Business Continuity 2010:
Midwest Market

2010 AT&T Business Continuity Study

DETROIT (MIDWEST REGION) Results

Key Findings

IT Plans for 2010

- IT budgets for 2010 are about the same or higher than those of the previous two years. Two-thirds (62%) 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. Three-fourths (77%) of executives indicate that their companies are investing in new technologies in 2010.

Business Continuity Plans

- The vast majority (86%) of executives in Detroit indicate their companies have a business continuity plan.

    - Six out of ten (62%) executives indicate their companies implement specific protective actions when the federal or state government issues an alert for an impending disaster.

    - A majority (53%) of these companies have had their business continuity plans fully tested in the past 12 months.

- A plurality (44%) 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 (65%) consider the use of managed or outsourced capabilities as part of their business continuity plan.

- Six out of 10 (61%) include their wireless network capabilities as part of their business continuity plan.

Security Threats

- A majority (55%) of these companies provide employees with access to social networking tools.

  - Most (72%) executives are concerned about the increasing use of social networking capabilities and its impact on security threats.

  - A similar proportion (73%) 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 (19%).

Communicating During Natural Disasters

- Two-thirds (65%) of Detroit executives indicate their companies have prioritized and set target recovery times for each of their key business processes.

- The vast majority (80%) indicates that they have special arrangements for communicating with key executives in the event of a disaster.

  - A similar proportion (81%) has e-mail or text messaging capabilities to reach employees outside of work.

  - Seven out of 10 (70%) have systems in place that enable most employees to work from home or remote locations; almost half

(44%) 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. Two-thirds (62%) of executives indicate that their IT budgets for 2010 are the same or higher than the previous two years; 36% indicate the budgets are about the same, and 26% indicate the budgets are higher. One-third (31%) indicates their IT budget for 2010 is lower than in the previous two years.

- Investment in new technologies will continue in 2010. Three-fourths (77%) of executives indicate that their companies are investing in new technologies in 2010.

    - Executives most frequently mention that they will be investing in virtualization (24%), mobile applications (17%), cloud computing (14%), unified communications (14%), digital media solutions (14%), telepresence (14%) and hosted services (13%).

Business Continuity Plans

- Business continuity planning is seen as a “priority” by three-fourths (76%) of IT executives in Detroit. Half (48%) indicate it has always been a priority for their business, and three out of 10 (28%) indicate it has become a priority in recent years due to natural disasters, security and terrorist threats.
    - One-fifth (22%) of the executives indicates business continuity is “not a priority.”
- The vast majority (86%) 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 (30%), followed by the CEO/CFO (26%) and the CIO/CTO (17%).
    - Concerning methods for communicating the specifics of the business continuity plan to employees, a plurality (43%) indicates the information is cascaded from senior leadership, and one-third (33%) indicates it is communicated through broad, generic communications to all employees.
    - Six out of ten (62%) indicate their companies implement specific protective actions when the federal or state government issues an alert for an impending disaster.
    - A majority (53%) of these 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 (32%) indicates 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.

- Two-thirds (65%) consider the use of managed or outsourced capabilities as part of their business continuity plan.

- Six out of ten (61%) include their wireless network capabilities as part of their business continuity plan.

    - One-third (36%) 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; 40% indicate mobile devices play a minor role.

    - Half (51%) indicate that their companies have virtualized the computing infrastructure.

    - One-third (37%) has implemented a business continuity plan for that virtualized infrastructure.

- Four out of 10 (40%) indicate that satellite communications are part of their company's communications network.

    - Satellite communications are most frequently used for communications in general (21%), data transmission (14%) and international communications (6%).

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

    - Power outages at facilities (20%)
    - IT failures (10%)
    - Extreme weather (10%)

- The need for a plan of action and backup systems are important lessons learned. About half (48%) 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 (10%) and the need for increased backup systems (8%).

Security Threats

- A majority (55%) of these companies provide employees with access to social networking tools. Four out of ten (43%) do not provide such access.
    - One-fourth (26%) indicates that social networking is generally accepted and widely used, while one-fifth (22%) indicates 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 (51%) are somewhat concerned, and one-fifth (21%) is very concerned.
    - A similar proportion (73%) is concerned about the increasing use of mobile networks and devices and their impact on security threats. Half (50%) are somewhat concerned, and one-fourth (23%) is very concerned.
- Overall, the threat that poses the biggest risk to security is hacking (19%). Other perceived threats include an internal accident (16%); internal sabotage (8%); customer, partner, or vendor access to internal systems (7%) and competitor espionage (7%).
    - 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

- Two-thirds (65%) of executives indicate their companies have prioritized and set target recovery times for each of their key business processes.
    - One-fourth (25%) has not prioritized and set recovery times.
- Most (80%) executives indicate that they have special arrangements for communicating with key executives in the event of a natural disaster.

- A similar proportion (81%) has e-mail or text messaging capabilities to reach employees outside of work.

- Seven out of ten (70%) have systems in place that enable most employees to work from home or remote locations; four out of ten (44%) 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 100 Information Technology (IT) executives in the Detroit 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 Detroit DMA (Designated Market Area). Surveys in Detroit 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 100 participating executives:

- One hundred percent (100%) have primary responsibility for business continuity planning
- Ninety-one percent (91%) represent companies with revenues in excess of $25 million; 9% represent state/local governments
- Thirty-six percent (36%) are VPs/Managers/Directors of IT or IS; 15% are the CTO, CFO, CEO or COO
- Sixty-nine percent (69%) represent companies with locations outside of the United States
- Executives represent 11 major industry areas (besides state/local government)