AT&T's Business Continuity Survey: 2008

Introduction

For the seventh consecutive year, AT&T has completed a survey of 500 Information Technology (IT) executives around the US. The goal was to learn what these executives were doing about business continuity, and how it figured in their overall IT strategy.

All the companies in the survey group had revenues in excess of $25 million, according to Dun and Bradstreet, and 73% represented companies with 100 or more employees, according to the respondents themselves. About 48% described their IT network as local, 22% as regional, 15% as international and 14% as national.

General Findings

Overall, business continuity planning was seen as a priority by seven out of ten (71%) IT executives. Four out of ten (43%) indicated it had always been a priority for their business, and more than a quarter (28%) indicated it has become a priority in recent years because of heightened awareness of natural disasters, security and terrorist threats. That positive finding is somewhat offset by the fact that three out of ten (28%) said business continuity planning was "not a priority".

While eight out of ten (80%) executives indicated their companies had a business continuity plan, one-fifth (18%) said they did not. This finding is proportional to the size of the enterprise. As company size increases, so does the likelihood that companies will have a plan (88% of those with 500 or more employees compared to 78% of those with 100 to 499 employees and 75% of those with fewer than 100 employees).

The survey also found that companies are more diligent about updating their plans than they are about testing them. A majority (59%) of companies have had their plans updated in the past 12 months, but fewer (46%) have had the plans fully tested during the same time period. Executives in south-central Texas were most likely to say their plans had been updated in the past year, while those in Chicago were least likely to make the same claim (65% and 54% compared to 59%, nationally). In addition, executives in New York were most likely to indicate their plans had been fully tested in the past year, while Seattle/Portland executives were the least likely to report recent testing (53% and 39%, compared to 46% as a national average).

Nationally, half (50%) of all companies had implemented specific protective actions when the federal or state government issued an alert for an impending disaster. South-Central Texas companies were most likely to take such actions (65% compared to 50%, nationally), while Seattle/Portland companies were least likely to do so (39% compared to 50%, nationally). As with planning in general, this is proportional to company size, and larger companies are more likely to report taking protective measures (59% of those with 500 or more employees compared to 47% of those with 100 to 499 employees and 45% of those with less than 100 employees).

Updates and Changes

Six out of ten (60%) companies have made some type of business change in the past year which would warrant updating their business continuity plans. However, only 28% updated the plans due to such changes, which include new or expanded marketing efforts, expanded office space or relocations, new or expanded online customer service and ordering capabilities or mergers and acquisitions.

So while such changes typically did not result in continuity plan updates, nearly half (48%) of the executives indicated that in the next year, they planned to test their continuity plans whenever there was a major change in business operations. Nearly half (48%) also indicated that in the future, testing would be done on a regularly-scheduled basis.

Cyber Security

In this survey, three out of four (74%) executives indicated that cyber security was part of their company's overall business continuity plan, and a majority (55%) viewed cyber security as a concern. On a scale of one to five, where "5" means a top concern, and "1" means not a concern, more than one quarter (28%) rated cyber security as a "5," and more than another quarter (27%) rated it a "4". Two-thirds (69%) of IT executives predicted that hacking would emerge as the most significant threat to cyber security over the next five years. The next most frequently mentioned threat areas were all internal – half (56%) predicted that an internal accident would be a threat, followed by internal sabotage (47%) and exposure through remote working arrangements (44%).

at&t

Hosting Arrangements

Six out of ten (60%) IT executives viewed security, reliability and cost as concerns when thinking about using a hosted environment. One-third (37%) were also concerned about the complexity of these arrangements. Executives in New York tended to be most concerned about security (73% compared to 65%, nationally) and reliability (66% compared to 60%, nationally).

Over a quarter (28%) of the survey group had experienced problems in the last year with a lack of storage space on their company's servers. Companies with 100 or more employees are the most likely category to have experienced this problem (32% of those with 500 or more employees and 31% of those with 100 to 499 employees compared to 17% of those with less than 100 employees).

