point_of_view

business_continuity

Riding the Storm

An AT&T and Cisco Systems survey and white paper in cooperation with The Economist Intelligence Unit

Preface

AT&T and Cisco Systems, Inc. are grateful for the support of the Economist Intelligence Unit in helping to produce this report, which explores how companies approach business continuity planning and is based on the following research activities:

- *The Economist Intelligence Unit conducted a wide-ranging global survey of 240 senior executives about their organisations' business continuity planning.*
- *To supplement the survey results, the Economist Intelligence Unit conducted in-depth interviews with experts in business continuity planning and senior executives responsible for ensuring business continuity.*

Executive Summary

Disasters regularly force companies to suspend key business operations, yet many company executives are still doing too little to prepare their companies for the eventuality. A new survey by the Economist Intelligence Unit on behalf of AT&T and Cisco shows widespread neglect of business continuity planning – despite the fact that senior management can now be held liable for any losses that could reasonably be avoided. Failure to put in place well considered business continuity plans aimed at preventing or at least mitigating losses could be very costly in terms of profitability, reputation and market value.

Business continuity planning (BCP) goes beyond disaster recovery, which is geared towards IT and does the job of picking up the pieces after a disaster has hit. BCP ensures that an organisation's entire infrastructure and processes can function in the event of an interruption. An effective business continuity plan must address a range of issues from loss of personnel following a disaster to handling a hostile media. It needs to be integrated into business processes rather than added as an afterthought.

To explore companies' policies towards business continuity, the Economist Intelligence Unit conducted a global survey of 240 executives on behalf of AT&T and Cisco, and carried out in-depth interviews with business continuity professionals. These are some of the key findings:

- *More than a third of companies either have no business continuity plan, or are unsure if they have one. Despite 28% of companies having experienced a full shutdown of key business operations as a result of a disaster, companies are only slowly improving their contingency planning. Only two thirds of the companies surveyed have business continuity plans in place, although this proportion rises to three-quarters among US companies.*

- *Companies are sceptical about their ability to manage threats to key assets. Less than half of the survey participants have confidence in their organisation's ability to fully protect their businesses from threats to digital assets and general infrastructure. Moreover, only a minority of companies are confident in their ability to ensure the safety of their employees in the event of a disaster.*

- *Business continuity plans are not being tested sufficiently. Less than half of companies that had plans in place had tested them in the past year, according to the survey. Without regular testing, business continuity plans are almost worthless.*

- *Insurers are demanding that companies have sound business continuity plans in place. Without a well-developed business continuity strategy, insurers are unlikely to underwrite a company's risk, or may feel compelled to demand very high premiums. By contrast, a well thought-out and comprehensive business continuity plan can help lower insurance premiums.*

- *Dedicated business continuity managers – and departments – will play an increasingly important role. Companies interviewed for this report believe that a deep knowledge of the workings of the organisation – and how information flows through it – is more important than technology expertise when it comes to being an effective business continuity manager.*

Introduction

Disaster recovery often means 'too late' in today's networked business environment. Often, nothing short of continuous operation of key business processes can be tolerated. In certain sectors a system failure lasting only a few minutes can cause lasting damage.

Against this backdrop, the survey conducted by the Economist Intelligence Unit on behalf of AT&T and Cisco aims to assess the progress companies have made in developing robust business continuity solutions. What types of risks and events have companies addressed in their contingency and continuity planning? How regularly do they test the plan? Where do executives perceive the biggest threats to continuity? Which are the hardest to manage?

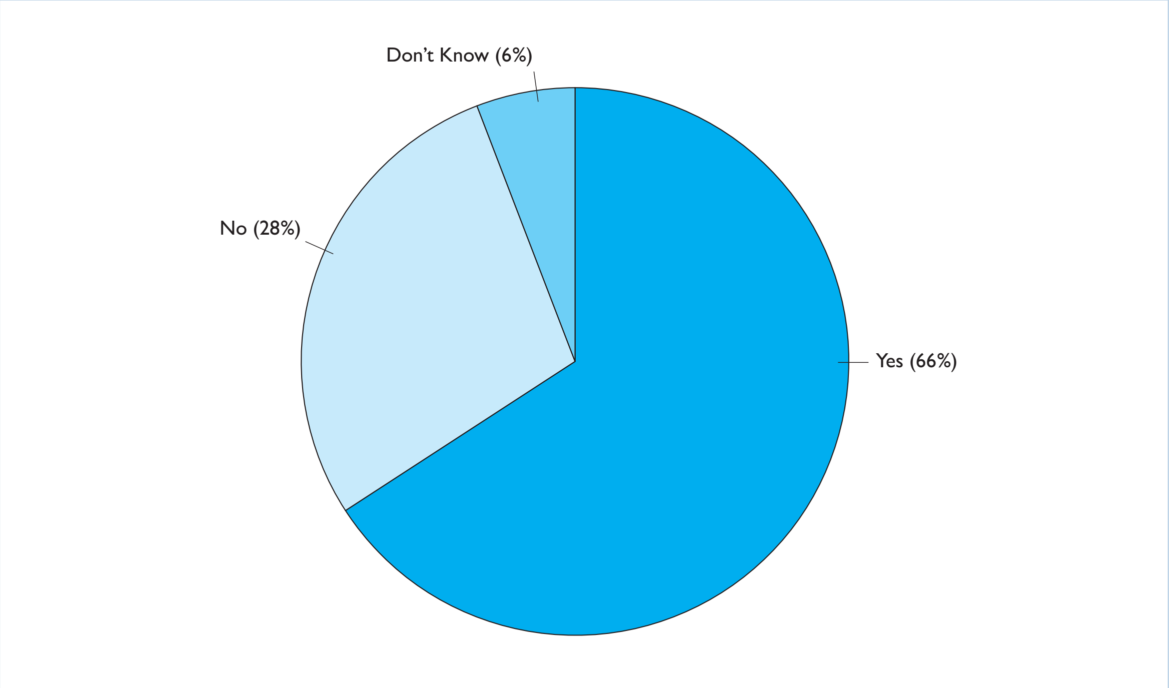
Disaster – more likely that you think

Nearly half of the companies surveyed claim that planning for business continuity has 'always' been a priority for their company, and a further 18% say it has become so because of rising security and terrorist threats. Nevertheless, more than a third either have no business continuity plan, or are not sure whether they have one or not. "There's a lot of room for improvement," says Steve Mellish, chairman of the Business Continuity Institute (BCI), which has some 1,700 members in 45 countries. "Companies have focused on designing IT recovery plans, but that is not enough. They need to put in place business continuity plans to protect themselves against disruption to business processes, damage to key infrastructure and loss of personnel."

Often companies only get cracking on their business continuity plans once they have experienced an interruption to their operations or when customers or business partners demand they make better provisions. Generally, it is hard to persuade executives to invest in business continuity planning, as it tends not to result in tangible operational benefits. This is a risky approach because the likelihood of having to suspend key business operations as a result of a disaster is far from remote. A startling finding of the survey is that more than a quarter of companies have experienced a disaster leading to a full shutdown of key business operations.

On a more positive note, the current regulatory climate may encourage more companies to take the issue of business continuity more seriously in the future. "The biggest driver for spend on business continuity is regulatory compliance," says Ian Bond, a consulting engineer at Cisco. "This is seen by executives as a 'must-spend' area". Bond cites Basel II, internationally agreed regulatory advice for the financial services industries, as one example of a compliance initiative that defines operational risk assessment for banking and financial services businesses, which in turn drives the adoption of continuity solutions.

Does your company have a business continuity plan?



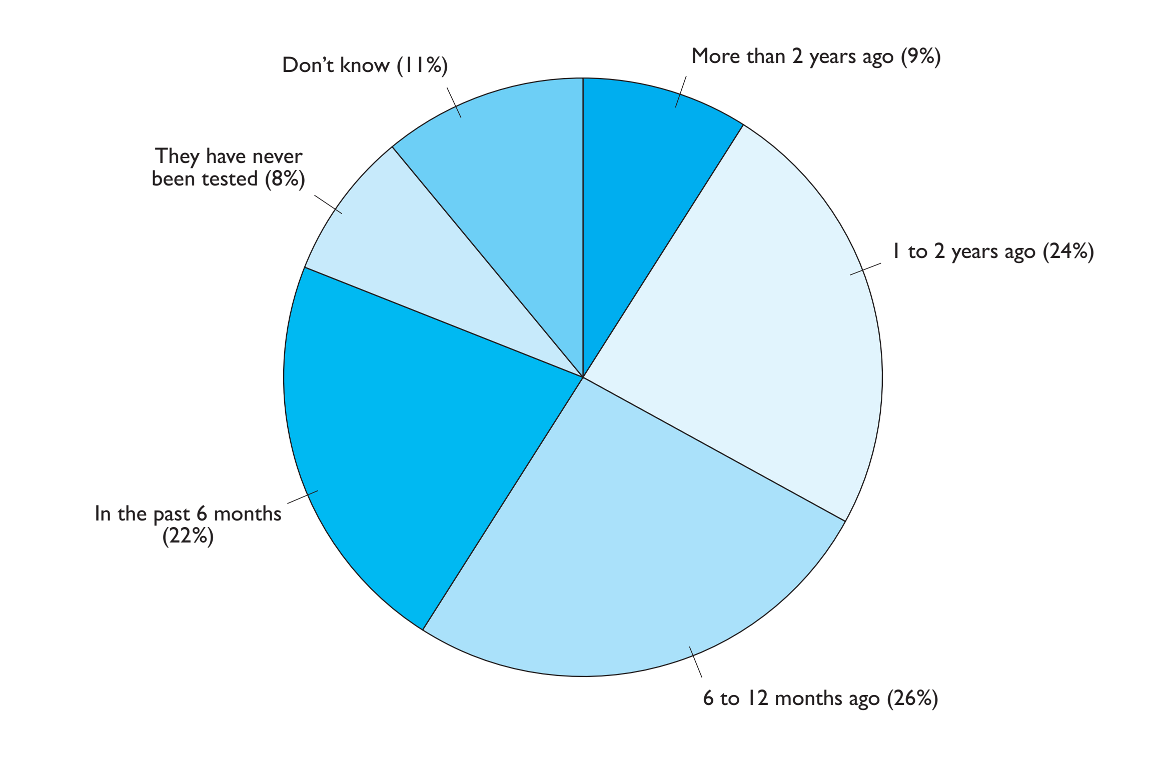
Source: AT&T and Cisco/Economist Intelligence Unit Ensuring Business Continuity March - April 2005

US companies generally have more detailed business continuity planning than their international peers. Events such as the 9/11 attack and increasingly frequent natural disasters have prompted US companies to boost investment. A survey conducted in the US by AT&T last year found that nearly three-quarters of US companies had a business continuity plan in place, and this despite the fact US companies are less likely to face a disaster in the first place. A much lower proportion than the world-wide average – one in five US companies – has suffered a disaster resulting in their organisation having to cease operations for a period of time.

