Risk Management & Business Continuity Planning

Advance planning is critical to keep business operations running smoothly in the event of a disaster such as a hurricane or a terrorist attack. This report report details why business continuity and risk management are increasingly hot topics these days, and what companies are doing to mitigate their risk and to respond to a potential catastrophic event. A survey of senior executives on the matter is included. For more information about this report, contact Glenn Curtis, glenn.curtis@thomson.com.

Executive Summary

- Business Continuity Planning (BCP) and Risk Management are topics that every board should discuss. In fact, BCP planning should be an ongoing process where solutions are tailored to the company's needs.
- BCP plans must be multi-faceted. That is, they must ensure that a company's employees, suppliers and customers can talk with each other even if the company's headquarters are shut down. Effective BCP plans must also allow employees to have access to critical data on a timely basis. This in turn involves the integration of various systems and the training of all employees.
- Insurance and hedging continue to be an integral part of risk management.

Survey Results:

- 56% of survey respondents said that their company has experienced a major business interruption of one day or more. The top reasons for the interruption: Computer virus, labor strike, power failure, natural disaster. (See page 9.)
- 86% of survey respondents said that their company has a plan in place to deal with a potential business interruption. (See page 9.)
- Just 8% of respondents said that 9/11 was the motivating force behind the adoption of their company's BCP plans. Meanwhile, 52% said that there was no specific catalyst and that plans were developed over the years. (See page 9.)

Table of Contents:

Overview: Risk Management and Business Continuity Planning:

Since the advent of commerce, merchants have instinctively done things to protect their businesses from risk. However, post 9/11 the subject really came to the forefront of boardroom thinking. Now, more than ever, corporations are forced to think "what if?"

Of course planning for every type of catastrophe isn't possible. After all, there are too many variables. However, this hasn't and shouldn't prevent risk managers and the C-Suite from attempting to mitigate risk. In fact, risk management and mitigation is vital because if a business fails to sustain its operations it faces numerous other challenges and risks.

For example:

- Shareholders and employees may sue the company for failing to plan or to implement changes to ensure continuity.

- Shareholders might abandon the company or initiate litigation proceedings alleging management's negligence.

Some sobering statistics:

- According to the U.S.Department of Labor Statistics 40% of all companies that experience a disaster never re-open and roughly 25% of the remaining companies close within two years.

- If the U.S. were to experience an avian flu pandemic, a February 2006 Sun Microsystems white paper suggests that as much as "30 to 50 percent of the workforce may get sick or be absent from work."

In short, these statistics suggest that the failure of companies to continue to address and plan for the "what ifs" could lead to a catastrophic outcome for employees, consumers, and shareholders. Thus the need for Business Continuity Planning or “BCP.”

With that in mind, what are companies actually doing to provide for continuity in case of emergency?

How Companies Are Proactively Planning and Managing Risk:

Obviously how companies are planning depends upon upon the firm and industry. However, there are some constants. For example:

1) Many firms are focusing on improving remote connectivity solutions (in other words technology that allows employees to connect to their desktop from home).

2) Companies increasingly are erecting backup facilities and establishing contingency plans to facilitate business in the event of a disaster.

3) There is a push to hire officers, directors, corporate counsels and IROs with legal and crisis communication experience.

4) The utilization of insurance, reserves, and hedging is becoming increasingly important as a means of mitigating financial risk.

Below we will examine each in more detail.

1) Remote Technology:

Why is remote technology becoming so popular?

For the simple reason that in the event of an emergency employees may not be able to physically go to work.

Consider this:

According to a recent survey conducted by Thomson Financial, 56% of respondents said their companies have experienced an interruption or have been shut down for one day or longer. (See page 8.) However, 34% of companies do not maintain a backup work facility! (See page 11.)

Of course, there are other, somewhat more practical reasons for the development of remote connectivity solutions as well. For example, telecommuting is becoming more and more popular.

According to a recent IDC (International Data Corporation) study, the number of individuals that telecommute at least three days per week from home during normal business hours stands at about 8.9 million. And going forward as Blackberry devices, iPhones, and other wireless gadgetry becomes more prevalent these numbers are expected to increase.

The good news: 88% of survey respondents indicated that their employees have some sort of remote access capability. (See page 12.)

The Downside To Remote Access Technology:

Of course, in spite of this amazing technology, remote access systems aren't quite the panacea that some may think they are. And that is because providing security for remote transactions is, and is expected to be much more difficult going forward than building out in-house security.

This is primarily because while connectivity solutions such as Virtual Private Networks (VPN's) have improved throughout the years, the individual must still usually connect to their network by utilizing another system or hub (such as a PC or server) which could be having difficulties or experience security breaches of its own. Of course this isn't the only problem. In fact, a myriad of difficulties continue to plague those that work remotely and those that are responsible for advancing and maintaining the technology.

Other issues include:

- Corrupted VPN programs or disks
- Faulty broadband connections or dial up numbers
- Viruses - Incidentally, 52% of survey respondents said that their company has been hacked or a virus has had an adverse impact on their company's network. (See page 12.)
- Server difficulties
- Electrical problems
- Password/Firewall errors or deficiencies

With all of that in mind, some industries have made greater strides in this field than others. For example, the financial services industry, (post 9/11) has substantially built out its remote access capabilities.

Why has such progress been made in the financial services industry?

