Business Continuity
2010: Southern Market

# 2010 AT&T Business Continuity Study

SOUTHERN REGION Results

## Key Findings

### IT Plans for 2010

- IT budgets for 2010 are about the same or higher than those of the previous two years. Two-thirds (67%) of executives indicate that their IT budgets for 2010 are the same or higher than the previous two years.

- Investment in new technologies will continue in 2010. Seven out of 10 (71%) executives indicate that their companies are investing in new technologies in 2010.

### Business Continuity Plans

- The vast majority (85%) of executives in the Southern region indicate their companies have a business continuity plan.

  - Almost three out of four (72%) indicate their companies implement specific protective actions when the federal or state government issues an alert for an impending disaster.

  - A majority (61%) of these companies have had their business continuity plans fully tested in the past 12 months.

  - One-third (32%) of these companies require their suppliers and other vendors to have a business continuity plan in place in order to do business with them.

  - Two-thirds (65%) consider the use of managed or outsourced capabilities as part of their business continuity plan.

  - Seven out of 10 (70%) include their wireless network capabilities as part of their business continuity plan.

**Security Threats**

- Almost half (46%) of these companies provide employees with access to social networking tools.

  - Most (82%) executives are concerned about the increasing use of social networking capabilities and its impact on security threats.

  - A similar proportion (79%) is concerned about the increasing use of mobile networks and devices and their impact on security threats.

- Overall, the threat that poses the biggest risk to security is hacking (25%).

**Communicating During Natural Disasters**

- Most (81%) Southern region executives indicate their companies have prioritized and set target recovery times for each of their key business processes.

- The vast majority (88%) indicate that they have special arrangements for communicating with key executives in the event of a disaster.

  - A similar proportion (91%) has e-mail or text messaging capabilities to reach employees outside of work.

  - Eight out of 10 (82%) have systems in place that enable most employees to work from home or remote locations; more than half

(57%) have automated calling systems to reach employees by telephone or cell phone outside of work.

## Detailed Findings

### IT Plans for 2010

- IT budgets for 2010 are about the same or higher than those of the previous two years. Two-thirds (67%) of executives indicate that their IT budgets for 2010 are the same or higher than the previous two years; 35% indicate the budgets are about the same, and 32% indicate the budgets are higher. One-third (32%) indicate their IT budget for 2010 is lower than in the previous two years.

- Investment in new technologies will continue in 2010. Seven out of 10 (71%) executives indicate that their companies are investing in new technologies in 2010.

  - Executives most frequently mention that they will be investing in mobile applications (26%), virtualization (18%), cloud computing (16%), hosted services (13%), unified communications (9%), digital media solutions (9%) and telepresence (7%).

### Business Continuity Plans

- Business continuity planning is seen as a “priority” by three-fourths (77%) of IT executives in the Southern region. Half (48%) indicate it has always been a priority for their business, and three out of 10 (29%) indicate it has become a priority in recent years due to natural disasters, security and terrorist threats.

  - One-fifth (23%) of the executives indicate business continuity is “not a priority.”

- The vast majority (85%) of these executives indicate their companies have a business continuity plan. Following are specific details about these plans.

  - Executives most frequently indicate that the business unit in charge of managing the business continuity plan is the IT Department (29%), followed by the CIO/CTO (26%) and the CEO/CFO (21%).

- Concerning methods for communicating the specifics of the business continuity plan to employees, half (50%) indicate the information is cascaded from senior leadership, and one-third (31%) indicate it is communicated through broad, generic communications to all employees.

- Almost three-fourths (72%) indicate their companies implement specific protective actions when the federal or state government issues an alert for an impending disaster.

- A majority (61%) of these companies have had their business continuity plans fully tested in the past 12 months. Only 4% indicate that their plans have never been tested.

    - One-fifth (20%) indicate that testing includes all locations worldwide.