Putting the plan through its paces

US companies are also shown to be more rigorous in their testing of business continuity plans. A business continuity plan is not worth the paper it's printed on unless tested regularly: "No business continuity programme works without tests," says Jeffrey Kuhn, managing director, business continuity, with the Bank of New York (see box). Only 48% of companies in the survey have tested their business continuity plans in the past year.

When did your organisation last fully test its business continuity plans? (answers drawn from respondents with a business continuity plan in place)



Source: AT&T and Cisco/Economist Intelligence Unit Ensuring Business Continuity March - April 2005

The frequency and thoroughness with which companies need to test their plans vary according to the circumstances. For instance, if a test involves moving people or infrastructure once a year to simulate a hurricane and restore operations, it is only necessary to move 20% of the workforce. According to Jerry Shammas, director of AT&T's business continuity and recovery services, "you can still continue operations, and capture what didn't work well." It also depends on the asset: network and data storage tests need to be done more frequently. "IT is constantly changing, and plans, practices and procedures need to be current – if there's been a lot of change you may want to carry out tests twice a year or more," says Shammas.

The Bank of New York – survival strategies

Business continuity at the Bank of New York is critical to the smooth execution of financial services throughout the world. The Bank is based in Manhattan, and had to evacuate more than 8,000 staff following the attacks of 9/11. According to Jeffrey Kuhn, the bank's managing director of business continuity, "it wouldn't have recovered without the business continuity plans made prior to 9/11."

The bank has committed hundreds of millions of dollars to business continuity across its facilities and data centres, and as part of the current reporting structure Kuhn now has a direct line to a senior executive vice-president who in turn reports directly to the chairman. Updates are presented to the board two or three times a year so that the firm is fully apprised of its business continuity capabilities. "It's ingrained in the organisation," says Kuhn.

Since 9/11, the bank has taken a more regional approach to business continuity in preparation for a multi-site event. Kuhn sees geographical diversification as one of the "strongest tools" in the bank's business continuity plans. This approach is combined with high availability technology techniques for critical applications, so back-up equipment is available to take over instantly, using technologies such as data replication and clustering. "This is very expensive," Kuhn says, "but it minimises the risk of data loss and recovery time."

A further lesson from the events of 9/11 has been to separate business operations from IT sites and to move data centres out of New York. Banking operations have been graded into three levels of priority:

- 'Critical': e.g. government clearance and funds-transfer. The bank has three active sites each able to continue operating in the event of the others failing. All three are located in different regions of the USA.

- 'Important': e.g. management fund accounting – these are again split across multiple locations, and can recover in 24 hours.
- 'Routine': this encompasses the rest of the bank. Data is instantaneously copied to another location and staff are briefed to move to back-up locations. Suppliers are on hand to ship in equipment when needed.

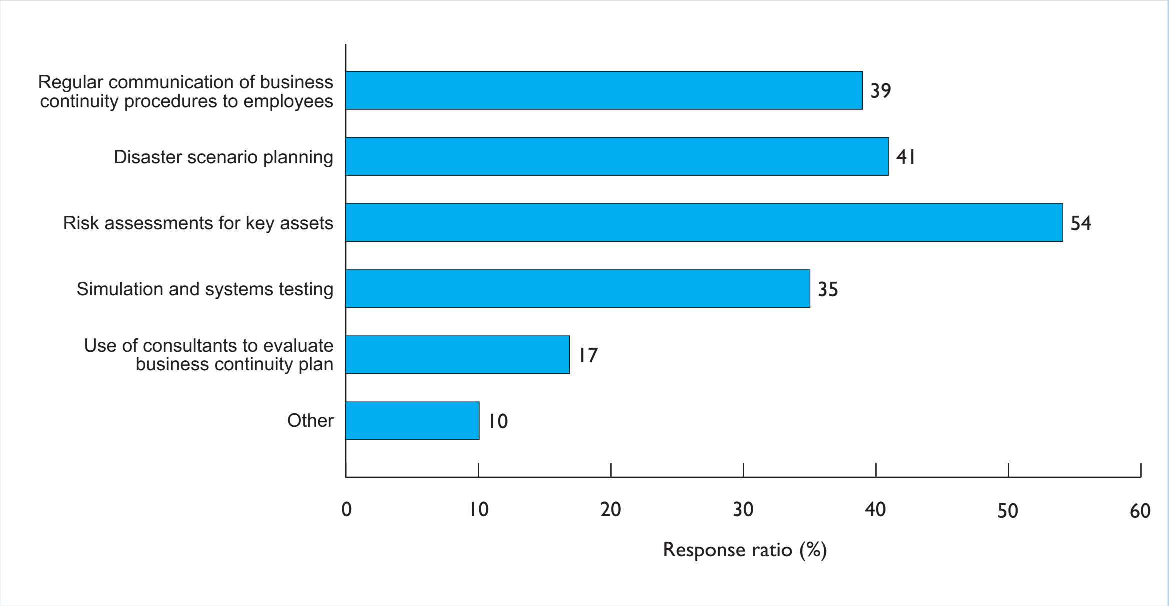
"Geographical diversity is not the easiest thing to accomplish," says Kuhn. It requires staff to be available locally, and to avoid the 'tornado belt', proximity to a nuclear power plant, geographic faults and so on. Altogether in the USA Kuhn believes there are no more than 10 appropriate regions for large-scale data centres. New staff in geographically diverse locations are trained for up to six months, and the redundancy of personnel and additional real estate increase costs by approximately 10-15%.

In this intense environment, the bank performs hundreds of business continuity tests per year. One recent test included relocating 10% of the Manhattan staff during the Republican Party's Convention. Another effective method is 'conference room testing' in which a small percentage of the staff does a simulation, asking questions such as whom to contact, what happens if there is an explosion during evaluation and so on.

The bank has 10 fully dedicated business continuity staff in the USA, a further 10 internationally, and more than 200 co-ordinators world-wide with responsibility for business continuity. The biggest challenges? "If you can't communicate and move a lot of people, you've got a lot of challenges," says Kuhn.

As for the most common methods used to develop and test business continuity plans, risk assessments for key assets are cited by more than half of the companies surveyed and disaster scenario planning by two-fifths. Business continuity procedures are regularly communicated to employees in more than a third of organisations, and a similar proportion conducts simulation and systems testing. Anthony Smyth, a partner with Ernst & Young who leads the business continuity team, says that middle and lower management involvement is often overlooked in organisations: "There's no substitute for those who have to do the work," he says. Furthermore, ensuring that business continuity plans are in place and understood internally is insufficient. According to the BCI's Steve Mellish organisations also need to verify the business continuity plans of their suppliers and partners.

Which of the following methods does your organisation use to develop and test its continuity plans?



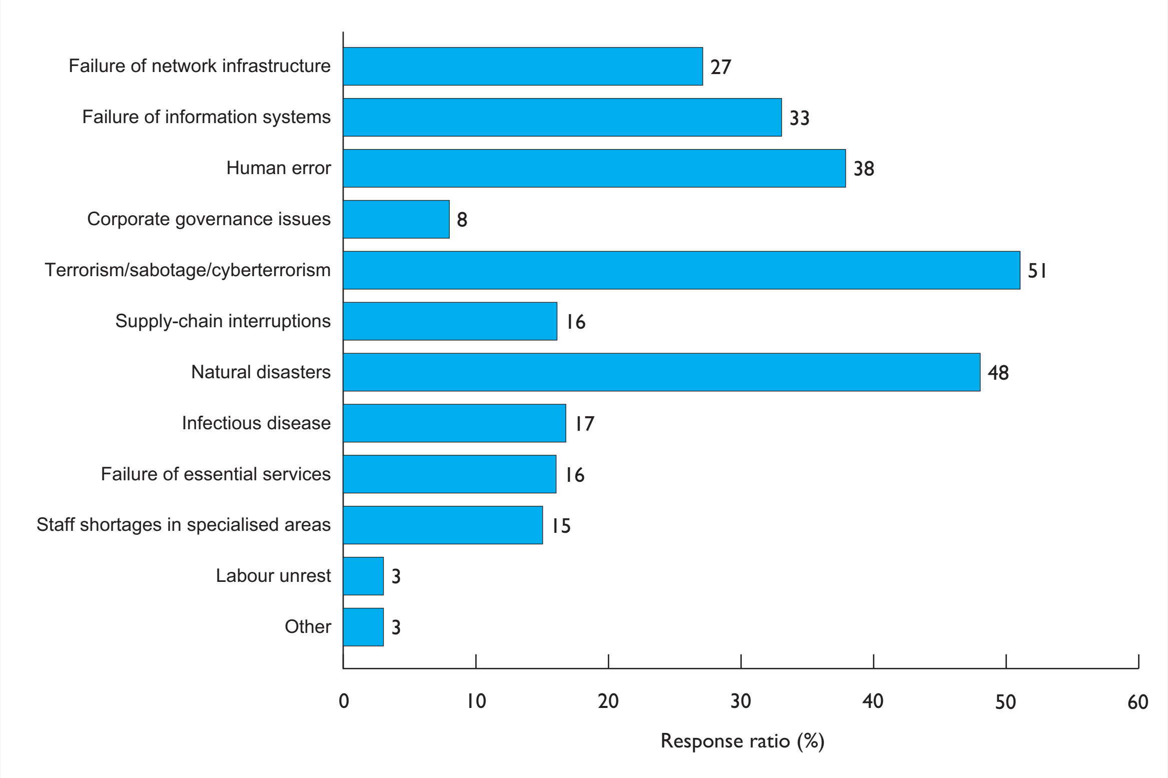
Source: AT&T and Cisco/Economist Intelligence Unit Ensuring Business Continuity March - April 2005

