2007 AT&T Business Continuity Study
MEMPHIS/NASHVILLE Results

Methodology

The following results are based on a telephone survey of 100 Information Technology (IT) executives in the Memphis and Nashville metropolitan regions. The sample of participating companies was drawn from Dunn and Bradstreet's business list of companies with at least $10 million in revenue located in the Memphis and Nashville DMAs (Designated Market Area). Interviewing was conducted between January 24 and February 5, 2007, and the interviews averaged 10 minutes in length. Of the 100 companies, 42 are located in the Memphis DMA and 58 are located in the Nashville DMA.

Of the 100 participating executives:

- 49% are Managers/Directors of IT or IS
- 49% provide oversight and project management for their company's business continuity plans, 25% are part of a team designing or evaluating the plan, and 23% recommend the purchase of IT or security products for the plan
- 42% represent companies with revenues in excess of $20 million (Dunn and Bradstreet's information)
- 62% represent companies with 100 or more employees (information supplied by respondents)

Key Findings

- **Business continuity planning is seen as a "priority" by three-fourths (77%) of IT executives in the Memphis/Nashville regions**. Half (49%) indicate it has always been a priority for their business, and one-fourth (28%) indicate it has become a priority in recent years due to natural disasters, security, and terrorist threats.

    - **Compared to the national results, Memphis/Nashville executives are the most likely to indicate that business continuity planning has always been a priority (49% compared to 40%, nationally).**

- **Similarly, seven out of ten (71%) Memphis/Nashville executives indicate their companies have a business continuity plan.** About one-fourth (28%) indicate their company does not have a plan, and 1% don't know if the company has a plan or not.

    - A majority (58%) of companies has had these plans updated in the past 12 months, and a plurality (47%) have had them tested during the same time period. None indicate that their plans have never been updated, and only 6% indicate the plan has never been tested.

- The types of business continuity measures that companies have already taken in Memphis/Nashville include implemented Internet security measures (69%), established redundant servers and/or backup sites (59%), educated employees (61%), and used a service provider for outsourcing (39%).

- **More than eight out of ten (85%) Memphis/Nashville executives indicate that cyber security is part of their company's overall business continuity plan.** Only one out of seven (14%) indicate cyber security is not part of the plan, and 1% don't know if it is or not.

  - Actions that Memphis/Nashville companies have taken when it comes to cyber security include educated employees (68%), defined corporate security policies (61%), and contracted with an outside service provider to manage security (30%).

  - Viruses and worms are the most significant perceived threats to cyber security in the minds of Memphis/Nashville executives. Three-fourths (76%) indicate this is one of the most significant threats, followed by "hackers" (46%).

- **Only half (49%) of Memphis/Nashville IT executives view cyber security as a concern.** On a scale of one to five, where "5" means a top concern and "1" means not a concern, one-fourth (22%) rate cyber security as a "5," and another one-fourth (27%) rate it a "4."

- **Of the 10 market areas included in the study, the Memphis/Nashville region ranks fifth in business continuity preparedness.**

  - The Business Continuity Rankings (from 1 to 10) were computed for each market based on responses on three components: ***Business Continuity Plan*** (having a plan, last time updated/tested, taking action when alerted by federal or state governments); ***Actions Taken on Plan*** (business continuity measures in place including Internet security measures, establishing redundant servers, educating employees, and using a service provider for outsourcing); and **Cyber Security** (cyber security is part of overall plan, actions implemented including educating employees, defining corporate security policies, and contracting with an outside service provider to manage security).

- **The rankings for the ten market areas are:**

  1. **New York**
  2. **Houston**
  3. **San Francisco**
  4. **Boston**
  5. **Memphis/Nashville**
  6. **Atlanta**
  7. **Chicago**
  8. **Los Angeles**
  9. **Minneapolis/St. Paul**
  10. **Cleveland**

- **If Memphis/Nashville executives can't sleep at night, it is because they are worrying about viruses/worms, security breaches, and natural disasters.** One-third (32%) indicate that worrying about viruses/worms is most likely to keep them up at night followed by security breaches (23%), natural disasters (23%), corporate/eCommerce sites crashing (9%), and man-made disasters (9%).

