

Digital risk

The challenge for the CRO



A report from the Economist Intelligence Unit
Co-sponsored by:





SOME SAY A SINGLE TECHNOLOGY FAILURE COULD STOP PRODUCTION.
SOME SAY FAILURE TO ADAPT COULD CLOSE THE BUSINESS.
WE SAY POWER ON.

We don't back down from risk, we embrace it.
We insure network risk. Introducing ACE Dataguard™ network
risk insurance. To learn more visit www.aceeuropeangroup.com



**ace european
group**

INSURING PROGRESSSM



Preface

Digital risk: The challenge for the CRO is the third in a series of reports from the Economist Intelligence Unit's Global Risk Briefing, a research programme targeted at senior executives responsible for managing corporate risk. James Watson was the author of this report, and Gareth Lofthouse was the editor. The Global Risk Briefing is sponsored by Ace, Cisco, Deutsche Bank, IBM and KPMG.

The research for this paper is based on a survey of 218 senior risk managers, as well as interviews with senior risk managers and information technology (IT) risk managers. The Economist Intelligence Unit bears sole responsibility for the content of this report.

Our thanks to everyone who shared their time and insights in this report.

September 2005



Digital risk

The challenge for the CRO

Executive summary

Digital risk—a term describing the risks arising from increased dependency on information technology (IT) systems and digital processes—has become a major challenge for risk managers today. As firms have implemented complex IT systems to automate much of their businesses, so the risks associated with those systems have risen, ranging from system failure to data leaks and electronic security breaches.

Managing those risks creates several new challenges for chief risk officers (CROs). First, most risk managers don't have a technology background, so managing digital risk requires tight collaboration between the risk and IT functions. Second, the same technology that enables firms to digitise their business processes also allows criminals and insiders to commit new forms of fraud and theft. Third, new technologies create new threats, requiring firms constantly to reassess and adapt their strategy for managing digital risk.

This report focuses on the challenge of dealing with the risks posed by the increased dependency on digital

interactions and processes. It draws on a survey of senior executives from a cross-section of industries, as well as interviews with senior risk managers. This research sheds light on why IT has become a major source of risk, and on what professional risk managers are doing about it. The report includes the following main findings:

● **IT risk is now a board-level issue.** IT risk is one of the most significant threats posed to companies' global business operations today, with 48% of senior risk managers saying it represents a high or very high threat to their businesses. IT is now sufficiently important in more than one-third of firms to require close oversight from the chief executive officer (CEO). Although the chief information officer (CIO) remains the primary person responsible for IT risk in most companies, one-third of CROs now spend at least 15% of their time dealing with it, according to the survey.

● **Digital threats are putting companies' reputations and customer relationships at risk.** One-third of respondents say their firms have suffered significant financial damage as a result of electronic security breaches, such as hacking, in the past year; 18% don't know if they have or not. Almost 60% have incurred financial losses as a result of major system failure and downtime over the past year, with nearly one-quarter experiencing three or more such outages over the same period. Executives in the survey say they most fear the impact of such problems on their relationships with customers, along with damage to the reputation of their firms.

● **The enemy is becoming more sophisticated.** More than anything else, executives worry about the growing sophistication of hackers and other cyber criminals. Fully 55% of respondents cite this as a major

Survey and ranking methodology

The findings in this report are based on a survey of 218 senior executives responsible for managing risk; 32% of the participants were based in the US, 33% were based in Europe, and 24% were based in Asia-Pacific. All survey findings in this report and press release are drawn from a survey conducted in August 2005. Of the companies participating in the survey, 40% were from the financial services sector. Respondents from 16 other industries participated in the survey, including professional services, IT and technology, manufacturing, energy and natural resources, and entertainment, media and publishing.



difficulty in managing digital risk. The emergence of new, organised attacks on corporate targets, combined with increasingly professionalised hackers, means the cost of security breaches will continue to grow.

● **Mobile workforces are expanding the boundaries of risk.** Senior risk managers say remote working, wireless networking and related technologies such as Internet-based telephony are all adding significantly to their firms' exposure to electronic threats. Fully 57% say rising levels of remote working are adding to the overall risk levels faced by their companies. Traditional security solutions, such as electronic firewalls, are becoming less effective as more employees interact via open networks and carry sensitive data on portable devices.

● **Outsourcing is adding to the burden.** IT outsourcing, especially when it is directed overseas, is significantly increasing companies' exposure to risk, bringing new complexity to the challenge of managing digital risks. In the survey, 42% of respondents say it adds some level of risk to their firms' overall exposure.

Consequently, 69% of CROs are now involved in the selection of an outsourcing provider, while 38% have a significant involvement in the matter.

● **CIOs and CROs must clearly stake out their roles to deal with IT risk most effectively.** There is a grey area between the responsibilities of the CRO and CIO in dealing with IT risk, partly owing to the complex nature of technology and the challenge of communicating technical issues. Two-fifths of risk managers rate their understanding of IT risks as moderate or poor, and 42% cite poor communication between the IT and risk functions as a significant difficulty in managing technology risk. But leaving digital risk entirely to the IT department is not advisable: 48% of respondents say that one of the chief difficulties in managing IT risks is over-reliance on IT management to come up with effective risk management solutions. As firms place more reliance on IT, it will be in their interest to ensure that the company's risk specialists understand their respective roles in managing digital risks.



Digital risk The challenge for the CRO

Introduction

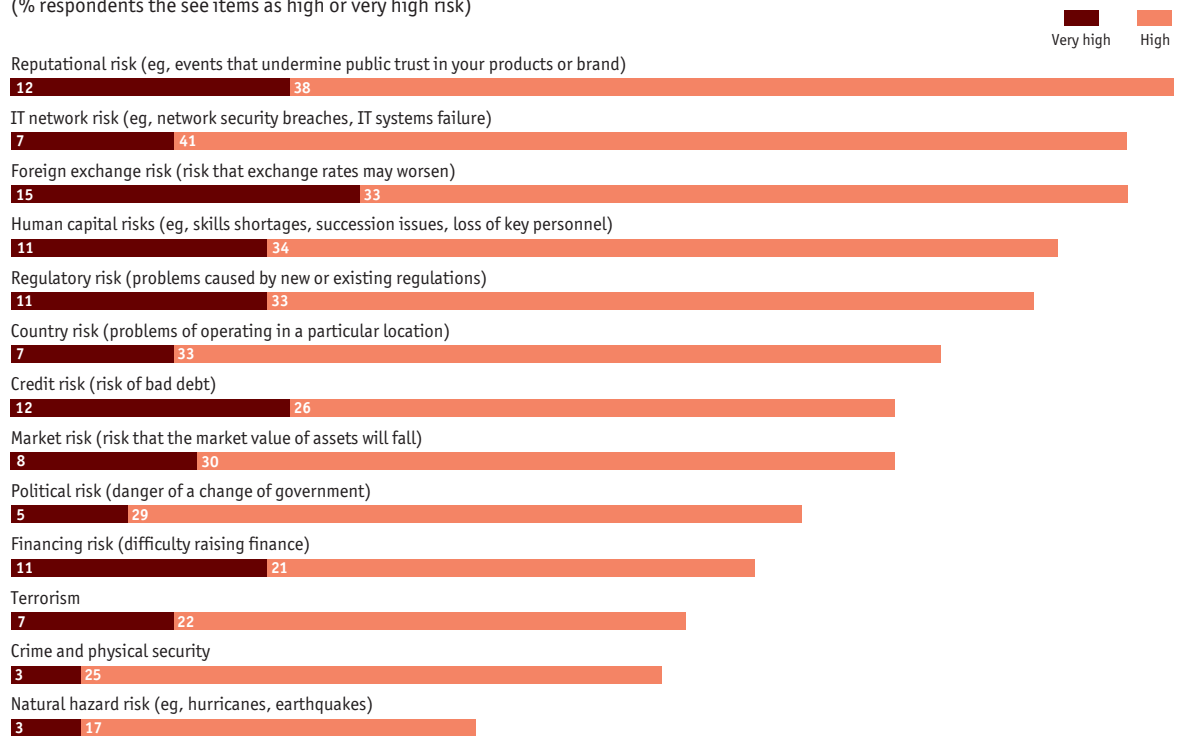
Over the past decade IT has become inseparable from the way companies conduct their business. Money has been poured into IT systems to digitise finance and accounting systems, enterprise resource planning, human resources and every other element of the business. Few firms are able to ignore these advances, for fear of losing competitive advantage to nimbler rivals.