What are they up against?

Of the 28% of companies that have had to suspend key business operations, natural disasters, terrorist attacks and systems failure are cited by over 60% as the cause of the disaster. Other reasons include employee malpractice and cyber attack, cited by 12% and 5% of respondents respectively.

Unsurprisingly, terrorism (including cyber-terrorism) and sabotage are seen by most companies as the hardest of all to predict and protect against. Companies are also especially concerned about their ability to cope with natural disasters such as flooding, hurricanes and even earthquakes, particularly in the US.

Which of the following sources of business continuity risk are the most difficult to anticipate and guard against?



Source: AT&T and Cisco/Economist Intelligence Unit Ensuring Business Continuity March - April 2005

Following the same pattern, network and IT system failures, and general 'human error', are seen as difficult to forecast and protect against – particularly as viruses and the activities of hackers become ever more sophisticated. By contrast, companies are more confident in their ability to cope with interruptions caused by events such as disease, supply chain failures and staff shortages. Only small numbers are concerned about the consequences of sudden labour unrest or a failure of corporate governance.

Faced with these challenges, companies are increasingly outsourcing many aspects of their business continuity plan to a third party provider. Managed services providers can offer data centre facilities and resilient networking solutions which would be pricey to build. "Cost reduction is usually the main driver for outsourcing," says Mike Newman, AT&T's director of global application services. "If you have short recovery time and recovery point objectives, it can be very expensive to implement by yourself."

A further growing trend is for global organisations to set up what Cisco's Ian Bond describes as "inter-regional capabilities". In this instance, a data centre in the USA could maintain business continuity by taking over from the Asia/Pacific site in times of crisis. This trend is partly prompted by the consolidation of regional data centres to cut costs. Organisations become more vulnerable and unable to swap locally between multiple sites. "They need to feel resilient, with a smaller number of larger sites," says Bond.

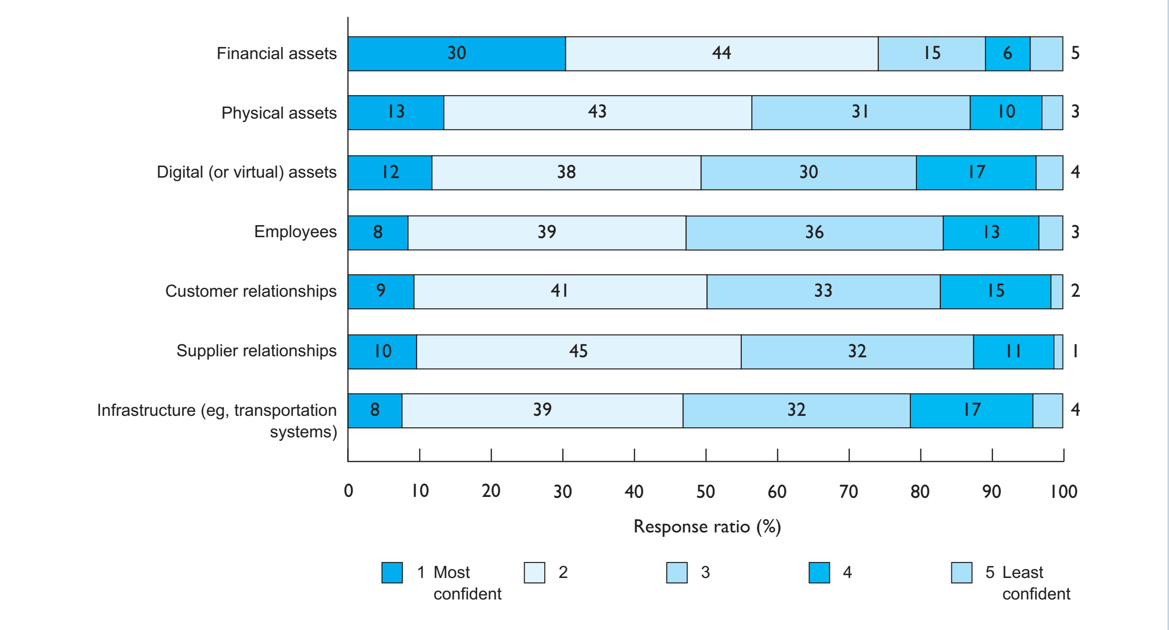
Protecting people

Organisations' confidence in their ability to protect themselves varies considerably by asset. Whereas three quarters of companies are confident they can protect their financial assets effectively, they are much less confident about their other assets. For instance, less than half of them feel sure about their organisation's ability to manage threats to business continuity from a breakdown in their digital (or virtual) assets, or in their infrastructure (e.g. transportation systems). A minority in the report expresses faith in how their company would cope with a graver issue: how well employees would be protected. They also have doubts about the vital areas of customer and supplier relationships, and how effectively these would be handled in the event of a disaster.

A shutdown does not need to be on a grand scale to cause havoc – few businesses on narrow margins can survive for long if their billing information becomes inaccessible. Many companies fall into the trap of covering themselves only for "failures on a grand scale", warns Ernst & Young's Smyth. "They think that because they've planned for catastrophic things, they're also covered for smaller disruptions. But it's the middle ground that causes most problems. That's where the least successful enactment of plans usually is."

Companies also face an ever-narrower margin for error. Whereas in the past they had the luxury of a few hours, or even days, to respond to a disaster, this is no longer the case. For example, even a temporary interruption to online services can generate very damaging publicity, wrecking a company's reputation and market value.

How confident are you of your organisation's ability to manage threats to business continuity in the following areas?

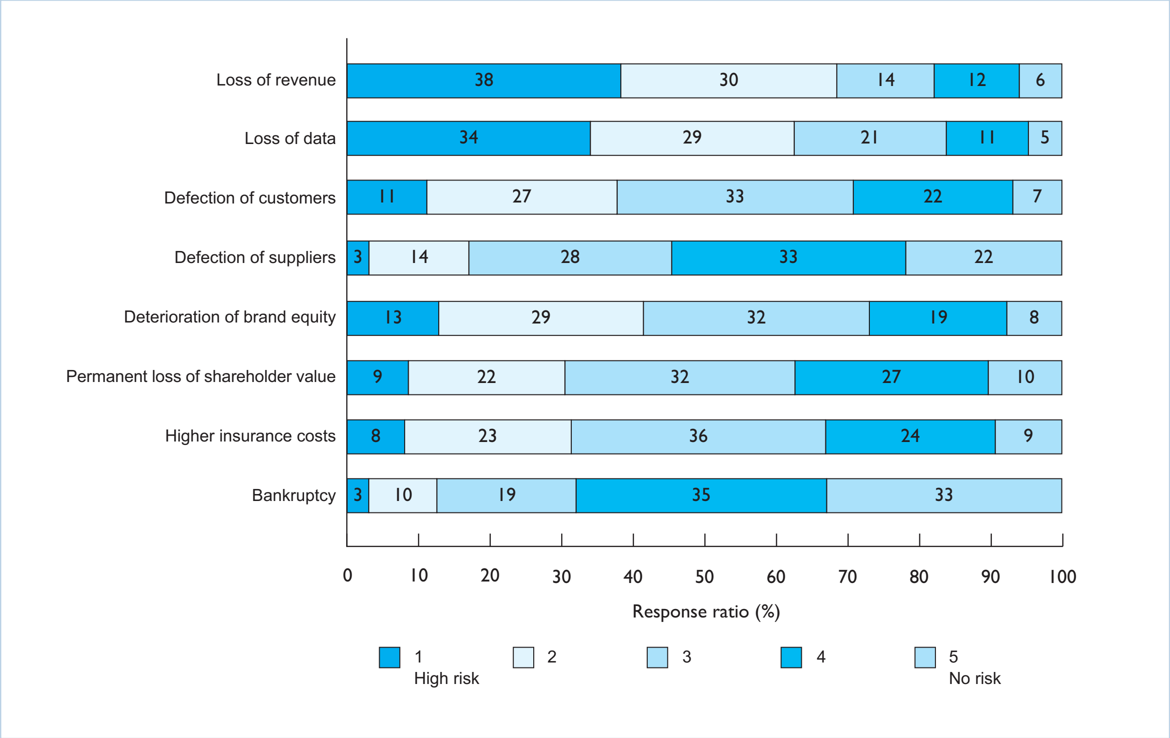


Source: AT&T and Cisco/Economist Intelligence Unit Ensuring Business Continuity March - April 2005

Facing the consequences

The consequences of a breakdown in business continuity can be very serious. Whereas few companies consider bankruptcy as a serious risk, over two-thirds fear loss of revenue and over three fifths loss of data. For example, various estimates put the corporate losses as a result of one virus, the Love Bug, at around $8 billion. Brand damage and defection of customers come lower on the risk scale than might be expected: around 40% regard these as amongst the principal dangers of an interruption to business continuity. As AT&T's Shammas says, "competition is often only a point and click away," for example for the customer of an airline reservation system. "Once they've tried another one, they're likely to stay with it." Less than a third of companies feel, though, that a crisis would permanently damage shareholder value.