- One-third (32%) of these companies require their suppliers and other vendors to have a business continuity plan in place in order to do business with them.

- Two-thirds (65%) consider the use of managed or outsourced capabilities as part of their business continuity plan.

- Seven out of 10 (70%) include their wireless network capabilities as part of their business continuity plan.

    - Almost half (45%) indicate that at least 50% of their company's employees use mobile devices.

    - Almost half (47%) indicate that employee use of mobile devices plays a major role in the business continuity plan; 33% indicate mobile devices play a minor role.

    - Almost half (47%) indicate that their companies have virtualized the computing infrastructure.

    - One-third (34%) have implemented a business continuity plan for that virtualized infrastructure.

  - Four out of 10 (40%) indicate that satellite communications are part of their company's communications network.

    - Satellite communications are used for telephones (9%), international communications (6%), disaster communications (6%), data transmission (6%) and communications in general (5%).

  - Four out of 10 (40%) executives indicate that their company has invoked its business continuity plan. Reasons for invoking the plan most frequently involve:

    - Extreme weather (32%)
    - Power outages at facilities (22%)
    - IT failures (12%)

- The need for a plan of action and backup systems are important lessons learned. A majority (58%) of these companies have experienced a natural or man-made disaster that affected IT operations. Executives indicate that the biggest lesson learned from this experience was the need to plan ahead and have a plan of action (22%) and the need for increased backup systems (13%).

## Security Threats

- Almost half (46%) of these companies provide employees with access to social networking tools. A majority (54%) do not provide such access.

  - One out of seven (13%) indicates that social networking is generally accepted and widely used, while three out of 10 (30%) indicate it is generally accepted but used by only a few.

  - Most (82%) executives are concerned about the increasing use of social networking capabilities and its impact on security threats. Half (49%) are somewhat concerned, and one-third (33%) are very concerned.

  - A similar proportion (79%) is concerned about the increasing use of mobile networks and devices and their impact on security threats. More than half (55%) are somewhat concerned, and one-fourth (24%) are very concerned.

- Overall, the threat that poses the biggest risk to security is hacking (25%). Other perceived threats include an internal accident (15%), natural disasters (11%) and internal sabotage (10%).

  - While executives are concerned about how social networking capabilities and the use of mobile networks and devices may impact security, only 3% view social networking sites and none view mobile networks as the biggest security risks.

## Communicating During Natural Disasters

- Most (81%) executives indicate their companies have prioritized and set target recovery times for each of their key business processes.

  - One out of seven (15%) has not prioritized and set recovery times.

- Almost all (88%) executives indicate that they have special arrangements for communicating with key executives in the event of a natural disaster.

  - A similar proportion (91%) has e-mail or text messaging capabilities to reach employees outside of work.

  - Eight out of 10 (82%) have systems in place that enable most employees to work from home or remote locations; a majority (57%) have automated calling systems to reach employees by telephone or cell phone outside of work.

## Methodology

The results are based on an online survey of 104 Information Technology (IT) executives in the Southern region of the Unites States (Louisiana, Alabama, Mississippi and Florida). The study was conducted by e-Rewards Market Research with companies having total revenues of more than $25 million (except for state/local government participants). Surveys in the Southern region were obtained between February 23 and February 28, 2010.

- e-Rewards Market Research is one of the top online market research sample providers in the U.S. Through their B-to-B business panel, they have the ability to quickly target high level decision-makers and executives by industry, company size, functional role and purchasing role (among other attributes). Using a by-invitation only approach, they have recruited over two million business panelists who opt-in to survey requests.

Of the 104 participating executives:

- 100% have primary responsibility for business continuity planning
- 95% represent companies with revenues in excess of $25 million; 5% represent state/local governments
- 37% are VPs/Managers/Directors of IT or IS; 22% are the CIO, CTO, CFO, CEO or COO
- 56% represent companies with locations outside of the United States
- Executives represent 16 major industry areas (besides state/local government)