Necessity. As part of their efforts to ensure business continuity in the event of a terrorist strike, natural disaster, or other event (such as a flu pandemic), securities firms have aggressively been supplying their brokers and traders with software that will enable them to access their desktops and trading turrets from home in the event of a disaster.

2) Erecting Back Up Facilities and Forming Contingency Plans:

Again using the financial services industry as an example, many firms including the New York Stock Exchange have set up alternative facilities to conduct business, and have developed an extensive network of backup servers that store market and firm related data as a hedge against core infrastructure damage.

As a "backup to the backup," many firms have also purchased a large number of diesel generators in order to provide electricity (to run those servers, and desktops) in the event of a problem with the local power grid. In short, companies in virtually any industry can learn something from what the brokerage industry has accomplished over the last half decade. (Incidentally, for those who are curious, our research indicates that Lehman Brothers and Goldman Sachs appear very well prepared to deal with a potential disaster when compared with their peers.)

Still it is important to note that in spite of its preparation, the financial services industry is not immune from risk. And that's because making sure that all of these systems and "fail safes" will interact in times of emergency is a difficult if not imposible task. Not to mention that there is, and will always be, a human element that can botch the entire process.

More specifically, part of the problem that the financial services industry has is that although these interwoven systems are in place, individuals must be trained to operate them and repair them - even in times of emergency.

There are a host of other problems as well (for which these brokerage firms and the exchanges seemingly have no answers). For example:

• If there is a problem with the local power grid email notifications, and "calling trees" probably won't work.

• In the event of a true disaster are people going to even want to come back to work?

• What happens if there is a problem at the backup site, or evacuations prevent workers from getting to back up sites?

• What about compliance issues? How will the NASD/SEC react if traders and brokers are suddenly conducting their operations from home (Note that neither regulatory body has detailed plans in place for the compliance function.)

• Who will troubleshoot problems? At work we have all become accustomed to calling "IT." But at home, and during a disaster that might be impossible.

• Even if an individual has all of the software programs necessary to access their desktop and perform their job duties, they may not be able to contact counter-parties in order to effectuate a trade.

Again, there are no clear answers to these problems. In fact, several of the major brokerage firms with which I've spoken (but which have chosen to remain anonymous) have admitted that there are gaps in the planning process and in remote connectivity in general that may take years to solve, or that “may never be fixed.”

Unfortunately, the problems being experienced in other industries are similar or often worse.

For example, in the pharmaceutical industry where research and documentation is paramount, there is a huge demand for data storage/back up devices. And while the industry has made tremendous strides in making sure that communications will be up and running and that data will be accessible during times of emergency, what will happens if primary and backup servers are adversely affected? Or what happens if some data is corrupted or if remote access fails? Would there be a total shutdown without access to research data?

Also, even if data is available will pharmaceutical manufacturers be able to conduct clinical trials, and control their manufacturing operations on a largely remote basis in the event of a disaster? The fact is that nobody is sure exactly how the rubber will meet the road when put to the test.

Other industries are facing problems as well. For example, while consumer goods manufacturers and retailers may adequately secure their inventory and customer data, will it matter if nobody is able to purchase their wares because they can't get to a store, or if entire distribution networks are stymied as the result of severely inclement weather, high fuel prices, a terrorist attack, a flu pandemic or a natural disaster?

Or, even if computer systems are able to communicate (both internally and externally), and key executives are able to source raw materials in a secure, remote environment, will the company be able to process and assemble those goods into finished products? In short, this too is questionable.

Bottom Line:
By and large U.S. corporations have made enormous strides in making sure that there is continuity and some semblance of a secure environment when monitoring and mitigating risk during a disaster. However, in spite of these efforts it remains unclear how most companies would fare if a major natural disaster, terrorist strike, or power outage were to adversely impact a region, such as the northeastern United States, or for that matter, the entire nation.

3) Making Strategic Hires At The IRO, Board And Corporate Counsel Level:

More and more companies are employing in house counsels and using those individuals to help craft everything from press releases to marketing literature to SEC/NASD filings. Many companies have also sought to add individuals with litigation experience to their boards in hopes that they might provide better legal insight and advice to other board members, particularly during periods of crisis.

As a perfect example, notable attorney, civil rights activist, and former Clinton cabinet member Vernon Jordan has or currently sits on the board of directors at American Express, J.C. Penney, Bankers Trust, RJR Nabisco, Dow Jones & Co., and Xerox. Another good example: Philippe Dauman, Viacom's current CEO, who earned his stripes as an attorney, and worked his way up the ranks, having previously served as the company's corporate counsel.

In short, both have helped their respective employers to navigate through some difficult times. In Jordan's case, he made headlines helping cigarette maker RJR Nabisco work its way through various legal challenges. And Dauman is currently guiding Viacom through a copyright infringement suit it initiated against Google's YouTube. (Viacom claims that YouTube is legally responsible for allowing its users to upload videos from Viacom properties).

It is also important to note that the attorneys that are being hired by large corporations (as directors and corporate counsels) aren't simply trial attorneys or (generalist) private practice attorneys. In fact, legal experience coupled with prior industry experience is becoming more and more of a desirable trait as well. For example, Jordan gained valuable financial and corporate experience as Senior Managing Director with Lazard Freres & Co., an investment-banking firm. And this in turn is thought to have enhanced his abilities on boards such as American Express and Dow Jones.

Dauman had previously served as executive vice president in charge of strategic transactions, human resources and legal affairs, supervising Simon & Schuster, Paramount Pictures, and Showtime. This is thought to have made him extremely well-suited to take the helm at Viacom.

