2009 AT&T Business Continuity Study
SOUTHERN CALIFORNIA Results

Methodology

The following results are based on an online survey of 101 Information Technology (IT) executives in the Los Angeles, Orange County, and San Diego metropolitan areas. Thirty-four (34) interviews were conducted in the Los Angeles metropolitan area, 33 in Orange County, and 33 in the San Diego metropolitan area. The study was conducted by e-Rewards Market Research with companies having total revenues of more than $25 million. Surveys in these southern California markets 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 100 participating executives:

- All represent companies with revenues in excess of $25 million
- All have primary responsibility for business continuity planning
- 46% are VPs/Managers/Directors of IT or IS; 20% are the CIO, CFO, CEO, COO, or CTO
- 68% 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 equal to or lower than those of the previous two years.** Four out of ten (40%) executives indicate that their IT budgets for 2009 are remaining about the same, and 38% indicate budgets are lower than in the previous two years.

- **While budgets may be decreasing, investment in new technologies continues.** Six out of ten (59%) executives indicate that their companies are investing in new technologies in 2009.

Business Continuity Plans

- **The vast majority (81%) of southern California executives indicate their companies have a business continuity plan.**
  - Two-thirds (65%) indicate their companies implement specific protective actions when the federal or state government issues an alert for an impending disaster.
  - Half (52%) of these companies have had their business continuity plans fully tested in the past 12 months. Only 5% indicate that their plans have never been tested.
  - Three out of ten (30%) companies require their suppliers and other vendors to have a business continuity plan in place in order to do business with them.
  - Almost two-thirds (64%) consider the use of managed or outsourced capabilities as part of their business continuity plan.
  - Six out of ten (63%) include their wireless network capabilities as part of their business continuity plan.

Security Threats

- **More than four out of ten (42%) companies provide employees with access to social networking tools.** A majority (57%) do not provide such access.

- **Most (72%) executives are concerned about the increasing use of social networking capabilities and its impact on security threats.** Half (49%) are somewhat concerned, and one-fourth (23%) are very concerned.

- **Slightly more (77%) are concerned about the increasing use of mobile networks and devices and their impact on security threats.** Six out of ten (61%) are somewhat concerned, while only one out of seven (16%) is very concerned.

- **Overall, the threat that poses the biggest risk to security is hacking (26%).** Other perceived threats include customer, partner, or vendor access to internal systems (14%) and internal sabotage (13%).

Communicating During Natural Disasters

- **Seven out of ten (72%) southern California executives indicate their companies have prioritized and set target recovery times for each of their key business processes.**
  - One-fourth (23%) has not prioritized and set recovery times.

- **The vast majority (79%) of southern California executives indicate that they have special arrangements for communicating with key executives in the event of a natural disaster.**

    - A similar proportion (84%) has e-mail or text messaging capabilities to reach employees outside of work.

    - Three-fourths (75%) have systems in place that enable most employees to work from home or remote locations, and half (54%) 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 equal to or lower than those of the previous two years.** Four out of ten (40%) executives indicate that their IT budgets for 2009 are remaining about the same, and 38% indicate budgets are lower than in the previous two years. Only about one-fifth (21%) indicate budgets are higher than in the previous two years.

- **While budgets may be decreasing, investment in new technologies continues.** Six out of ten (59%) 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 software upgrades (13%), new computers and phones (11%), and new servers (11%).

Business Continuity Plans

- **Business continuity planning is seen as a "priority" by three-fourths (74%) of IT executives in southern California**. Half (50%) indicate it has always been a priority for their business, and one-fourth (24%) indicate it has become a priority in recent years due to natural disasters, security, and terrorist threats.

    - One-fourth (25%) of executives indicate business continuity is "not a priority."

- **The vast majority (81%) of southern California 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 (27%), followed by the CEO/CFO (26%).

  - Concerning methods for communicating the specifics of the business continuity plan to employees, equal proportions indicate the information is cascaded from senior leadership (36%) or communicated through broad, general communications to all employees (36%).

  - Two-thirds (65%) indicate their companies implement specific protective actions when the federal or state government issues an alert for an impending disaster.

  - Half (52%) of these companies have had their business continuity plans fully tested in the past 12 months. Only 5% indicate that their plans have never been tested.

    - One-third (34%) indicate that testing includes all locations worldwide.

  - Three out of ten (30%) companies require their suppliers and other vendors to have a business continuity plan in place in order to do business with them.

  - Almost two-thirds (64%) consider the use of managed or outsourced capabilities as part of their business continuity plan.

  - Six out of ten (63%) include their wireless network capabilities as part of their business continuity plan.

    - Four out of ten (38%) indicate that at least 50% of their company's employees use mobile devices.

    - Four out of ten (39%) indicate that employee use of mobile devices plays a major role in the business continuity plan; 36% indicate mobile devices play a minor role.

  - One-fourth (25%) of executives indicate that their company has invoked its business continuity plan. Reasons for invoking the plan most frequently involve:

    - Power outage at facilities (13%)
    - Fire (10%)
    - IT failure (9%)

- **The need for a plan of action and backup systems are important lessons learned.** About one-third (32%) 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 for increased backup systems (8%) and to plan ahead and have a plan of action in place (5%).

Security Threats

- **More than four out of ten (42%) companies provide employees with access to social networking tools.** A majority (57%) do not provide such access.
    - One out of seven (14%) indicates that social networking is generally accepted and widely used, while one-fifth (19%) indicate it is generally accepted but used by only a few.

- **Most (72%) executives are concerned about the increasing use of social networking capabilities and its impact on security threats.** Half (49%) are somewhat concerned, and one-fourth (23%) are very concerned.

- **Slightly more (77%) are concerned about the increasing use of mobile networks and devices and their impact on security threats.** Six out of ten (61%) are somewhat concerned, while only one out of seven (16%) is very concerned.

- **Overall, the threat that poses the biggest risk to security is hacking (26%).** Other perceived threats include customer, partner, or vendor access to internal systems (14%) and internal sabotage (13%).
    - While executives are concerned about how social networking capabilities and the use of mobile networks and devices may impact security, very few view social networking sites (1%) or mobile networks (1%) as the biggest security risks.

Communicating During Natural Disasters

- **Seven out of ten (72%) southern California executives indicate their companies have prioritized and set target recovery times for each of their key business processes.**
    - One-fourth (23%) has not prioritized and set recovery times.

- **The vast majority (79%) of southern California executives indicate that they have special arrangements for communicating with key executives in the event of a natural disaster.**
    - A similar proportion (84%) has e-mail or text messaging capabilities to reach employees outside of work.
    - Three-fourths (75%) have systems in place that enable most employees to work from home or remote locations, and half (54%) have automated calling systems to reach employees by telephone or cell phone outside of work.