Recovery Time Objectives

Two out of three (67%) executives have set target recovery times for each of their key business processes. Companies with 100 or more employees are most likely to have set target recovery times (70% of those with 500 or more employees and 69% of those with 100 to 499 employees compared to 57% of those with less than 100 employees). Companies that have business continuity plans are more likely than those who don't to have established recovery time targets (76% compared to 28%, respectively).

Communications

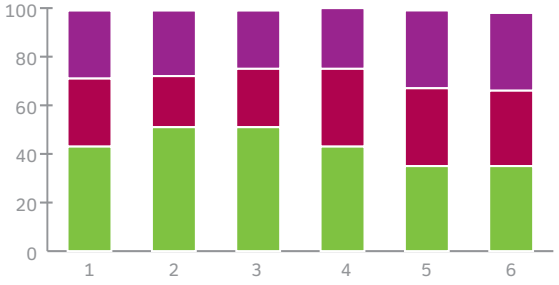
The vast majority (79%) of companies have instituted special arrangements for communicating with key executives during a natural disaster. A similar proportion (80%) have e-mail or text messaging capabilities to reach employees outside of work, and two-thirds (66%) have systems in place that enable most employees to work from home or remote locations. Only four out of ten (39%) companies have automated calling systems to reach employees by telephone or cell phone outside of work.

As company size increases, so does the likelihood that companies will have special arrangements for communicating with key executives (89% of those with 500 or more employees compared to 77% of those with 100 to 499 employees and 71% of those with less than 100 employees). There are similar numbers for e-mail or text messaging capabilities to reach employees outside of work (89% of those with 500 or more employees compared to 78% of those with 100 to 499 employees and 74% of those with less than 100 employees). This general pattern continues for companies that have systems in place that enable employees to work from home or remote locations (72% of those with 500 or more employees compared to 67% of those with 100 to 499 employees and 57% of those with less than 100 employees).

General Preparedness

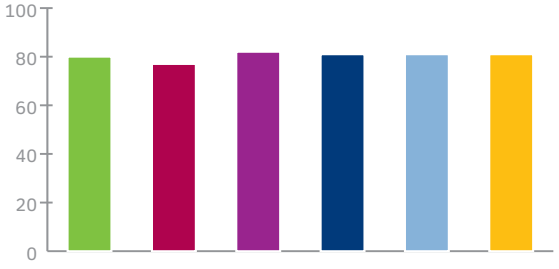
While business continuity planning is important to most companies, a sizable number do not view it as important and may be unprepared to deal with an emergency, either natural or man-made. Three out of ten (28%) indicated business continuity planning was not a priority at their company, one-fifth (19%) did not have or didn't know if their company had a business continuity plan. One-quarter (25%) indicated that cyber security was not part of their overall business continuity plan or didn't know if it was, and one-third (34%) had not prioritized or set target recovery times for key business processes or didn't know if this had been done. Finally, one-fifth (20%) did not have or didn't know of any special arrangements for communicating with key executives in the event of a disaster.

Which of the following statements best describes your business's approach to business continuity planning?



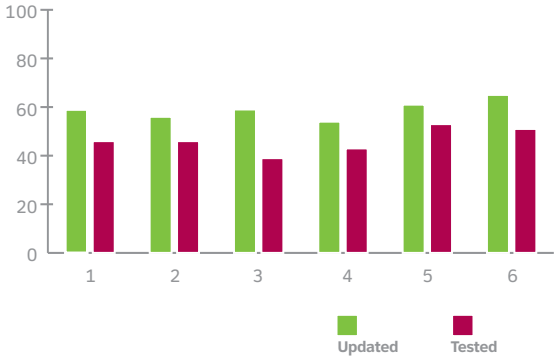
	Has always been a priority	Has been a priority due to disaster/ threats	Not a priority/ not important
1. Nationally	43%	28%	28%
2. Seattle/Portland	51%	21%	27%
3. North Carolina	51%	24%	24%
4. Chicago	43%	32%	25%
5. New York	35%	32%	32%
6. South-Central Texas	35%	31%	32%

