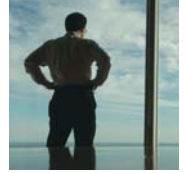


Coming to grips with IT risk

A report from the Economist Intelligence Unit
sponsored by SAP





Preface

Coming to grips with IT risk is an Economist Intelligence Unit briefing paper, sponsored by SAP. The Economist Intelligence Unit bears sole responsibility for this report. The Economist Intelligence Unit's editorial team executed the survey and wrote the report. The findings and views expressed in this report do not necessarily reflect the views of the sponsor. Terry Ernest-Jones was the author of the report and Rama Ramaswami was the editor. Mike Kenny was responsible for layout and design.

Our research drew on a global online survey in October 2006 of 145 senior executives. Our thanks are due to all survey respondents and interviewees for their time and insights.

March 2007



Executive summary

What is the greatest risk to any large business? Most executives would say it is information technology (IT) failure. Companies fear IT collapse more than they do terrorism, natural disasters, financial risk or regulatory constraints—and with good reason, for IT failure can make any business go into a tailspin. IT applications routinely underpin critical processes throughout a company: supply chain management, customer service, invoicing, payroll and regulatory compliance. Businesses have become utterly dependent on their IT systems. If a new web site application crashes or customer records get corrupted, it can be ruinous.

Nonetheless, most companies do not have sound IT risk management processes in place.

Many senior managers still view IT risk merely in terms of security. This perspective is far too narrow: IT risk should encompass possible damage to the full range of IT-related activity, including all aspects of

business continuity and the impact of late-running or under-performing IT projects.

This global survey of 145 senior executives, conducted by the Economist Intelligence Unit on behalf of SAP, aims to gain a deeper understanding of how companies define and mitigate IT risk. The following are some of our key findings:

- **Complexity is largely to blame for current risk levels.** The sheer complexity of IT applications and system architectures is the main source of risk exposure. Our survey reveals, however, that there is a shortage of skilled project managers who can handle unwieldy IT projects.

- **IT risk management structures are largely inadequate.** Only 13% of executives say their company has a comprehensive IT risk management structure in place. Although they believe senior management is aware of the financial risks associated with IT failure, only 11% describe their company's handling of IT risk as "highly effective."

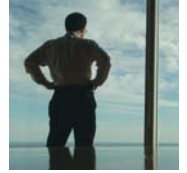
- **Customer service is the area most affected by IT failure.** This results from companies' growing reliance on real-time online interaction. If IT Systems fail, customers are only a click away from another company.

- **Following loss of customers, revenue loss is what executives fear most from IT failure.** When the system is down, customers will buy from other sites. Another feared consequence of IT failure is damage to brand and reputation, especially if customer information is compromised.

- **Unplanned downtime is considered the most damaging risk.** This is much more serious than other hazards such as viruses or the leaking of sensitive company data. The prospect of IT downtime is of particular concern in the manufacturing and financial services sectors.

About our survey

In October 2006 the Economist Intelligence Unit conducted an online survey of 145 senior global executives from a variety of industries on their companies' current and planned strategies for minimizing IT risk. Fifty-seven percent of the respondents are C-level executives. Thirty percent of the respondents are located in Western Europe, 31% in the Asia-Pacific region, 24% in North America, and the remainder in Latin America, Eastern Europe, and the Middle East and Africa. Of the respondents surveyed, 54% report that their organisation's annual revenues are less than US\$500m; 14% report revenues of US\$500m to US\$1bn; 14% post annual revenues of US\$1bn to US\$5bn; 4% report annual revenues of US\$5bn to US\$10bn; and 14% report annual revenues of more than US\$10bn. In addition to the survey, we conducted interviews with senior executives worldwide to get detailed responses and analyses.



● **Risk must be assessed early on.** IT risk and security considerations are usually addressed as an afterthought during major strategic moves such as mergers and acquisitions or outsourcing. Instead, these concerns should be dealt with from the start.

● **Prudent techniques and policies can lower IT project risk.** Many IT projects fail, but companies can take effective action to mitigate risk. The range of initiatives includes prototyping well in advance of the full rollout; using performance metrics to check budget overruns; and establishing channels of communication with senior management to ensure that the project meets changing business requirements.

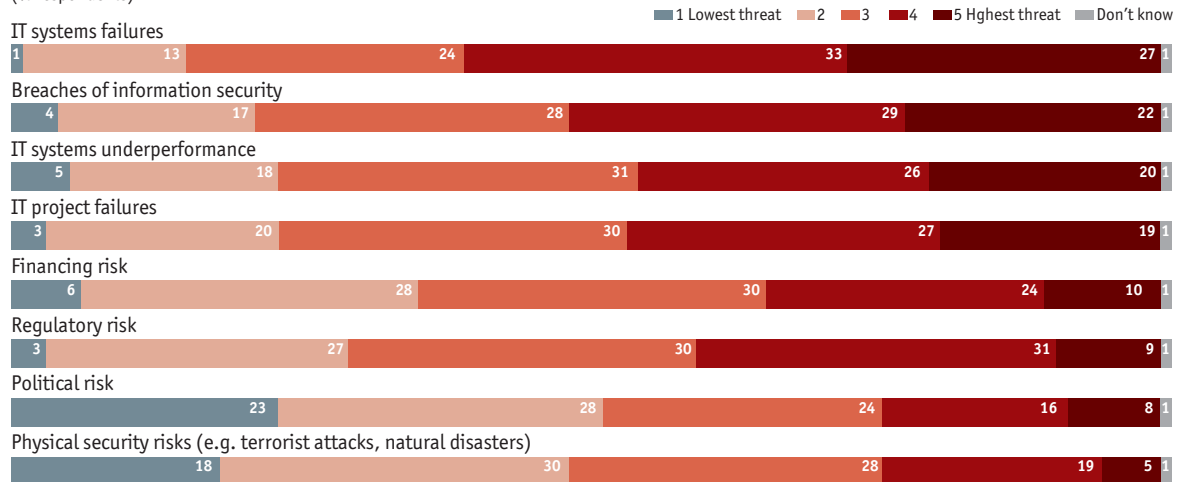


Coming to grips with IT risk

1. How threatening do you think each of the following business risks are to your company's operations?

Rate each on a scale of 1 to 5, where 1 = Lowest threat and 5 = Highest threat.

(% respondents)



Source: Economist Intelligence Unit survey.

Complexity raises risk

Most large companies find themselves in a dilemma. To stay ahead of their competitors, they must expand into new international markets and collaborate with partners across borders. They must introduce new technologies, such as multi-channel CRM for communicating with customers through a variety of media. They may need to merge with or acquire other companies. As a consequence, their IT systems become increasingly complex.

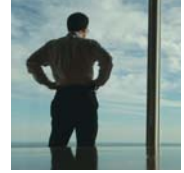
Yet 52% of our respondents feel that the growing complexity of their applications and system architectures has a negative impact and increases the likelihood of IT failure.

This is significantly higher than other factors that might lead to IT breakdown, such as regulatory systems to support data privacy and financial reporting, the expansion of IT outsourcing, and the increased use of wireless networks. Executives worldwide rank IT failure as the greatest risk to their business—far ahead of other factors such as financial risk or regulatory constraint. The threat of terrorism or of natural disaster is not nearly as worrying as

the possibility of IT collapse. This is especially true in the financial services sector and in both Europe and the US. The performance of IT is now central to how business operates, and our survey shows that executives feel that IT systems failure is the highest threat of all to the success of company operations (see chart 1).

