- The government of Canada's *A Guide to Business Continuity Planning* document is available at http://getprepared.ca/_fl/bcont_e.pdf.
- The U.S. Department of Homeland Security has a wealth of information available at http://www.ready.gov/business/. PDF downloads include a brochure, sample emergency plan, information on costs, emergency supplies checklist, insurance discussion form and computer inventory form.
- The Canadian Centre for Occupational Health and Safety website has a range of pandemic planning tools available at http://www.ccohs.ca/pandemic/tools.html.
- The Canadian Manufacturers and Exporters Association's *Influenza Pandemic—Continuity Planning Guide for Canadian Business* is available at http://www.cme-mec.ca/pdf/CME_Pandemic_Guide.pdf.