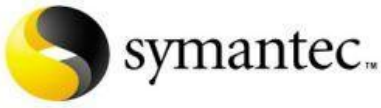
SYMANTEC SMB

SMB Disaster Preparedness

Survey Results
September 2009

Global Data



CONTENTS

EXECUTIVE SUMMARY

Small and mid-sized businesses (SMBs) are the lifeblood of the global economy. Comprising more than 99 percent of all businesses, SMBs employ more than half the world's workers. Most of the world's patents and more than half of the world's GDP come from small and mid-sized business.

But while SMBs are powerful forces in the world's economy, they often run lean and forgo basic protections against business risks due to lack of time, budget and staff resources.

In the 2009 SMB Disaster Preparedness survey, Symantec has uncovered a large discrepancy between how SMBs *perceive* their disaster readiness and their *actual* level of preparedness.

Furthermore, Symantec discovered that there are large, tangible costs to this lack of preparedness. SMBs can – and often do – lose business as a direct result of being unprepared for disasters.

Luckily, there are simple, effective measures SMBs can take to mitigate these risks and retain customers despite of the disasters they may face.

METHODOLOGY

Symantec surveyed 1,657 companies worldwide. Applied Research was selected to perform the survey and targeted the following personnel:

- Small and mid-sized businesses (10 – 499 employees)
- Companies who contract with SMBs for goods and services (we call these "customers")

In both cases we spoke with personnel responsible for their organization's network and computers.

Respondents were split as follows:

- 35 percent of respondents from small business (10 – 99 employees)
- 35 percent of respondents from mid-sized business (100 – 499 employees)
- 30 percent of respondents from customers of SMBs

The survey was performed in August and September 2009.