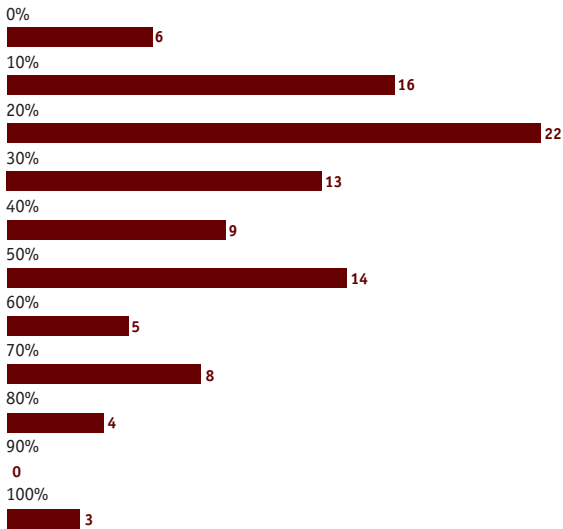
IT systems failure is cited as the greatest business risk by 27% of respondents, 6% more than the next highest risk, breaches in information security (22%). However, in North America, the risk of breaches in information security rank as high as the risk of systems failures (35%). Such events can severely disrupt business and can bring unwelcome attention from the press if personal information from myriads of customers is stolen.

Another potential problem, cited as the greatest risk by 19% of our respondents, is the failure of IT projects, which can entail massive losses. US car giant Ford abandoned an automated purchasing system soon after deployment, losing an estimated \$400 million. UK retailer J Sainsbury ditched a new supply chain system in which it had invested \$530 million. It seems that that the bigger the IT project, the more



8. Approximately what percentage of IT projects undertaken in your company over the past two years have been delivered late or over budget?

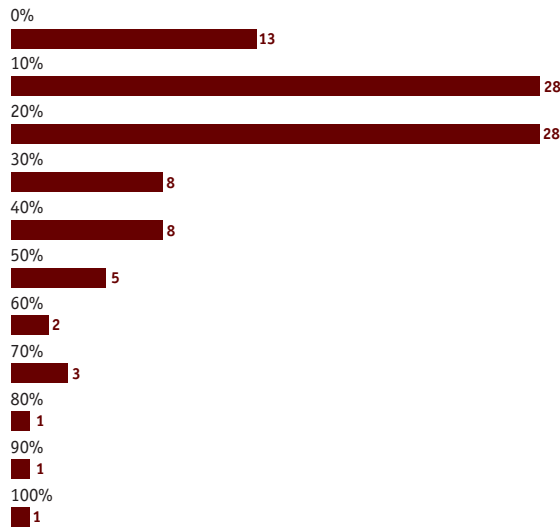
(% respondents)



Source: Economist Intelligence Unit survey.

9. Approximately what percentage of IT projects undertaken in your company over the past two years have failed to deliver the desired features and functions?

(% respondents)



Source: Economist Intelligence Unit survey.

likely it is to fail. Sixty-one percent of the survey respondents say that their senior management and board are fully aware of the potential financial risk caused by IT project failure or underperformance, although more than a third (34%) of the participants (and a worrying 42% in the Asia-Pacific region) say their senior management and board see IT risk only in terms of security breaches.

Late and over budget

Executives who think their IT risk is only about security ignore the risk inherent in all IT projects. Our survey sought to examine what actually happens when new IT projects are undertaken. Executives were asked what portion of the IT projects in their company have been delivered late or over budget in the past two years. One in five say that 60% or more of such projects have been delivered late or over budget, and only a small minority (6%) say that none of their projects have been delayed or exceeded budget. Only 13% of executives say all of their company's IT projects

have actually delivered all of the promised features in the past two years. The survey also indicates that IT project failure tends to occur more often at companies with revenues of over US\$500m than at companies with lower revenues (see charts 8 and 9).

The most common source of IT project failure is thought to be poor project management (including resource and budget management), cited by 43% of survey respondents. This is especially so in Europe, where 50% of executives cite this as the primary reason for IT project failure. Poor project management is also recognised as a significant problem in the government/ public sector, where over two-thirds of survey respondents say it is the primary cause of IT project failure.

The next most common reason—cited by one-quarter of survey respondents—for IT project failure is plain human mulishness, or resistance to change. This is especially common in larger firms (identified by 35% of respondents in organisations with over \$US500m in annual revenues). Many people just don't like to change their ways—or their computer



Coming to grips with IT risk

10. When IT projects in your company have failed to produce the desired results, what have been the primary causes?

Select up to two.
(% respondents)



Source: Economist Intelligence Unit survey.

programs. Another cause for IT project failure, cited by 21% of our group, is inadequate or loose governance of technical requirements (ie, “scope creep,” or the addition of more tasks or systems than initially specified, often leading to cost overruns, missed deadlines and loss of the original goals) (*see chart 10*).

A range of other menaces can mar or even destroy otherwise well-managed IT projects. These menaces include: inadequate post-project support and project quality assurance, failures of outsourcing/offshoring suppliers, unexpected changes in the enterprise or business environment, failure of implementation within the company, misalignment of IT strategy with business strategy, and deployment or rollout issues. The latter can be particularly complex when national borders must be crossed.

Companies also tend to examine risk, resilience and security issues towards the end of a project. That is a big mistake. “If it’s done when the system’s about to be switched on, it can knock a project back by a month while the holes are fixed,” says Piers Wilson, principal consultant and head of technical assurance

at Siemens Enterprise Communications. “This must be carried out at the earliest stages.”

After an IT project has gone live, in order to realize all of its benefits it is critical that full ongoing support be continued. Too often, human resources are withdrawn from the project just when they are most crucial. Companies where risk is managed properly do not disband their project team until the desired level of user satisfaction and key performance indicators have been achieved, well after launch.

A striking example of inadequate post-launch management is the UK government’s multi-million dollar Jobcentre Customer Management System, which handles claims for income support and allowances. After implementation, there was a 40% failure rate in processing claims. The system had a very poor reception from staff, perhaps because they were inadequately prepared for the change. An independent report identified poor training, a failure to listen to staff concerns and inflexibility in using the system as causes for the expensive fiasco.

Reducing the risk of failure

Companies have developed a wide range of techniques and policies for mitigating risk in IT projects. In firms that are most effective in lowering IT project risk, a strong partnership has been fostered between business and IT executives who “understand each other’s language.” There is also a sharp focus on project management.

Ensuring adequate funding and staffing before an IT project is launched is also a fundamental means of mitigating risk—an apparently obvious point that is routinely overlooked. Once the system is up and running, testing quality and performance in advance of its going live is a useful means of minimising failure later on—again something often ignored.

The likelihood of failure can also be lowered by reducing the scale of IT projects. As mentioned earlier, complex projects can easily malfunction. Many experts



advocate dividing large projects into multiple smaller ones to minimise risk, making full use of prototyping, in which small project components are developed and launched on “test users.” Prototyping serves many purposes. It helps ascertain that real end-user needs have been met; it helps define interfaces; it weeds out problems before they grow; and it ensures that the software covers contractual agreements. Meanwhile, performance metrics can be applied to the project, so that, for example, project managers can tell if half the budget has already been used when the project is only a third of the way through.

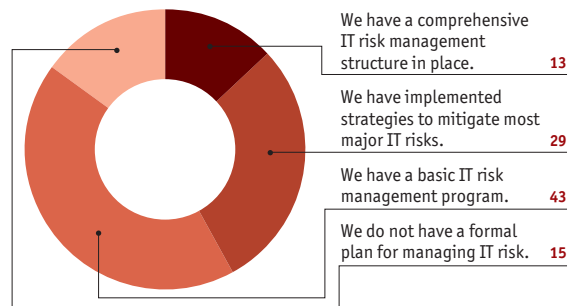
IT projects are frequently complex and long-term, and commitment and enthusiasm from the firm’s senior executives can wane. It is essential to have a “champion” at the most senior level of the company who will see the project through—especially as during the course of the project, the business requirements will probably change. The champion will need to communicate the new objectives to the project teams, and he or she must constantly ensure, through regular briefings from project leaders, that the project remains aligned with business objectives.