What are the principal risks of a breakdown in business continuity for your organisation?



Source: AT&T and Cisco/Economist Intelligence Unit Ensuring Business Continuity March - April 2005

Higher insurance costs are also seen as one of the principal risks associated with business continuity failures. In today's climate, companies have to 'sell' themselves to insurance companies to get coverage. Plans are coming under closer scrutiny from insurance companies and auditors: unless a well-developed business continuity strategy can be demonstrated, the insurer is unlikely to underwrite the risk. The BCI's Mellish points out that business continuity can help to save money by lowering premiums via "self-insurance" – in other words, by reducing the risk in the first place of business interruptions.

Who takes charge?

In the past, responsibility for business continuity has tended to be dropped ad hoc into a variety of different laps. The survey shows that the CFO is most likely to take responsibility for business continuity, but the CIO and chief planning officer are also probable candidates.. Although a growing number of organisations – 9% – now have a dedicated business continuity manager, 20% of respondents to the survey were unsure who is responsible, reinforcing the point that business continuity is still not being taken seriously enough.

This is not the case at Marriott International, a world wide hospitality company (see box). Penny Turnbull, the company's senior director of crisis management and business continuity, is an example of the relatively new breed of dedicated business continuity managers. She came into the role after working on Y2K planning at Marriott. When asked what skills are required, she says: "In general business continuity planning is not rocket science – unless we're talking specifically about the recovery of information systems and data." Common sense is important, as well as good presentation, communications and project management skills. Above all "you need to understand what the organisation does, and what's important in it and to it," she says.

Marriott – Do Not Disturb

In 2000 Marriott International, which operates hotels in 65 different countries and has around 133,000 employees, moved to centralise business continuity planning and to adopt an enterprise-wide approach. A business continuity position was set up within the Risk Management function, which co-ordinates business continuity planning throughout the organisation. "The mainstays are an oversight committee of senior executives, and a corporate policy which provides the planning framework," says Penny Turnbull, senior director of crisis management and business continuity.

There is a reporting process in which each business line and corporate department must certify it is compliant with the business continuity plan at the end of the fiscal year. Turnbull co-ordinates this and reports to the Senior Vice President of risk management who in turn reports to the Executive Vice President of financial information and enterprise risk management. She works closely with the information resources department (IT), which has overall responsibility for planning and implementing a policy to ensure the continuity of technology resources. The group has access to an offsite data processing facility for its critical IT systems, which can be used if disaster strikes.

Marriott is so geographically distributed, with 2,600 hotels round the world, that many risks are beyond its immediate control. "It is not as easy as planning for a single known event," Turnbull adds, "as you may not know what's coming round the corner, as happened with anthrax and SARS. We try to do as much mitigation as possible – not just responding to something that happens – and to minimise the risks." A key strategy is "keeping people aware and ensuring good communication. A situation which seems benign could quickly become more serious." Marriott has an escalating procedure for enacting plans – i.e. minor hurricane damage to a hotel does not necessarily impact at a corporate level.

Plans are required to be tested at least annually, if not more regularly. At the corporate level, 'table-top' exercises are a common testing methodology, usually lasting two hours to "walk through various scenarios". Fire and life safety tests are carried out locally, and a business continuity checklist has to be completed at the end of the year. Business continuity test results come back through the business continuity office, and for unsatisfactory results, tests have to be repeated. Even if there has been a false alarm, those involved are asked to analyse the effects.

Turnbull also sees documentation as crucial to business continuity: "Having a set of plans in someone's head is no good, but neither is a 300-page document." As well as regular tests to see if the plan is effective, an awareness campaign needs to be carried out – in Marriott's case distributed largely over the company's intranet – so people know what their roles are, and what the plans are about. "People need to know what's expected of them." Turnbull has to make sure awareness programmes are running properly and reports to the board on compliance.

An important personal factor is observed: "We've come to an understanding in the company that people shouldn't be afraid to talk about times when things haven't gone according to plan. If there's been an issue, it is important for people to sit down and ask how our procedures can be adapted and improved. Tests are also aimed at identifying areas where we can improve."

Preparing for the unthinkable: a checklist

If handled skilfully, business continuity not only keeps the company afloat during times of crisis, but can also improve its competitive position, and lead to a greater understanding of business processes in the organisation. The checklist below provides tips on how organisations can ensure their business continuity planning is as comprehensive and effective as possible.

- Does your organisation have an up-to-date business continuity plan for its mission critical activities and their dependencies? What can't you afford to lose in order to maintain critical business processes?

- Does the plan define how to revive those activities within a stated time frame? Aiming for 'zero downtime' could be very costly, and inappropriate for several areas of the business.

- Is business continuity adequately funded in your company? It may be less costly than you think, and can be developed gradually. The economy, as well as the handy ubiquity, of high speed IP networking must not be overlooked.

- Who writes up the business continuity plan? If done by IT there is a risk that too much attention will be paid to technology systems at the expense of business processes and people issues.

- Who is ultimately accountable for business continuity? Is the reporting line to that individual clear? Responsibility for business continuity must be a board level issue.

- How regularly are 'fire drills' staged to test business continuity plans, and ensure they are up to speed with recent changes in the organisations?

- Does your plan specify personnel roles and their accountability? Are they clear when they should invoke business continuity plans?

- Does the business continuity plan specify the level of response required, according to the type of emergency?

- How is the plan communicated to staff in the organisation? How do you check that the message has got across?

- How do you tackle the press and media following a crisis? The company's standing can actually increase if the publicity provoked by the crisis is properly managed.

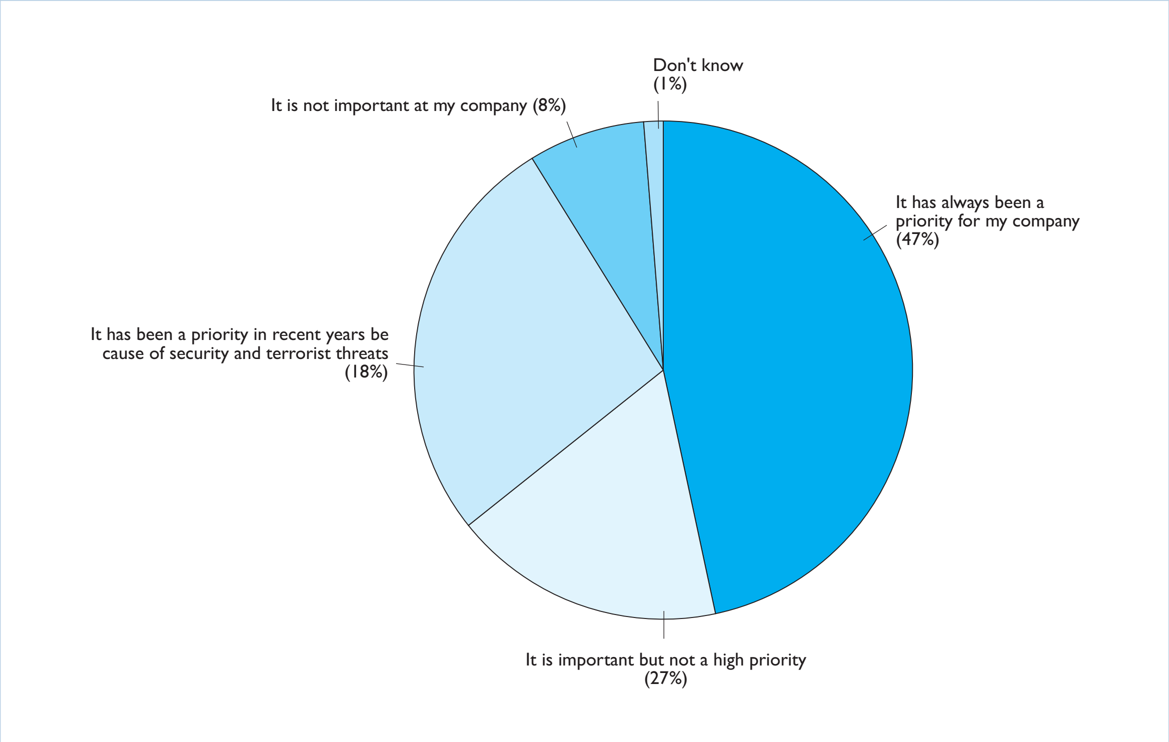
Appendix: 2005 AT&T / Economist Intelligence Unit (EIU)