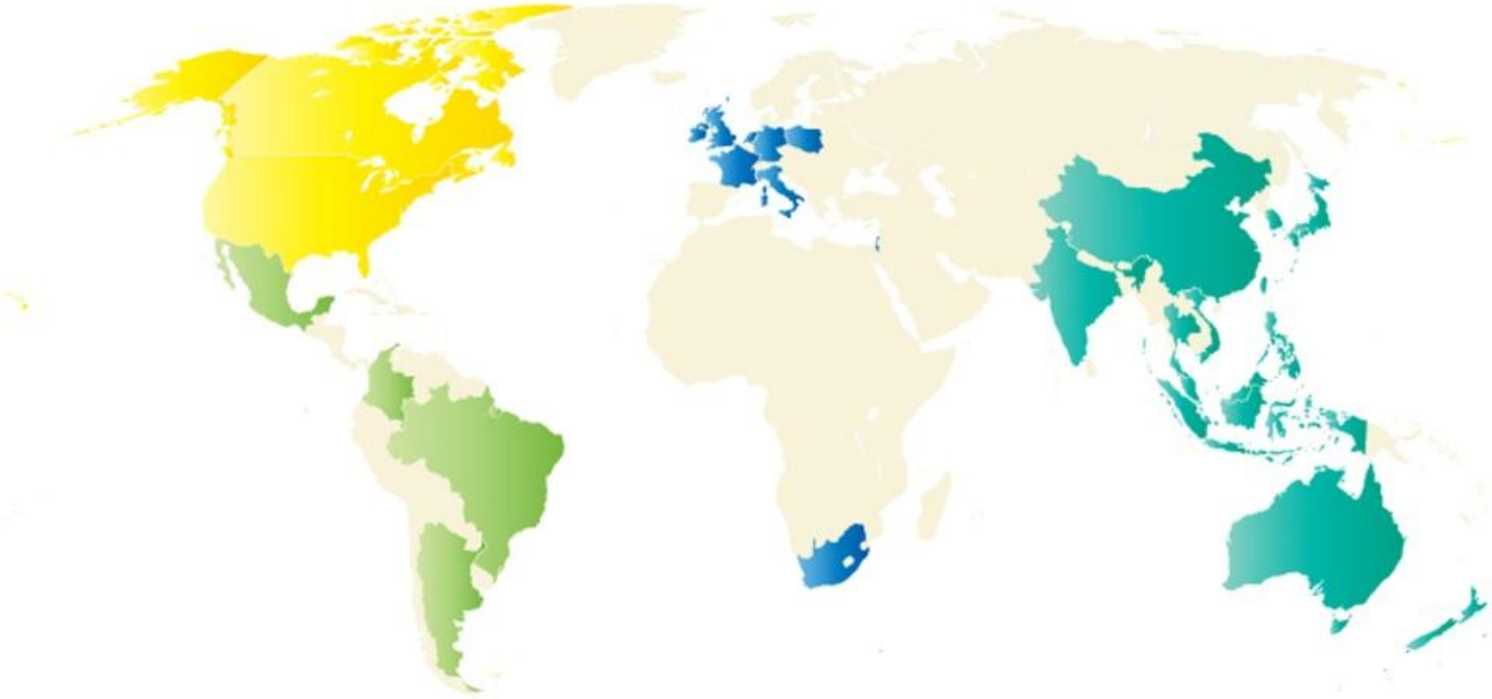
DEMOGRAPHICS

Symantec spoke with 1,156 SMBs and 501 companies who contract with SMBs for goods and services ("customers"). All SMBs included in the survey were either "small" (10-99 employees) or "midsized" (100-499 employees).

The survey includes companies from 28 countries around the world.

The SMB respondents came from a wide variety of industries and included a mix of management and staff.

The customers ranged in size from less than five to more than 1 million employees, with a median size of between 2,000 and 9,999. They come from a wide range of industries.



North America	
United States	250
Canada	49

Latin America	
Brazil	48
Mexico	47
Argentina	24
Columbia	24

EMEA	
United Kingdom	96
Germany	94
France	49
Italy	49
Poland	49
Isreal	49
Netherlands	49
South Africa	49

APJ	
China	94
Australia	94
Singapore	73
Japan	49
India	49
South Korea	49
Malaysia	49
New Zealand	49
Thailand	49
Philippines	49
Indonesia	49
Taiwan	26
Vietnam	26
Hong Kong	26

FINDING 1: SMBs CONFIDENT ABOUT DR

When it comes to disaster preparedness, small- and mid-sized businesses are quite confident. Most (82 percent) report they are somewhat/very satisfied with their disaster recovery (DR) plan. Further, most (84 percent) report their computer and technology systems are somewhat/very protected.

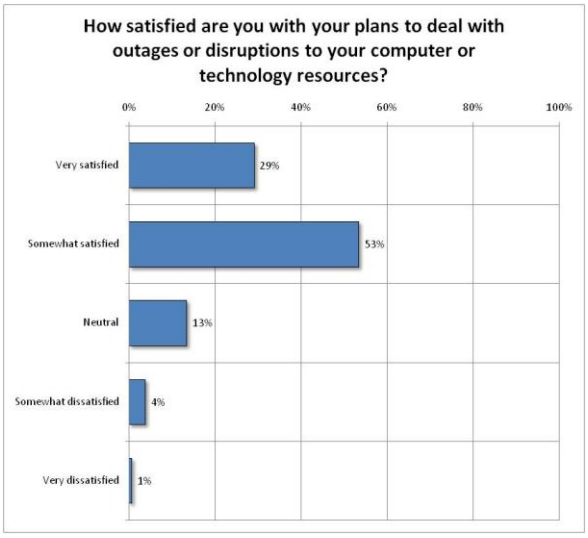
We also asked SMBs what would happen if they lost all their computers in a disaster (such as a fire) and had to rebuild. Would their customers be patient?

