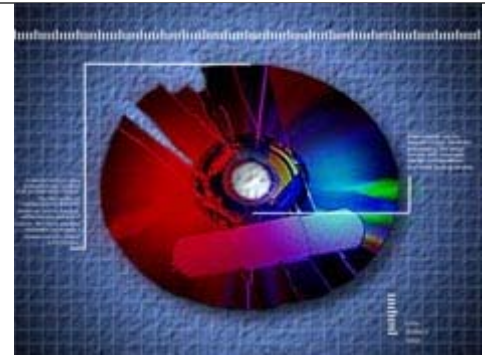

That '70s disaster recovery plan

2/18/2003 5:00:00 PM - Ernst & Young and Fusepoint Managed Services bring the industry up to 2003 with database hot changes and electronic journaling. Plus: Top 10 reasons for program failures

by Jennifer Brown



TORONTO -- As snow and ice storms cripple the eastern seaboard and headlines threaten war, CIOs might understandably be getting a little nervous about the stability of systems on the home front.

According to a study from [Contingency Planning Research](#), power outages and surges are the leading cause (31 per cent) of computer downtime of more than 12 hours. Storm damage amounts to 20 per cent; floods, 16 per cent; and fires and bombs, nine per cent.

"We have all these events looming in our consciousness these days — terrorism, war, ice storms, snow storms, floods, disk drive thefts and disk failures," said Michael Smith, principal with [Ernst & Young](#), speaking in Toronto Tuesday as part of a presentation sponsored by [Fusepoint Managed Services](#).

Smith says awareness around disaster recovery and business continuance has heightened as the need to rely on computer systems has increased and more people have access to critical systems. But few organizations are really doing anything about it. A quick survey of the audience of about 25 before him Tuesday at the Four Seasons Hotel revealed about half a dozen have a disaster recovery plan in place.

But when Gartner predicts that two out of five enterprises that experience a disaster will go out of business within five years of the event, companies might want to sit up and take notice.

"That's a pretty strong statement, but if you look at the first World Trade Center disaster in the early '90s, the companies that weren't prepared were significantly weakened by that event. The same was true for the Oklahoma City bombing," said Robert Offley, president and CEO of Fusepoint Managed Services.


Last year, an Ernst & Young survey of 80 CIOs and CEOs indicated computer system failure is a top concern for leading companies and six out of 10 said a system failure would pose a significant risk, yet the majority believe the likelihood of a catastrophic IT failure is low.

"The impact is high but the probability is low. That's when you buy insurance, isn't it?" said Smith. "But you can't just buy because it takes too long to pay. The bankruptcy proceedings may get the proceedings and not your company."


Smith points to unpaid insurance claims still outstanding from the Sept. 11 terrorist attacks as proof that buying a policy doesn't guarantee your business will be rescued from the ashes. He cited a bank in New York City that is still waiting for an \$845 million claim to be paid. "It had to be reported on the annual report and it affected the share value of the bank and they're still waiting for their money," said Smith.

For critical applications, Smith says standard disaster recovery — something first dev

 [Print story](#)

 [email to a friend](#)

 [Back](#)

 [Back to Top](#)