But these tremendous innovations bring with them a diverse range of threats—threats that evolve and proliferate with every new technological advance. The relatively new phenomenon of “phishing”, where criminals create precise copies of a company’s website and then convince unwitting customers to enter their

password and account details, is just the latest addition to an array of digital evils ranging from viruses to so-called denial-of-service attacks. Add to this non-malicious sources of IT risk, such as the damage caused by system failures or accidental disclosure of sensitive data, and it is clear that IT risk now constitutes a sizeable risk domain in its own right.

It’s a trend that risk managers are still coming to terms with. “Three years ago IT risk was seen as part of the IT function,” says Paul de Hoest, CRO at Egg Bank in the UK. “Risk didn’t have an overriding role to play, so the IT function focused on developing the next project. There’s no doubt that there’s been a big change,” he adds.

How significant a threat do the following risks pose to your company’s global business operation today?
(% respondents the see items as high or very high risk)



Source: Economist Intelligence Unit, 2005



Angus Burden, director of IT security at Barclays Bank and the person responsible for assessing IT risk within the business, agrees. "Three or four years ago, IT was one of those 'yes, it's important' functions, but it didn't have the visibility it needed. But new regulations, cyber-crime and the increasing use of technology as a factor in the race for competitive advantage have brought IT risks to the forefront," he says.

The reliance that firms put on IT today is having a direct effect on the role of the CRO. Nearly half of respondents polled for this report say IT poses either a high or very high risk to their company's global business operations.

Proliferating threats

As companies have become more reliant on IT systems, even minor technology problems can have severe ramifications for a business. Olivier Moumal, Director for Risk Management and Insurance at Belgian telecommunications firm Belgacom SA, says IT and network reliability is a key differentiator in his business. "Our clients... put pressure on their strategic suppliers like us, so we put a lot of time into ensuring that we're a resilient firm and on removing all aspects of [technology] risk from the business. Five years ago, we could stop for two to three days. Now, we can't stop for more than a few minutes, so the environment has really changed for us," he adds.

Most companies still struggle to avoid damaging IT problems, however. Over the past year about 60% of

executives in the survey incurred at least one major system failure or downtime. Firms are also having to battle with internal damage to or misuse of data or IT systems. Nearly 40% reported incidents of this nature.

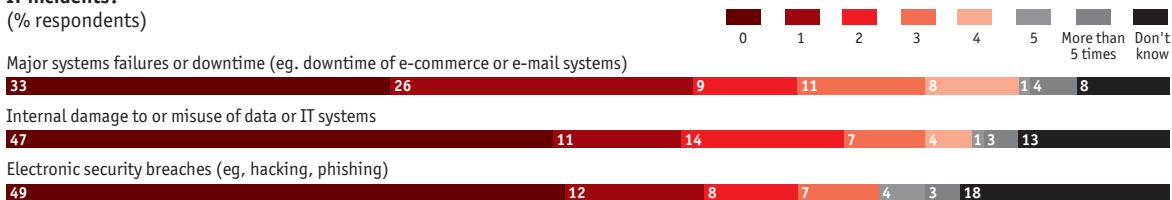
There is also evidence that electronic crime is becoming more commonplace and professional. About one-third of survey respondents experienced a breach of their systems as a result of some kind of hacking or phishing attempt, and a further 18% admitted they didn't know how often they had been victims of electronic crime. The financial damage caused by these crimes is significant. In the UK alone, the total estimated cost of electronic crime for companies with more than 1,000 employees was £2.4 billion in 2004, according to a recent survey by the National Hi-Tech Crime Unit (a UK-based crime squad established to tackle activities such as hacking).

The criminal threat is a major concern for the financial services sector in particular. Earlier this year the London offices of Japanese bank Sumitomo Mitsui Banking Corporation foiled an attempt to steal £220m. Keystroke-logging devices that record the buttons pressed on computer keyboards were used as a means of learning account numbers, passwords and other sensitive information. Insiders planted the devices, and hackers working overseas used the information to try to transfer funds out of the business.

"The threat of hackers is greater," agrees Egg Bank's Mr de Hoest. "They've changed from amateur efforts to semi-professional organised outfits. The sheer number of IT vulnerabilities to fix goes up incredibly every year, with more than 100% growth last year."

In the past 12 months, how many times has your organisation suffered significant financial damage as a result of the following IT incidents?

(% respondents)



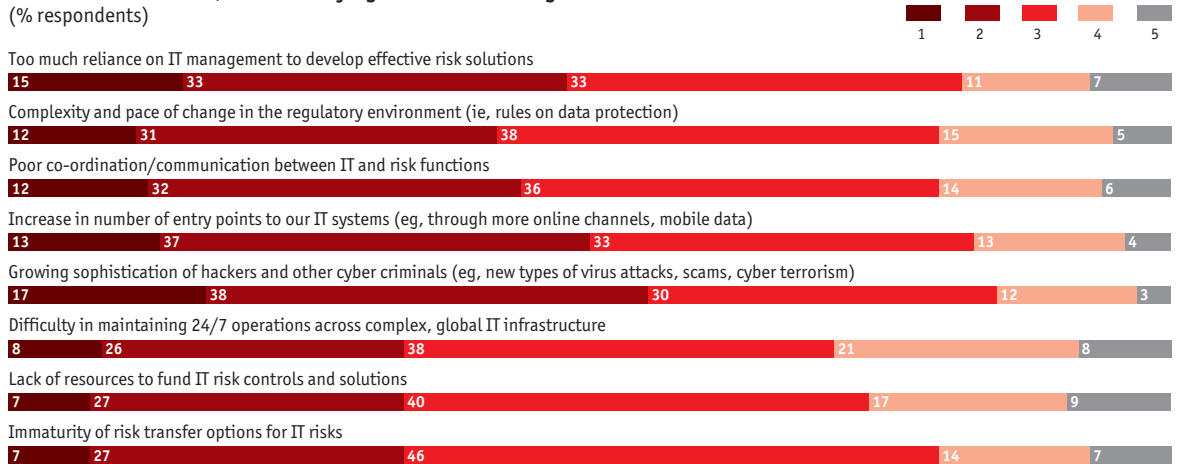
Source: Economist Intelligence Unit, 2005