Survey results

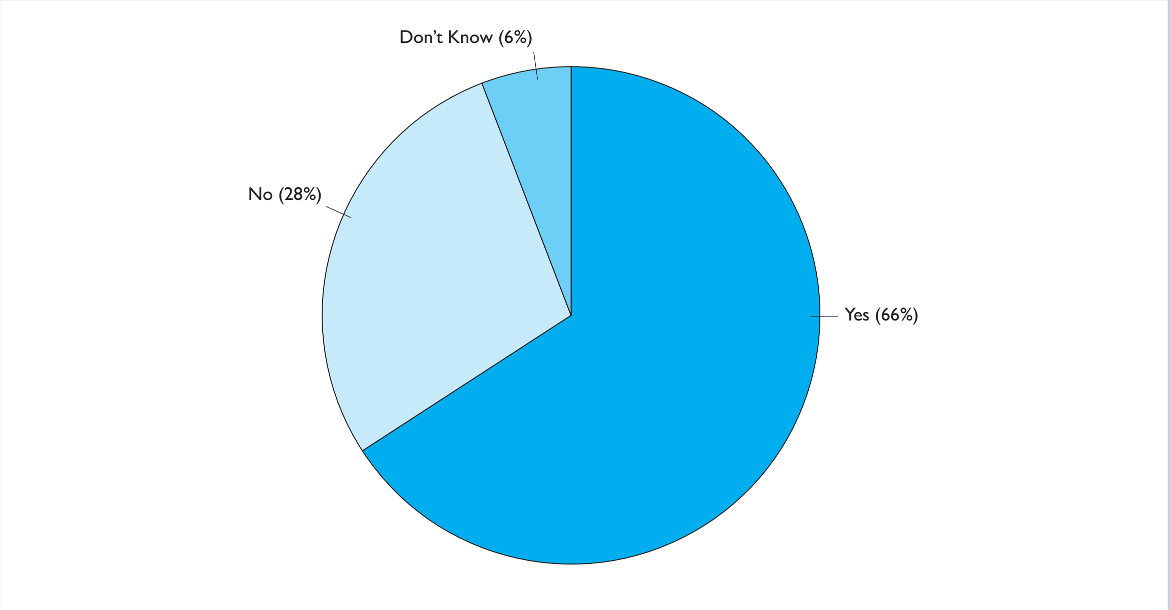
240 executives worldwide participated in an online survey on Ensuring Business Continuity for this whitepaper. Our thanks are due to everyone who participated. Note that answers may not add to 100%, because of rounding or because respondents could give multiple answers to certain questions.

Business Continuity

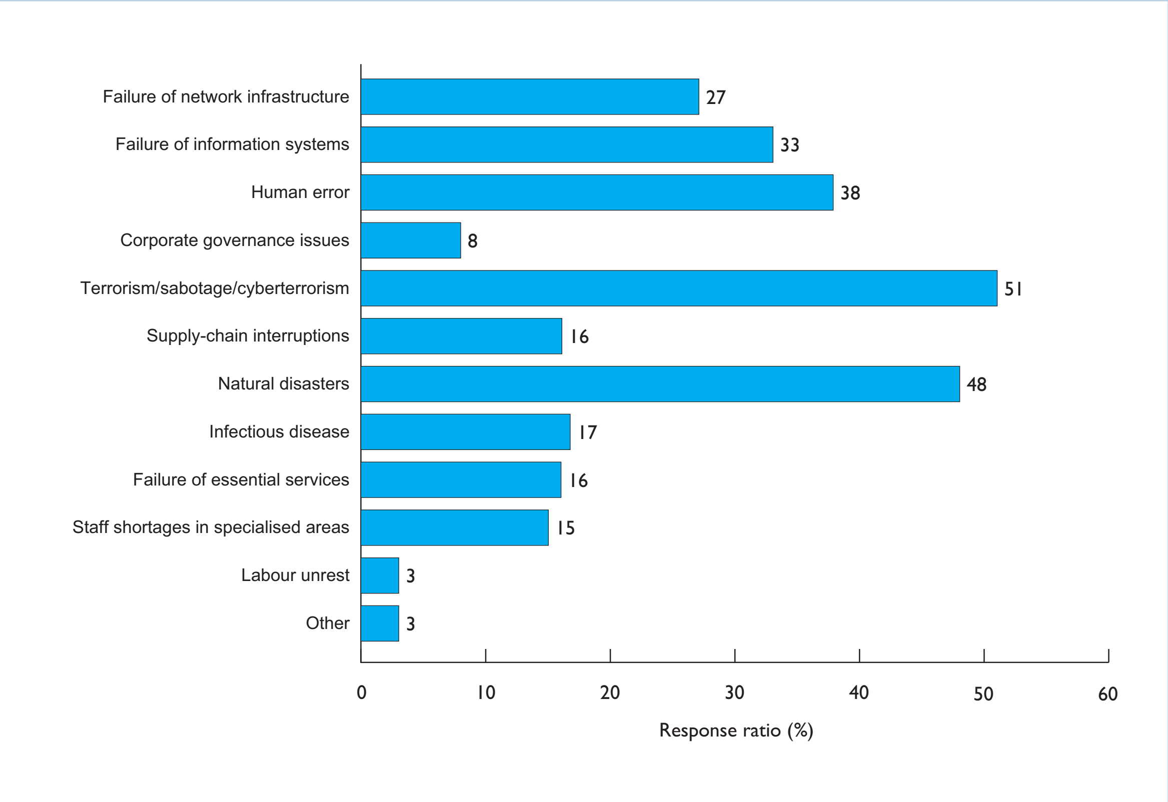
Which of the following statements best describes your company's position on business continuity?



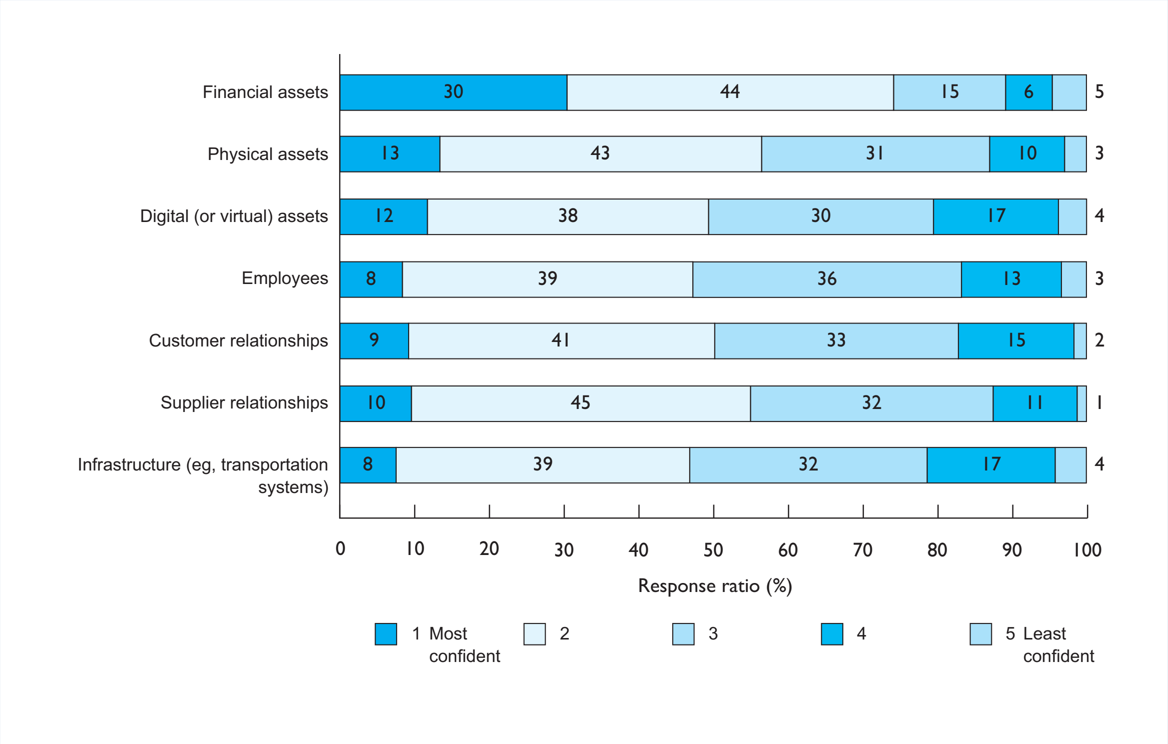
Does your company have a business continuity plan?



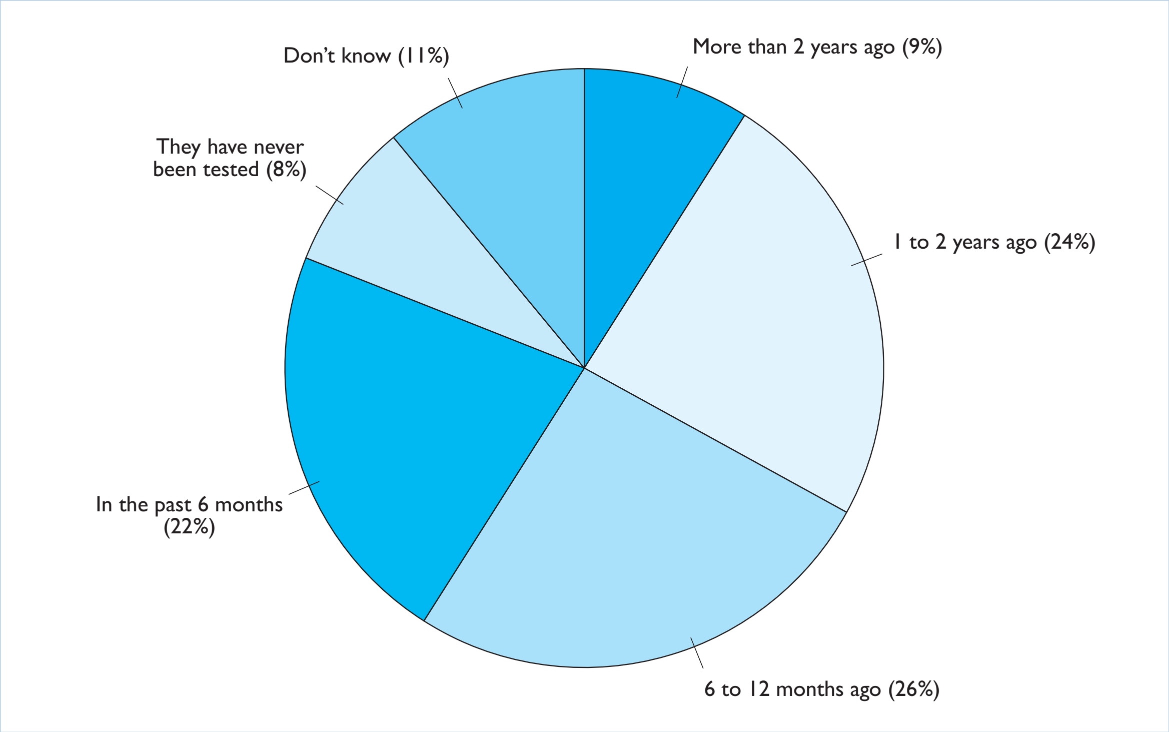
Which of the following sources of business continuity risk are the most difficult to anticipate and guard against?