Boards are also increasingly seeking out individuals with "connections." That is, individuals that can help open up doors and cut through costly red tape for corporations whether it be in a particular domestic market or in an entirely different country especially in times of emergency.

In fact, that is one major reason why individuals such as former secretary of state, Henry Kissinger have been highly sought after by U.S.corporations with overseas ambitions. For the record, Kissinger has sat on the board of directors at Holinger International, Gulfstream Aerospace, and Freeport-McMoRan and he helped those entities navigate various overseas transactions.

Note: Almost 30% of survey respondents said that legal and crisis management experience is a factor when hiring senior managers and directors. (See page 10.)

4) Utilizing Insurance/Reserves/Hedging To Mitigate Financial Risk:

Insurance:

A couple of decades ago most companies had basic insurance coverage. They may have supplied health insurance for their employees, and have had basic liability and fire insurance coverage. But few companies felt that they needed additional coverage to protect themselves against (for example) libelous comments made by a director, or against the death of a key employee.

However, in today's society more and more corporations are buying insurance coverage to protect against a range of risks.

For example, Directors and Officers (D&O) coverage has become more commonplace as investors are increasingly suing not only the company but individual board members (personally) as well. In fact, coverage in the millions of dollars per individual is almost expected on large corporate boards.

Key person insurance is also becoming increasingly popular. In fact it is not uncommon too see even small companies these days with multi-million dollar key person coverage on the life of their chief executive officer. And with the advent of Sarbanes Oxley, and the numerous other duties that chief financial officers have had to assume over the last few years, companies are expected to increasingly obtain key person insurance on those individuals as well.

Reserves:

Then there is the issue of accounting reserves. In order to mitigate risk and smooth earnings particularly when a company sees a large potential liability down the road, it has become increasingly popular to book reserves.

Take, for example, the well-publicized Merck/Vioxx case. As a means of helping ensure that enough money will be available to fight thousands of claims that the anti-inflammatory drug had adverse side effects, the well-known pharmaceutical company has booked hundreds of millions of dollars in reserves. This way if the case remains in the courts for a prolonged period of time, the company may not have to borrow against a future quarter to pay those legal expenses.

And if the cases are ultimately settled or thrown out by a judge?

Even better! Then Merck could theoretically reverse any unused reserves and book a huge windfall in that quarter.

In short, because the investment community has developed a habit of punishing companies that record huge one-time unexpected expenses, the tendency to book quarterly "piecemeal" reserves has and is expected to become more popular.

Hedging Transactions:

There was a time when only companies that were involved directly in the production of commodities such as oil, cotton, or lumber (for example) would hedge their financial risk in the futures market. However, that has changed.

In fact, it has become increasingly more common for multinationals to hedge their risk on everything from the price of oil (that goes into the trucks that haul their wares), to the currencies of nations in which they operate. And even if a company is not engaging in outright hedging through a securities market, it may (like Wal-Mart for example has in recent years) establish "natural hedges." They'll purposely set aside cash in certain currencies such as the Yen or the Canadian dollar based upon current need.

Note that 48% of survey respondents indicated that their company engages in hedging transactions. The most popular items that are being hedged include interest rates and oil. (See page 11.)

Going forward, the sentiment is that the number of companies that hedge, and the dollar amount spent on hedging will only increase from here. Note that 30% of survey respondents indicated that commodity pricing is the biggest risk to their firm (See page 11.)

Why is hedging expected to become more prevalent?

Very simply it's because certain goods and commodities are becoming increasingly subject to drastic shifts in supply and demand (and price). And public companies that have to answer to their shareholders and meet quarterly estimates aren't able to weather such volatility without engaging in such transactions.

Hedging against currency fluctuations is becoming increasingly popular as domestic companies make their foray into overseas markets. And whereas companies used to hedge only a couple of key currencies (such as the Yen, or the Euro), they are now often forced to hedge in as many markets as they operate.

How Smaller Companies Are Dealing With Security:

It is not uncommon for large corporations to spend hundreds of thousands or even millions of dollars to build out adequate security safeguards. However, what do small and medium sized companies that can't afford to lay out that kind of money do?

Outsource. In fact, many smaller companies are outsourcing their security needs to Managed Security Service Providers (MSSP). MSSPs are independent entities that provide anti-virus, web filtering, firewall, and intrusion detection and prevention services to their clients for a fee. As a rule, utilizing an MSSP costs a fraction of maintaining an internal security component. Their use also prevents companies from having to hire and retain a staff of security experts.

Incidentally, due to increased regulations such as Sarbanes Oxley, companies are increasingly relying on MSSPs to monitor their email system(s) for the willful or inadvertent transmission of confidential and/or sensitive data. In some cases MSSPs are being used to determine which keywords or types of attachments monitoring devices would search for. And then the emails within those set parameters are being reviewed in greater detail or intercepted completely.

Going forward MSSPs are expected to gain in popularity particularly as the cost of labor and insurance rises. The litigious nature of our society (and the need to document communications) is also expected to be another major catalyst behind their use.

How Companies Are Communicating Risk Management And BCP Plans:

When it comes to risk management and business continuity planning IROs are staying in the loop. They tend to be in on key meetings with the board and with the chief technology officer of their company and typically are capable of effectively communicating the organization's strategy to investors.