Digital risk

The challenge for the CRO

How significant are the following difficulties in managing IT network risk in your company?
 Rate on a scale of 1 to 5, where 1=Very significant and 5=Insignificant.
 (% respondents)

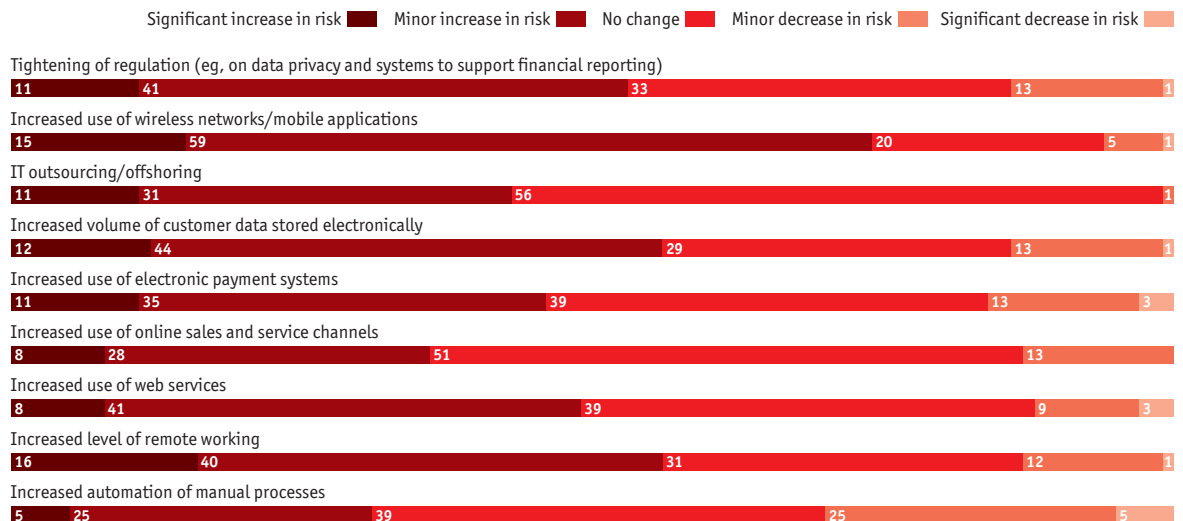


Source: Economist Intelligence Unit, 2005

More than half of executives in the survey see the growing sophistication of hackers, cyber-criminals and an assortment of other digital scams as one of the biggest challenges in managing digital risks. And although system failure, viruses and data leaks are seen as posing the greatest threat to business over the next three years, 28% see hackers as a major worry.

IT failures and security breaches constitute a direct threat to the bottom line, but an even greater concern is how they may affect the way the company is perceived. Executives in the survey are more concerned about the damage that IT risks may cause to customer relationships (37%) and damage to corporate reputation (32%) than about loss of

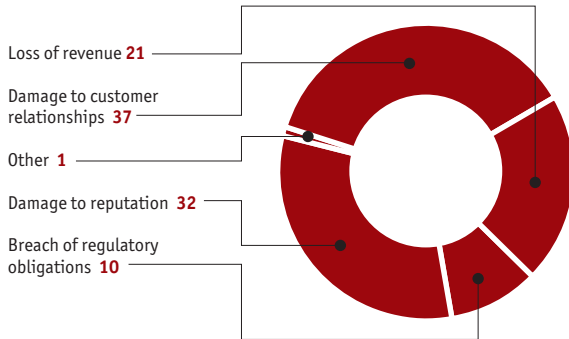
How do the following IT-related trends affect your company's risk exposure?
 (% respondents)



Source: Economist Intelligence Unit, 2005



Which of the following represents the biggest threat to your business as a result of IT failures or breaches of security?
(% respondents)



Source: Economist Intelligence Unit, 2005

revenue (21%) caused by an IT problem. Egg Bank's Mr de Hoest says the concern with threats such as phishing is the impact that they may have on the bank's customers. "Phishing is a fraud risk that affects our customers," he says. "We're meeting the challenge, but it's tough."

Changing business practices, such as the increased use of remote working, are also adding to the problem. More than half of those polled say the capability for employees to work anywhere and at any time is adding to their firms' exposure.

Mike Grenham, an information security manager at

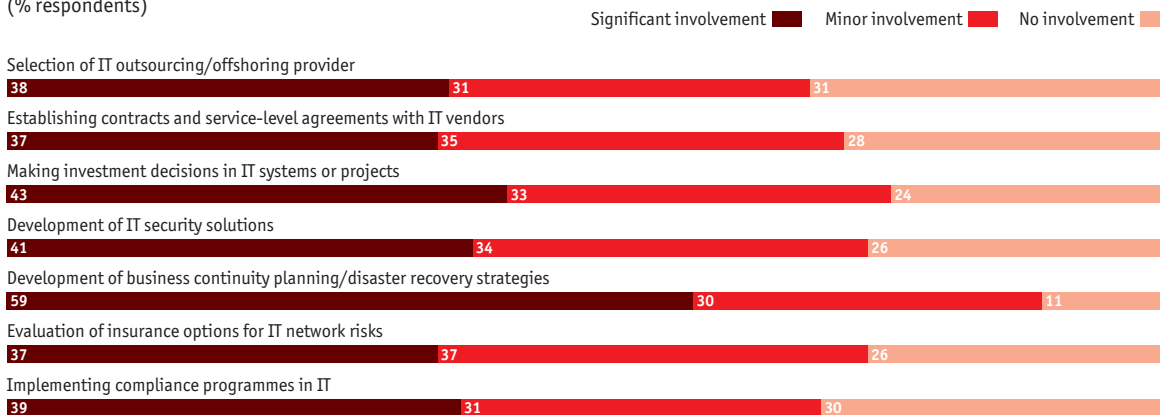
British Airways with responsibility for overseeing IT risk assessments, says the risks associated with remote working are significant. "Providing more connectivity to more people in more locations is a challenge. It's not just an issue of putting in a firewall anymore; we need to protect what's on people's laptops," he says. Adding to the challenge is the rapid spread of wireless networks and related technologies, such as voice over Internet protocol (VoIP), that allow phone calls to be routed over the Internet at lower cost. Almost three-quarters of respondents say the use of mobile applications increases their company's risk exposure.

"Deperimitisation is an issue," comments Mr Burden of Barclays Bank. "As we get more mobile workers and people working remotely, how do we protect them against viruses and other digital threats?"

The risks of IT outsourcing

IT outsourcing and offshoring add another dimension to the challenge of risk management. More than two-fifths of respondents say IT outsourcing is increasing their firms' risk exposure, with 11% saying it increases risk significantly. Consequently, 69% of CROs are now involved in the selection of an outsourcing provider.

