



## 2006 AT&T Business Continuity Study DALLAS Results Summary

### Methodology

The following results are derived from a telephone survey of 100 Information Technology (IT) executives in the Dallas 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, St. Louis, Seattle, and Washington, DC.

### Dallas Market Key Findings

- **While business continuity planning is seen as a "priority" by 68% of IT executives in the Dallas area – consistent with the 70% national average – those who have a plan are perhaps more prepared than any other market surveyed.** In fact, 54% say their plans have been updated in the last 6 months, more than any other market along with Miami (54%). Just 10% said they haven't updated their plan in over one year, and only 1% said their business continuity plan hasn't been updated at all.
- **In addition, 42% of Dallas IT executives with a business continuity plan say it's been tested in the last six months – again more than any other market and underscoring Dallas's high level of preparedness relative to most other cities.**
- **A relatively high 54% of companies surveyed in Dallas say they implement specific protective actions when the state or federal government issues an alert for an impending disaster, compared with 50% nationally.** This figure is the second highest percentage of any other market surveyed, next to Miami.

### Dallas Market Results Summary

#### **Priority of Business Continuity Planning**

Business continuity planning is decisively seen as a "priority" by 68% of Dallas IT executives, consistent with the 68% overall average.

- Almost one-third (31%) of Dallas IT execs say business continuity planning is "not a priority."
- Of those who say business continuity planning is not a priority in Dallas, a surprising 71% say it's because "the probability of a disaster causing a business disruption is small." An additional 65% say "other issues take priority" or that "systems in place are already sufficient" (65%).

## **The Importance of Having a Business Continuity Plan**

In all, 79% of Dallas IT executives say they have a business continuity plan in place, among the highest percentages of all markets surveyed. In addition, just 20% say they don't have a plan.

- Dallas IT executives also appear very prepared in terms of updating their business continuity plans – 54% say their plans have been updated in the last 6 months, more than any other market, along with Miami (54%).
- Just 10% said they haven't updated their plan in over one year, and only 1% said their business continuity plan hasn't been updated at all. In addition, 42% of Dallas IT executives with a business continuity plan say it's been tested in the last six months – again more than any other market and underscoring Dallas's high level of preparedness relative to most other cities.

## **Protective Actions for Government Warnings**

A moderately high 54% of companies surveyed in Dallas say they implement specific protective actions when the state or federal government issues an alert for an impending disaster, compared with 50% nationally. This figure is also the second highest percentage of any other markets surveyed, next to Miami (85%).

- Overall, 44% of Dallas IT execs still say they don't take any action when the state or federal government issues an alert for an impending disaster – equal to the 44% national average.

## **Implementing Business Continuity Measures**

Overall, 92% of companies in Dallas with a business continuity plan say they've implemented Internet security measures such as firewalls, intrusion detection, hacker protection, and/or password authentication systems.

- In addition, 84% of those who have a plan in place in Dallas say they've already established backup or redundant servers, compared to 82% nationally.
- Also, 80% of Dallas companies with a business continuity plan say they are “educating employees” as a protective continuity measure, slightly less than the overall average of 82%.

## **Suffering from a Disaster**

In all, just 24% of Dallas IT executives say their organization has ever suffered from a disaster at one point or another, compared to 28% overall.

- Of those who have suffered from a disaster in Dallas, most (54%) say they were impacted by a blackout.
- An additional 46% of those who said they've been impacted by a disaster say they were affected by cyber attacks or viruses.

- Thirty-three percent (33%) of those impacted by a disaster in Dallas say it cost them less than \$100,000 a day. An additional 25% said it cost them more than \$100,000 a day, but none said it cost their organization more than \$1 million per day.
- More than anything, Dallas IT executives who say their company suffered from a disaster say it primarily “negatively impacted customer relationships” (33%), and resulted in a “loss in employee confidence” (29%).
- However, 79% of these companies in Dallas who have suffered from a disaster say they’ve taken actions to reduce business interruptions in the future.

### **Cyber Security**

Overall, 86% percent of executives who have responsibility for business continuity planning in Dallas say cyber security is part of their overall business continuity plan in 2006, moderately higher than 81% nationally.

- Just 14% say that cyber security is NOT part of their overall business plan.

Of those who say cyber security is part of their overall business plan, most say “educating employees” (93%) and “defining corporate security policies” (90%) are the steps they have taken when it comes to cyber security.

- In Dallas, a relatively high 40% 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 Dallas IT executives surveyed; 75% agree these are one of the most significant threats, followed by “hackers” 42%.

- Other perceived threats to cyber security include SPAM (41%), internal sabotage (28%), and an internal accident (27%).

Dallas IT executives largely see cyber security as a “top concern” for their organization. In all, 30% 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. An additional 22% rated cyber security a “4.”

- Most (36%) rated cyber security as a “3,” while just 12% rated cyber security a “2” or lower.
- The overall mean score of 3.7 is largely consistent with the 3.7 national average.