However in spite of this according to our recent survey, 60% of respondents said that their company has not communicated its BCP plans to the public. (See page 10.)

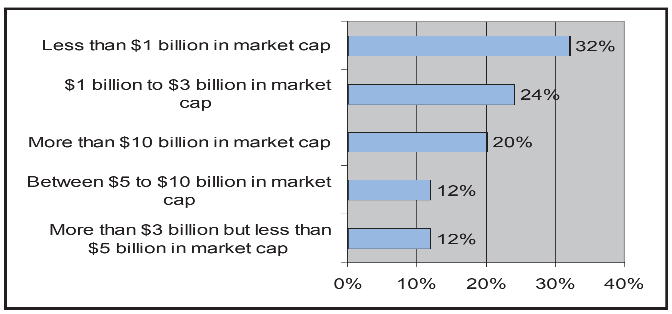
IROs (and the C-Suite) that do communicate strategy however, are increasingly relaying their company's plans at one-on-one meetings, or at breakout sessions at investment conferences, or if an investor should inquire.

It is also wise and in fact becoming more common practice to outline the company's strategy in detail on the web - on the company's corporate website. That way all investors and consumers will be aware of the company's policies, procedures and efforts to mitigate risk in the event of a major business interruption or event.

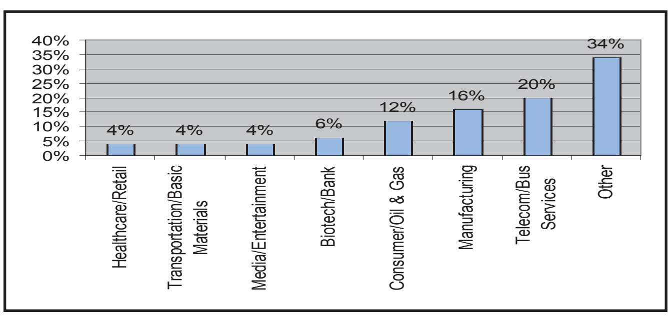
The Survey:

As part of an effort to gauge how companies are addressing the issues of business continuity planning and risk management, Thomson Financial conducted an anonymous online survey of 400 directors, board members and others intimately involved with these topics at U.S. based companies and received 50 responses. Respondents came from a cross section of industries (from biotech to retail), and are employed at public companies of varying sizes (ranging from under $100 million in market cap to multi-billion dollar market caps).

What is the market capitalization of your company?



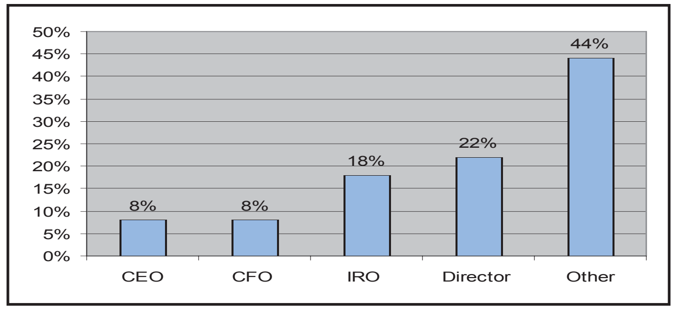
In what industry does your company operate?



Those that answered "other" offered the following responses:

- "Pharma."
- "Leisure."
- "Insurance."
- "Reinsurance."
- "Law."
- "Technology."
- "Media and education."

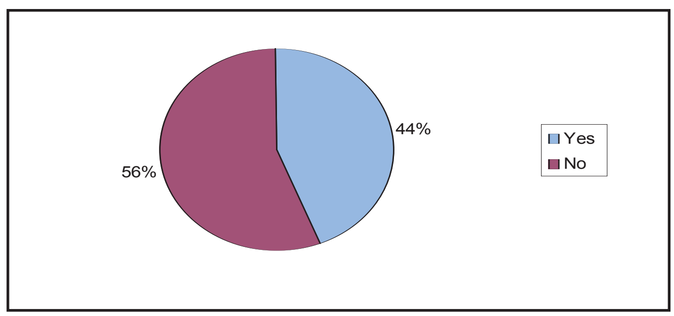
What is your title?



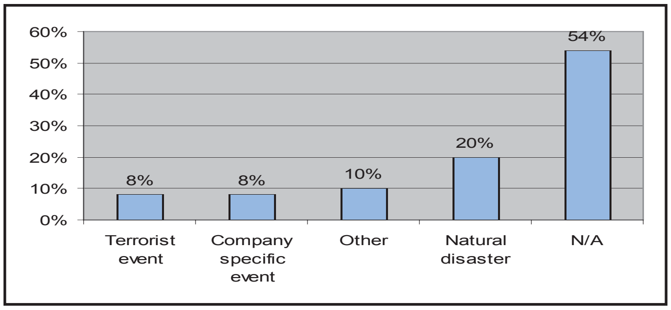
Those that answered "other" offered the following responses:

- "General Counsel."
- "Senior Counsel."
- "SR. VP.
- "IR Analyst."
- "Accounting Manager."
- "Associate General Counsel."

Has your company ever experienced a major interruption of business - meaning an interruption or shutdown of one day or more?