How much involvement does your CRO (or equivalent) have in the following strategic IT activities?
(% respondents)



Source: Economist Intelligence Unit, 2005



Digital risk

The challenge for the CRO

Managing risk in IT outsourcing entails not just an evaluation of the outsourcing provider's IT capability, but also of its financial stability. "We're outsourcing and the reliability of the vendors we use is crucial," says Mr Moumal of Belgacom. "The trend is quite difficult for the risk function. If you outsource, you rely on a partner who could be bankrupted," he warns.

Within Belgacom, all contact with third-party providers is vetted by the risk department, with suppliers rated against a financial scoreboard. The review looks at the resilience and financial strength of the partners, as well as the penalties and liabilities included within the contract's service-level agreements. "We also use milestone projecting, so that we can always ensure that a supplier is on track with the project," says Mr Moumal.

Another major concern with outsourcing contracts that involve offshore providers is the minefield of regulatory and legislative issues involved. Of particular concern are the rules regarding sending data offshore, following a number of incidents in 2005 involving the misuse of sensitive data by fraudsters working for offshore providers.

Putting IT risk on the CRO's radar

The complex nature of IT makes it an inherently difficult problem to assess. This is one of the reasons why, for 58% of firms, final responsibility for IT risk still rests with the CIO or chief technology officer (CTO). A further 36% regard the chief executive,

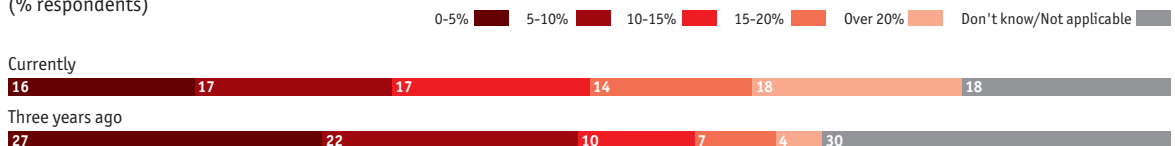
president or chairman as the person most accountable. But CROs are no longer far behind: 32% say they now assume the main responsibility.

Over the past three years there has also been a major increase in the amount of time that risk managers allocate to the issue. About one-third of companies—compared with just 11% three years ago—say their top managers spend at least 15% of their time dealing with IT-related threats. The percentage of risk managers spending almost no time on managing IT risks has nearly halved, from about 27% three years ago to less than 16% now.

The growing involvement of the risk department in IT issues is also expanding the number of activities that the CRO is involved with. Three-fifths of companies surveyed say their top risk manager is significantly involved in the development of business-continuity planning and disaster-recovery strategies. Three-quarters say the CRO has some level of influence when investment decisions are made for IT systems or projects.

Within Egg Bank, the CIO and CRO work together to agree the firm's overall spending on ways to mitigate IT threats. Mr de Hoest provides a recommendation on what the bank's overall appetite for IT risk is, but the actual level of spending is determined by the CIO.

How much time does your company's CRO (or equivalent) devote to managing IT risks today, compared with three years ago?
(% respondents)



Source: Economist Intelligence Unit, 2005



IT and enterprise risk management

What is the risk manager's role in addressing IT risk? The CIO is more likely to have the technical expertise to spot IT risks, but the CRO has an increasingly pivotal role to play by addressing these issues within the wider context of enterprise risk management (ERM). Just over half of executives polled say the bulk of their focus is on identifying how IT risks threaten elements of the wider business. Making sure the board is aware of any possible IT risks is a key concern for 48% of respondents, and 44% focus their attention on ensuring that any work being done complies with regulations.

IT risk is harder to manage than more established forms of business risk, not least because the firm's IT risk exposure is so difficult to quantify. With credit risk, companies can set an appetite in terms of what constitutes an acceptable level of risk. But according to Mr de Hoest, with threats such as hacking the question becomes one of how much the bank should invest in order to mitigate against an unknown level of risk.

Part of the challenge is to categorise and identify the multitude of threats that constitute digital risk. In practice, this entails extending the discipline of ERM into the realm of corporate IT. All the risk managers interviewed for this report, for example, say their organisation maintains some form of central technology-risk dashboard, which contains a high-level summary of the main IT threats faced by the business.

"Our central technology-risk dashboard is how we articulate risks. It's a one-page document, which is supplemented with more detailed additional information," says Mr Burden. The dashboard highlights what threats the company might be facing, along with any internal controls that are in place to address these vulnerabilities. It also reviews related governance controls and the business's operational capabilities.

Others, like Egg Bank, have a chart of vulnerabilities, with each item given a rating. "We've got a ranking system—high, medium, low—of what's most critical and what would affect the most people," says Mr de Hoest. The bank's operational risk committee gets a monthly report on the IT function, which assesses its biggest threats and how those link to the agreed appetite for risk within the business. It also highlights key risk indicators, such as system downtime and site availability.

But although a central register is a practical tool for concisely expressing the threats the business faces, compiling it accurately typically requires close collaboration between the IT and risk function. For many firms, this is a challenge. More than half of executives surveyed say poor communication between IT and the risk function causes some level of difficulty within their organisation. Part of the issue stems from the difficulty risk managers face in getting to grips with specialist IT issues. Two-fifths of the executives surveyed rate their understanding of technology risks as either moderate or limited.

"Communicating IT risks in business terms is a challenge," says Mr Grenham of British Airways. "IT

What is the role of your company's CRO (or equivalent) in regard to IT network risk? Select all that apply. (% respondents)



Source: Economist Intelligence Unit, 2005



Digital risk

The challenge for the CRO

can be expensive and you won't get support unless you can express its benefits in business terms."

Part of the solution lies in a more detailed understanding of how business processes are underpinned by technology within an organisation. This helps to establish what elements of the business might be threatened by certain kinds of risks. At Belgacom, the technology architecture is defined in terms of what business processes it supports. The various business units then work with the IT department to determine what level of downtime those processes can sustain. "In the past, there's been an issue of the IT department being too technical," says Mr Moumal. "Now, the business leads the process and IT fits in with that."

Different businesses take varying approaches to how closely their IT and risk departments collaborate. But there is no doubt that greater reliance on corporate IT and digital processes is increasing companies' overall risk exposure, and that as a result the risk department must become intimately involved in understanding the role of IT in the business. Although the bulk of firms still rely on the expertise of the CIO, the CRO must bring the disciplines of ERM to the realm of digital risk. There remains a grey area in terms of where precisely the line between the two departments is drawn. Although there is no definitive answer to the question, the issue is something that CROs will be increasingly grappling with in the future.



