BUSINESS CONTINUITY – NATIONAL
SUMMARY OF RESULTS

Overview

Despite the vital importance of business continuity in the age of instantaneous information exchange, business continuity planning is not a high priority at four in ten companies surveyed. Many companies are placing their confidence in the systems they already have in place or, in effect, crossing their fingers that their company won't be the victim of a disaster that cripples their ability to do business.

Even among companies with business continuity plans, however, one in four haven't updated their plan in the past 12 months and four in ten haven't tested it in the past year or ever. Clearly, many American businesses are gambling their futures by not taking appropriate steps to safeguard their ability to continue operations in the event of a terrorist attack or other disaster.

Priority of Business Continuity Planning

♦ Only one-third of company officers who have responsibility for business continuity planning (34%) say business continuity has always been a priority for their company, while 26% say it has only become a priority in recent years due to security and terrorist threats. Thirty-five percent say business continuity planning is important but not a high priority, while 4% admit it isn't important at their company.

  - Companies with more than 500 employees place only slightly more importance on business continuity than smaller companies (65% vs. 56%).
  - Not surprisingly, far more companies that have a plan say business continuity has always been a priority (44%) than companies without a plan (13%).
  - Business continuity planning is a high priority at companies that have suffered a business disaster as well as those which haven't (60% for both).
  - Officers at companies in Houston (45%), Florida (45%), and New Jersey (43%) are the most likely to say business continuity planning has always been a priority at their companies, while those in Washington state (24%) and the Pacific Rim (25%) are the least likely.

Having a Business Continuity Plan

♦ Two in three company officers who have responsibility for business continuity planning (67%) say their organization has a business continuity plan.

  - Companies with 500 or more employees are more likely than smaller companies to have a plan (75% vs. 63%).
  - Only 43% of companies where business continuity is not a priority have a plan, compared with 83% of companies where it is a priority.
  - Seven in ten companies that have suffered a disaster (70%) have a plan, while 66% of companies that haven't suffered a disaster have one as well.
  - Florida businesses are the most likely to have a plan (74%), while those in the Southwest are the least likely (57%).

♦ Most organizations with a business continuity plan have updated it within the last six months (41%) or the last six to twelve months (33%). About one-fourth (23%) say it was last updated more than a year ago and one percent admit they have never updated their plan.

- Almost half of companies with more than 500 employees (47%) have updated their plan in the last six months, compared with 37% of smaller companies.
- Eight out of ten companies where business continuity is a priority (79%) have updated their plans in the past year, compared with only 58% of companies where continuity planning is not a priority.
- About half of companies that suffered a business disaster (46%) have updated their plans within the past six months, but 41% of companies that have been spared a disaster have done the same.
- Companies in New Jersey (54%), Georgia (51%) and Michigan (51%) are the most likely to have updated their plans in the past six months, while those in Washington State (23%) are the least likely to have updated their plans in that time period.

♦ More than half of companies (56%) have fully tested their plan within the past year, with 26% saying it was tested within the past six months and 30% in the past six to twelve months. One in four (23%) say their plan was last tested more than a year ago and another 17% concede their plan has never been tested.

- Businesses with 500 or fewer employees are about as likely to have fully tested their plan in the past year (53%) as companies with more than 500 employees (59%).
- Companies which have not suffered disasters in the past are just as likely to have tested their plans in the past year as companies which have suffered a disaster (56% for both).
- One-third of companies where business continuity has always been a priority (32%) have tested their plans in the past six months, compared to 15% of those where business continuity is not a priority.
- Nearly two in three companies where business continuity is a priority (62%) have tested their plans in the past year, compared with only 38% of companies where continuity planning is not a priority.
- Florida companies are the most likely to have tested their plans in the past year (70%), while those in Michigan and New Jersey (each 49%) are the least likely to have tested their plans in that time.
- Companies in the Southwest (37%) and in Houston (36%) are the most likely to have tested their plans in the past six months, which is the proper time frame to test plans.

Monitoring Public Alert Systems

♦ Three in four company officers who have responsibility for business continuity planning (73%) say they monitor public alerting systems for warnings about terrorist threats or other potential disasters, with network or cable TV (52%), the Emergency Alert System (36%) and NOAA weather radio (32%) the most common systems monitored.