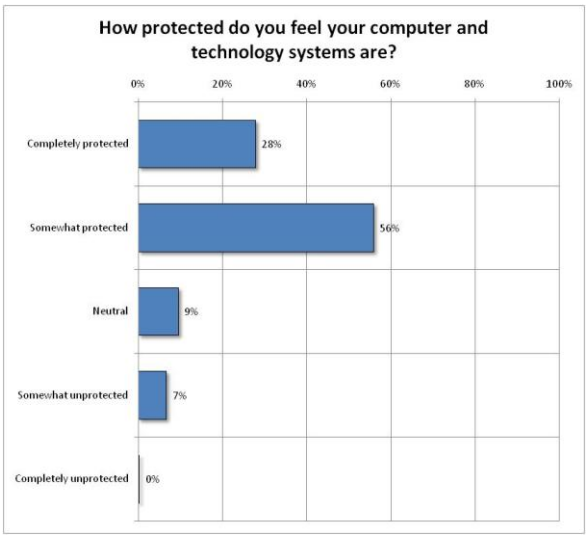
Two thirds (67 percent) believe their customers would either "wait patiently until our systems were back in place" or they "would call us to get what they could, but would wait patiently for the rest until our systems were back in place."

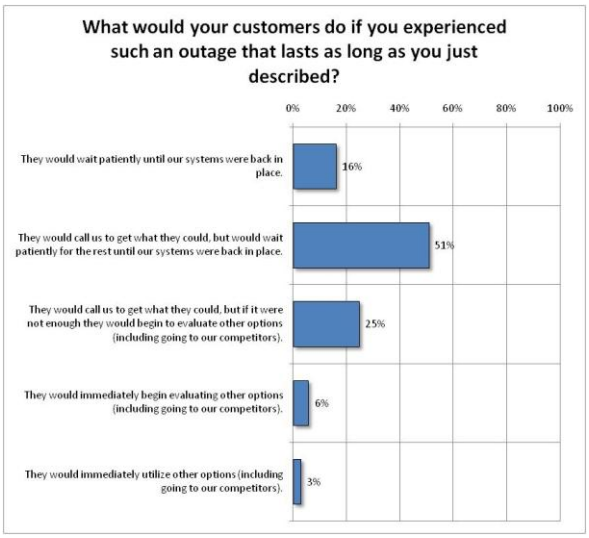
Just one third (34 percent) of the SMBs felt their customers would evaluate other options that included looking at competitors.

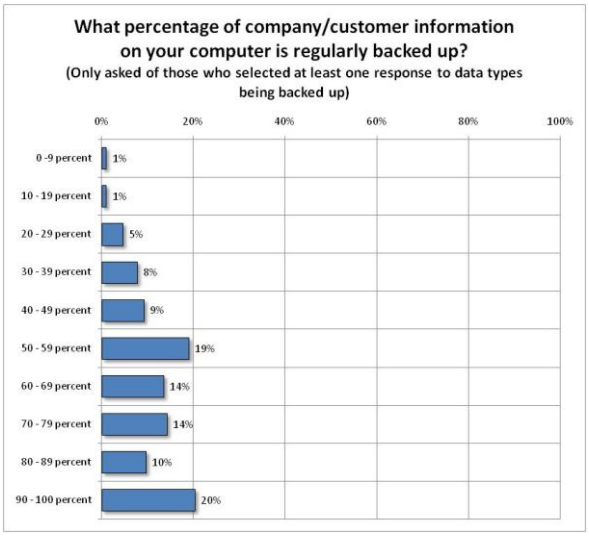
Is this confidence justified? Our second finding says no.

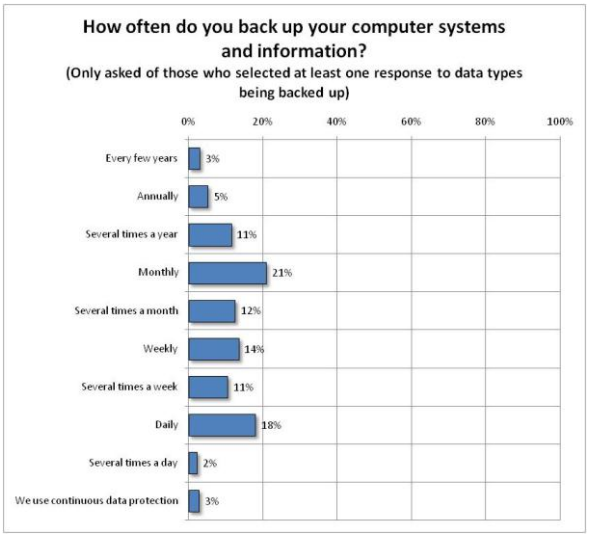
.