Aware but not engaged

“Awareness of IT risk has been rising, but it has not yet translated into risk management in most organisations,” says Marc Ronez, managing director of the Singapore-based Asian Risk Management Institute. This is echoed by several experts and is confirmed by the survey results. Only 13% of executives surveyed believe their company has a comprehensive IT risk management structure in place. Even fewer, just 11%, describe their company’s handling of IT risk as “highly effective.” The majority of respondents (65%) give a lukewarm verdict, saying that their approach is only “somewhat effective.” A sizeable number, 24%, are more disparaging, calling their approach either somewhat or highly ineffective (see charts 14 and 15).

14. Which of the following statements best describes your company’s approach to managing IT risk?

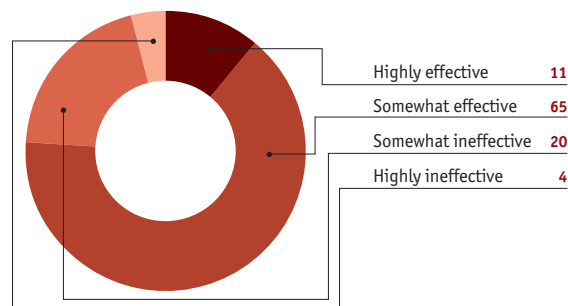
Select one.
(% respondents)



Source: Economist Intelligence Unit survey.

15. How effective do you consider your company’s management of IT risk?

Select one.
(% respondents)



Source: Economist Intelligence Unit survey.

Assessments of IT risk management are more positive in the financial services sector, where none of the respondents say that their company is ineffective and in North America, where the vast majority of survey respondents say that their organisation’s approach is somewhat effective (71%) or highly effective (21%), but there is clearly work to be done. The importance executives attach to IT risk is at some variance with the structures they have implemented to manage the risk. Mr Ronez is confident, however, that in the next two to three years, organisations will focus more effort on IT risk management.



'Techies' vs. 'suits'

At many companies, a major problem is the traditional disconnect between hard-pressed IT staff ("techies") and business executives ("suits"). Too often, IT risk is assessed by IT people who do not—and cannot be expected to—understand its impact upon the business. They naturally see risk in their own terms, and are generally more tolerant of it than are business people. Although IT staff have a clear picture of what can go wrong, business executives need to review what IT failure would mean to the organisation. When there is an IT bias towards measuring risk, a costly project can turn out to be a resounding technical success—but a business failure.

Conversely, inadequate understanding of IT issues by senior business management is an even greater problem, according to our survey. Twenty-six percent of our respondents say senior business management has inadequate understanding of IT issues, while only 15% say IT lacks understanding of wider business risk issues. Thirty-five percent of European respondents, in particular, cite lack of understanding by senior business management as a major obstacle to improving IT project management.

The mutual lack of understanding between techies and suits requires top-down remedies. Building strong partnerships between business and IT management may be the most important factor in mitigating IT risk. Shared risk management between business and IT is often the way to proceed. Kevin Bott, CIO of the transportation and logistics firm Ryder (*see sidebar, "Building blocks' help Ryder mitigate IT risk," p. 12*), recommends a "joint effort."

A business analyst who can liaise between IT and other business functions is a valuable asset. Michael Rasmussen, VP of governance for risk and compliance research at the consulting firm Forrester Research, says these individuals are rare. Not only must they understand IT risk in business terms, but they must be able to communicate it throughout the organisation.

"They need to be evangelists," Mr Rasmussen says. In the US, business schools are developing IT programs that will help train such analysts.

A more methodical approach

The task of managing IT risk is far-reaching and needs to extend way beyond the technology itself. Audrey Pantas, chief information risk officer at Xerox, heads up a global network of 50 team members who work with her to ensure the continuity of IT operations. At Xerox, she says, "We take a multi-tiered approach to protecting information assets and customer data by focusing on policy, process, product and people to reduce risk. Policies and standards are the foundation of our information risk program." These take into consideration the business risk profile, legal and regulatory requirements and corporate principles. "We've established standard processes to assess risk, evaluate evolving threats and respond swiftly to emergency situations. Annual information risk assessments are carried out to review the state of operational processes and technical controls."

Andrew Barstow, a partner with Ernst & Young from the technology and security risk services group, agrees with the need for continual monitoring. He says, "Where IT risk is managed well, there's a structured approach. Risk assessment needs to be done on an ongoing basis." The company's risk analysis should include interviews with all system owners and managers throughout the company. These talks can reveal, for example, that a legacy system is reliant on too few staff for maintenance. Clear procedures and responsibilities must be established for overall risk management.

Some companies take a formal approach, appointing an IT risk manager and a cross-functional committee to review IT risk on a regular basis. Too often, however, IT risk assessment is handled in a somewhat random way, especially during radical shifts in strategy. "When organisations merge or change



business strategy, risk and security are often treated as an afterthought,” Mr Barstow says.

Persistent offenders

What are the main IT risks that companies face? Which cause the most damage? Our survey reveals that unplanned IT systems downtime is the IT problem that caused financial harm most frequently in the past three years, particularly in the manufacturing and financial services sectors. Fifty-nine percent of our respondents say that their companies have incurred financial damage because of IT systems downtime. Perhaps surprisingly, unplanned downtime has caused much harm more often than “malware” such as viruses and worms, which play havoc with a company’s e-mail and other core applications. Only 45% of our respondents cite viruses and worms as causing financial damage (see chart 4).

Slow or unreliable systems performance (mentioned by 51% of our group) and delays in implementing new projects (cited by 48%) tend

to cause financial damage more often than does malware. Project implementation delays are especially frequent in causing financial damage in Europe. Other sources of financial damage from IT failure include leakages of sensitive data and loss of senior IT staff. Only a few executives (12%) in our survey cite failure to meet compliance requirements as a source of financial loss.

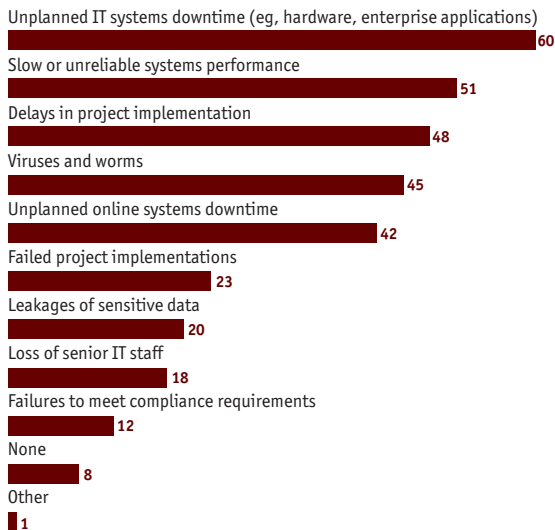
The changing IT risk landscape

The executives we surveyed believe that over the coming three years, IT risk will only get worse. According to our respondents, almost every IT risk area will pose greater problems in the next three years than it has in the past three years. Among our respondents, 44% fear increased risk of financial damage due to leakage of sensitive data—more than double the share of respondents who say this has occurred in the past three years (20%). Risk of financial damage is also expected to increase

4. In the past three years, which of the following IT-related problems have caused financial damage to your company?

Select all that apply.

(% respondents)

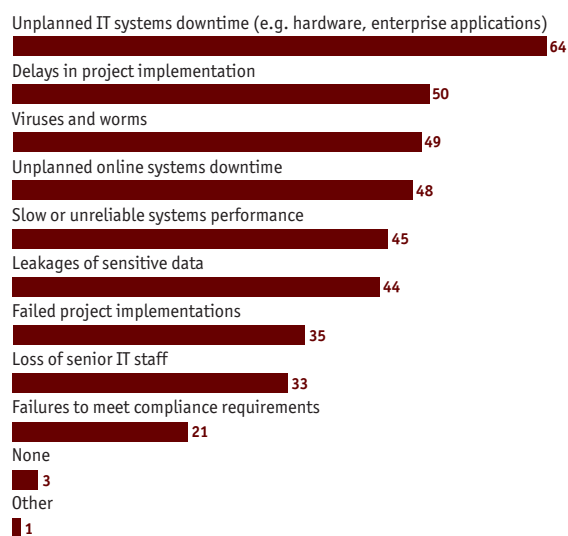


Source: Economist Intelligence Unit survey.

