2009 AT&T Business Continuity Study
HOUSTON Results

Methodology

The following results are based on an online survey of 100 Information Technology (IT) executives in the Houston metropolitan area. The study was conducted by e-Rewards Market Research with companies having total revenues of more than $25 million in the Houston DMA (Designated Market Area). Surveys in Houston were obtained between February 9 and February 12, 2009.

- e-Rewards Market Research is one of the top online market research sample providers in the U.S. Through their B2B 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 2 million business panelists who opt-in to survey requests.

Of the 100 participating executives:

- All represent companies with revenues in excess of $25 million
- All have primary responsibility for business continuity planning
- 39% are VPs/Managers/Directors of IT or IS; 14% are the CIO, CFO, CEO, or COO
- 73% represent companies with locations outside of the United States
- Executives represent 14 major industry areas

Key Findings

IT Plans for 2009

- **IT budgets for 2009 are lower or equal to those of the previous two years.** Almost four out of ten (37%) executives indicate that their IT budgets for 2009 are lower than in the previous two years. Another three out of ten (30%) indicate the budgets are about the same.

- **While budgets may be decreasing, investment in new technologies continues.** Six out of ten (61%) executives indicate that their companies are investing in new technologies in 2009.

Business Continuity Plans

- **The vast majority (82%) of Houston executives indicate their companies have a business continuity plan.**
    - Three-fourths (73%) indicate their companies implement specific protective actions when the federal or state government issues an alert for an impending disaster.
    - Two-thirds (68%) of companies have had their business continuity plans fully tested in the past 12 months.
    - One-third (35%) of all companies require their suppliers and other vendors to have a business continuity plan in place in order to do business with them.
    - Six out of ten (63%) consider the use of managed or outsourced capabilities as part of their business continuity plan.
    - Seven out of ten (70%) include their wireless network capabilities as part of their business continuity plan.

Security Threats

- **Four out of ten (43%) companies provide employees with access to social networking tools.** A majority (55%) do not provide such access.
- **Two-thirds (65%) are concerned about the increasing use of social networking capabilities and its impact on security threats.** Half (48%) are somewhat concerned, and 17% are very concerned.
- **A similar proportion (65%) is concerned about the increasing use of mobile networks and devices and their impact on security threats.** Half (50%) are somewhat concerned, and 15% are very concerned.
- **Overall, the threat that poses the biggest risk to security is hacking (30%).** Other perceived threats include an internal accident (18%), internal sabotage (11%), and customer/partner/vendor access to internal systems (10%).

Communicating During Natural Disasters

- **Three-fourths (77%) of Houston executives indicate their companies have prioritized and set target recovery times for each of their key business processes.**
- **The vast majority (89%) of Houston executives indicate that they have special arrangements for communicating with key executives in the event of a natural disaster.**

- A similar proportion (85%) has e-mail or text messaging capabilities to reach employees outside of work.

- Three-fourths (76%) have systems in place that enable most employees to work from home or remote locations, and six out of ten (62%) have automated calling systems to reach employees by telephone or cell phone outside of work.

Detailed Findings

IT Plans for 2009

- **IT budgets for 2009 are lower or equal to those of the previous two years.** Almost four out of ten (37%) executives indicate that their IT budgets for 2009 are lower than in the previous two years. Another three out of ten (30%) indicate the budgets are about the same. Only one-fourth (27%) indicate that the IT budget for 2009 is higher than in the previous two years.

- **While budgets may be decreasing, investment in new technologies continues.** Six out of ten (61%) executives indicate that their companies are investing in new technologies in 2009.

  - Executives most frequently mention that they will be investing in different types of upgrades including software upgrades (19%), Internet services/Web services upgrades (8%), firewall/security upgrades (4%), communications upgrades (3%), Wi-Fi wireless upgrades (3%), and data warehousing/storage upgrades (2%).

Business Continuity Plans

- **Business continuity planning is seen as a "priority" by eight out of ten (82%) IT executives in the Houston area**. More than half (53%) indicate it has always been a priority for their business, and three out of ten (29%) indicate it has become a priority in recent years due to natural disasters, security, and terrorist threats.

  - Fewer than one out of five (17%) executives indicate business continuity is "not a priority."

- **The vast majority (82%) of Houston 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 CEO/CFO (24%), the IT Department (24%), or the CIO/CTO (19%).

  - Concerning methods for communicating the specifics of the business continuity plan to employees, 32% indicate the information is cascaded from senior leadership, while 35% indicate is it communicated through broad, general communications to all employees.

- Three-fourths (73%) indicate their companies implement specific protective actions when the federal or state government issues an alert for an impending disaster.

- Two-thirds (68%) of 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-third (35%) indicate that testing includes all locations worldwide.

- One-third (35%) of all companies require their suppliers and other vendors to have a business continuity plan in place in order to do business with them.

- Six out of ten (63%) consider the use of managed or outsourced capabilities as part of their business continuity plan.

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

    - Half (50%) indicate that at least 50% of their company's employees use mobile devices.
    - Half (52%) indicate that employee use of mobile devices plays a major role in the business continuity plan; 29% indicate mobile devices play a minor role.

- A majority (52%) of executives indicate that their company has invoked its business continuity plan. Reasons for invoking the plan most frequently involve:

    - Extreme weather (45%)
    - Power outages at facilities (29%)
    - Floods (19%)
    - IT failures (14%)
    - Utility outages (14%)

- **The need for backup systems and a plan of action are important lessons learned.** A majority (58%) of executives 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 for increased backup systems (13%), the need to plan ahead and have a plan of action (9%), and the need to have multiple means of communication (8%), and locations available as off site back up (8%).

Security Threats

- **Four out of ten (43%) companies provide employees with access to social networking tools.** A majority (55%) do not provide such access.

- One-fourth (23%) indicate that social networking is generally accepted but used only by a few, while 15% indicate it is generally accepted and widely used.

- **Two-thirds (65%) are concerned about the increasing use of social networking capabilities and its impact on security threats.** Half (48%) are somewhat concerned, and 17% are very concerned.

- **A similar proportion (65%) is concerned about the increasing use of mobile networks and devices and their impact on security threats.** Half (50%) are somewhat concerned, and 15% are very concerned.

- **Overall, the threat that poses the biggest risk to security is hacking (30%).** Other perceived threats include an internal accident (18%), internal sabotage (11%), and customer/partner/vendor access to internal systems (10%).

- While executives are concerned about how social networking capabilities and the use of mobile networks and devices may impact security, only 4% view social networking capabilities and 1% view mobile networks as the biggest security risks.

Communicating During Natural Disasters

- **Three-fourths (77%) of Houston executives indicate their companies have prioritized and set target recovery times for each of their key business processes.**
    - One out of six (16%) has not prioritized and set recovery times.

- **The vast majority (89%) of Houston executives indicate that they have special arrangements for communicating with key executives in the event of a natural disaster.**
    - A similar proportion (85%) has e-mail or text messaging capabilities to reach employees outside of work.
    - Three-fourths (76%) have systems in place that enable most employees to work from home or remote locations, and six out of ten (62%) have automated calling systems to reach employees by telephone or cell phone outside of work.

###