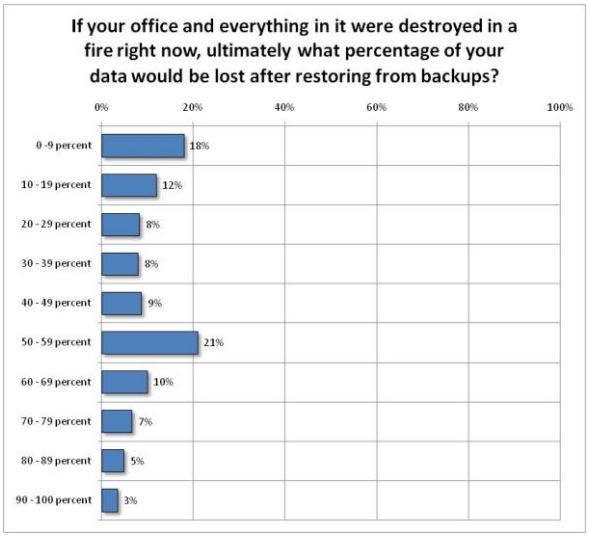












FINDING 2: SMBs NOT PREPARED

SMBs may be optimistic about their disaster preparedness, but our study shows that optimism is misplaced.

First, most SMBs (76 percent) report they live in a region that is susceptible to natural disasters (such as hurricanes, tornadoes, earthquakes).

Furthermore, SMBs report they frequently experience outages or downtime. The average SMB experienced three outages within the past 12 months, with the leading causes being virus or hacker attacks, power outages or natural disasters.

With this kind of exposure, and with the confidence SMBs display about their disaster preparedness, one would think SMBs have solid disaster recovery plans in place. However this is not universally soothe case—almost half (47 percent) report they do not yet have a plan to deal with such disruptions.

Disaster preparedness encompasses many things, but if there is a core activity it would be backing up important information. Here the SMBs again showed an alarming lack of readiness. First, the average SMB backs up only 60 percent of its company and customer data. Second, they do so infrequently. Only one in five (23 percent) back up on a daily basis and 40 percent backup monthly or less.

This inattention to data backup is echoed by the fact that more than half (55 percent) of the SMBs feel they would lose 40 percent of their company data if their computing systems were wiped out in a fire.

In short, our study found that while SMBs were confident about their level of disaster preparedness, in reality they are remarkably unprepared. How much does this affect their relationship with their customers? Quite a bit, as we found in our third finding.

FINDING 3: CUSTOMERS SERIOUS ABOUT DR

How important is it that SMBs have reliable computing systems? It is very important, as it turns out. Two in five (42 percent) SMB customers have actually switched vendors in the past because they "felt their vendor's computers or technology systems were unreliable."

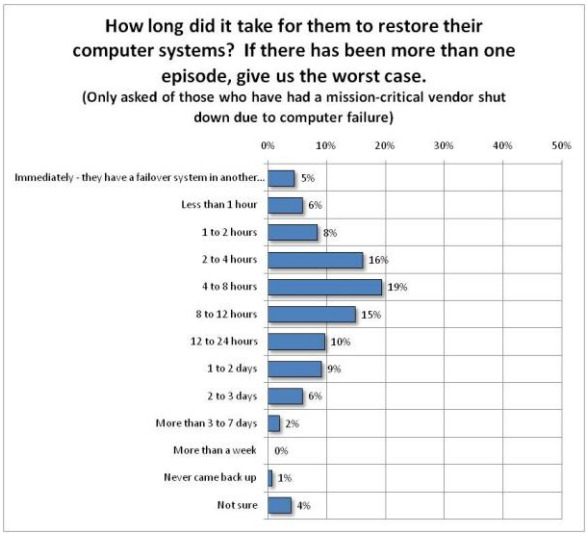
This concern is well founded, as 28 percent of the customers surveyed have seen one or more of their SMB vendors shut down due to computer failure. These outages were impactful as well, with 42 percent lasting eight hours or more. One in four customers (26 percent) reported losing some/a lot of important data because of a vendor's disruption.

