2009 AT&T Business Continuity Study
FLORIDA Results

Methodology

The following results are based on an online survey of 101 Information Technology (IT) executives in three Florida markets. Thirty-four (34) interviews were conducted in the Miami metropolitan area, 34 in the Orlando metropolitan area, and 33 in the Tampa metropolitan area. The study was conducted by e-Rewards Market Research with companies having total revenues of more than $25 million. Surveys in Florida were obtained between February 9 and February 14, 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 two million business panelists who opt-in to survey requests.

Of the 101 participating executives:

- All represent companies with revenues in excess of $25 million
- All have primary responsibility for business continuity planning
- 50% are VPs/Managers/Directors of IT or IS; 17% are the CIO, CFO, CEO, COO, or CTO
- 60% represent companies with locations outside of the United States
- Executives represent 17 major industry areas

Key Findings

IT Plans for 2009

- **IT budgets for 2009 are lower than those of the previous two years.** Almost half (47%) of all executives indicate that their IT budgets for 2009 are lower than in the previous two years. Another three out of ten (29%) indicate that budgets are about the same.

- **While budgets may be decreasing, investment in new technologies continues.** Two-thirds (66%) of executives indicate that their companies are investing in new technologies in 2009.

Business Continuity Plans

- **Almost all (89%) Florida executives indicate their companies have a business continuity plan.**

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

    - Six out of ten (62%) companies have had their business continuity plans fully tested in the past 12 months. Only 4% indicate that their plans have never been tested.

    - Four out of ten (44%) 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 (72%) include their wireless network capabilities as part of their business continuity plan.

Security Threats

- **Four out of ten (44%) companies provide employees with access to social networking tools.** A majority (54%) do not provide such access.

- **A majority (71%) of executives are concerned about the increasing use of social networking capabilities and its impact on security threats.** Four out of ten (43%) are somewhat concerned, and one-fourth (28%) are very concerned.

- **A similar proportion (69%) is concerned about the increasing use of mobile networks and devices and their impact on security threats.** Four out of ten (45%) are somewhat concerned, and one-fourth (24%) are very concerned.

- **Overall, the threat that poses the biggest risk to security is hacking (32%).**

Communicating During Natural Disasters

- **The vast majority (85%) of Florida executives indicate their companies have prioritized and set target recovery times for each of their key business processes.**

- **Almost all (91%) Florida executives indicate that they have special arrangements for communicating with key executives in the event of a natural disaster.**

    - A similar proportion (95%) has e-mail or text messaging capabilities to reach employees outside of work.

  - Three-fourths (74%) have systems in place that enable most employees to work from home or remote locations, and a majority (55%) 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 than those of the previous two years.** Almost half (47%) of all executives indicate that their IT budgets for 2009 are lower than in the previous two years. Another three out of ten (29%) indicate that budgets are about the same, and only about one-fourth (23%) indicate budgets are higher than in the previous two years.

- **While budgets may be decreasing, investment in new technologies continues.** Two-thirds (66%) of executives indicate that their companies are investing in new technologies in 2009.

  - Executives most frequently mention that they will be investing in new equipment or different types of upgrades including new computers and phones (18%), software upgrades (11%), new servers (4%), upgrading to a new Internet system (4%), management software (4%), and communications upgrades (4%).

Business Continuity Plans

- **Business continuity planning is seen as a "priority" by eight out of ten (82%) IT executives in Florida**. Half (51%) indicate it has always been a priority for their business, and one-third (31%) indicate it has become a priority in recent years due to natural disasters, security, and terrorist threats.

  - Fewer than one out of five (18%) executives indicate business continuity is "not a priority."

- **Almost all (89%) Florida 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 (36%), followed by the IT Department (32%).

  - Concerning methods for communicating the specifics of the business continuity plan to employees, 50% indicate the information is cascaded from senior leadership, while 30% indicate is it communicated through broad, general communications to all employees.

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

  - Six out of ten (62%) companies have had their business continuity plans fully tested in the past 12 months. Only 4% indicate that their plans have never been tested.

    - Three out of ten (29%) indicate that testing includes all locations worldwide.

  - Four out of ten (44%) 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 (72%) 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.
    - A majority (52%) indicates that employee use of mobile devices plays a major role in the business continuity plan; 33% indicate mobile devices play a minor role.

  - Half (51%) of all executives indicate that their company has invoked its business continuity plan. Reasons for invoking the plan most frequently involve:

    - Extreme weather (44%)
    - Power outages at facilities (18%)
    - Telecommunications failure (13%)
    - IT security incident (12%)
    - IT failures (11%)

- **The need for a plan of action and backup systems are important lessons learned.** Four out of ten (40%) 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 in place (21%).

Security Threats

- **Four out of ten (44%) companies provide employees with access to social networking tools.** A majority (54%) do not provide such access.
    - One out of six (17%) indicate that social networking is generally accepted and widely used, while one-fifth (22%) indicate it is generally accepted but used by only a few.
- **A majority (69%) of executives are concerned about the increasing use of social networking capabilities and its impact on security threats.** Four out of ten (43%) are somewhat concerned, and one-fourth (28%) are very concerned.
- **A similar proportion (71%) is concerned about the increasing use of mobile networks and devices and their impact on security threats.** Four out of ten (45%) are somewhat concerned, and one-fourth (24%) are very concerned.
- **Overall, the threat that poses the biggest risk to security is hacking (32%).** Other perceived threats include customer, partner, or vendor access to internal systems (10%), an internal accident (9%), internal sabotage (9%), and competitor espionage (9%).
    - 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 2% view mobile networks as the biggest security risks.

Communicating During Natural Disasters

- **The vast majority (85%) of Florida executives indicate their companies have prioritized and set target recovery times for each of their key business processes.**
    - Only one out of ten (10%) has not prioritized and set recovery times.
- **Almost all (91%) Florida executives indicate that they have special arrangements for communicating with key executives in the event of a natural disaster.**
    - A similar proportion (95%) has e-mail or text messaging capabilities to reach employees outside of work.
    - Three-fourths (74%) have systems in place that enable most employees to work from home or remote locations, and a majority (55%) have automated calling systems to reach employees by telephone or cell phone outside of work.