5. In the next three years, which of the following IT-related problems pose the risk of causing financial damage to your company?

Select all that apply.

(% respondents)



Source: Economist Intelligence Unit survey.



Coming to grips with IT risk

due to loss of senior IT staff and the failure to meet compliance requirements. Unplanned systems downtime (hardware and enterprise applications) will still be a significant threat, according to 64% of respondents; 48% expect online systems downtime to cause financial damage in the next three years, up from 42% currently. Fewer respondents, however, expect financial damage to be caused by slow or unreliable systems performance over the next three years than over the past three years (see chart 5).

Companies will face an ever more sophisticated hacker who uses viruses, worms and other tools for financial gain. Hackers will increasingly engage in activities that bring down websites, such as mounting “denial of service” attacks in which they flood websites with fake customer messages. They will also engage in sophisticated “phishing,” by which they can send e-mail to corporate employees, perhaps posing as their supervisors to gain personal details that can then be used for fraud.

Defending the castle

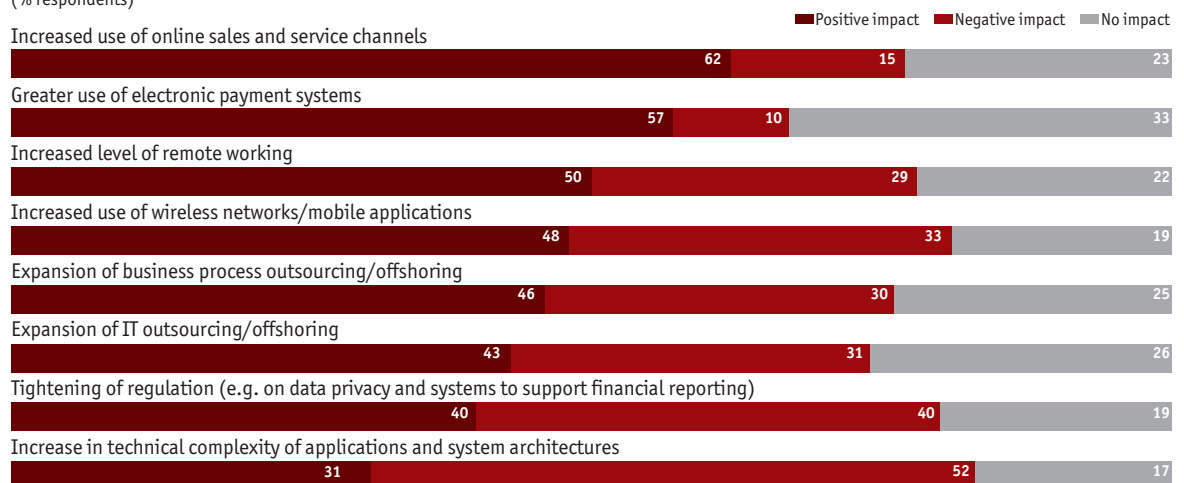
Audrey Pantas says that Xerox is actively monitoring alerts issued by its intrusion detection systems. These are deployed at key points in the infrastructure to help maintain network security. Xerox has also “fortified its electronic perimeter,” Ms Pantas says, by deploying anti-virus and anti-spyware software at the corporate gateways. The perimeter, however, is disappearing because of virtual offices and a diverse employee base operating from various points around the globe. So Xerox has “strengthened its identification, authentication, and authorisation requirements to account for the disappearing perimeter,” according to Ms Pantas.

Since internal IT security breaches are usually brought about by human rather than technical error, straightforward staff awareness training, on subjects such as how to handle data on mobile devices, can prove effective in safeguarding the organisation.

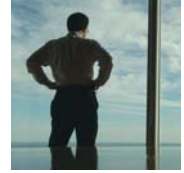
Alas, many factors that make for ease of doing business, such as mobile devices and electronic payment systems, also incur increased IT security risks (see chart 2).

2. In your opinion, what kind of impact do/will the following trends have on your company's exposure to IT risk?"

Rate each as positive impact, negative impact or no impact.
(% respondents)



Source: Economist Intelligence Unit survey.



Where it hurts

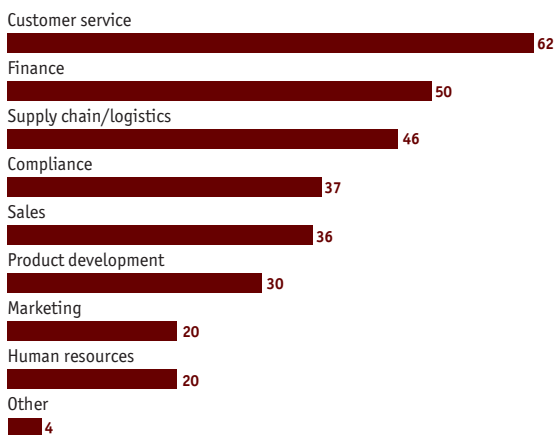
IT failure can severely damage every business operation except, perhaps, the company picnic. Almost all areas are vulnerable to IT collapse, but customer service is the most exposed. Increased online interaction makes uptime and the efficient running of service systems absolutely vital: if the website isn't running properly—even if it's just a little slow—the customer can easily defect to a competitor's website.

The finance functions, especially in the Asia-Pacific region, are considered very vulnerable to IT failure. And the supply chain is another frequently cited area of vulnerability, especially in North America. HR and marketing, being less time-critical, are not hit as hard by IT mishaps (see chart 3).

Different cultures, different fears. When asked which of different outcomes of IT failure were the most feared, there was some regional variation, with the executives from North America ranking the loss of revenue as their greatest fear, while Asia Pacific-based executives ranked loss of customers highest and European executives ranked damage to their company's brand or reputation highest (see chart 7).

3. Which areas of your operations do you think are vulnerable to IT failure?

Select all that apply.
(% respondents)



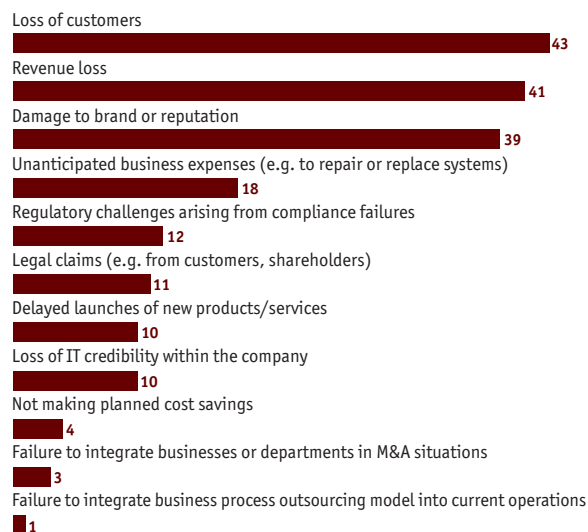
Source: Economist Intelligence Unit survey.

Quiet but dangerous

When reviewing risk, it is important to remember that major damage can come from what appear to be small glitches. These are routinely overlooked in favour of protecting the organization from “the big one.” “There’s too much focus on pure failure,” says Eric Holmquist, VP and director of risk management at Advanta Bank Corp. “But what happens if a project ‘kind of’ fails?” He cites the example of data corruption in customer records: Business executives may not see this, but the consequences can be devastating. Similarly, what happens if an invoicing system runs aground in some back office—and cash flow stops cold? Subtle IT failures can be the most deadly.