Does your organization have a business continuity plan? % Yes



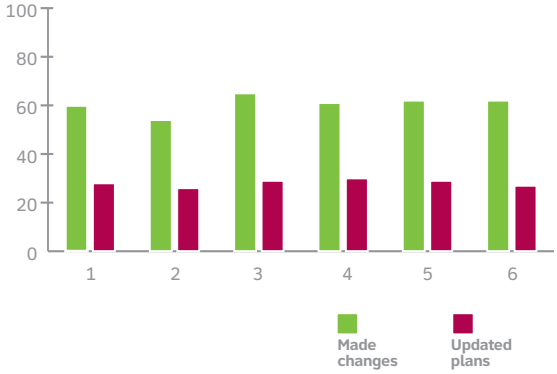
Nationally	80%
Seattle/Portland	77%
North Carolina	82%
Chicago	81%
New York	81%
South-Central Texas	81%

When was the plan last updated/fully tested? % Within the Past 12 Months



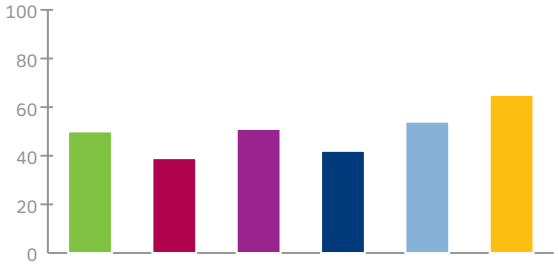
	Updated	Tested
1. Nationally	59%	46%
2. Seattle/Portland	56%	46%
3. North Carolina	59%	39%
4. Chicago	54%	43%
5. New York	61%	53%
6. South-Central Texas	65%	51%

In the past year, has your business made any of the following changes? Did you update your business continuity plan due to any of these changes? % Yes



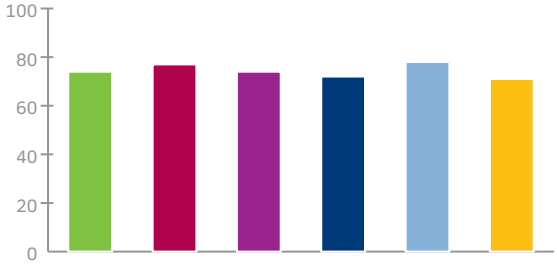
	Made changes	Updated plans
1. Nationally	60%	28%
2. Seattle/Portland	54%	26%
3. North Carolina	65%	29%
4. Chicago	61%	30%
5. New York	62%	29%
6. South-Central Texas	62%	27%

When the federal or state government issues an alert for an impending disaster, do you implement specific protective actions? % Yes



Nationally	50%
Seattle/Portland	39%
North Carolina	51%
Chicago	42%
New York	54%
South-Central Texas	65%

Is cyber security part of your overall business continuity plan? % Yes

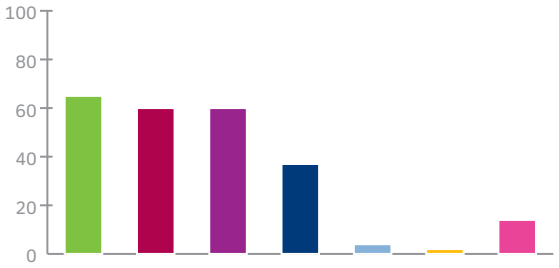


Nationally	74%
Seattle/Portland	77%
North Carolina	74%
Chicago	72%
New York	78%
South-Central Texas	71%

Using a scale where "5" means it is a top concern and "1" means it is not a concern at all, where would you place cyber security as a concern for your organization? % Rate as a "5" or "4"

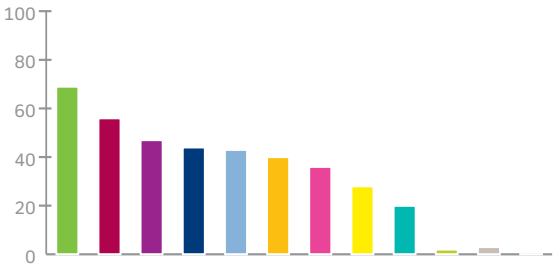
	Rated a "5"	Rated a "4"
1. Nationally	28%	27%
2. Seattle/Portland	31%	26%
3. North Carolina	32%	27%
4. Chicago	35%	21%
5. New York	23%	30%
6. South-Central Texas	21%	30%