Conclusion

Information technology has already had a huge impact on firms and its role is set to increase rather than diminish in the years ahead. Organisations that are serious about understanding how IT failure can impact the business will need to hammer out precisely how the IT and risk functions will collaborate in managing the issue. CROs that don't have IT on their risk portfolio already will increasingly have to take it into account in the future. The discipline of ERM needs to

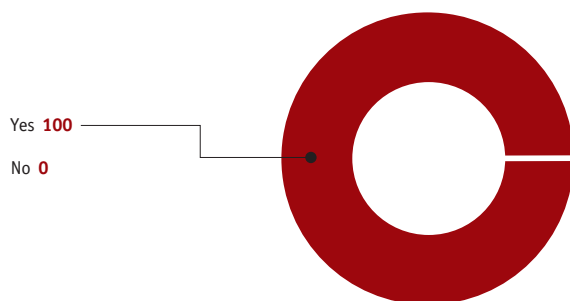
be applied to a range of IT planning issues, such as technology evaluation and business-continuity and offshoring strategies. "The challenge is to enlarge the risk analysis to the critical business functions, the software applications, databases and network connections they rely on," says Mr Moulal. "A failure to have the right information at the right time and at the right place can be disastrous," he warns.

Appendix: Digital risk

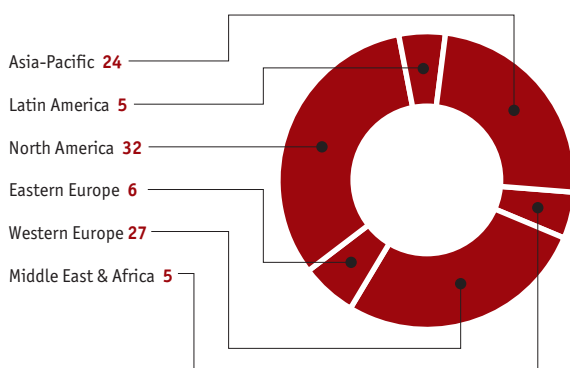
The challenge for the CRO

The Economist Intelligence Unit conducted an online survey of 123 senior executives in the retail and consumer goods industry. The survey was conducted in September 2005, and our thanks are due to all those who shared their time and insights.

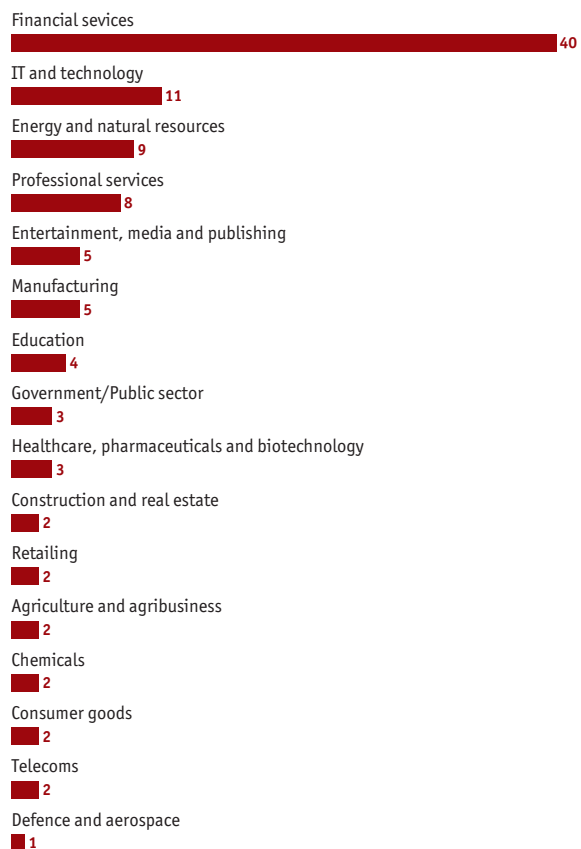
Do you have responsibility for, or influence over, strategic decisions on risk management in your company?
(% respondents)



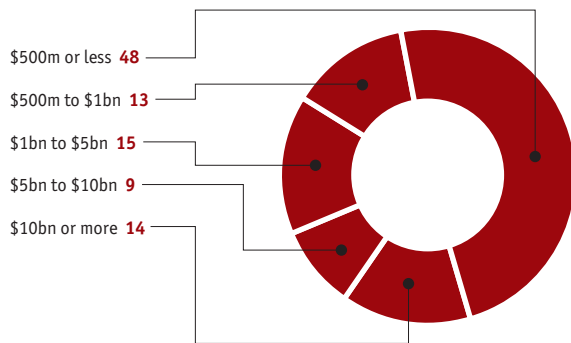
In which region are you personally based?
(% respondents)



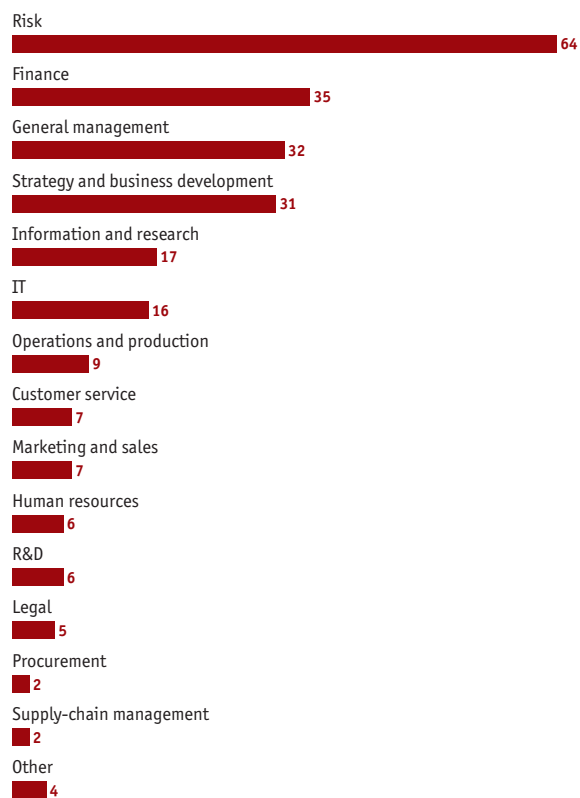
What is your primary industry?
(% respondents)



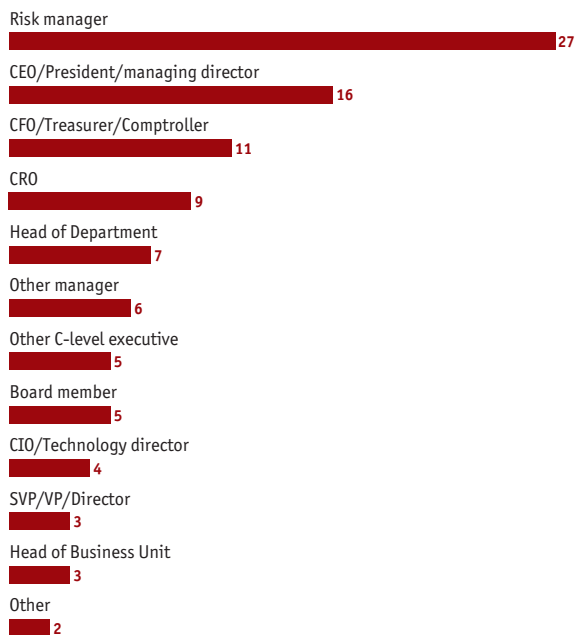
What are your organisation's global annual revenues in US dollars?
(% respondents)



What are your main functional roles?
Please choose no more than 3 functions.
(% respondents)