7. Which of the following outcomes of IT failure are most feared within your company?

Select up to two.
(% respondents)



Source: Economist Intelligence Unit survey.



Coming to grips with IT risk

'Building blocks' help Ryder mitigate IT risk

In 1933, armed with a \$35 black Model A Ford truck, James A. Ryder started a transportation business in Miami, hauling concrete. The next year he doubled his fleet to two. Now Ryder has more than 160,000 vehicles and is a global supplier of transport and logistics and supply chain solutions. With revenues topping US\$11bn in 2005, Ryder has a considerable IT risk to manage.

Kevin Bott, Ryder's CIO, is involved in three main areas: managing supply chain outsourcing, which requires high systems availability to keep goods moving; leasing the tens of thousands of vehicles; and supervising internal back office systems, some of which require very sophisticated risk management, partly driven by Sarbanes-Oxley Act regulatory requirements.

Mission-critical systems require 99.1% uptime, while 98% availability is the goal

for less vital systems. But "99.1% is very hard to achieve," Mr Bott says. Failover networks and servers are crucial parts of his technical defence, combined with advanced monitoring tools. Ryder deploys between 300 and 400 monitors for some of its largest customers, and "they can find out about risks fast enough to prevent them happening," says Mr Bott.

Risk management is shared between IT and business, who meet to discuss risk before projects start. If creating solutions for customers, they, too, are invited to discuss risk before embarking on the project. Notes Mr Bott, "Security is built into everything we do." People, processes and tools all have to be up to standard for effective risk management: "It's usually the people side that bites you."

Ryder has been outsourcing some of its IT service for about 10 years, using a help centre in the Philippines. However, the policy is to have no servers or source code offshore, and desktops are "locked down."

Mr Bott views outsourcing risk mostly in terms of geo-political occurrences and natural disasters. For instance, once 100 inches of rain fell in Mumbai, India, in two days, and all the phone lines were down. A wide geographical spread of suppliers, though "pricy," is preferable for mitigating risk, he says. With all outsourced suppliers, Ryder deals with risk considerations in the initial contract.

Mr Bott says there is little that can replace experience gained from similar projects and instances. Risk usually occurs when people are doing something for the first time in their lives. Applying this philosophy, Bott believes that when creating a brand new solution for a customer, IT risk can be mitigated by deploying "building blocks" that have already been used—and by trying to limit the number of new ones. "From the risk point of view, it's best to have nothing new," he says, although he often uses a single new "block" per solution.

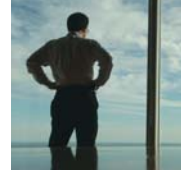
The buck stops . . . where?

Who takes primary responsibility for IT risk management? Most likely it is either the IT director or the CIO (The CIO is cited much more frequently by respondent from larger companies, with revenues of more than US\$500mn). In a small number of cases, the CFO or COO is in control. In only rare instances does all responsibility reside with a dedicated chief risk officer. According to Andrew Barstow of Ernst & Young, for day-to-day control, larger organisations usually have an IT risk person in the internal audit function.

IT skills deficits

Our survey indicates that that the lack of skills amongst IT staff—especially in project management—is a risk in itself. Many respondents do not believe that their IT staff is sufficiently skilled at managing the increasing complexity of applications and systems architectures. Worldwide, IT staff competence gaps are considered a significant reason for companies not improving their IT project management and performance.

The IT staff skill-set deficit is less often cited by European respondent and by those in companies with revenues of more than US\$500m (*see chart 13*).



13. Which of the following are the main obstacles in your company to improving IT project management and performance?

Select up to two.
(% respondents)



Source: Economist Intelligence Unit survey.

IT risk checklist

IT risk cannot be eliminated, but it can be lowered.

Here are some recommendations from the experts:

- Take a holistic view of IT risk. Do not narrow the focus to compliance or security, but consider the whole business span, including customer service, outsourcing, vendor reliability, new technology and new IT projects.
- Develop mutual understanding between IT heads and other business executives. They should each be aware of each other's risks and priorities.
- Ensure that there is full support for a large IT project at the most senior level of the company, with an executive champion who will see the project through past launch.
- Define IT project requirements clearly before setting out, an obvious precaution that is routinely overlooked. Beware of "scope creep."
- Ensure that risk and security concerns are considered at the earliest stage of project planning. Often these concerns are addressed too late—just before launch.
- Check that the IT project supports wider corporate goals.
- Divide large projects into smaller units, and prototype them to lower risk and enable users to spot problems before the "big bang."
- Train users thoroughly at the implementation stage, where many projects flounder. Users must be trained to take advantage of every aspect of the new system. Without their knowledge and cooperation, even the best system won't work.
- If outsourcing, check the partner's risk levels and make sure that provision is made in the contract for adequate risk management.
- Test business continuity plans regularly and analyse the results.
- Be proactive in anticipating risk. Diagnostic tools are available to identify serious IT problems before they occur.



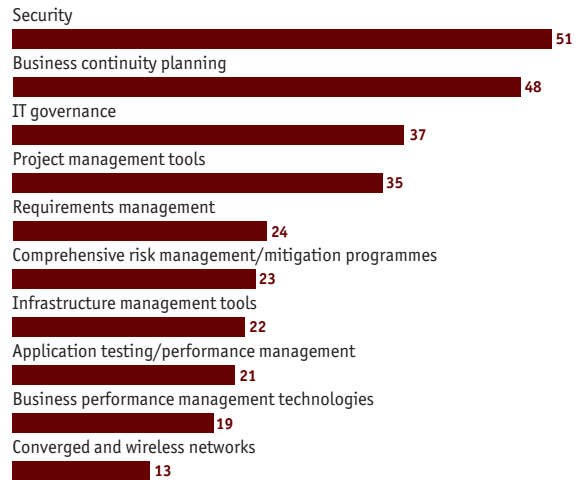
Conclusion

Investments in IT security will become increasingly important in the years ahead. As organisations expand their global supply chains, move into new territories, increase collaboration with international partners, and encourage their workforce to become more mobile, their IT systems will inevitably become more complex. As we have seen, complexity is a major factor in IT failure.

On the other hand, as Siemens’s Mr Wilson puts it, while previously there was an “ongoing battle to convince the CEO that IT risk was an important subject,” today there is far greater awareness of the importance of IT security. This very awareness, Wilson believes, will make organisations safer, as it will encourage them to implement ways to minimize risk.

This is borne out by our survey. Overall, more than half of survey respondents say their organisation will be focusing their IT risk management investments on security over the next year. In addition, in 2007, many corporations, especially the larger ones, will be focusing their investment on business continuity planning. Other areas, rounding out the top four areas targeted for IT risk management investments will be in funding IT governance and project management tools. application testing/performance management and infrastructure management tools. It looks like organisations are finally arming themselves to fight the growing danger of IT security risk (see chart 18).

18. In striving to improve IT risk management, in which areas will your company focus its investments over the next 12 months? Select all that apply.
(% respondents)



Source: Economist Intelligence Unit survey.