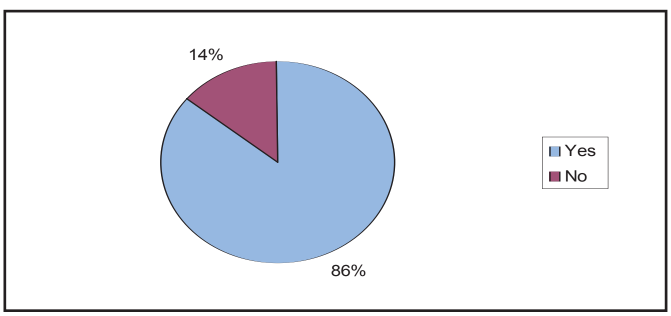
If so, what was the cause?



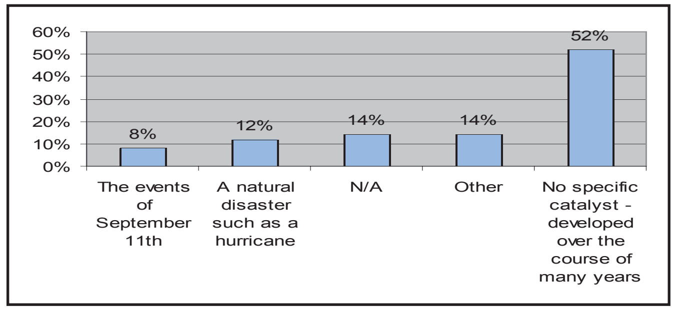
Those that answered "other" offered the following responses:

- "Virus."
- "Labor Strike."
- "Hydro blackout."
- "Power failure."

Does your company have a plan to deal with the risk of business interruption?



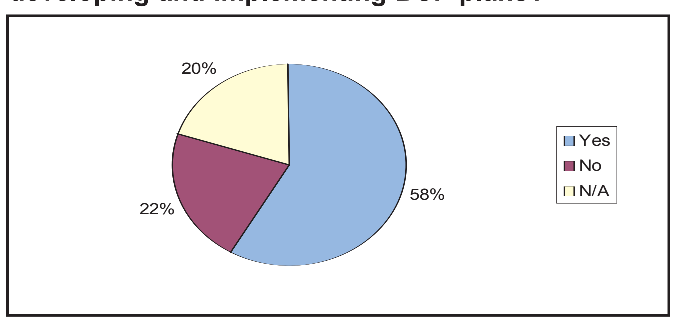
What was the driving force behind your company's adoption of Business Continuity Planning?



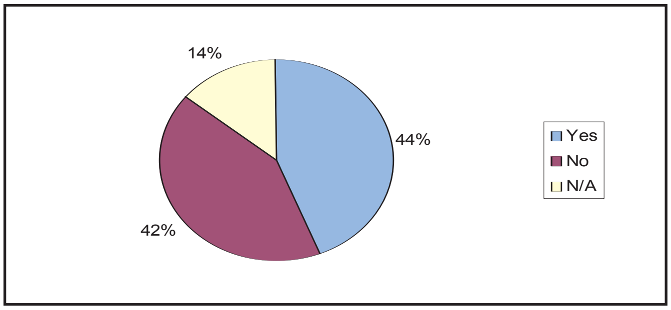
Those that answered "other" offered the following responses:

- "At request of one our board members."
- "Both over a number of years and due to 9/11."
- "Regulatory Requirements."
- "To provide safety for our employees and to protect our assets and business operations in the event of a disaster. Should a disaster occur, it is essential not only to our employees, but to our shareholders, business partners, customers and community that we serve that we are able to respond quickly and recover our critical business processes."
- "SOX 404."
- "Government regulations."
- "Best Business Practice."

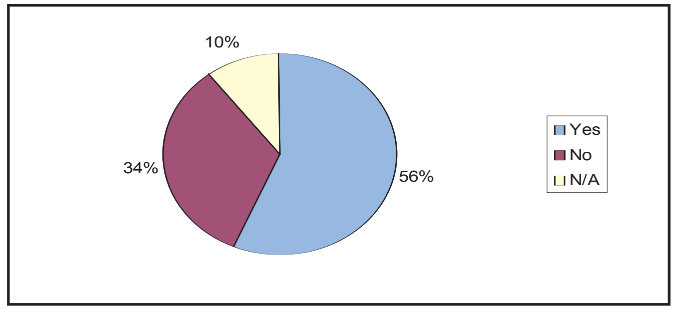
Has your company's Chief Information Officer (CIO) been more active than in previous years with regards to developing and implementing BCP plans?



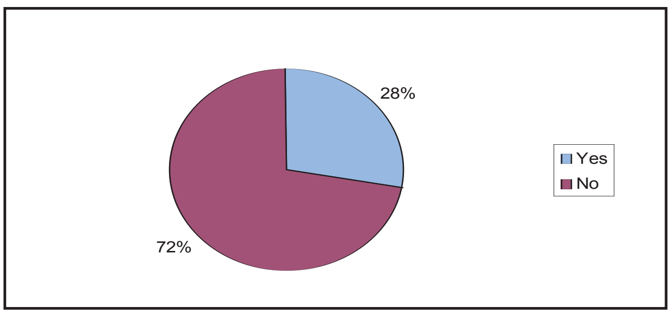
Do you expect your CIO's prominence within the company to grow in the coming years?