- Larger companies are slightly more likely to monitor a system (78%) than the smaller ones (70%).
- Companies that have a business continuity plan are more likely to monitor public warning systems (78%) than those who don't have a plan (64%).
- Companies that have suffered a disaster are just as likely to monitor alert systems (79%) as companies that have not (73%).
- Companies in Florida (88%), Washington D.C. (84%) and Wisconsin (83%) are the most likely to monitor public alert systems, while those in Chicago (52%) are least likely.

♦ Only 11% of companies implement specific protective actions when the federal terrorist alert level rises.

- Companies that have a business continuity plan are almost three times as likely as those who do not have a plan (14% vs. 5%) to implement specific protective actions when the terrorist alert level rises.
- Houston companies are the most likely to take action (23%), while those in Kansas/Missouri (5%) and Ohio (4%) are least likely.

Implementing Business Continuity Measures

- ♦ The vast majority of companies have implemented Internet security measures such as firewalls, intrusion detection, hacker protection and/or password authentication (65%), or plan to in the next six months (18%). In addition, most have established (57%) or plan to establish in the next six months (18%) redundant servers and/or backup sites. About four in ten (30%) have used a service provider for outsourcing or plan to use one in the next six months (11%).

  - Many companies where business continuity has not been a priority plan to take various actions in the next six months, including 30% who plan to implement Internet security measures and 24% who plan to establish redundant servers.
  - Among firms where business continuity is a priority, about eight in ten (81%) have already implemented Internet security measures and three in four (72%) have established redundant servers. Only 38% have used an outsourcing service.
  - Companies with more than 500 employees are more likely than smaller companies to have already implemented Internet security measures (73% vs. 60%) and have established redundant and/or backup servers (68% vs. 50%).
  - Florida (74%), Houston (69%) and Kansas/Missouri companies (69%) are the most likely to have already implemented Internet security measures, while those in the Pacific Rim (27%) are the most likely to be planning to do this.
  - Companies in Washington D.C. (66%) and Florida (65%) are the most likely to have already established redundant servers and/or backup sites, while those in the Southwest (49%) and the Pacific Rim (45%) the least likely to have done so.
  - Washington D.C., Florida, and Kansas/Missouri (all 39%) are the most likely to have already used an outsourcing provider, while those in Wisconsin are the most likely to be planning to in the next six months (19%).

Suffering from a Disaster

- ♦ Less than one-fifth of all the companies (16%) suffered a disaster that resulted in their organization having to cease operations for a period of time.

  - Florida companies are the most likely to have suffered a disaster (26%), principally with all of the hurricanes they were hit with in 2004. Twenty-four percent of Michigan companies suffered a disaster, due to the 2003 blackout. Companies in the Pacific Rim are the most likely to have been spared a disaster (10%).

- ♦ The most common disasters suffered vary by market. For a majority of Michigan companies (67%), it was electrical blackouts, while Florida disasters are mostly weather-related (77%).

- ♦ Two in three companies which suffered a disaster lost business because of it (65%), generally less than $100,000 a day (45%), although 16% say it cost their organization $100,000 to less than $500,000 a day. Two companies say it cost them $500,000 to less than a million dollars a day and three percent say it cost their business one million dollars a day or more. Only 8% say the stoppage cost the company nothing, while 26% admit they don’t know how much it cost the company per day.

- ♦ Three-fourths of companies that suffered a disaster (75%) have taken actions as a result of the disaster to reduce business interruptions in the future.

Cyber Security

- ♦ Three-fourths of all company officers who have responsibility for business continuity planning (75%) say cyber security is part of their overall business continuity plan.

  - Most companies where business continuity planning has always been a priority or has just recently become a priority include cyber security in their overall plan (82%), while 65% of the companies where business continuity is not a priority include cyber security in their overall business continuity plan.
  - At least seven out of ten companies across all markets include cyber security as part of their overall business continuity plan.

- ♦ Almost all company officers who say cyber security is part of their business continuity plan say they have taken actions when it comes to cyber security (97%). The most common action is the education of their employees (89%), followed by defining corporate security policies (83%) and contracting an outside service provider to manage security (27%).

