Symantec 2011 SMB Disaster Preparedness Survey

Global Results

January 2011

✔Symantec™

CONTENTS

EXECUTIVE SUMMARY

For the second year, Symantec's SMB Disaster Preparedness Survey revealed that SMBs are not taking disaster preparedness for their computer and networking systems as seriously as they should.
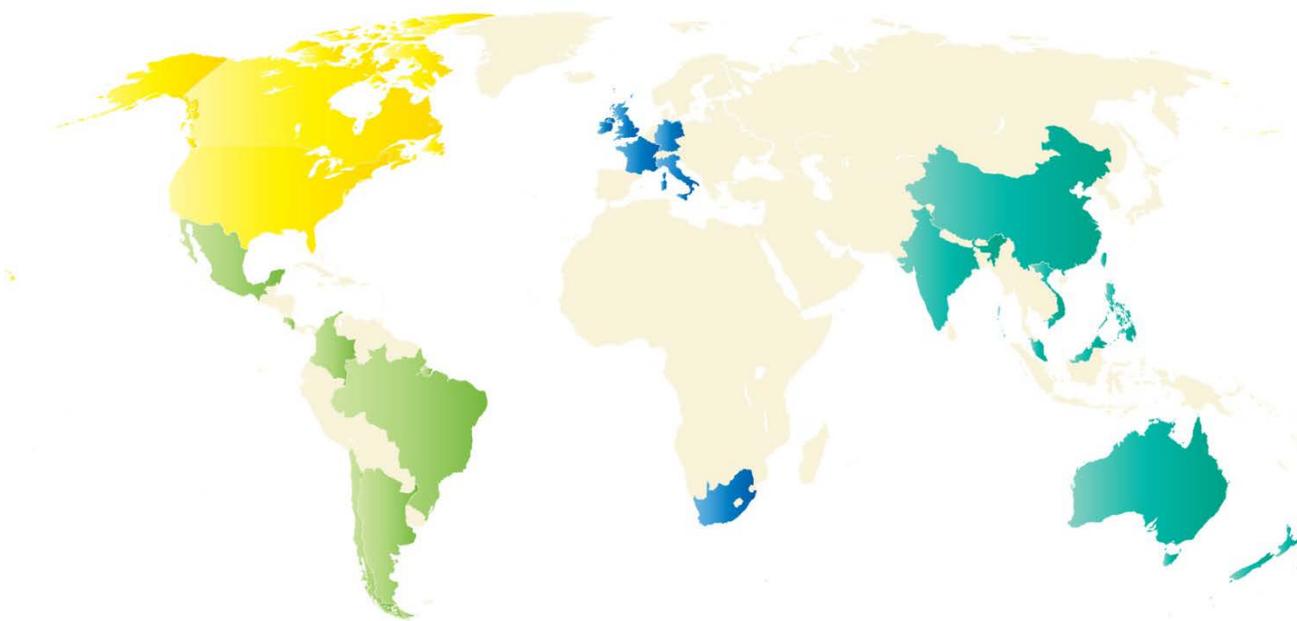
SMBs are at risk and the survey found that most don't take action to prepare for disasters until after they have experienced loss from downtime.

The result is that this lack of preparation has a significant impact on their customers and their business.

METHODOLOGY

Applied Research performed a telephone survey in November 2010.
The survey included 1,288 small and medium businesses with 5 to 1,000
employees and 552 customers of SMBs from 23 countries worldwide.
The survey covered a variety of industries

The confidence level of this survey is 95 percent +/- 2.7 percent for
questions asked of SMBs and +/- 4.2 percent for questions asked of
customers of SMBs.

North America (300)		Latin America (300)		EMEA (340)		APAC (900)	
United States	200	Brazil	100	United Kingdom	100	Australia	100
Canada	100	Mexico	80	Italy	80	New Zealand	100
		Chile	30	France	80	Hong Kong	100
		Argentina	30	Germany	80	India	100
		Colombia	30			China	100
		Costa Rica	20			Taiwan	100
		Caribbean	10			Singapore	100
						Malaysia	100
						Philippines	50
						Vietnam	50

Symantec.

FINDING 1:
Despite warnings, most SMBs are still not prepared for disaster

Respondents were asked about their company's state of readiness to deal with an outage or disruption to their computer or technology resources. Only half (50 percent) responded that they already have a plan in place. That's up slightly from 47 percent last year. Fourteen percent do not have a plan, nor do they have any intention to create one.