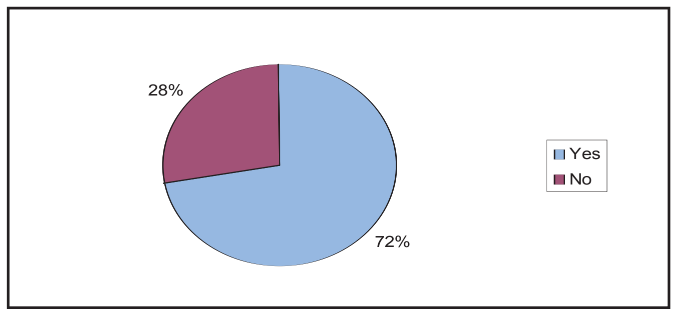
Are your employees fully aware of their responsibilities in the event of a disaster and/or are they aware of the company's broader BCP plans?



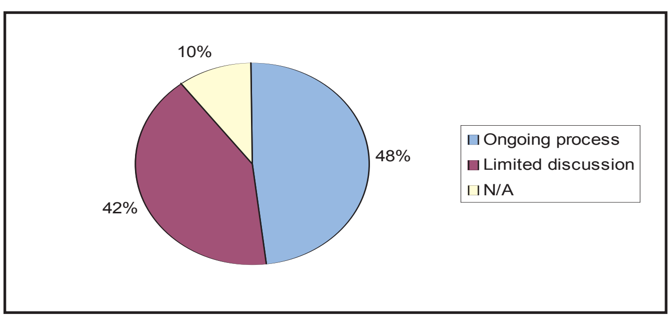
Is legal and crisis communication experience a factor when hiring senior managers or directors?



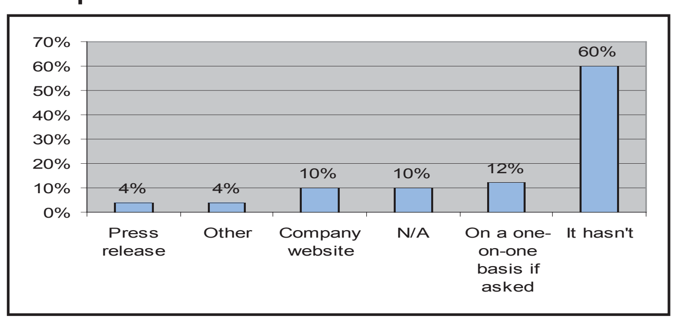
Do you feel that your company is prepared to deal with a significant business interruption?



Is BCP planning an ongoing process for your company or is it a subject that is not discussed often?



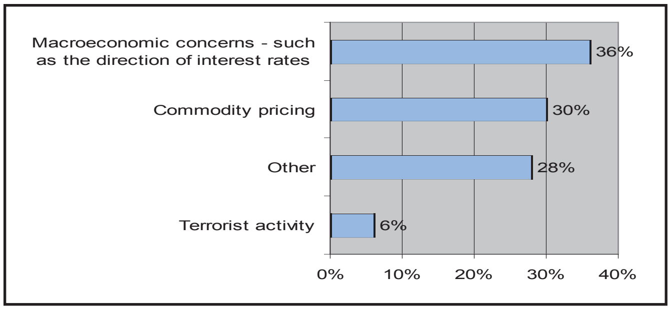
How has your company communicated its BCP plans to the public?



Those that answered "other" offered the following responses:

- "Government regulation."
- "With local government officials."

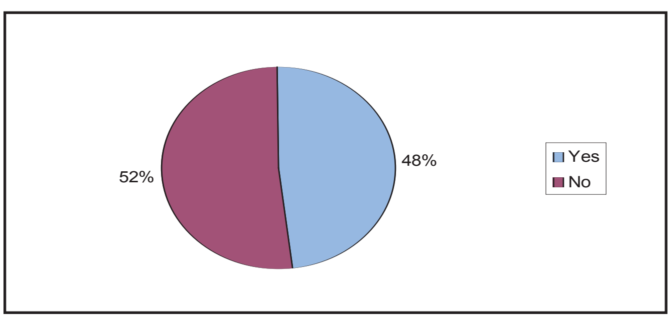
What do you perceive as the biggest risk to your firm?



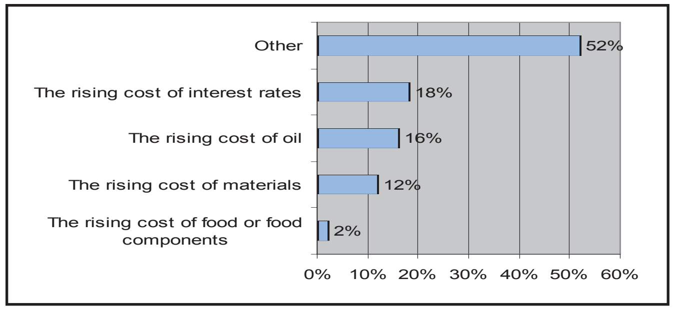
Those that answered "other" offered the following responses:

- "Changes in how the public gets its news."
- "Hackers."
- "Regulation/Legislation."
- "Pricing of services."
- "Natural disasters."
- "Economic Trends."
- "Supply and Demand shortages."
- "Over Capitalization."
- "Competition."
- "Large scale natural disasters in two areas of the country simultaneously."

Does your company engage in hedging transactions?



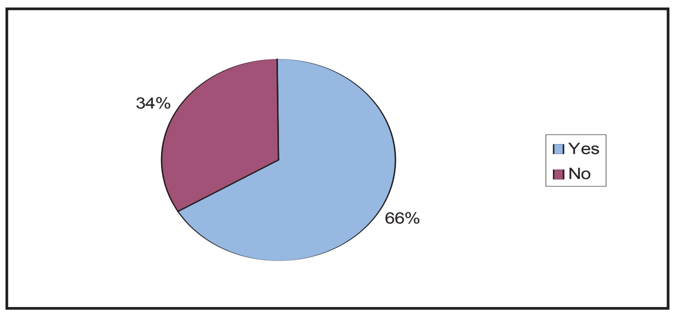
If so, what does it hedge against?