Detailed Findings

Priority of Business Continuity Planning

- **Business continuity planning is seen as a "priority" by three-fourths (77%) of IT executives in the Memphis/Nashville areas**. Half (49%) indicate it has always been a priority for their business, and one-fourth (28%) indicate it has become a priority in recent years due to natural disasters, security, and terrorist threats.

    - Nonetheless, one-fourth (23%) of Memphis/Nashville execs say business continuity planning is "not a priority" or "not important" at their company.

    - Reasons for business continuity planning not being a priority include other issues take priority (11%), systems in place are considered sufficient (11%), the probability of a disaster causing business disruption is small (11%), the probability of a major disaster at the company is small (6%), and business continuity planning is too expensive (5%).

Business Continuity Plans

- **Seven out of ten (71%) Memphis/Nashville executives indicate their companies have a business continuity plan.** About one-fourth (28%) indicate their company does not have a plan, and 1% don't know if the company has a plan or not.

    - A majority (58%) of companies have had these plans updated in the past 12 months, and a plurality (47%) have had them tested during the same time period. None indicate that their plans have never been updated, and only 6% indicate the plan has never been tested.

    - One-third (37%) of executives indicate they implement specific protective actions when the state or federal government issues an alert for an impending disaster.

    - The types of business continuity measures that companies have already taken in Memphis/Nashville include implemented Internet security measures (69%), established redundant servers and/or backup sites (59%), educated employees (61%), and used a service provider for outsourcing (39%).

    - In the next six months, Memphis/Nashville companies plan to implement business continuity measures including educating employees (20%), establishing redundant servers and/or backup sites (13%), implementing Internet security measures (13%), and using a service provider for outsourcing (15%).

Experience with Disasters

- **One-fourth (26%) of Memphis/Nashville companies have suffered from a natural or man-made disaster.** The majority of companies (74%) have no experience with disasters.

  - The most frequently experienced disasters include tornados (12%), blackouts (8%), other extreme weather or snow (7%), hurricanes (7%), fires (6%), and floods (5%). Compared to the national results, Memphis/Nashville companies are most likely to have experienced tornados (12% compared to 2%, nationally).

  - Financial damages from disasters tended to be less than $500,000. Ten companies had financial damages of less than $100,000, two had damages of $100,000 to $500,000, and two had damages of $500,000 to $1,000,000.

  - The non-financial impact of the disasters appears minimal with only 6 executives indicating the disaster negatively impacted customer relationships, 3 indicating the disaster resulted in a reduction in the workforce, 2 indicating the disaster resulted in a loss of employee confidence, 2 mentioning the disaster tarnished their company's reputation, 2 mentioning a negative impact on supplier relationships, and 1 mentioning a loss of stockholder confidence. Nineteen executives indicate their companies experienced none of these non-financial damages.

  - Even so, almost all (20 out of 26) companies that suffered a disaster did take action to reduce business interruptions in the future.

Cyber Security

- **More than eight out of ten (85%) Memphis/Nashville executives indicate that cyber security is part of their company's overall business continuity plan.** Only one out of seven (14%) indicate cyber security is not part of the plan, and 1% don't know if it is or not.

  - Actions that Memphis/Nashville companies have taken when it comes to cyber security include educated employees (68%), defined corporate security policies (61%), and contracted with an outside service provider to manage security (30%).

  - Viruses and worms are the most significant perceived threats to cyber security in the minds of Memphis/Nashville executives. Three-fourths (76%) indicate this is one of the most significant threats, followed by "hackers" (46%).

  - Other perceived threats to cyber security include SPAM (40%), internal sabotage (23%), an internal accident (28%), and customer, partner, and/or vendor access to internal systems (22%).

- **Only half (49%) of Memphis/Nashville IT executives view cyber security as a concern.** On a scale of one to five, where "5" means a top concern and "1" means not a concern, one-fourth (22%) rate cyber security as a "5," and another one-fourth (27%) rate it a "4."

    - One-fourth (28%) rate cyber security as a "3," while 23% rate it as not a concern (a "2" or a "1").

IT Worries

- **If Memphis/Nashville executives can't sleep at night, it is because they are worrying about viruses/worms, security breaches, and natural disasters.** One-third (32%) indicate that worrying about viruses/worms is most likely to keep them up at night, followed by security breaches (23%), natural disasters (23%), corporate/eCommerce sites crashing (9%), and man-made disasters (9%).