There were some differences according to company size. Fifty-seven percent of small businesses don't have a plan, compared to 47 percent of medium businesses.
Of the respondents who do plan to implement a plan in the future, 16 percent plan to do so within 30 days, 34 percent plan to do so between one and three months, and 25 percent plan to do so between three and six months.

Even though only half of respondents have a plan, 81 percent of all respondents are somewhat/very satisfied with their plans to deal with outages or disruptions, whether formal or informal; indeed, 84 percent state that their computer systems are somewhat/completely protected.

When those who do not have a plan were asked why not, roughly half (52 percent) don't think computer systems are critical to the business. Forty-one percent said that it never occurred to them to put together a plan, and 40 percent said that disaster preparedness is not a priority.

FINDING 2:
SMBs are at risk

It is alarming that more SMBs do not have plans to help them deal with disasters and keep their computer systems up and running, especially when one considers that 65 percent of SMBs reside in regions that they consider susceptible to natural disasters.

In fact, SMBs experienced a median of 6 outages in the past year. The top three reasons for downtime include cyberattacks, power outages, employee errors, and upgrades, with each occurring a median of once per company in the last year.

The survey found that SMB information is not protected. Only half of companies surveyed back up at least 60 percent of their data, and less than half back up their data weekly or more frequently. Only 23 percent back up daily.

Key data is not always backed up, either. Of those surveyed, 31 percent do not back up email, 21 percent do not back up application data, and 17 percent do not back up customer data. Respondents also reported that a disaster would cause information loss. Forty-four percent of SMBs said they would lose at least 40 percent of their data in the event of a disaster.

FINDING 3:
SMBs do not act until it is too late

Of SMBs with a disaster preparedness plan, half (50 percent) implemented the plan due to either an outage or data loss. Fifty-two percent put together their plans within the last six months. However, only 28 percent have actually tested their recovery plans, which is a critical component of disaster preparedness.

Again, there were some differences according to company size. Thirty-six percent of small businesses with a disaster preparedness plan implemented their plan within the last six months, compared to 58 percent of medium businesses.

FINDING 4:
Not being prepared can have a negative impact

Disasters can have a significant financial impact on SMBs. Downtime costs SMBs a median of $12,500 per day. It costs small businesses a median of $3,000 per day and medium businesses a median of $23,000 per day.

Outages also have a considerable effect on SMB customers. SMB customers reported that SMB outages cost them $10,000 per day, and 29 percent said they lost "some" or "a lot of" data as a result of disasters impacting their SMB vendors.

Downtime also causes customers to leave with 54 percent of SMB customer respondents reporting they have switched SMB vendors due to unreliable computing systems, a 12 percent increase compared with last year's survey.

For many SMBs, disasters could also put them out of business. Forty-four percent of SMB customers stated that their SMB vendors have temporarily shut down due to a disaster.

SYMANTEC'S RECOMMENDATIONS

- **Don't wait until it's too late:** It is critical for SMBs to not wait until after a disaster to think about what they should have done to protect their data. Not only is downtime costly from a financial perspective, but it could mean the complete demise of the business. SMBs can't wait until it is too late, and they need to begin mapping out a disaster preparedness plan today. A plan should include identification of key systems and data that is intrinsic to the running of the business. Basically, identify your critical resources.

- **Protect information completely:** To reduce the risk of losing critical business information, SMBs must implement the appropriate security and backup solutions to archive important files, such as customer records and financial information for the long term. Natural disasters, theft and cyberattacks can all result in data and financial loss, so SMBs need to make sure important files are saved not only on an external hard drive and/or company network, but in a safe, off-site location.

- **Get employees involved:** SMB employees play a key role in helping to prevent downtime and should be educated on computer security best practices and what to do if information is accidentally deleted or cannot easily be found in their files. Since SMBs have few resources, all employees should know how to retrieve the businesses' information in times of disaster.

- **Test frequently:** After a disaster hits is the worst time to learn that critical files were not backed up as planned. Regular disaster recovery testing is invaluable. Test your plan anytime anything changes in your environment.

- **Review your plan:** If frequent testing is not feasible due to resources and bandwidth, SMBs should at least review their disaster preparedness plan on a quarterly basis.