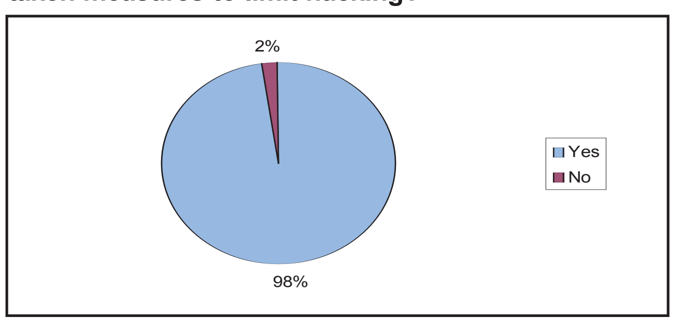
Those that answered "other" offered the following responses:

- "Currency fluctuation."
- "Fuel and interest rates."
- "Cost of recovery."

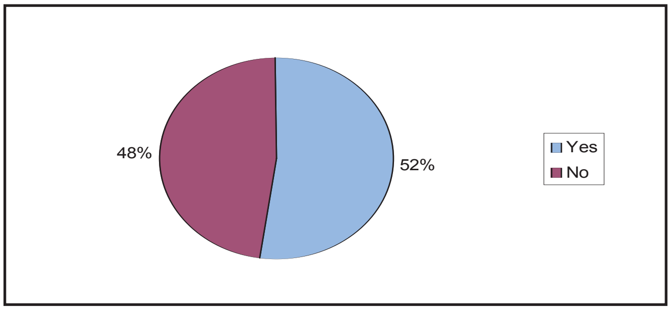
Does your company maintain a backup work facility?



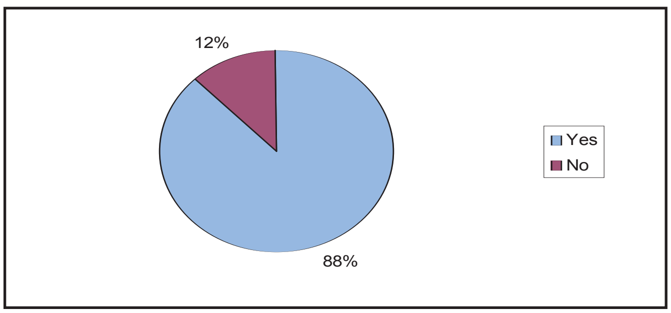
Has your company installed anti-virus software, and/or taken measures to limit hacking?



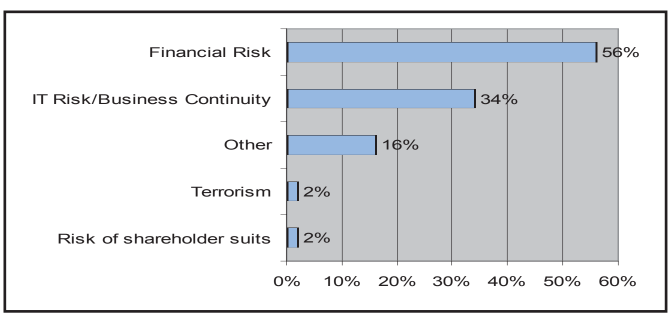
Has your company ever been hacked, or has a virus had an adverse impact on your network?



Do your employees have remote access capabilities in case they are unable to physically get to work?



What is the greatest risk to overall operational efficiency?



Those that answered "other" offered the following responses:

- "Supply chain."
- "Weather - impacts consumer demand and weekly shipments."
- "Technology Issues."
- "Keeping focus."
- "Hedge Fund activism."
- "Internet hackers."
- "Natural Disaster."

Are there any other comments that you would like to add with regards to this subject and/or this survey?

- "Given any terrorist event, there is nothing predictable or preventable to plan for, Except to have secondary reliable communication between the core employees. With that communication, you can then use 20/20 hindsight to make the best of that known situation. And that alternative presupposes the core leadership is pre-provisioned with pc and satellite capability at each home."

- "BCP is at a level that is losing interest, we need to gain management support, post 9/11 levels."

- "BCP is an area that is gaining attention of more senior management attention and will become a more integral part of future decisions, particularly with respect to back-up capabilities."

THOMSON TEARSHEET: Recommendations and Actions

Place BCP and Risk Management on the Front Burner:

• Boards must overcome inertia and make business continuity planning and risk management part of their ongoing discussions. In addition, actions should be taken to mitigate risk and to tailor a plan specific to the needs of the company. That plan should be reviewed periodically.

Set Up Technology To Promote Business Continuity:

• Remote connectivity solutions are at the forefront of the planning process. Key employees must have access to their desktops and be able to conduct business as if they were physically in the office.

• Back up off-site servers, generators, call trees and work facilities should be an integral part of the process. Keep in mind that communication among employees, suppliers and customers is a must if the business is to keep running during an emergency.

Consider Risk Management Experience When Taking On Directors:

• Public companies should focus on hiring directors with risk management and crisis communication experience. The objective is to hire professionals that will help steer the organization through difficult times, and communicate the company's message in a meaningful and productive way.