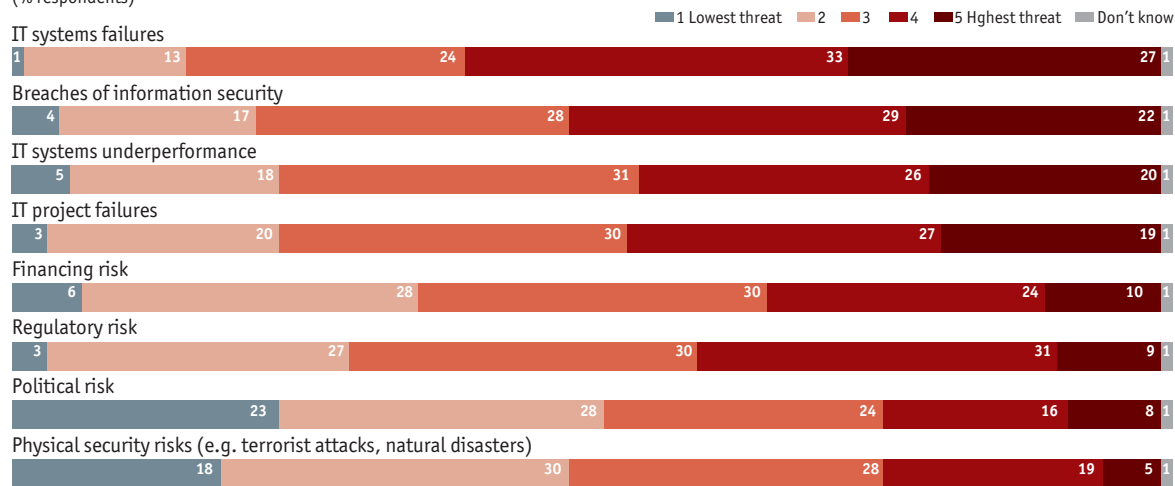
Appendix

In October 2006, the Economist Intelligence Unit conducted an online survey of 145 senior global executives. Our sincere thanks go to all those who took part in the survey. Please note that not all answers add up to 100%, because of rounding or because respondents were able to provide multiple answers to some questions.

1. How threatening do you think each of the following business risks are to your company's operations?

Rate each on a scale of 1 to 5, where 1 = Lowest threat and 5 = Highest threat.

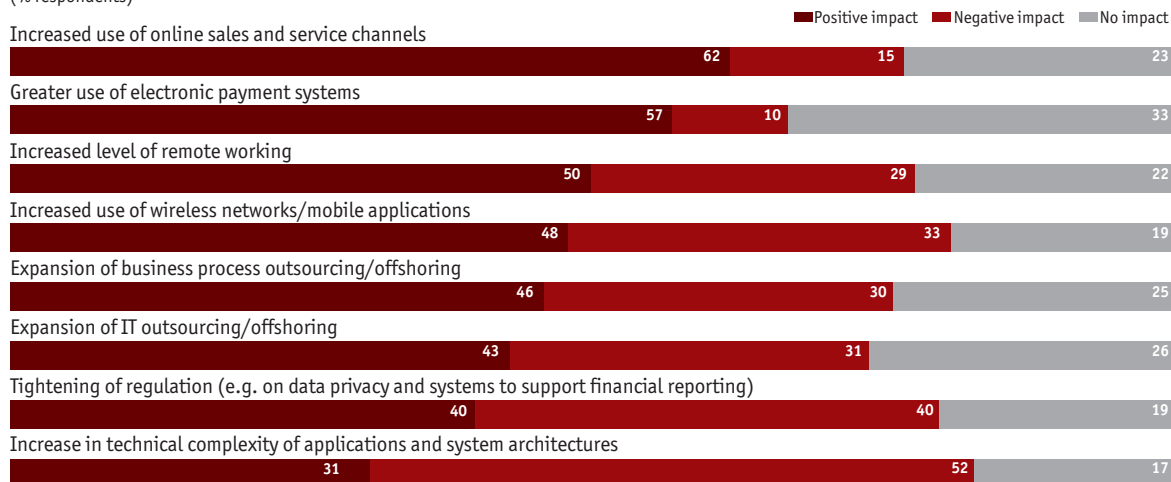
(% respondents)



2. In your opinion, what kind of impact do/will the following trends have on your company's exposure to IT risk?"

Rate each as positive impact, negative impact or no impact.

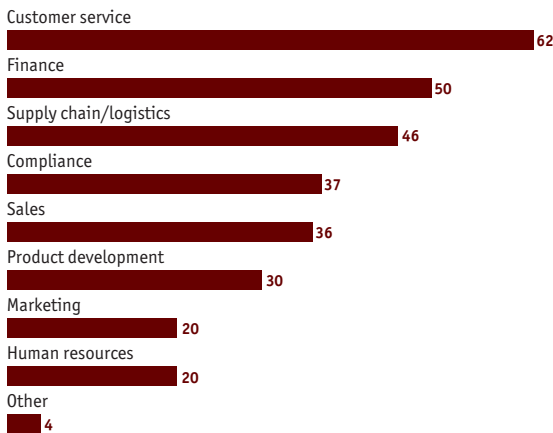
(% respondents)



Appendix: Survey results
Coming to grips with IT risk

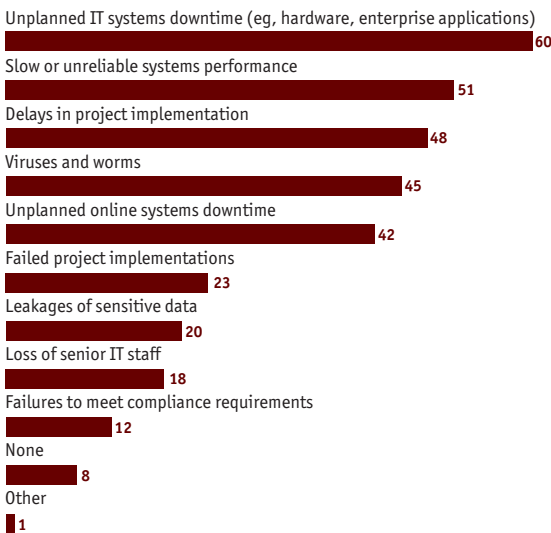
3. Which areas of your operations do you think are vulnerable to IT failure?

Select all that apply.
(% respondents)



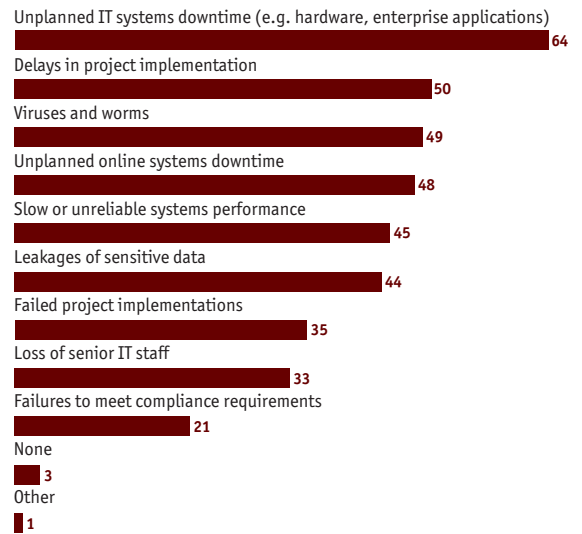
4. In the past three years, which of the following IT-related problems have caused financial damage to your company?

Select all that apply.
(% respondents)



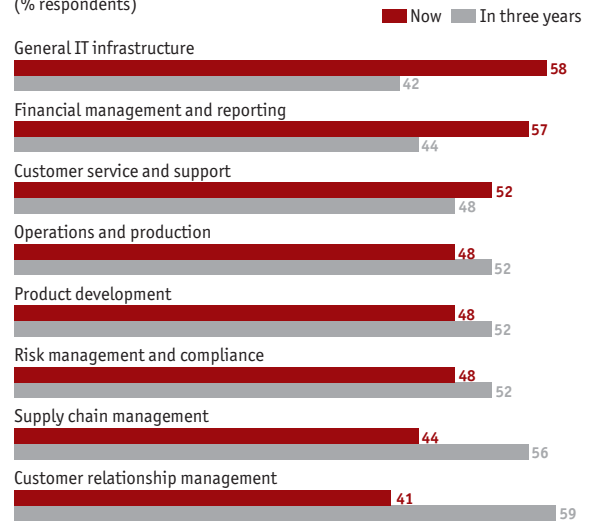
5. In the next three years, which of the following IT-related problems pose the risk of causing financial damage to your company?