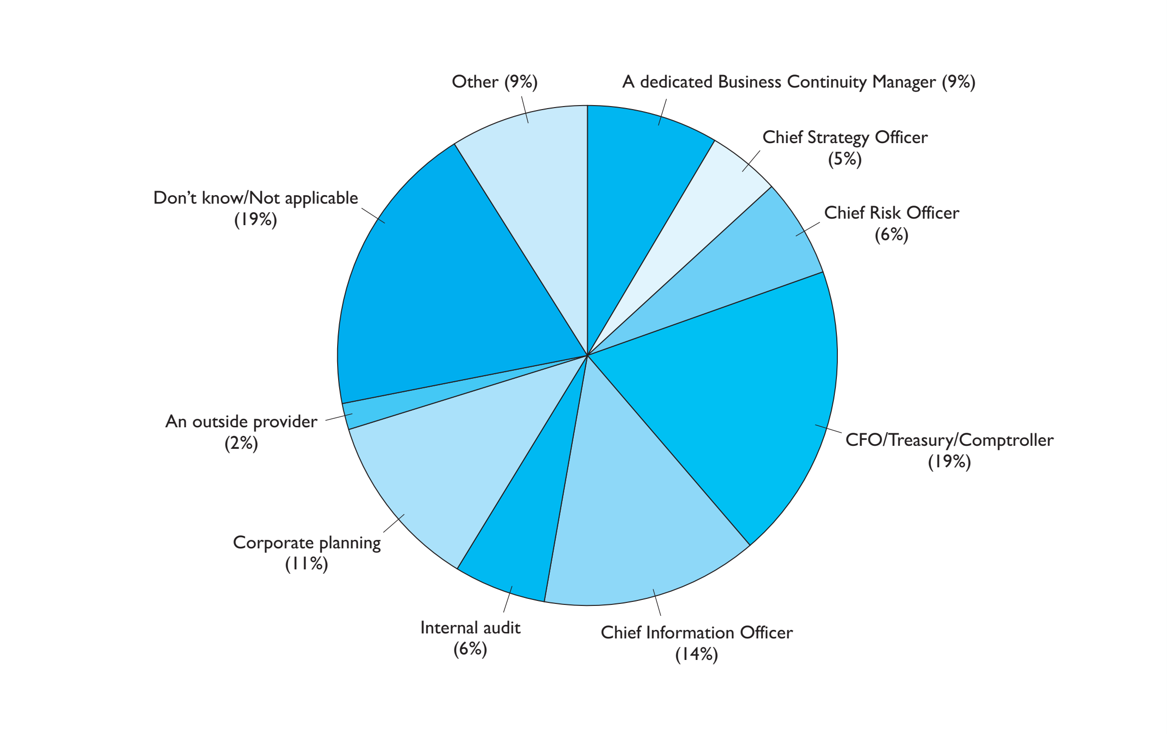
How confident are you of your organisation's ability to manage threats to business continuity in the following areas?



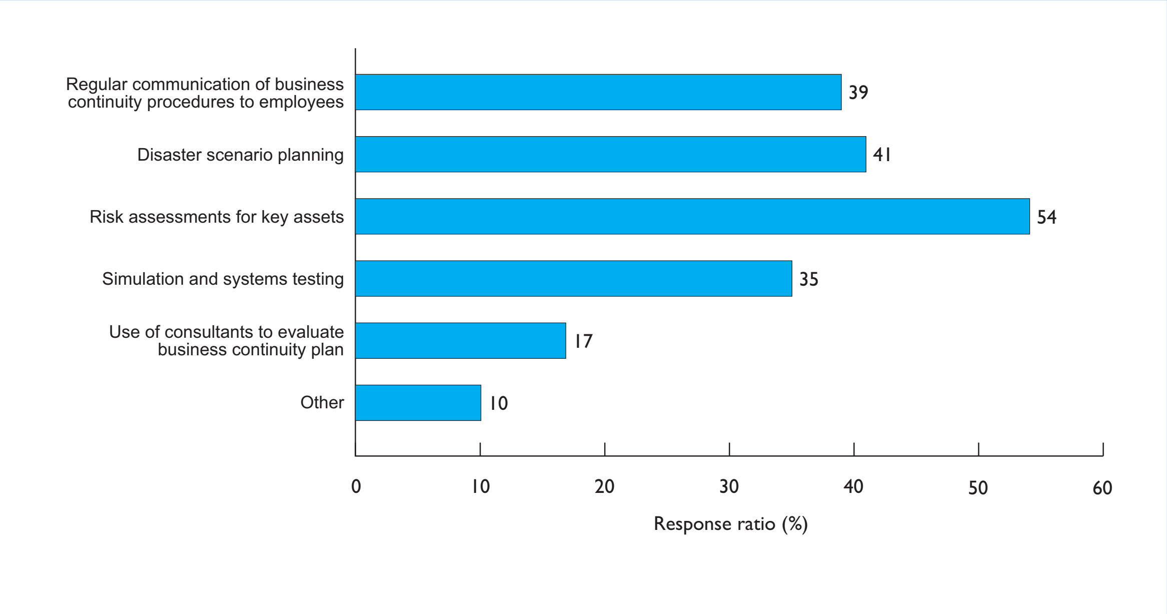
When did your organisation last fully test its business continuity plans? (answers drawn from those respondents that have a business continuity plan in place)



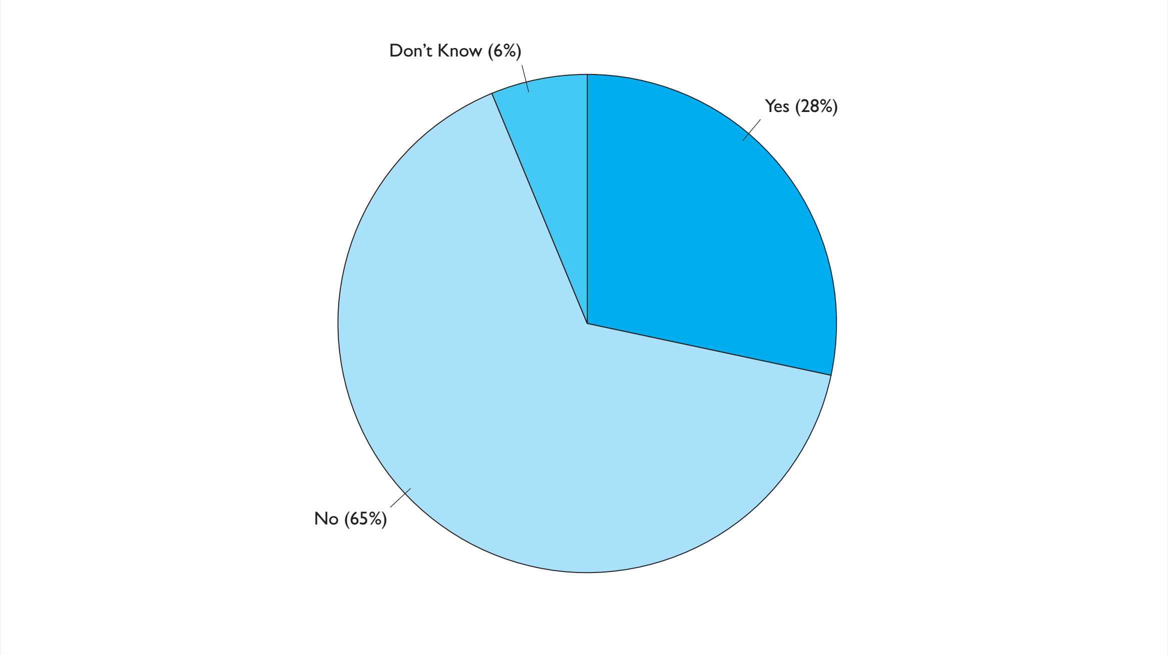
Who is responsible for your organisation's business continuity planning?



