Business Continuity 2010:
San Francisco/San Ramon

2010 AT&T Business Continuity Study

San Francisco/San Ramon Results

Key Findings

IT Plans for 2010

- **IT budgets for 2010 are about the same or higher than those of the previous two years.** Three-fourths (75%) 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.** Eight out of 10 (79%) executives indicate that their companies are investing in new technologies in 2010.

Business Continuity Plans

- **The vast majority (81%) of executives in the San Francisco/San Ramon area indicate their companies have a business continuity plan.**

    - Two-thirds (64%) indicate their companies implement specific protective actions when the federal or state government issues an alert for an impending disaster.

- A majority (52%) of these companies have had their business continuity plans fully tested in the past 12 months.

- Half (49%) 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 (67%) consider the use of managed or outsourced capabilities as part of their business continuity plan.

- Six out of 10 (62%) include their wireless network capabilities as part of their business continuity plan.

Security Threats

- **A majority (58%) 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.

  - Three-fourths (76%) are 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 (27%).**

Communicating During Natural Disasters

- **Most (77%) San Francisco/San Ramon executives indicate their companies have prioritized and set target recovery times for each of their key business processes.**

- **Seven out of ten (73%) indicate that they have special arrangements for communicating with key executives in the event of a disaster.**
    - A similar proportion (77%) has e-mail or text messaging capabilities to reach employees outside of work.
    - More than two-thirds (69%) have systems in place that enable most employees to work from home or remote locations; about half (45%) 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.** Three-fourths (75%) of executives indicate that their IT budgets for 2010 are the same or higher than the previous two years; 42% indicate the budgets are about the same, and 33% indicate the budgets are higher. Only one-fifth (20%) indicates their IT budget for 2010 is lower than in the previous two years.
- **Investment in new technologies will continue in 2010.** Eight out of 10 (79%) executives indicate that their companies are investing in new technologies in 2010.
    - Executives most frequently mention that they will be investing in virtualization (29%), cloud computing (28%), unified communications (20%) and mobile applications (18%).

Business Continuity Plans

- **Business continuity planning is seen as a "priority" by the vast majority (84%) of IT executives in the San Francisco/San Ramon area**. More than half (56%) indicate it has always been a priority for their business, and almost three out of 10 (28%) indicate it has become a priority in recent years due to natural disasters, security and terrorist threats.

    - Only one out of seven (16%) executives indicates business continuity is "not a priority."

- **The vast majority (81%) of these executives indicate their companies have a business continuity plan.** Following are specific details about the plans.

    - Executives most frequently indicate that the business unit in charge of managing
      the business continuity plan is the IT Department (31%), followed by the CIO/CTO (29%) and the CEO/CFO (12%).

    - Concerning methods for communicating the specifics of the business continuity plan to employees, one-third (32%) indicates the information is cascaded from senior leadership, while four out of ten (42%) indicate it is communicated through broad, generic communications to all employees.

    - Two-thirds (64%) indicate their companies implement specific protective actions when the federal or state government issues an alert for an impending disaster.

    - A majority (52%) of these companies have had their business continuity plans fully tested in the past 12 months. Only 3% indicate that their plans have never been tested.

- Two-fifths (40%) indicate that testing includes all locations worldwide.

- Half (49%) 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 (67%) consider the use of managed or outsourced capabilities as part of their business continuity plan.

- Six out of 10 (62%) 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.

  - Three out of four (79%) indicate that employee use of mobile devices plays a major/minor role in the business continuity plan; 39% indicate mobile devices play a major role.

  - Half (54%) indicate that their companies have virtualized the computing infrastructure.

  - Four out of ten (42%) have implemented a business continuity plan for that virtualized infrastructure.

- Three out of 10 (29%) indicate that satellite communications are part of their company's communications network.

  - Satellite communications are used for communications in general (8%), disaster communications (6%), as alternatives to cell phones (4%) and international communications (4%).

  - Three out of 10 (31%) executives indicate that their company has invoked its business continuity plan. Reasons for invoking the plan most frequently involve:

    - Power outages at facilities (23%)
    - Extreme weather (15%)
    - IT failures (14%)

- **The need for a plan of action and backup systems are important lessons learned.** Almost half (47%) 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 (16%).

Security Threats

- **A majority (58%) of these companies provide employees with access to social networking tools.**

  - One-fourth (26%) indicates that social networking is generally accepted and widely used, while three out of 10 (28%) 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. More than half (56%) are somewhat concerned, and one-fourth (26%) are very concerned.

  - A similar proportion (76%) is concerned about the increasing use of mobile networks and devices and their impact on security threats. More than half (56%) are somewhat concerned, and one-fifth (20%) are very concerned.

- **Overall, the threat that poses the biggest risk to security is hacking (27%).** Other perceived threats include an internal accident (12%) and internal sabotage (11%).

- 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 sites and none view mobile networks as the biggest security risks.

Communicating During Natural Disasters

- **Most (77%) executives indicate their companies have prioritized and set target recovery times for each of their key business processes.**
  - One-fifth (19%) has not prioritized and set recovery times.
- **Seven out of ten (73%) executives indicate that they have special arrangements for communicating with key executives in the event of a natural disaster.**
  - A similar proportion (77%) has e-mail or text messaging capabilities to reach employees outside of work.
  - Seven out of 10 (69%) have systems in place that enable most employees to work from home or remote locations; a majority (45%) have automated calling systems to reach employees by telephone or cell phone outside of work.

Methodology

The following results are based on an online survey of 108 Information Technology (IT) executives in the San Francisco/San Ramon metropolitan area. 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) in the San Francisco/San Ramon DMA (Designated Market Area). Surveys were obtained between March 5 and March 12, 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 108 participating executives:

- One hundred percent (100%) have primary responsibility for business continuity planning
- Ninety-eight percent (98%) represent companies with revenues in excess of $25 million; 2% represent state/local governments
- Fifty percent (50%) are VPs/Managers/Directors of IT or IS; 21% are the CIO, CTO, CFO, CEO or COO
- Seventy-two percent (72%) represent companies with locations outside of the United States
- Executives represent 16 major industry areas (besides state/local government)