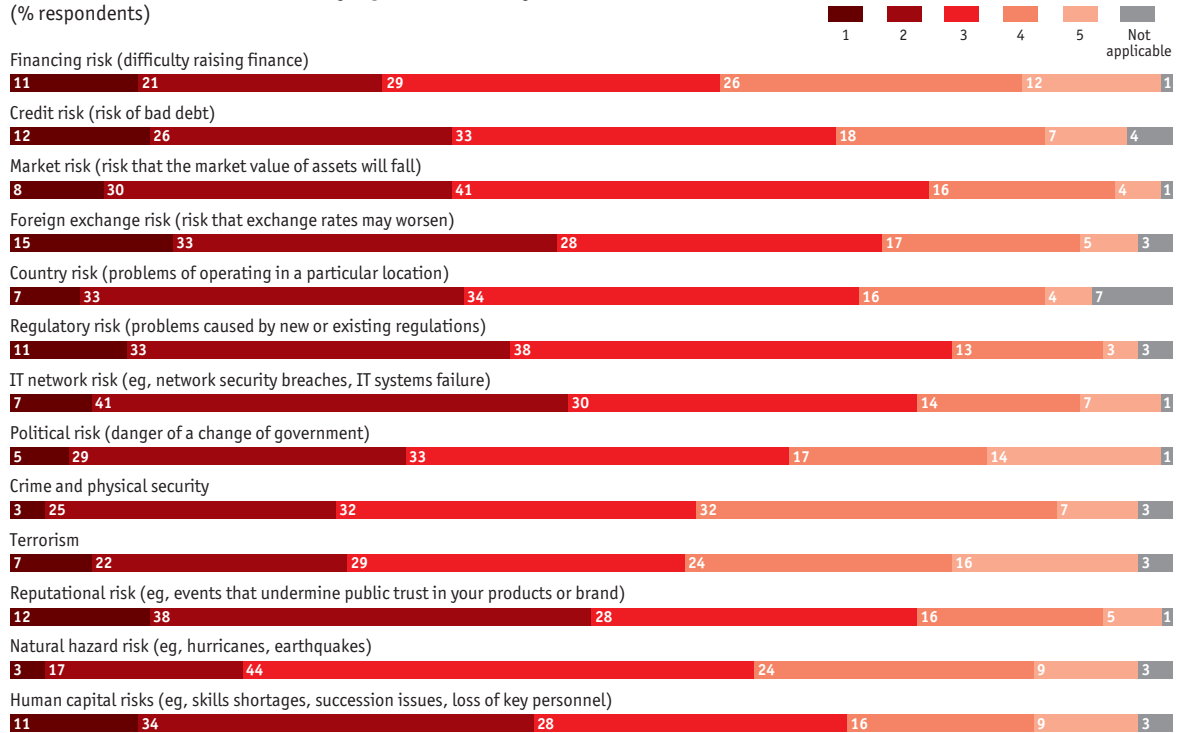


Which of the following best describes your title?
(% respondents)



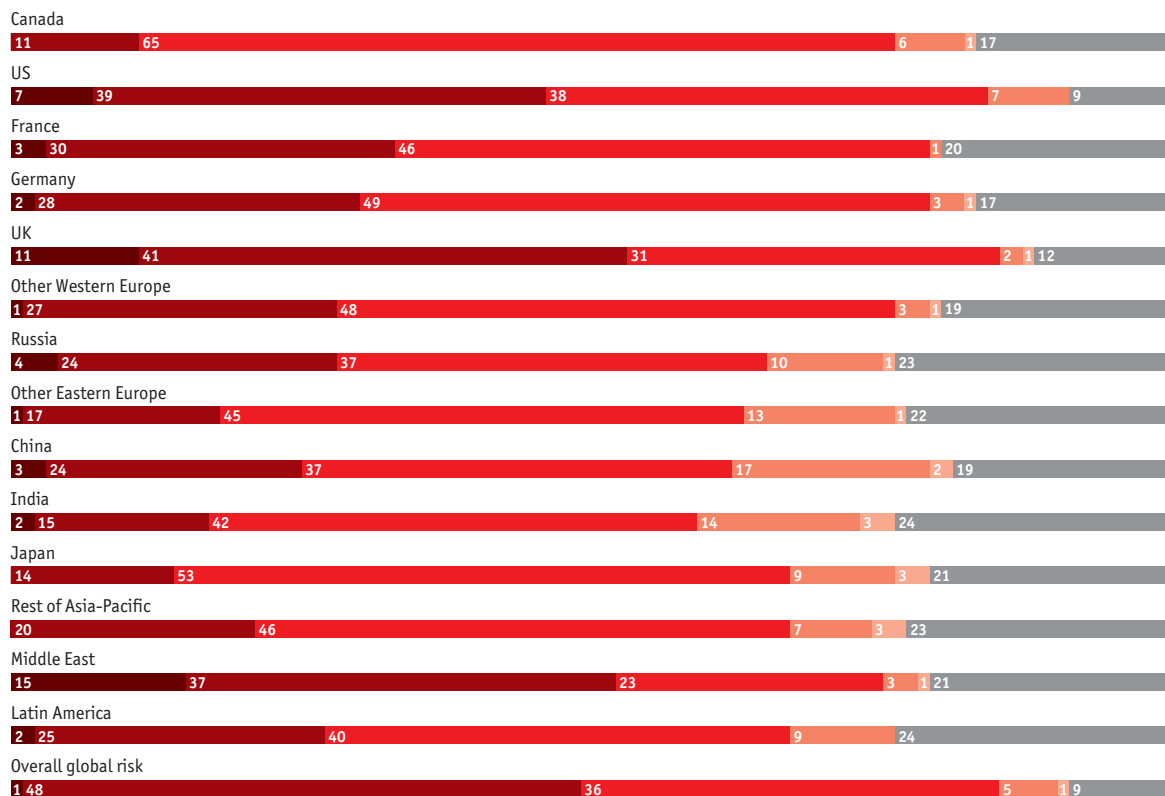
Appendix: Digital risk
The challenge for the CRO

How significant a threat do the following risks pose to your company's global business operation today?
Rate on a scale of 1 to 5, where 1=Very high risk and 5=Very low risk.
(% respondents)



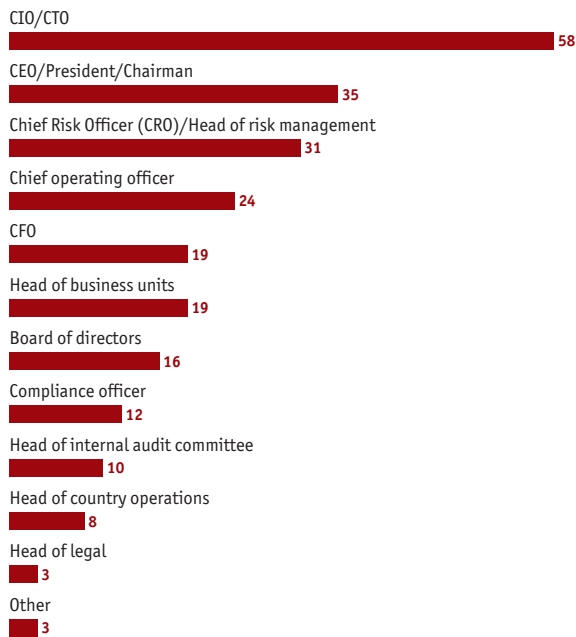
How has your organisation's assessment of risk in each of the following countries and regions changed over the last three months?
(% respondents)

