2006 AT&T Business Continuity Study
ST. LOUIS Results Summary

Methodology

The following results are derived from a telephone survey of 100 Information Technology (IT) executives in the St. Louis metropolitan region. "Overall" or "national" data comparisons reflect the complete results of a telephone survey of 1,000 IT executives encompassing 10 markets in the United States, including Atlanta, Chicago, Dallas, Detroit, Los Angeles, Miami, New York City, Seattle, St. Louis, and Washington, DC.

St. Louis Market Key Findings

- **Relative to the nine other markets surveyed, St. Louis is unprepared when it comes to business continuity planning.** Most notably, the city ranks at or near the bottom in a number of key survey categories, including:
  - The number of organizations that see business continuity planning as an organizational priority.
  - The number of companies that actually have a continuity plan in place.
  - The percentage of companies that haven't tested their plan in more than a year or not at all.

- **Business continuity planning is seen as a "priority" by just 65% of IT executives in the St. Louis area, the second fewest of any other market surveyed.** In fact, one-third (33%) say it's "not a priority."

- **Nearly half (45%) of St. Louis IT executives surveyed said their plan hasn't been tested in over one year (23%) or has never been tested at all (22%).** However, 52% who have a business continuity plan in St. Louis say their plan has at least been UPDATED in the last 6 months, among the highest percentage of all markets.

St. Louis Market Results Summary

Priority of Business Continuity Planning

Business continuity planning is seen as a "priority" by just 65% of IT executives in the St. Louis area, the second fewest of any other market surveyed.

- In fact, one-third (33%) say it's "not a priority."

- Of those who say business continuity planning is NOT a priority in St. Louis, 67% say "other issues take priority" or that "systems in place are already sufficient" (52%).

The Importance of Having a Business Continuity Plan
Overall, 65% of St. Louis IT executives say they have a business continuity plan in place, again fewer than the nine other markets surveyed. Consequently, 32% of St. Louis IT execs say they don't have a plan in place, indicating the city's businesses may be more at risk than any other market surveyed.

- However, 52% who have a business continuity plan in St. Louis say their plan has been updated in the last 6 months, among the highest percentage of all markets.

- Nevertheless, 22% of St. Louis organizations surveyed haven't updated their plan in over one year compared to 17% overall.

- In addition, 45% of St. Louis IT executives surveyed said their plan hasn't been tested in over one year (23%) or has never been tested at all (22%).

Protective Actions for Government Warnings
Consistent with other non-coastal markets, just 46% of companies surveyed in St. Louis say they implement specific protective actions when the state or federal government issues an alert for an impending disaster, compared with 50% nationally.

- Consequently, 51% of St. Louis IT execs say they don't take any action when the state or federal government issues an alert for an impending disaster.

Implementing Business Continuity Measures
Overall, 97% of companies in St. Louis with a business continuity plan say they've implemented Internet security measures such as firewalls, intrusion detection, hacker protection, and/or password authentication systems.

- Three-quarters of St. Louis organizations (74%) who have a plan in place say they've already established backup or redundant servers – a relatively low figure compared to 82% nationally.

- Also, 83% of St. Louis companies with a business continuity plan say they are "educating employees" as a protective continuity measure, consistent with 82% among the other markets surveyed.

Suffering from a Disaster
One-quarter (25%) of St. Louis IT executives say their organization has suffered from a disaster at one point or another, compared to 28% overall in other markets.

- Of those who have suffered from a disaster in St. Louis, the largest percentage (48%) say they were impacted by "other extreme weather," and 40% added they suffered from a flood.

- An additional 36% of those who said they've been impacted by a disaster say they were affected by a blackout, while 28% added they were impacted by fire.

- Most organizations surveyed in St. Louis which have suffered from disasters in the past say it cost them less than $100,000 a day (48%). Just 20% say it cost them more than $100,000 a day, and no company said it cost them more than $1 million.

- St. Louis IT executives who say their company suffered from a disaster indicated "negatively impacted customer relationships" (24%) was the predominant non-financial damage which resulted, followed by "reductions in employee workforce" (12%).

- However, 80% of these companies in St. Louis who have suffered from a disaster say they've taken actions to reduce business interruptions in the future – slightly higher than the 78% overall average.

Cyber Security
Overall, 80% percent of executives who have responsibility for business continuity planning in St. Louis say cyber security is part of their overall business continuity plan in 2006, consistent with 81% nationally.

- Just 14% say that cyber security is NOT part of their overall business plan – slightly lower than the average of most other markets surveyed (17% overall).

Of those who say cyber security is part of their overall business plan, most say "educating employees" (86%) and "defining corporate security policies" (76%) are the steps they have taken when it comes to cyber security.

- In St. Louis, 33% say they've contracted an outside service provider to manage security, compared to the 33% national average.

Viruses, worms, and spyware are the most significant perceived threats to cyber security in the minds of St. Louis IT executives surveyed; 70% agree these are one of the most significant threats, followed by "SPAM" (38%).

- Other perceived threats to cyber security include hackers (36%), an internal accident (26%), and denial of service attacks (22%).

Few St. Louis IT executives see cyber security as a "top concern" for their organization. In all, just 21% rated it as a five on a scale of one to five -- where "5" means cyber security is a top concern, and "1" means cyber security is NOT a concern – compared to 28% in all other markets. More (36%) rated cyber security a "4."

- A number of St. Louis IT executives rated cyber security a more moderate concern, as 24% rated cyber security a "3," while 18% rated cyber security a "2" or lower.

- The overall mean score of 3.5 is lower than the 3.7 national average.