Business Continuity 2010
Philadelphia/Pittsburgh

2010 AT&T Business Continuity Study

Philadelphia/Pittsburgh Results

Key Findings

IT Plans for 2010

- **IT budgets for 2010 are about the same or higher than those of the previous two years.** Seven out of ten (72%) 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.** Two-thirds (66%) of executives indicate that their companies are investing in new technologies in 2010.

Business Continuity Plans

- **The vast majority (81%) of executives in Philadelphia/Pittsburgh indicate their companies have a business continuity plan.**

  - Half (54%) of these executives 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.

  - Four out of ten (39%) 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 (57%) consider the use of managed or outsourced capabilities as part of their business continuity plan.

  - Six out of 10 (59%) include their wireless network capabilities as part of their business continuity plan.

Security Threats

- **Half (49%) of these companies provide employees with access to social networking tools.**

  - Most (75%) executives are concerned about the increasing use of social networking capabilities and its impact on security threats.

  - A similar proportion (78%) 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 (32%).**

Communicating During Natural Disasters

- **Two-thirds (66%) of Philadelphia/Pittsburgh executives indicate their companies have prioritized and set target recovery times for each of their key business processes.**

- **The vast majority (81%) indicates that they have special arrangements for communicating with key executives in the event of a disaster.**

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

- Three-fourths (77%) have systems in place that enable most employees to work from home or remote locations; half (53%) 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.** Seven out of ten (72%) executives indicate that their IT budgets for 2010 are the same or higher than the previous two years; 41% indicate the budgets are about the same, and 31% indicate the budgets are higher. One-fourth (23%) indicates their IT budget for 2010 is lower than in the previous two years.

- **Investment in new technologies will continue in 2010.** Two-thirds (66%) of executives indicate that their companies are investing in new technologies in 2010.

  - Executives most frequently mention that they will be investing in virtualization (22%), cloud computing (18%), hosted services (17%), unified communications (17%) and digital media solutions (13%).

Business Continuity Plans

- **Business continuity planning is seen as a "priority" by seven out of ten (70%) IT executives in Philadelphia/Pittsburgh**. Half (53%) indicate it has always been a priority for their business, and one-fifth (17%) indicates it has become a priority in recent years due to natural disasters, security and terrorist threats.

  - More than one-fourth (27%) of the 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 these plans.

  - Executives most frequently indicate that the business unit in charge of managing the business continuity plan is the IT Department (27%) or the CEO/CFO (27%) followed by the CIO/CTO (20%).

  - Concerning methods for communicating the specifics of the business continuity plan to employees, one-third (36%) indicates the information is cascaded from senior leadership, and another one-third (33%) indicates it is communicated through broad, generic communications to all employees.

  - More than half (54%) 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 8% indicate that their plans have never been tested.

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

  - Four out of ten (39%) companies require their suppliers and other vendors to have a business continuity plan in place in order to do business with them.

  - A majority (57%) considers the use of managed or outsourced capabilities as part of their business continuity plan.

  - Similarly, 59% include their wireless network capabilities as part of their business continuity plan.

    - One-third (35%) indicates 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; 33% indicate mobile devices play a minor role.

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

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

  - One-fourth (27%) indicates that satellite communications are part of their company's communications network.

    - Satellite communications are most frequently used for communications in general (5%), disaster communications (4%) and international communications (4%).

  - One-fifth (22%) of executives indicates that their company has invoked its business continuity plan. Reasons for invoking the plan most frequently involve:

    - Extreme weather (16%)

    - Power outages at facilities (14%)

    - IT failures (8%)

- **The need for a plan of action and backup systems are important lessons learned.** Four out of ten (41%) 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 (10%).

Security Threats

- **Half (49%) of these companies provide employees with access to social networking tools.** Half (50%) do not provide such access.

- Only 14% indicate that social networking is generally accepted and widely used, while three out of ten (30%) indicate it is generally accepted but used by only a few.
- Most (75%) executives are concerned about the increasing use of social networking capabilities and its impact on security threats. Half (51%) are somewhat concerned, and one-fourth (24%) is very concerned.
- A similar proportion (78%) is concerned about the increasing use of mobile networks and devices and their impact on security threats. Almost two-thirds (62%) are somewhat concerned, and 16% are very concerned.

- **Overall, the threat that poses the biggest risk to security is hacking (32%).** Other perceived threats include an internal accident (17%); internal sabotage (10%); and customer, partner, or vendor access to internal systems (9%).
  - While executives are concerned about how social networking capabilities and the use of mobile networks and devices may impact security, none view social networking sites and only 1% view mobile networks as the biggest security risks.

Communicating During Natural Disasters

- **Two-thirds (66%) of executives indicate their companies have prioritized and set target recovery times for each of their key business processes.**
  - One-fourth (24%) has not prioritized and set recovery times.
- **Most (81%) 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 (77%) have systems in place that enable most employees to work from home or remote locations; more than half (53%) 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 113 Information Technology (IT) executives in the Philadelphia and Pittsburgh metropolitan areas. 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 Philadelphia and Pittsburgh 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 113 participating executives:

- Seventy-two percent (72%) work for companies in the Philadelphia metropolitan area, and 28% work for companies in the Pittsburgh area
- 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
- Forty-eight percent (48%) are VPs/Managers/Directors of IT or IS; 23% are the CTO, CFO, CEO, COO or CIO
- Sixty-one percent (61%) represent companies with locations outside of the United States
- Executives represent 12 major industry areas (besides state/local government)