  - Most companies with more than 500 employees say they have defined corporate security policies (90%) when it comes to cyber security, while 79% of companies with 500 employees or less have done the same.
  - Florida companies are the most likely to have educated their employees when it comes to cyber security (96%), while Washington D.C. companies are the most likely to have defined corporate security policies (91%). Companies in Wisconsin are the most likely to have contacted an outside service provider to manage security (38%).

- ♦ Upon hearing a list of ten possible cyber security threats, company officers across the board strongly agree that the most significant threat to companies like theirs is viruses and worms (46%), finishing far ahead of SPAM (13%) or hackers (11%).

- ♦ Using the same list of possible cyber security threats, when choosing the top three threats, the majority agree that viruses and worms is the one of the top three most significant threats (82%). Other threats to cyber security include SPAM (44%), hackers (44%), internal accidents (28%), internal sabotage (26%), denial of service attacks (17%), remote workers (14%), customer, partner, and/or vendor access to internal systems (14%), competitor espionage (6%), and terrorist attacks (5%).

  - Companies where there are more than 500 employees believe internal sabotage is one of the top 3 most significant threats (31%), while only 24% of companies with 500 or fewer employees believe the same.
  - Over half of the companies in the Pacific Rim (54%), in Ohio and in the Southwest (both 51%) believe that SPAM is one of the top three most significant cyber security threats.
  - Over half of the companies in the Southwest (53%), Chicago and Georgia (52%) believe that hackers are a significant threat to cyber security.
  - About one-third of the companies in Florida (36%), the Southwest (34%), and Michigan (33%) view internal sabotage as a top threat to cyber security.
  - Due to it's proximity to New York City, companies in New Jersey rate terrorist attacks the highest out of all the markets (10%).

- ♦ On a scale of 1 to 5, where 5 means cyber security is a top concern and 1 means cyber security is not a concern at all, about one-fifth (22%) of company officers believe cyber security is a top concern, while another 33% rated cyber security as a four. About three out of ten companies (29%) rated cyber security as a three. Only four percent say cyber security is not a concern at all. The mean rating for concern about cyber security is 3.6 among all markets surveyed.

- Two-thirds of the companies where business continuity is always a priority rate cyber security as a four or a five (66%), compared to 42% of the companies where business continuity is not a priority.
- The businesses which have a plan in the event of a disaster rate cyber security as a four or a five (62%), while only 41% of those companies without a plan rate cyber security as a four or five.
- The highest mean rating for cyber security is a 3.8, given by those companies in Florida and Washington D.C. The lowest mean rating for cyber security was a 3.3, given by those companies in Washington State.
- In addition to the Florida and Washington D.C. markets, over one-fourth of companies in Wisconsin and the Southwest rate cyber security as a five.

*Methodology

These results are based upon 1286 telephone interviews conducted by Opinion Research Corporation among business people who have responsibility at their organization for business continuity planning, particularly when it comes to telecommunications, websites and data networking. Interviews were conducted in Houston, New Jersey, Florida, Ohio, Washington D.C., Georgia, Michigan, Kansas/Missouri, Chicago, Wisconsin, the Pacific Rim, the Southwest, and in Washington State. The Pacific Rim market included San Diego, CA, Hawaii, Alaska, and Oregon. The Southwest market included Arizona, New Mexico, Nevada, and Utah. Interviews were conducted January 24-August 19, 2005.

The bulk of the respondents provide oversight and project management of their business continuity plan (43%), while 27% are part of the project team designing and/or evaluating the plan and 27% recommend the purchase of IT or security products and/or services for the plan. The most common job titles of those interviewed were IS/IT manager/director (56%), those in IT/Tech (9%), Managers (7%) and CIOs (7%).

Respondents were interviewed in the following industries: services (32%), manufacturing (21%), wholesale trade (16%), retail trade (12%), finance, insurance and real estate (8%), transportation, communications, and utilities (5%), and construction (5%).

Sample for this study was selected using a dual approach. First, large companies (with revenues of $10 million or more), and local business with 50 or more employees selected from the following industry classifications: printing and publishing, banks, investment firms, brokers, insurance carriers and agents, business services, health services, legal services and engineering and management services.