Thinking now about a hosted environment, which is defined as the business of housing, serving, and maintaining Web servers for one or more Web sites. What are your concerns about using a hosted environment for your company? National Results



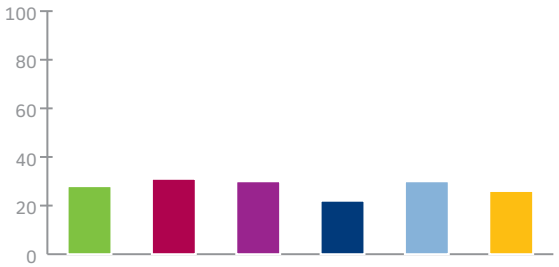
Security	65%
Reliability	60%
Cost	60%
Complexity	37%
Something else	4%
Don't know	2%
No concerns	14%

Thinking five years down the road, what do you think will emerge as the most significant threats to cyber security? National Results



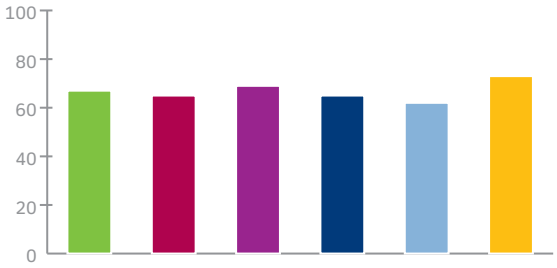
Hacking	69%
Internal accident	56%
Internal sabotage	47%
Remote workers	44%
Denial of service attacks	43%
Botnets	40%
Customer, partner of vendor access to internal systems	36%
Terrorist attacks	28%
Competitor espionage	20%
Other	2%
None of the above	3%
Don't know	1%

In the past year, have you experienced problems with insufficient storage space on your computers or servers for virtual records? % Yes



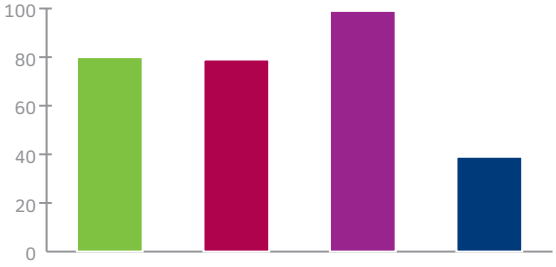
Nationally	28%
Seattle/Portland	31%
North Carolina	30%
Chicago	22%
New York	30%
South-Central Texas	26%

Has your company prioritized and set target recovery times for each of your key business processes? % Yes



Nationally	67%
Seattle/Portland	65%
North Carolina	69%
Chicago	65%
New York	62%
South-Central Texas	73%

In the event of a natural disaster, do you have: % Yes National Results



E-mail or text messaging capabilities to reach employees outside of work	80%
Special arrangements for communicating with key executives	79%
Systems in place that enable most employees to work from home or remote locations	66%
Automated calling systems to reach employees outside of work	39%

Survey Methodology

These results are based on a telephone survey of 500 Information Technology (IT) executives in five U.S. metropolitan/regional areas. The sample of participating companies was drawn from Dun and Bradstreet's business list of companies with at least $10 million in revenue located in each of area. The metropolitan areas are based on DMAs (Designated Market Areas). Interviewing was conducted between April 2 and April 17, 2008, and the interviews averaged 10 minutes in length.

The survey involved 100 interviews in each of the five DMAs: New York, Chicago, Seattle/Portland, South-Central Texas (San Antonio/ Austin/Houston) and North Carolina (Charlotte/Raleigh/Greensboro). Of the 500 participating executives, 47% were Managers/Directors of IT or IS, 39% provided oversight and project management for their company's business continuity plans, 31% were part of a team designing or evaluating the plan and 27% recommended the purchase of security products/services for the plan.

For more information contact your AT&T Representative or visit us at www.att.com/business.

05/27/08 AB-1338

at&t
Your world. Delivered.