2009 AT&T Business Continuity Study
DETROIT Results

Methodology

The following results are based on an online survey of 100 Information Technology (IT) executives in the Detroit metropolitan areas. The study was conducted by e-Rewards Market Research with companies having total revenues of more than $25 million in the Detroit DMA (Designated Market Area). Surveys in Detroit 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; 14% are the CIO, CFO, CEO, or COO
- 72% 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 lower than those of the previous two years.** A majority (51%) of executives indicate that their IT budgets for 2009 are lower than in the previous two years.

- **While budgets may be decreasing, investment in new technologies continues.** Seven out of ten (70%) executives indicate that their companies are investing in new technologies in 2009.

- **Two-thirds (67%) expect the new U.S. administration to have a positive impact on the IT industry.** One-fourth (25%) thinks the administration will have a major positive impact, while 42% think it will have a minor positive impact.

Business Continuity Plans

- **The vast majority (82%) of Detroit executives 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 (54%) 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.
    - Four out of ten (42%) 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 (62%) consider the use of managed or outsourced capabilities as part of their business continuity plan.
    - Seven out of ten (71%) include their wireless network capabilities as part of their business continuity plan.

Security Threats

- **The majority (55%) of these companies provide employees with access to social networking tools.** Four out of ten (43%) do not provide such access.
- **Three-fourths (77%) of Detroit executives are concerned about the increasing use of social networking capabilities and its impact on security threats.** The majority (57%) are somewhat concerned, and one-fifth (20%) are very concerned.
- **A similar proportion (74%) is concerned about the increasing use of mobile networks and devices and their impact on security threats.** Half (47%) are somewhat concerned, and more than one-fourth (27%) are very concerned.
- **Overall, the threat that poses the biggest risk to security is hacking (29%).** Other perceived threats include internal sabotage (15%), an internal accident (11%), and customer, partner, or vendor access to internal systems (10%).

Communicating During Natural Disasters

- **Seven out of ten (70%) Detroit executives indicate their companies have prioritized and set target recovery times for each of their key business processes.**

- **The vast majority (81%) of Detroit 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.

    - Eight out of ten (80%) have systems in place that enable most employees to work from home or remote locations; half as many (40%) 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.** A majority (51%) of executives indicate that their IT budgets for 2009 are lower than in the previous two years. One-fourth (23%) indicate that budgets are remaining about the same, while another one-fourth (23%) indicate budgets are higher than in the previous two years.

- **While budgets may be decreasing, investment in new technologies continues.** Seven out of ten (70%) 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 (13%), communications upgrades (8%), management software (8%), software upgrades (6%), new servers (6%), virtualization (5%), upgrades to a new Internet system (3%), data warehousing/storage upgrades (3%), and firewall/security upgrades (2%).

Business Continuity Plans

- **Business continuity planning is seen as a "priority" by two-thirds (64%) of IT executives in the Detroit area**. Four out of ten (42%) indicate it has always been a priority for their business, and one-fifth (22%) indicate it has become a priority in recent years due to natural disasters, security, and terrorist threats.

    - One-third (35%) of the executives indicate business continuity is "not a priority."

- **The vast majority (82%) of Detroit 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 (38%), followed by the CEO/CFO (24%).

    - Concerning methods for communicating the specifics of the business continuity plan to employees, 39% indicate is it communicated through broad, general communications to all employees, while 33% indicate the information is cascaded from senior leadership.

    - 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 (54%) 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.

        - More than one-third (37%) indicate that testing includes all locations worldwide.

    - Four out of ten (42%) 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 (62%) consider the use of managed or outsourced capabilities as part of their business continuity plan.

    - Seven out of ten (71%) include their wireless network capabilities as part of their business continuity plan.

        - Four out of ten (43%) indicate that at least 50% of their company's employees use mobile devices.

        - Four out of ten (45%) indicate that employee use of mobile devices plays a major role in the business continuity plan; 32% indicate mobile devices play a minor role.

    - More than one-fourth (28%) of executives indicate that their company has invoked its business continuity plan. Reasons for invoking the plan most frequently involve:

        - Power outages at facilities (18%)
        - IT failures (14%)
        - Extreme weather (11%)
        - Telecommunications failure (8%)
        - Utility outage (8%)

- **The need for a plan of action and backup systems are important lessons learned.** More than one-third (37%) 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 (11%) and the need for increased backup systems (7%).

Security Threats

- **The majority (55%) of these companies provide employees with access to social networking tools.** Four out of ten (43%) do not provide such access.

    - One-fifth (18%) indicate that social networking is generally accepted and widely used, while one-third (33%) indicate it is generally accepted but used by only a few.

- **Three-fourths (77%) of Detroit executives are concerned about the increasing use of social networking capabilities and its impact on security threats.** The majority (57%) are somewhat concerned, and one-fifth (20%) are very concerned.

- **A similar proportion (74%) is concerned about the increasing use of mobile networks and devices and their impact on security threats.** Half (47%) are somewhat concerned, and more than one-fourth (27%) are very concerned.

- **Overall, the threat that poses the biggest risk to security is hacking (29%).** Other perceived threats include internal sabotage (15%), an internal accident (11%), and customer, partner, or vendor access to internal systems (10%).

    - While executives are concerned about how social networking capabilities and the use of mobile networks and devices may impact security, only 4% view mobile networks and 3% view social networking sites as the biggest security risks.

Communicating During Natural Disasters

- **Seven out of ten (70%) Detroit executives indicate their companies have prioritized and set target recovery times for each of their key business processes.**

    - One-fifth (22%) has not prioritized and set recovery times.

- **The vast majority (81%) of Detroit 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.

    - Eight out of ten (80%) have systems in place that enable most employees to work from home or remote locations; half as many (40%) have automated calling systems to reach employees by telephone or cell phone outside of work.