Significant increase in risk ■ Slight increase in risk ■ No change ■ Slight decrease in risk ■ Significant decrease in risk ■ Don't know ■

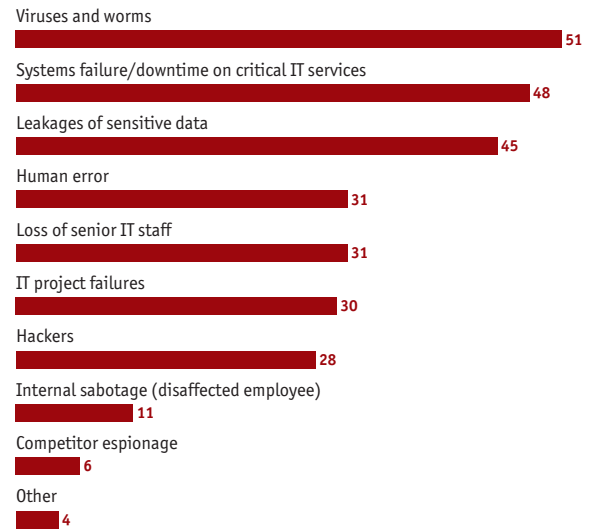


Appendix: Digital risk
The challenge for the CRO

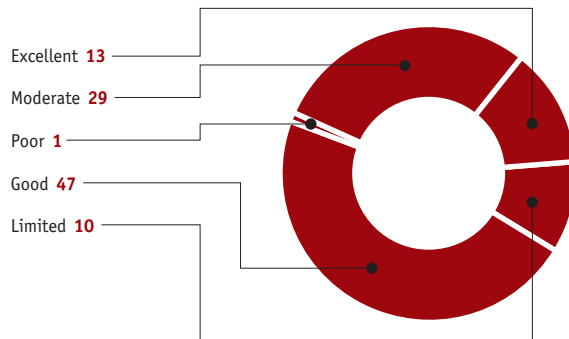
Who has significant responsibility for IT network risk in your company? Select all that apply.
(% respondents)



Which of the following pose the greatest IT risk at your company over the next three years? Select three options.
(% respondents)

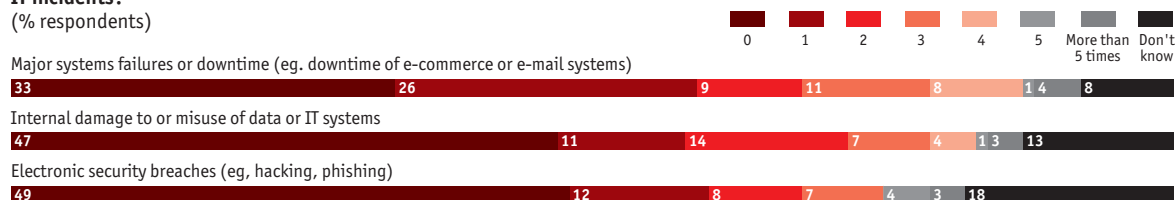


How would you rate your own understanding of the IT network risks facing your business?
(% respondents)



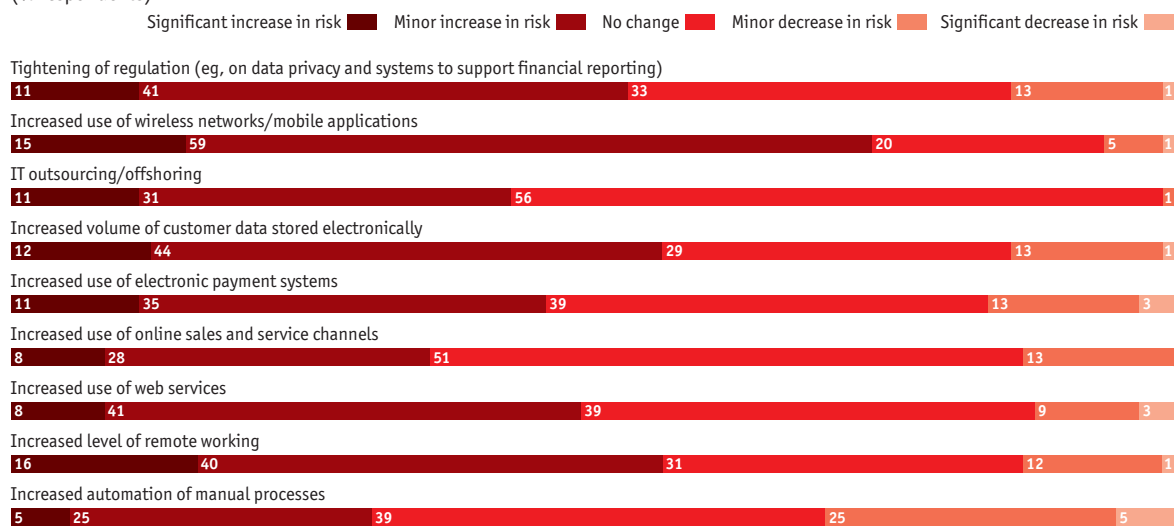
In the past 12 months, how many times has your organisation suffered significant financial damage as a result of the following IT incidents?

(% respondents)



How do the following IT-related trends affect your company's risk exposure?

(% respondents)



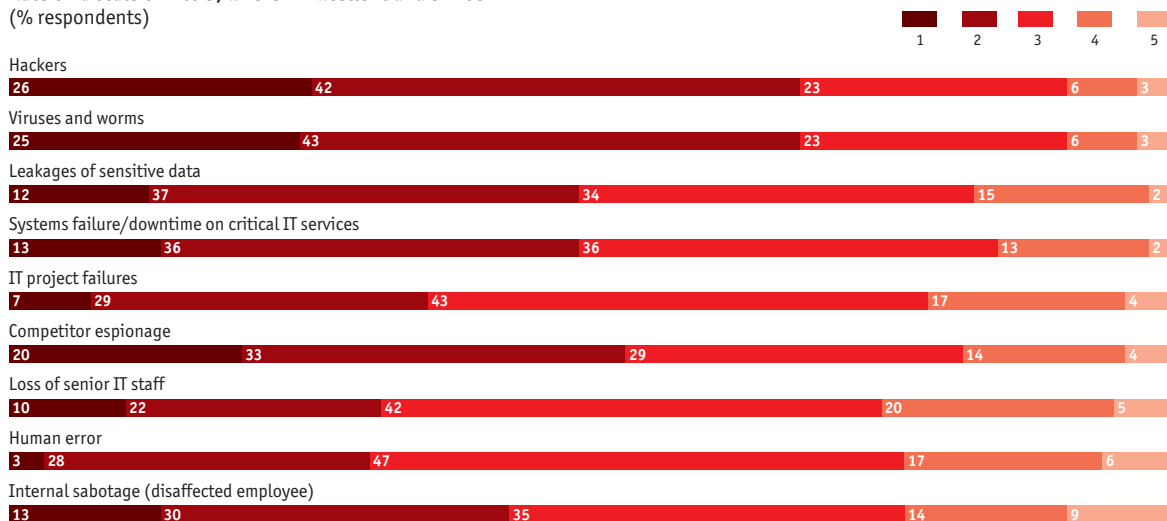
Appendix: Digital risk

The challenge for the CRO

How effective are your company's safeguards against the following IT network risks?

