

## 57% of SMBs Have No Disaster Recovery Plan

**Symantec study finds that one in four of the small and midsize businesses surveyed don't view computer systems as critical to business.**

By [Kevin Casey](#), [InformationWeek](#)  
January 11, 2011

One in two small and midsize businesses (SMBs) have no recovery plan in the event of a network outage, data loss, or other IT disaster, according to a study released Tuesday by Symantec.

That represents an increase from a similar study Symantec conducted a year ago, when 47% had no program in place. Small businesses -- defined in the report as firms with between 5 and 99 workers -- may be at particular risk: 57% have no disaster recovery plan. 47% of midsize companies with between 100 and 1,000 employees didn't have a recovery process in place.

"Obviously, at a high level, SMBs are still not prepared for disaster," said Bernard Laroche, senior director of SMB product marketing. "From our standpoint, it's not good news."

Of the firms without a disaster recovery plan, 41% said it had never occurred to them. 36% said they intend to implement one within the next six months. More than half (52%) said they don't think computer systems are critical to business -- that translates roughly to one in four of all of the businesses polled.

"This is probably the most shocking revelation of the survey," Laroche said. "That's pretty alarming."

Symantec's 2011 SMB Disaster Preparedness Survey included 1,288 businesses worldwide with between 5 and 1,000 employees -- as well as 552 customers of those companies -- across a broad range of industries. A "disaster" could be anything that causes an outage or data loss, whether natural or human-made. The new findings arrive in spite of a different Symantec report, published in June, that showed SMBs are [increasingly fearful of online threats and data loss](#).

The businesses polled experienced on average six outages during 2010, with the top reasons given including [cyberattacks](#), power failures, and natural disasters.

Those outages are expensive, according to Symantec's data, to the tune of \$12,500 vaporized from the business' bottom line per day of downtime. Customers of SMBs also feel the pain: Outages at their SMB vendors cost them \$10,000 per day, and 44% said they have had a smaller vendor temporarily shut down because of a technology failure. 29% of the customers in the study said they have lost "some" or "a lot of" data owing to a vendor's disaster.

The potential price tag on outages -- \$50,000 for four days worth, for example, based on Symantec's numbers -- might not slow down a Fortune 500 firm, but could stagger smaller companies with tighter cash flow. The longer-term damage could be worse: 54% of SMB customers in the survey said they have switched vendors before because of unreliable IT systems.

"It could be a very simple ROI, very simple math," Laroche said, for SMBs concerned about the costs of a disaster recovery measures. He added that a disaster recovery plan can become part of a company's sales pitch, and that some large enterprise clients will often have minimum requirements in this arena just to enter a bid for their business. "Having a DR plan in place becomes almost a competitive advantage in some cases."

Businesses that already have a disaster recovery plan were frequently motivated by a previous incident -- half of them implemented their plan after an outage or data loss. 52% said their plan was less than six months old.

"When something happens, they are acting fairly quickly," Laroche said, but they may be acting too late.

Companies that are taking precautions prior to a problem may not be doing enough. Though the study did not directly address the effectiveness of existing disaster recovery plans, Symantec advised two fundamental steps to ensure the such a plan will work: First, test it regularly with simulated outages and other disaster scenarios. Second, make employees aware of the plan and actively promote compliance. The survey found that among those SMBs with a plan in place, only 28% have tested it.