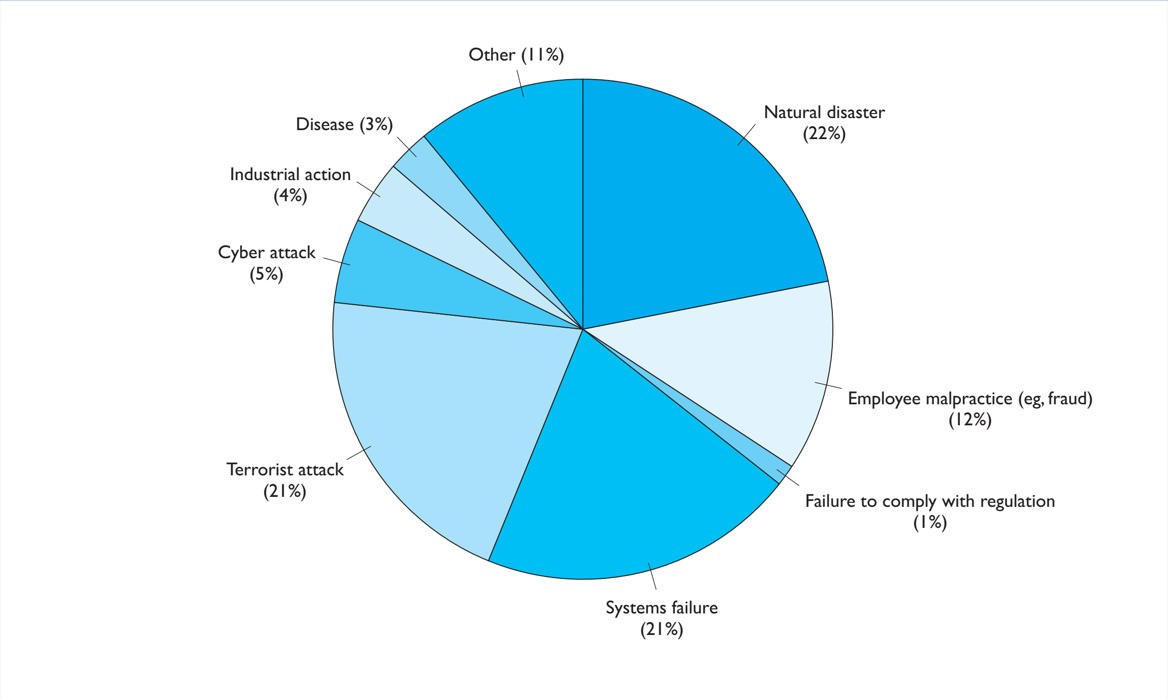
Which of the following methods does your organisation use to develop and test its continuity plans?



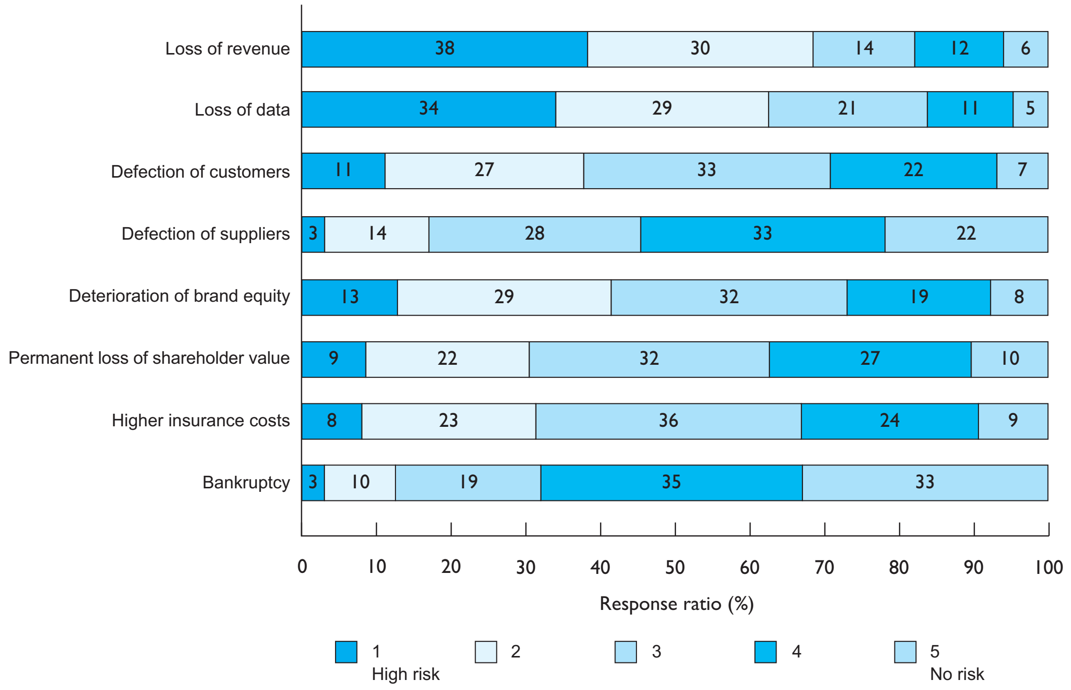
Has your company ever had to suspend key business operations as a result of a disaster?



If you answered "yes" to the question above, what was the disaster?

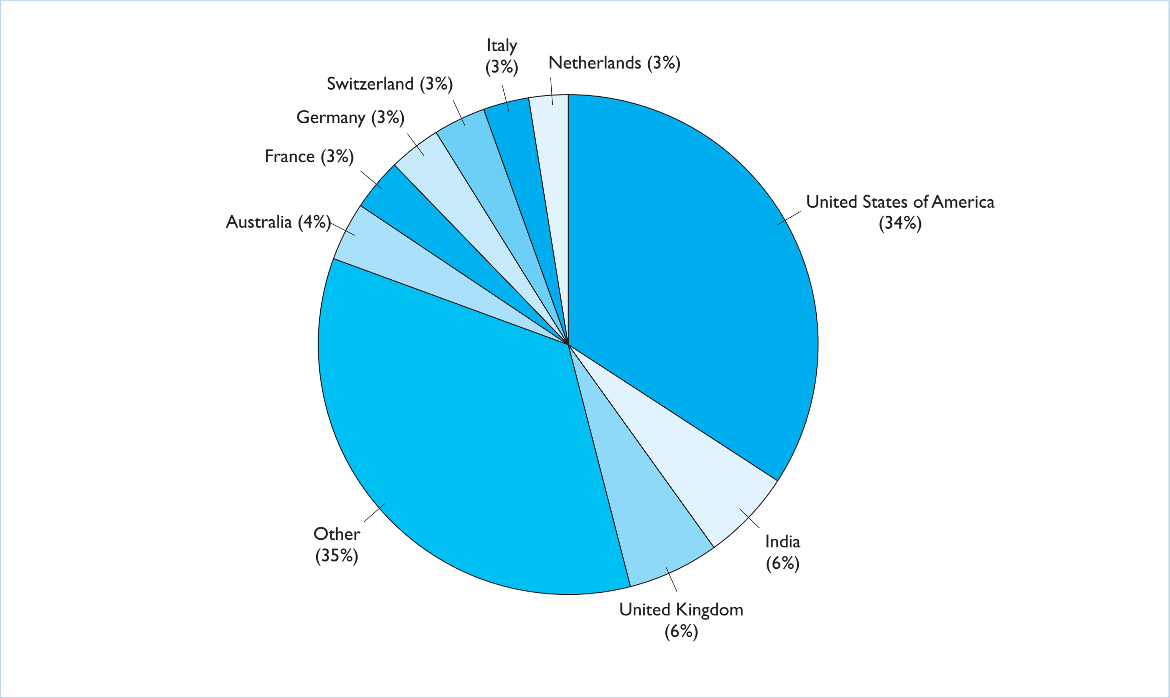


What are the principal risks of a breakdown in business continuity for your organisation?

