

The ***Disaster Recovery Journal*** reported in 2002 that 43% of firms that suffer a massive data loss will never reopen, and 51% will reopen just to shut down permanently within two years.

**Gartner** analysts say that by the end of 2005, 20% of enterprises will experience a serious (beyond virus) Internet security incident.

Conservative estimate is that 20% of the country's \$7trillion economy is vulnerable to weather shifts and events

***Ants Leetma; Director of the Climate Prediction Center in Camp Springs Maryland.***

- ◆ Data backup falls short; only 6% of enterprises experiencing catastrophic data loss survive
- ◆ 43% never re-open after the disaster
- ◆ Another 51% close down < 2 years due to business re/mis-direction
- ◆ 1993 WTC bombing – 143 enterprises went out of business

***University of Texas Disaster Study***

52% of U.S. IT Exec's feel their company data is very vulnerable while just 14% of business Exec's feel the same

***CPM Magazine, September/October 2003. Survey conducted by RoperASW – sponsored by EMC.***

"Of the thousands of enterprises who have taken the Disaster Readiness Scorecard of best practices, 75% are in the Danger Zone, 21% Need improvement, and only 4% meet Best Practices." ***"Prove It" disaster readiness consortium***

"Only 37% of enterprises test their data backup processes. Of those 37% of enterprises, only 23% of them retrieve and restore critical enterprise data within the recovery window."

***"LiveVault white paper, Spring – 2004.***

- ◆ 1/3 of Fortune 1000 firms still no more prepared than 9-11-01
- ◆ Only 10% of employees know what to do in a catastrophe
- ◆ 1/3 of enterprises surveyed operate without a formal DR plan
- ◆ 2/3 of enterprises surveyed still have serious vulnerabilities

***KC Star, Sept. 8, 2003***

More than one-third of the world's leading company's report that they are not sufficiently prepared to protect top revenue sources, according to the 2003 'Protecting Value' study. Unsurprisingly, 100% of the companies surveyed reported that a major disruption to a top revenue source would have a negative impact on earnings, with 28% stating such an event would threaten business continuity.

The study, conducted by commercial and industrial property insurer ***FM Global, the Financial Executives Research Foundation and the National Association of Corporate Treasurers (NACT)***, polled nearly 400 CFOs, treasurers and risk managers at both US and international companies from a broad variety of industries.

Among the other findings of the second annual study:

- ◆ 80% of companies report no significant shift in their risk management outlook post-September 11th - either strategically or operationally
- ◆ Improper management and employee practices represent the leading hazard affecting top revenue sources  
Property-related hazards, such as fire and natural disaster, collectively continue to pose the greatest threat to revenue sources
- ◆ 88% of financial executives and 83% of risk managers say their companies' level of preparation to recover from a major disruption to a top revenue source is less than 'excellent'
- ◆ Current business continuity plans may not be sufficiently aligned with top revenue sources at many leading corporations

According to a survey of IT managers conducted by **Dynamic Markets Ltd., and sponsored by VERITAS**, in 76% of companies, the decision-making process for disaster recovery is limited to IT staff, despite the potential impact to the entire business. In responding companies from the US, only 5% of CEOs and 4% of non-IT managers have decision-making responsibilities when it comes to defining disaster recovery strategy.

According to the research, man-made disasters such as 9/11 are a greater concern than natural disasters. While only 6% of respondents felt exposed to hurricanes and tornadoes, more than four times this amount worried about terrorism (25%). Technological failure ranks highest in the list of perceived threats, with the top five most common threats that large companies feel exposed to ranking as follows:

- ◆ Hardware failure (61%)
- ◆ Software failure and viruses (both 59%)
- ◆ Fire (56%) Hackers (36%)
- ◆ Accidental employee error (31%)

Of those surveyed, 47% say the main criterion they use to calculate the amount spent on disaster recovery is the financial risk associated with each potential disaster. The potential threat of terrorism is the most expensive threat that companies have calculated, at \$115 million. Respondents believe the five most likely consequences of a disaster if no plan was in place would be: data loss (64%), decreased employee productivity (57%), damage to customer relationships (50%), reduction in profits (49%), and reduction in revenue (37%).