Utilize Insurance/Hedging To Mitigate Financial Risk:

• D&O insurance and hedging techniques should be employed as a course of business to mitigate financial risk. Incidentally, the IRO should be familiar with the techniques the company is using so that they will be able to accurately communicate them with the Street.

Plan Now To Optimize Communication With The Street in the Event of Crisis:

• The investment community should be made aware of the company's business continuity plans. While some companies have chosen to do this via a press release, other companies have chosen to do this on a one-on-one basis, and/or through the company's IR website. Regardless of the method, again IROs and CFOs that are investor facing should be cognizant of the means used and to the degree to which the company believes it is protected against certain types of disasters.

Sources:

“Business Continuity: Be Prepared for a Bad Moment,” David Rosenbaum, CIO, July 31, 2007

“Business Continuity Planning – At the Top of the “To Do” List,” Cynthia A. Bonnette, Bankers Online, January

"Business Continuity During an Influenza Pandemic," White Paper, Sun Microsystems, February 2006

“Business Continuity: How the Events of September 11 are affecting business plans for disaster recovery and business resumption,” Gregg Greer, Thesis, Baylor University, May 13, 2002

“Business Continuity Planning Is a Challenge for CIOs,” Vandana Mangal, Computerworld, April 7, 2004

“Communication in a Crisis,” Meryl Natchez, Continuity Insights, July/August 2007

“Email Scheme Targets Executives,” Riva Richmond, Wall Street Journal October 10, 2007, Page B5

“How to Involve the Business to Create a Solid Continuity Plan,” Carrie Matthews, CIO, October 1, 2005

“The Legal Issues of Disaster Recovery Planning,” Tari Schreider, Disaster Recovery Journal, April 1998

“Microsoft, Yahoo Tweak Privacy Policies,” Michael Liedtke, Associated Press, July 23, 2007

“A New Battleground for Computer Security,” Riva Richmond, Wall Street Journal, March 6, 2007, Page D1

“Rethinking Risk Management,” Kerry Massaro and Anthony Guerra, Wall Street & Technology, October 24, 2005

“Risks Worth Taking,” Mark Layton, Treasury & Risk, May 2007

“Sidebar: Security Management for the Littler Guy,” Drew Robb, Computer World, February 7, 2005

"Telecommuting Security Concerns Grow," Ellen Messmer, Info World, April 18, 2006

“Weathering The Odds,” Duncan Wood, Treasury and Risk June 2007

Innovative Solutions to Build and Maintain Shareholder Value

Thomson Financial Corporate Services
With 15 years of experience serving the Investor Relations needs of more than 4,500 corporations worldwide, partner with Thomson and leverage our significant investments in content, people, and technology to navigate today's dynamic markets. Combine Thomson's sophisticated desktop solutions, unrivaled advisory services, and industry-leading communications technologies to:

- Understand and explain what is driving valuation relative to your peers and to the overall market.
- Identify and target potential investors.
- Predict the reaction of your shareholders to corporate and market changes.
- Implement reliable, effective and compliant communications programs to reach and engage your internal and external audiences.
- Measure the effectiveness of your overall IR efforts

To learn more about this report, or how Thomson Financial can help you achieve your objectives, please contact Glenn Curtis at glenn.curtis@thomson.com.

Glenn Curtis
Director, Strategic Research
195 Broadway
New York, NY 10007
Phone (646) 822-2554
Fax (646) 822-2622

Contact us at:
www.thomson.com/financial
tfcorporate@thomson.com

North America: 866 915-9891
Europe: +44 207 369 7199
Asia: +852 2533 5564

Important Notice

This disclaimer is in addition to and not in replacement of any disclaimer of warranties and liabilities set forth in a written agreement between Thomson and you or the party authorizing your access to the Service ("Contract Disclaimer"). In the event of a conflict or inconsistency between this disclaimer and the Contract Disclaimer the terms of the Contract Disclaimer shall control.

By accessing these materials, you hereby agree to the following:

These research reports and the information contained therein are for your internal use only and redistribution of this information is expressly prohibited. These reports, including the information and analysis, and any opinion or recommendation included in the reports are not intended for investment purposes and do not constitute investment advice or an offer, or an invitation to make an offer, to buy or sell any securities or any derivatives related to such securities. Nor do these reports constitute or contain legal advice. If you require legal advice, you should consult with your own counsel.

Thomson does not warrant the accuracy of the reports for any particular purpose and expressly disclaims any warranties of merchantability or fitness for a particular purpose; nor does Thomson guarantee the accuracy, validity, timeliness or completeness of any information or data included in these reports for any particular purpose. Thomson is under no obligation to provide you with any current or corrected information. Neither Thomson, nor any of its affiliates, directors, officers or employees, will be liable or have any responsibility of any kind for any loss or damage (whether direct, indirect, consequential, or any other damages of any kind even if Thomson was advised of the possibility thereof) that you incur in connection with, relating to or arising out of these materials or the analysis, views, recommendations, opinions or information contained therein, or from any other cause relating to your access to, inability to access, or use of these materials, whether or not the circumstances giving rise to such cause may have been within the control of Thomson.

The information provided in these materials is not intended for distribution to, or use by, any person or entity in any jurisdiction or country where such distribution or use would be contrary to law or regulation or which would subject Thomson or its affiliates to any registration requirement within such jurisdiction or country.