Select all that apply.
(% respondents)



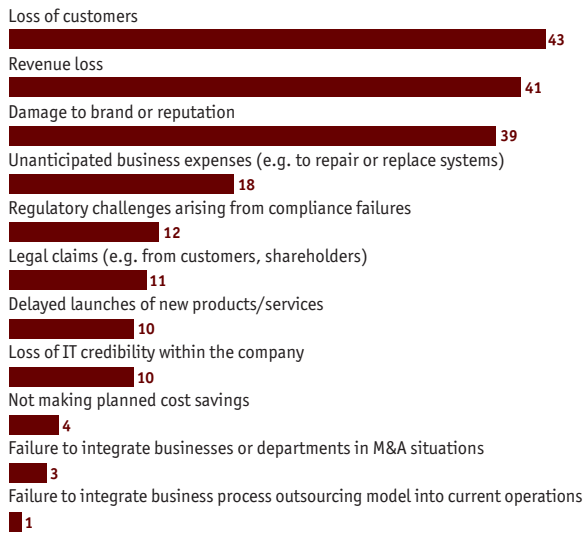
6. What are the top three areas for IT investment at your company now, and which do you think will be the top three areas over the next three years?

Select three in each column.
(% respondents)



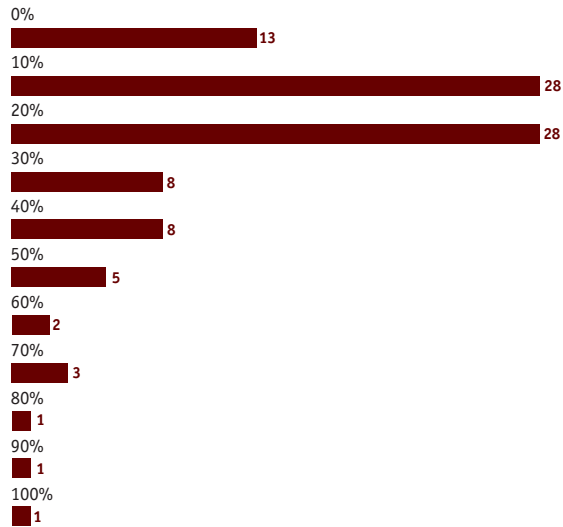
7. Which of the following outcomes of IT failure are most feared within your company?

Select up to two.
(% respondents)



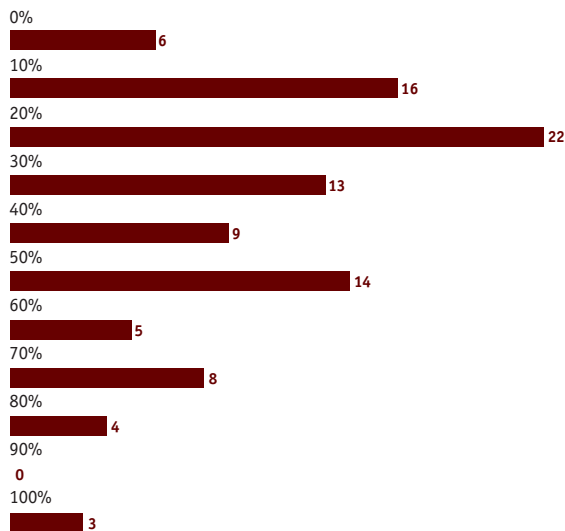
9. Approximately what percentage of IT projects undertaken in your company over the past two years have failed to deliver the desired features and functions?

(% respondents)



8. Approximately what percentage of IT projects undertaken in your company over the past two years have been delivered late or over budget?

(% respondents)



10. When IT projects in your company have failed to produce the desired results, what have been the primary causes?

Select up to two.
(% respondents)



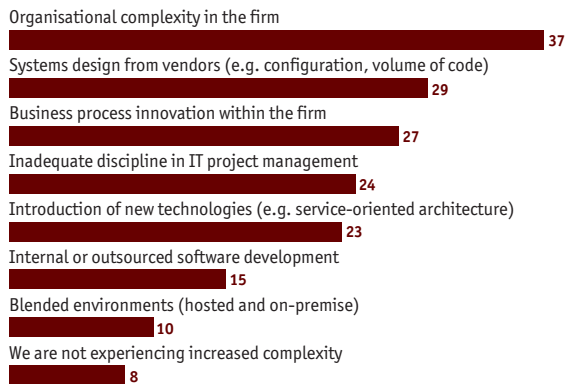
Appendix: Survey results

Coming to grips with IT risk

11. What are the main sources of increased complexity in the IT systems, architectures and processes used in your firm?

Select up to two.

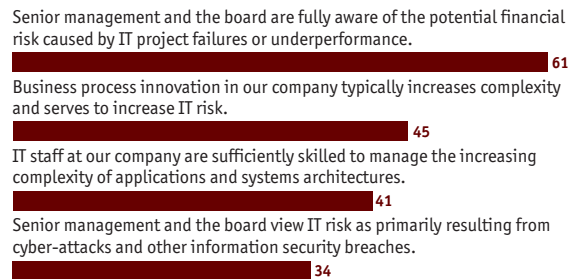
(% respondents)



12. From the following list, please select the statements with which you agree.

Select all that apply.

(% respondents)



13. Which of the following are the main obstacles in your company to improving IT project management and performance?

Select up to two.

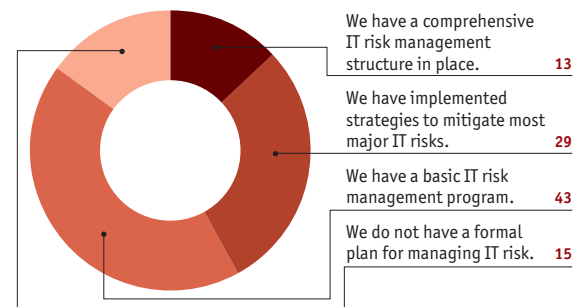
(% respondents)



14. Which of the following statements best describes your company's approach to managing IT risk?

Select one.

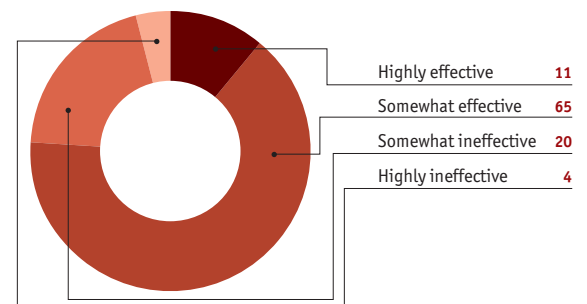
(% respondents)



15. How effective do you consider your company's management of IT risk?

Select one.

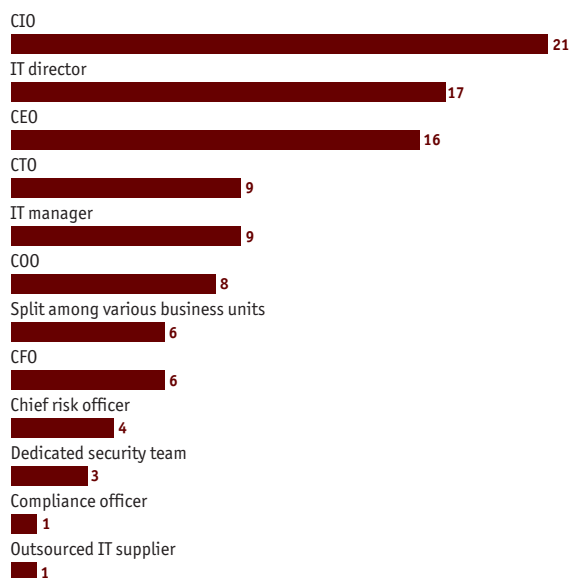
(% respondents)



16. Which department/individual has primary responsibility for managing IT risk in your company?

Select one.