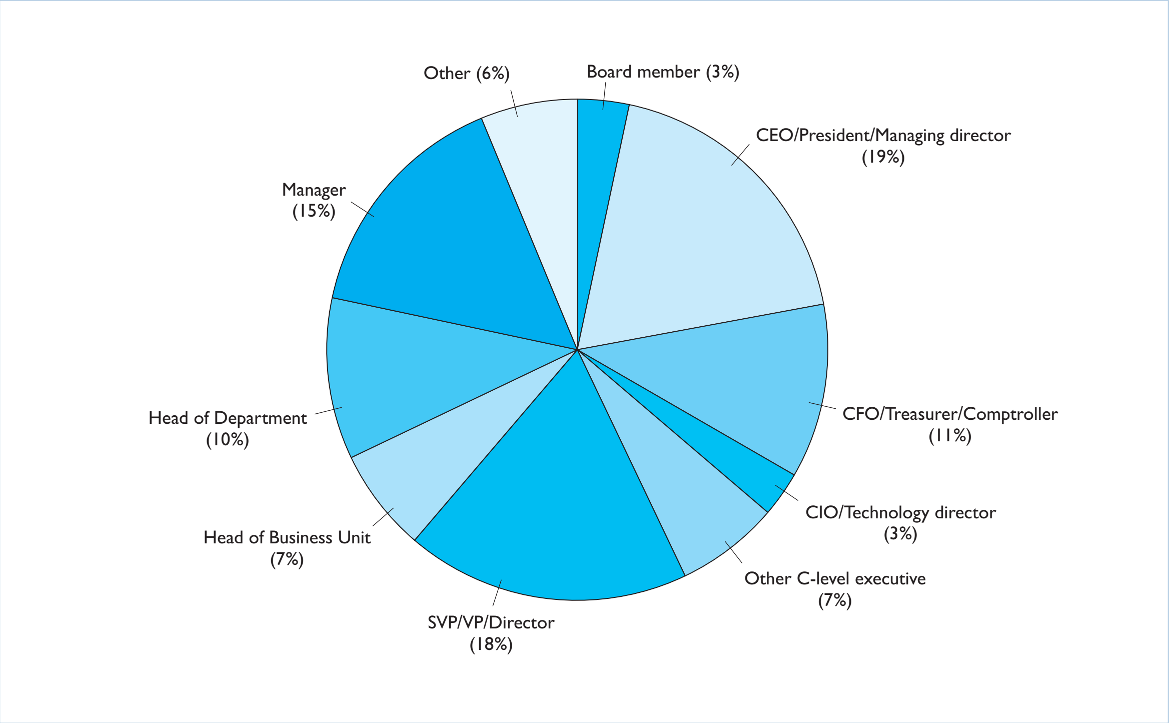


Survey Demographics

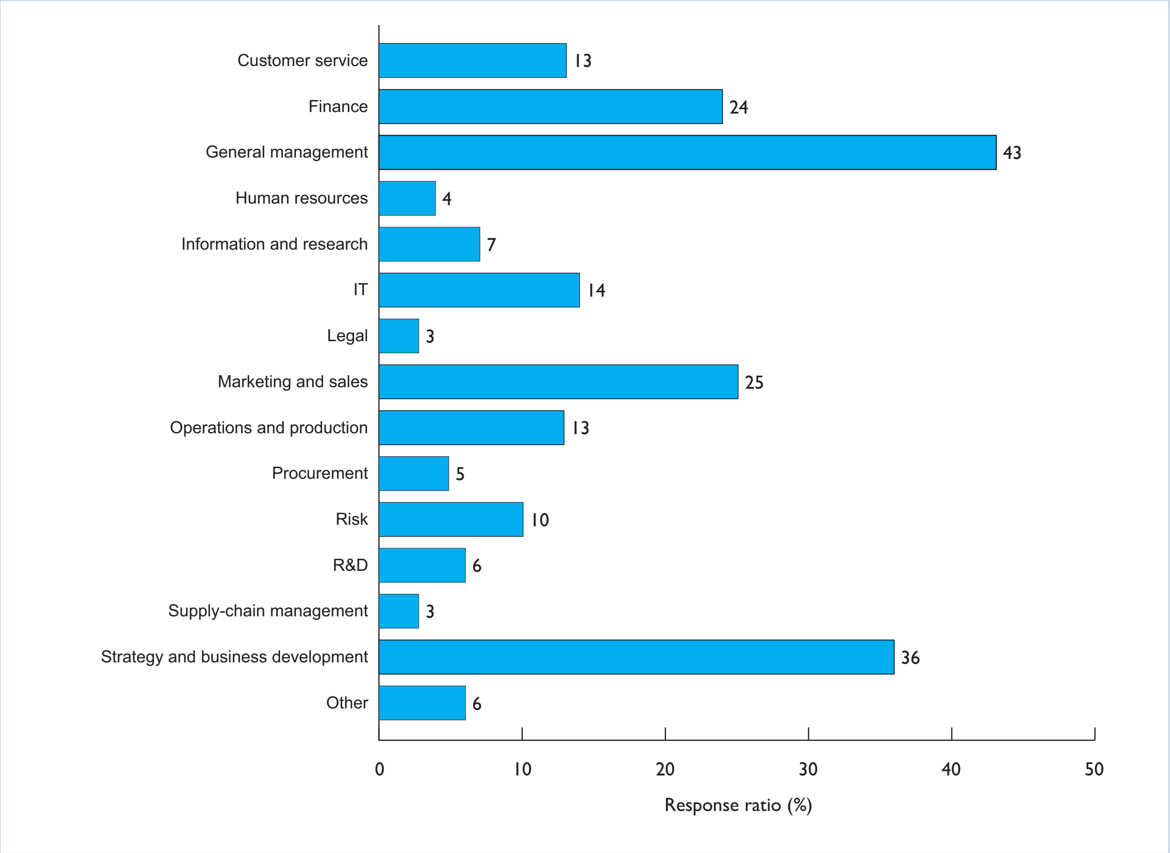
Geographical Region



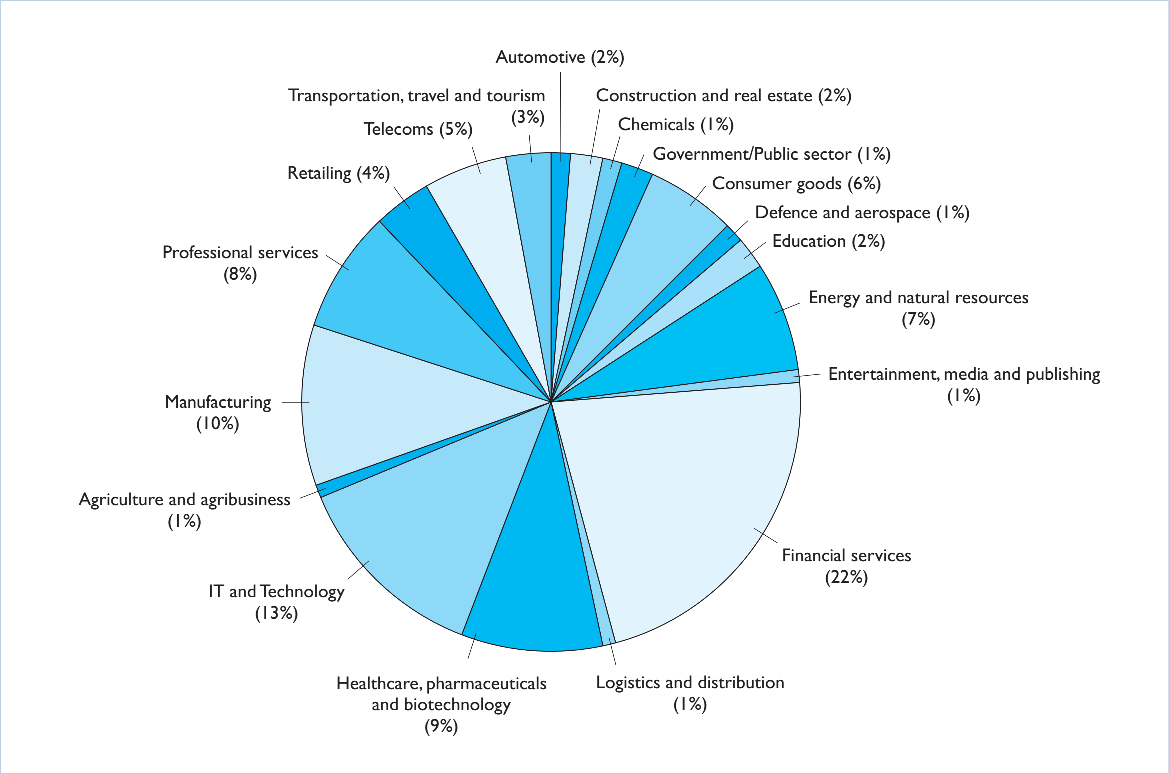
Job Title



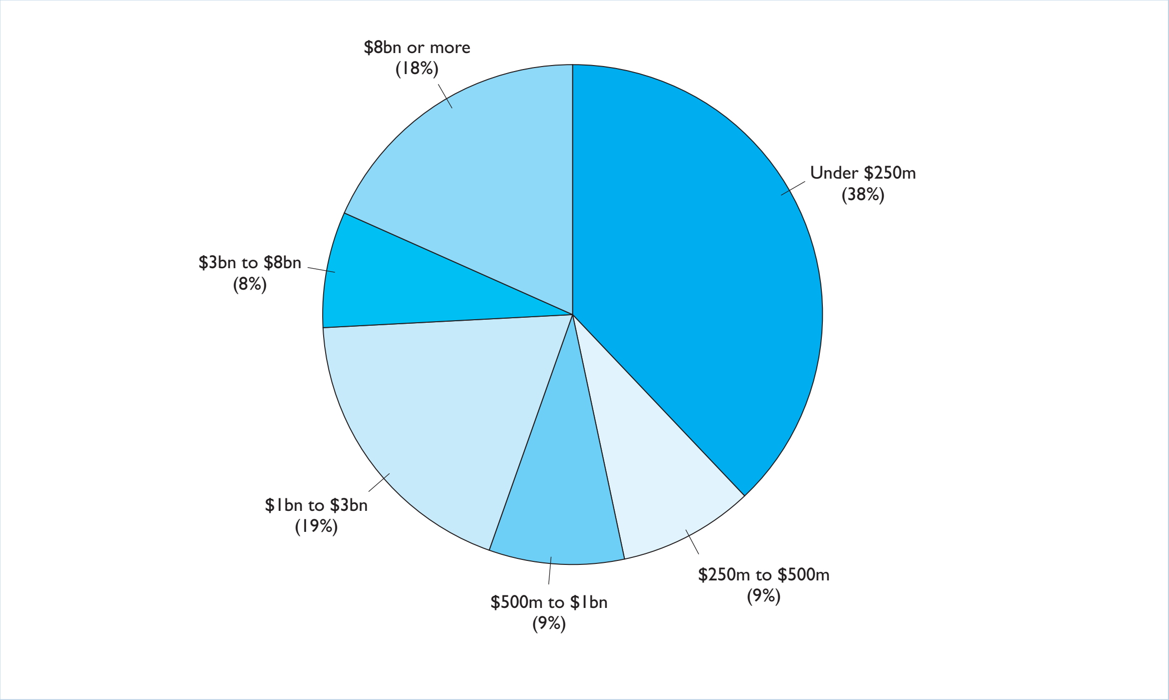
Main Functional Roles



Industry



Annual Revenues in US$



To learn more about AT&T Services, contact your local AT&T representative, or visit our web site at **www.att.com/emea**

AT&T

The world's networking company℠

Cisco Powered

www.att.com/emea

ATT-WP-001-BC
06/2005