



2009 AT&T Business Continuity Online Study
BALTIMORE/WASHINGTON, D.C. Results
2/18/09

Methodology

The following results are based on an online survey of 101 Information Technology (IT) executives in the Baltimore/Washington, D.C. metropolitan areas. Fifty interviews were conducted in the Baltimore metropolitan area and 51 in the Washington, D.C. metropolitan area. The study was conducted by e-Rewards Market Research with companies having total revenues of more than \$25 million. Surveys in Baltimore/Washington, D.C. 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 101 participating executives:

- All represent companies with revenues in excess of \$25 million
- All have primary responsibility for business continuity planning
- 36% are VPs/Managers/Directors of IT or IS; 23% are the CIO, CFO, CEO, or COO
- 64% represent companies with locations outside of the United States
- Executives represent 16 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 30% indicate budgets are lower than in the previous two years.
- **While budgets may be decreasing, investment in new technologies continues.** Two-thirds (66%) of the executives indicate that their companies are investing in new technologies in 2009.
- **Two-thirds (66%) expect the new U.S. administration to have a positive impact on the IT industry.** One-fourth (26%) thinks the administration will have a major positive impact, while 40% think it will have a minor positive impact.

Business Continuity Plans

- **The vast majority (79%) of Baltimore/Washington, D.C. 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 (51%) of the companies have had their business continuity plans fully tested in the past 12 months.
 - One-fourth (27%) of all companies require their suppliers and other vendors to have a business continuity plan in place in order to do business with them.
 - A majority (54%) consider the use of managed or outsourced capabilities as part of their business continuity plan.
 - Six out of ten (60%) include their wireless network capabilities as part of their business continuity plan.

Security Threats

- **One-third (37%) of these companies provide employees with access to social networking tools.** A majority (60%) do not provide such access.
- **Eight out of ten (80%) are concerned about the increasing use of social networking capabilities and its impact on security threats.** Half (48%) are somewhat concerned, and 32% are very concerned.
- **A similar proportion (78%) is concerned about the increasing use of mobile networks and devices and their impact on security threats.** Half (47%) are somewhat concerned, and one-third (31%) are very concerned.
- **Overall, the threat that poses the biggest risk to security is hacking (33%).** Other perceived threats include an internal accident (13%), internal sabotage (8%), competitor espionage (7%), and DOS attacks (7%).

Communicating During Natural Disasters

- **Two-thirds (65%) of Baltimore/Washington, D.C. executives indicate their companies have prioritized and set target recovery times for each of their key business processes.**
- **The vast majority (85%) of Baltimore/Washington, D.C. executives indicate that they have special arrangements for communicating with key executives in the event of a natural disaster.**

- A similar proportion (87%) has e-mail or text messaging capabilities to reach employees outside of work.
- Three-fourths (76%) have systems in place that enable most employees to work from home or remote locations, and half (50%) 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 30% indicate budgets are lower than in the previous two years. Only about one-fourth (28%) indicate budgets are higher than in the previous two years.
- **While budgets may be decreasing, investment in new technologies continues.** Two-thirds (66%) of 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 (18%), software upgrades (12%), new servers (7%), virtualization (5%), data warehousing/storage upgrades (5%), and upgrades to a new Internet system (4%).
- **Two-thirds (66%) expect the new U.S. administration to have a positive impact on the IT industry.** One-fourth (26%) thinks the administration will have a major positive impact, while 40% think it will have a minor positive impact.

Business Continuity Plans

- **Business continuity planning is seen as a “priority” by three-fourths (77%) of IT executives in the Baltimore/Washington, D.C. area.** Four out of ten (42%) indicate it has always been a priority for their business, and one-third (35%) indicate it has become a priority in recent years due to natural disasters, security, and terrorist threats.
 - Fewer than one out of four (23%) executives indicate business continuity is “not a priority.”
- **The vast majority (79%) of Baltimore/Washington, D.C. 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 (39%), followed by the CEO/CFO (26%).

- Concerning methods for communicating the specifics of the business continuity plan to employees, 37% indicate the information is cascaded from senior leadership, while 36% indicate it is communicated through broad, general communications to all employees.
- Two-thirds (65%) indicate their companies implement specific protective actions when the federal or state government issues an alert for an impending disaster.
- Half (51%) of these companies have had their business continuity plans fully tested in the past 12 months. Only 9% indicate that their plans have never been tested.
 - One-fourth (26%) indicate that testing includes all locations worldwide.
- One-fourth (27%) of all companies require their suppliers and other vendors to have a business continuity plan in place in order to do business with them.
- A majority (54%) consider the use of managed or outsourced capabilities as part of their business continuity plan.
- Six out of ten (60%) include their wireless network capabilities as part of their business continuity plan.
 - Four out of ten (40%) indicate that at least 50% of their company's employees use mobile devices.
 - Four out of ten (44%) indicate that employee use of mobile devices plays a major role in the business continuity plan; 31% indicate mobile devices play a minor role.
- One-fourth (26%) of executives indicate that their company has invoked its business continuity plan. Reasons for invoking the plan most frequently involve:
 - Extreme weather (18%)
 - Power outages at facilities (16%)
 - Floods (12%)
 - IT failures (12%)
 - Telecommunications failure (12%)
 - Fire (12%)
- **The need for a plan of action and backup systems are important lessons learned.** About one-third (31%) 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 (8%) and the need for increased backup systems (5%).

Security Threats

- **More than one-third (37%) of these companies provide employees with access to social networking tools.** A majority (60%) do not provide such access.
 - One-fifth (19%) indicate that social networking is generally accepted and widely used, while 16% indicate it is generally accepted but used by only a few.
- **Most (80%) executives are concerned about the increasing use of social networking capabilities and its impact on security threats.** Half (48%) are somewhat concerned, and one-third (32%) are very concerned.
- **A similar proportion (78%) is concerned about the increasing use of mobile networks and devices and their impact on security threats.** Half (47%) are somewhat concerned, and about one-third (31%) are very concerned.
- **Overall, the threat that poses the biggest risk to security is hacking (33%).** Other perceived threats include an internal accident (13%), internal sabotage (8%), competitor espionage (7%), and DOS attacks (7%).
 - While executives are concerned about how social networking capabilities and the use of mobile networks and devices may impact security, only 6% view social networking sites and 3% view mobile networks as the biggest security risks.

Communicating During Natural Disasters

- **Two-thirds (65%) of Baltimore/Washington, D.C. 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.
- **The vast majority (85%) of Baltimore/Washington, D.C. executives indicate that they have special arrangements for communicating with key executives in the event of a natural disaster.**
 - A similar proportion (87%) has e-mail or text messaging capabilities to reach employees outside of work.
 - Three-fourths (76%) have systems in place that enable most employees to work from home or remote locations, and half (50%) have automated calling systems to reach employees by telephone or cell phone outside of work.