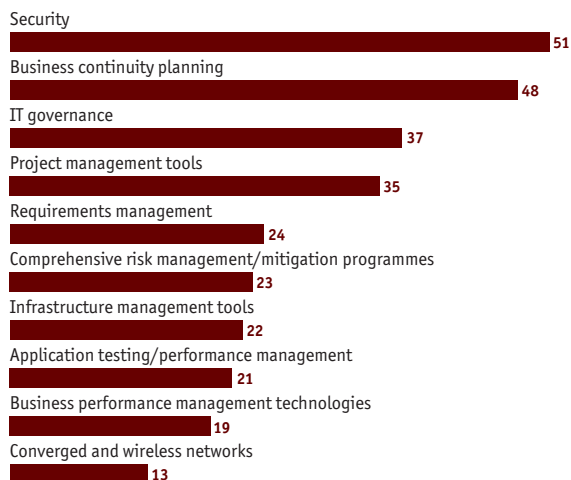
(% respondents)



18. In striving to improve IT risk management, in which areas will your company focus its investments over the next 12 months?

Select all that apply.

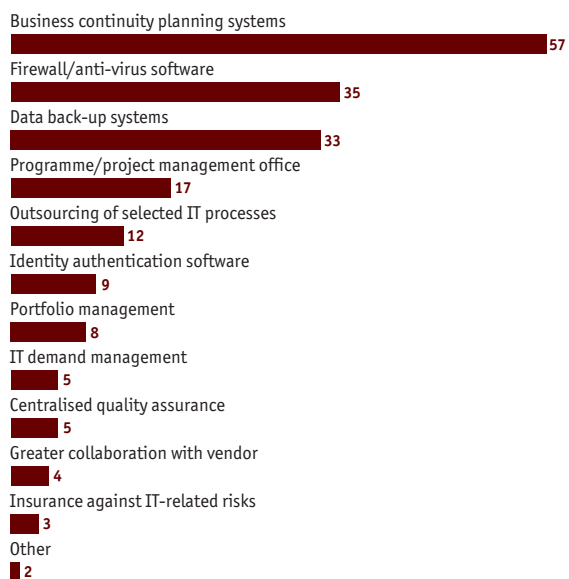
(% respondents)



17. Which of the following tools and strategies does your company consider most important for managing IT risk over the next three years?

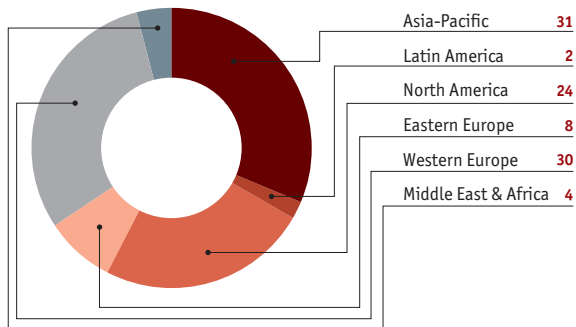
Select up to two.

(% respondents)

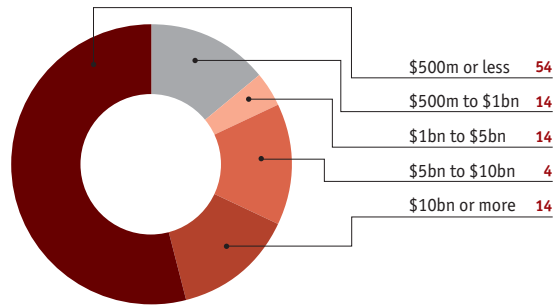


About the respondents

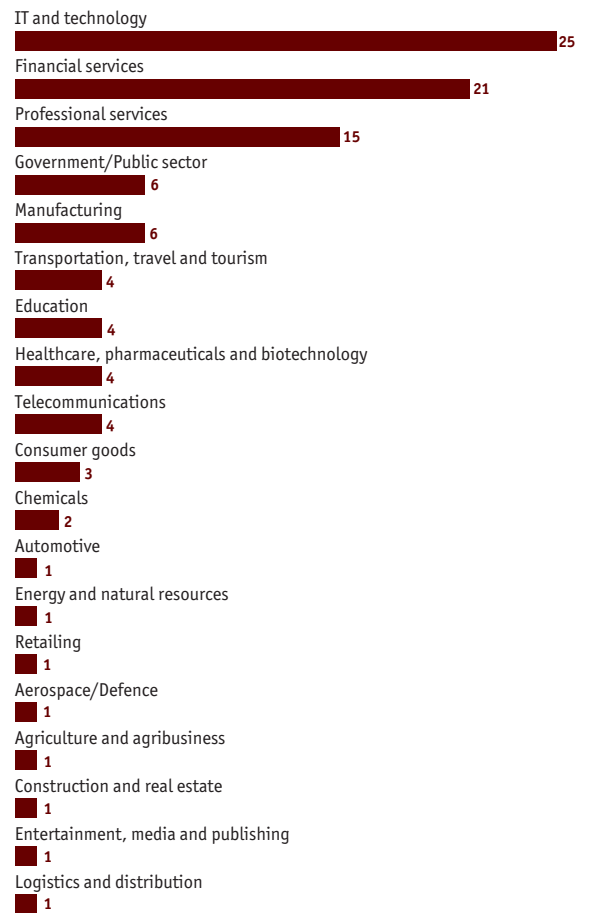
In which region are you personally based?
(% respondents)



What are your organisation's global annual revenues in US dollars?
(% respondents)

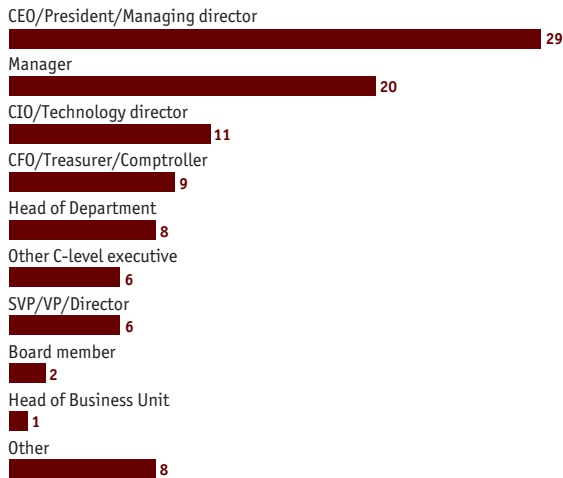


What is your primary industry?
(% respondents)



Which of the following best describes your title?

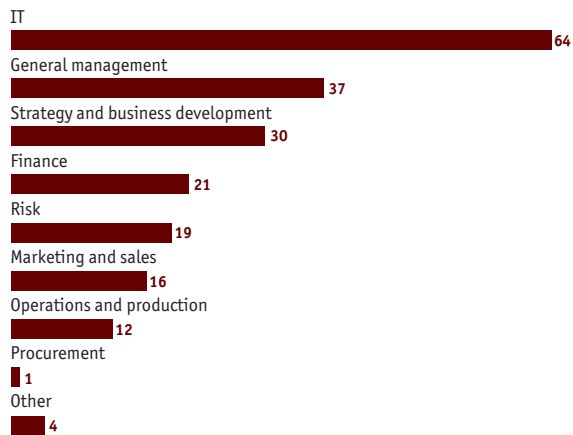
(% respondents)



What are your main functional roles?

Please choose no more than three functions.

(% respondents)



Whilst every effort has been taken to verify the accuracy of this information, neither The Economist Intelligence Unit Ltd. nor the sponsor of this report can accept any responsibility or liability for reliance by any person on this white paper or any of the information, opinions or conclusions set out in the white paper.

LONDON
26 Red Lion Square
London
WC1R 4HQ
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8476
E-mail: london@eiu.com

NEW YORK
111 West 57th Street
New York
NY 10019
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
E-mail: newyork@eiu.com

HONG KONG
60/F, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: hongkong@eiu.com