



## 2007 AT&T Business Continuity Study HOUSTON Results

### Methodology

The following results are based on a telephone survey of 100 Information Technology (IT) executives in the Houston metropolitan area. 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 the Houston DMA (Designated Market Area). Interviewing in Houston was conducted between January 24 and February 13, 2007, and the interviews averaged 10 minutes in length.

Of the 100 participating executives:

- 56% are Managers/Directors of IT or IS
- 47% provide oversight and project management for their company's business continuity plans, 27% are part of a team designing or evaluating the plan, and 25% recommend the purchase of security products/services for the plan
- 77% represent companies with revenues in excess of \$25 million (Dun and Bradstreet's information)
- 70% represent companies with 100 or more employees (information supplied by respondents)

### Key Findings

- **Business continuity planning is seen as a "priority" by eight out of ten (80%) IT executives in the Houston area.** One-third (35%) indicate it has always been a priority for their business, and almost half (45%) indicate it has become a priority in recent years due to natural disasters, security, and terrorist threats.
- **Similarly, three-fourths (78%) of Houston executives indicate their companies have a business continuity plan.** One-fifth (20%) indicate their company does not have a plan, and 2% don't know if the company has a plan or not.
  - A majority (62%) of companies have had these plans updated in the past 12 months, and more than one-third (38%) have had them tested during the same time period. Few have never had their plans updated (1%) or have never had them tested (11%).
  - The types of business continuity measures that companies have already taken in Houston include implemented Internet security measures (72%), educated employees (65%), established redundant servers and/or backup sites (65%), and used a service provider for outsourcing (34%).

- A majority (58%) of Houston companies implement specific protective actions when the federal or state government issues an alert for an impending disaster.
- **Compared to the national results, Houston companies are more likely to indicate that business continuity planning has become a priority in recent years because of natural disasters, security, and terrorist threats (45% compared to 29%, nationally), to indicate that their companies have business continuity plans (78% compared to 72%, nationally), to have updated their plans in the past 12 months (62% compared to 57%, nationally), and to implement specific protective actions when the federal or state government issue as alert for an impending disaster (58% compared to 34%, nationally).**
- **Three-fourths (78%) of Houston executives indicate that cyber security is part of their company's overall business continuity plan.** Only one-fifth (19%) indicate cyber security is not part of the plan.
  - Actions that Houston companies have taken when it comes to cyber security include defined corporate security policies (66%), educated employees (63%), and contracted with an outside service provider to manage security (25%).
  - Viruses and worms are the most significant perceived threats to cyber security in the minds of Houston IT executives. Almost three-fourths (72%) indicate this is one of the most significant threats, followed by "hackers" (44%).
- **Six out of ten (62%) Houston 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-third (32%) rate cyber security as a "5," and three out of ten (30%) rate it a "4."
- **Of the 10 market areas included in the study, Houston ranks second, after New York, 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).

- **New York is first (highest in preparedness) followed by Houston in the Business Continuity Rankings, while Cleveland ranks tenth (lowest in preparedness). 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 Houston IT executives can't sleep at night, it is because they are worrying about viruses/worms, security breaches, and natural disasters.** One-third (33%) indicate that worrying about viruses/worms is most likely to keep them up at night, followed by security breaches (26%), natural disasters (22%), man-made disasters (8%), and corporate/eCommerce sites crashing (8%).

### **Detailed Findings**

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

- **Business continuity planning is seen as a “priority” by eight out of ten (80%) IT executives in the Houston area.** One-third (35%) indicate it has always been a priority for their business, and almost half (45%) indicate it has become a priority in recent years due to natural disasters, security, and terrorist threats.
  - Only 17% of Houston execs say business continuity planning is “not a priority.”
  - Reasons for business continuity planning not being a priority include the probability of a disaster causing business disruption is small (13%), other issues take priority (10%), the probability of a major disaster at the company is small (7%), systems in place are considered sufficient (8%), and business continuity planning is too expensive (3%).

### *Business Continuity Plans*

- **Three-fourths (78%) of Houston executives indicate their companies have a business continuity plan.** One-fifth (20%) indicate their company does not have a plan, and 2% don't know if the company has a plan or not.
  - A majority (62%) of companies have had these plans updated in the past 12 months, and more than one-third (38%) have had them tested during the same time period. Few have never had their plans updated (1%) or have never had them tested (11%).
  - A majority (58%) 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 Houston include implemented Internet security measures (72%), educated employees (65%), established redundant servers and/or backup sites (65%), and used a service provider for outsourcing (34%).
  - In the next six months, Houston companies plan to implement business continuity measures including implementing Internet security measures (17%), establishing redundant servers and/or backup sites (15%), educating employees (10%), and using a service provider for outsourcing (5%).

### *Experience with Disasters*

- **Three out of ten (31%) Houston companies have suffered from a natural or man-made disaster.** The majority of companies (69%) have no experience with disasters.
  - The most frequently experienced disasters include hurricanes (28%), floods (11%), blackouts (9%), other extreme weather or snow (8%), and cyber attacks (7%).
  - Compared to the national results, Houston companies are more likely to indicate that their companies have suffered disasters (31% compared to 24%, nationally), specifically hurricanes (28% compared to 6%, nationally).
  - For Houston companies, financial damages from disasters tended to be less than \$500,000. Twelve companies had financial damages of less than \$100,000, four had damages between \$100,000 and \$1 million, and four had damages of \$1 million or more.

- Given the low experience levels with disasters, the non-financial impact of the disasters appears minimal, with seven indicating it resulted in a reduction in employee workforce, four executives indicating the disaster negatively impacted customer relationships, three indicating it resulted in a loss of employee confidence, two indicating it negatively impacted supplier relationships, one mentioning the disaster tarnished their company's reputation, and one mentioning a loss of stockholder confidence. Seventeen executives indicate their companies experienced none of these non-financial damages.
- Even so, most (26 out of 31) companies that suffered a disaster did take action to reduce business interruptions in the future.

### *Cyber Security*

- **Three-fourths (78%) Houston executives indicate that cyber security is part of their company's overall business continuity plan.** Only one-fifth (19%) indicate cyber security is not part of the plan.
  - Actions that Houston companies have taken when it comes to cyber security include educated employees (63%), defined corporate security policies (66%), and contracted with an outside service provider to manage security (25%).
  - Viruses and worms are the most significant perceived threats to cyber security in the minds of Houston IT executives. Almost three-fourths (72%) indicate this is one of the most significant threats, followed by "hackers" (44%).
  - Other perceived threats to cyber security include SPAM (42%), an internal accident (30%), internal sabotage (30%), and customer, partner, and/or vendor access to internal systems (17%).
- **Six out of ten (62%) Houston 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-third (32%) rate cyber security as a "5," and three out of ten (30%) rate it a "4."
  - Another one-fourth (27%) rate cyber security as a "3," while only 10% rate it as not a concern (a "2" or a "1").

### *IT Worries*

- **If Houston IT executives can't sleep at night, it is because they are worrying about viruses/worms, security breaches, and natural disasters.** One-third (33%) indicate that worrying about viruses/worms is most likely to keep them up at night, followed by security breaches (26%), natural disasters (22%), man-made disasters (8%), and corporate/eCommerce sites crashing (8%).