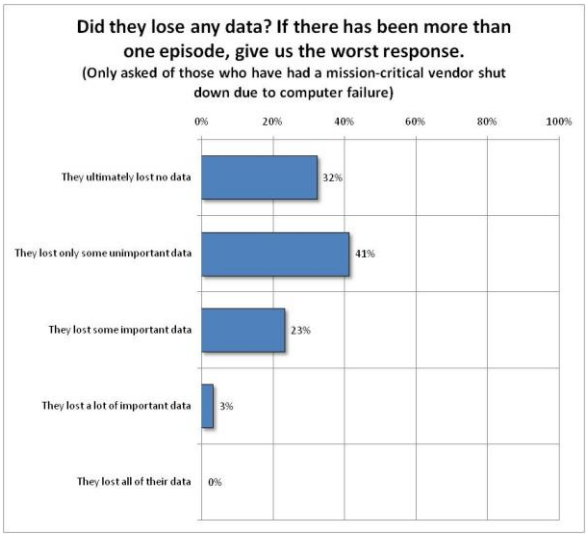
The customers estimated the cost of these outages as being $15,000 per day on average.

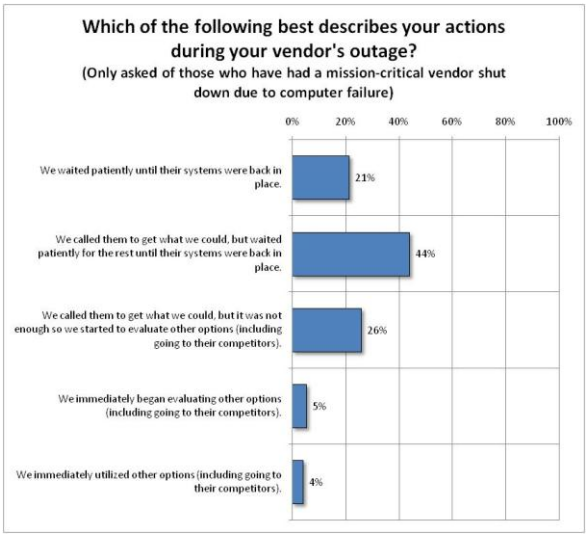
The net effect of these outages was not good for the SMB. First, the customers were upset. On a scale of 1 to 10 they reported a 6 to 7 in terms of being inconvenienced and 6 to 7 in terms of being upset.

More importantly, one third (35 percent) of the customers evaluated other vendors as a result. And, 63 percent of the customers reported that downtime damaged their perception of the SMB vendor, further showing damage to the relationship.

For SMBs, the cost of being complacent about disaster preparedness is clearly high. But there are simple things they can do to mitigate their risk.







RECOMMENDATIONS

Although 47 percent of SMBs do not have a formal disaster preparedness plan, of those without plans, nearly 89 percent say they will create one within the next six months. As these organizations create plans, Symantec recommends the following based on survey findings and best practices:

Determine your needs: SMBs should take time to decide what critical information should be secured and protected. Customer, financial and business information, trade secrets and critical documents should be prioritized. In addition, SMBs should monitor industry reports that help to identify and prevent threats that SMBs face.

Engage trusted advisors: With limited time, budget and employees, SMBs can look to a solution provider to help create plans, implement automated protection solutions and monitor for trends and threats. They can also educate employees on retrieving information from backups when needed and suggest offsite storage facilities to protect critical data.

Automate where you can: Automating the backup process ensures that it is not overlooked. SMBs can reduce the costs of downtime by implementing automated tools that minimize human involvement and address other weaknesses in disaster recovery plans.

Test annually: Recovering data is the worst time to learn that critical files were not backed up as planned. Disaster recovery testing is invaluable and SMBs should seek to improve the success of testing by evaluating and implementing testing methods that are non-disruptive.