Rate on a scale of 1 to 5, where 1=Excellent and 5=Poor

(% respondents)



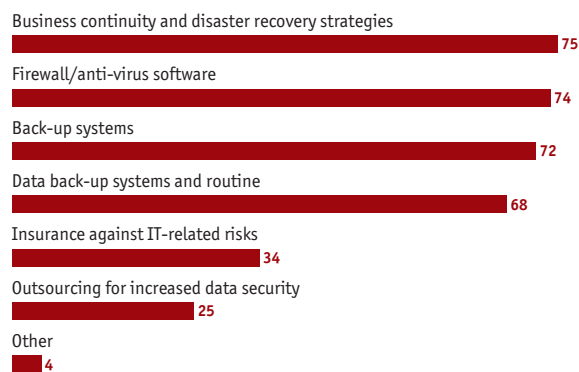
What is the role of your company's CRO (or equivalent) in regard to IT network risk? Select all that apply.

(% respondents)



Three years from today, which of the following tools and strategies will be most important for managing IT network risk? Select all that apply.

(% respondents)



How much involvement does your CRO (or equivalent) have in the following strategic IT activities?

(% respondents)

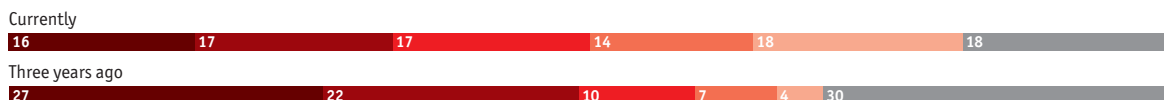
Significant involvement ■ Minor involvement ■ No involvement ■



How much time does your company's CRO (or equivalent) devote to managing IT risks today, compared with three years ago?

(% respondents)

0-5% ■ 5-10% ■ 10-15% ■ 15-20% ■ Over 20% ■ Don't know/Not applicable ■



How significant are the following difficulties in managing IT network risk in your company?

Rate on a scale of 1 to 5, where 1=Very significant and 5=Insignificant.

(% respondents)

1 ■ 2 ■ 3 ■ 4 ■ 5 ■

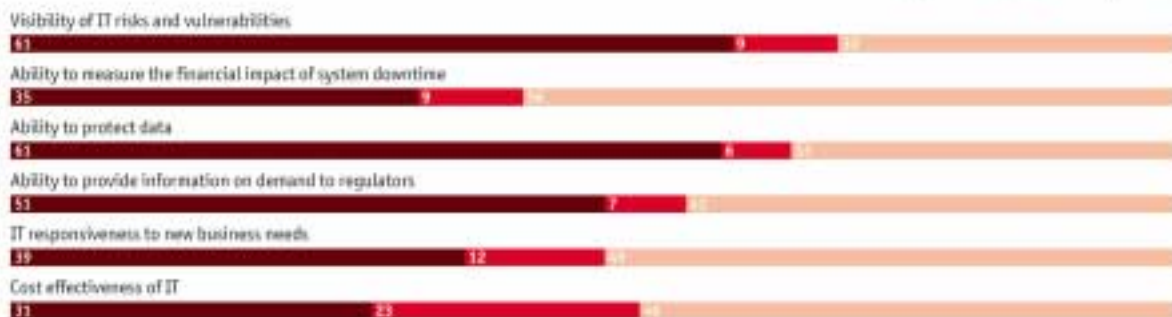


Appendix: Digital risk
The challenge for the CRO

Are your company's capabilities in the following areas better, worse or unchanged as a result of regulatory compliance initiatives in recent years?

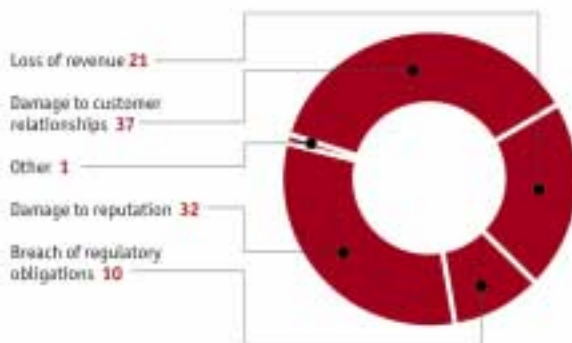
(% respondents)

Better ■ Worse ■ Unchanged ■



Which of the following represents the biggest threat to your business as a result of IT failures or breaches of security?

(% respondents)



Although every effort has been taken to verify the accuracy of this information, neither the Economist Intelligence Unit 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 this white paper.



ace european group

INSURING PROGRESSSM

ACE

The ACE European Group comprises the businesses of **ACE Europe, ACE Global Markets** and **ACE Tempest Re (Europe)**.

With an established presence in 16 countries across Europe and Freedom of Services permissions to operate in 27 European countries, ACE Europe provides a range of tailored Property and Casualty, Accident and Health and Personal Lines solutions for a diverse range of clients.

Headquartered in London, ACE European Group Limited is regulated by the Financial Services Authority and has been assigned an A+ (strong) financial strength rating from Standard & Poor's and an A (excellent) rating from AM Best.

The ACE Group of Companies is a global leader in insurance and reinsurance serving a diverse group of clients. Headed by ACE Limited (NYSE: ACE), a component of the Standard & Poor's 500 stock index, the ACE Group conducts its business on a worldwide basis with operating subsidiaries in more than 50 countries.

For further information visit www.ancelimited.com

Dataguard

ACE's Dataguard product has been specifically designed for companies who have a dependency on their computer network. It bridges the gaps in cover with traditional property insurance policies and provides peace of mind through comprehensive protection against first party financial loss arising from malicious or accidental incidents to computer networks or telecommunications systems. Dataguard also offers assistance in data reconstruction and company image re-establishment costs.

Computerguard

ACE Computerguard covers financial losses resulting from physical damage to, and breakdown of, computers. Cover includes the cost of replacing damaged computer hardware, the reinstatement of lost programmes or data, and the increased working costs as a result.

For further information on **Dataguard** or **Computerguard**, contact:

Benelux

Sijo Oudendag on +31 10 289 3582

France

Patrick Pouillot on +33 1 55 91 48 39

Germany

Joachim Sumpf on +49 69 75613 279

Italy

Riccardo Scalici on +39 2 2709 5617

Spain

Francisco Lázaro on +34 91 837 6801

UK

Shaun Cooper on +44 20 7173 7338

ACE European Group offices

United Kingdom

Headquarters

ACE Building
100 Leadenhall Street
London EC3A 3BP
+44 20 7173 7000 tel
+44 20 7173 7800 fax

Austria

Teinfaltstr.4
A-1010 Vienna
+43 1 710 93 55 tel
+43 1 710 95 20 fax

Belgium

Avenue des Nerviens 9-31
Nerviërsiaan 9-31
1040 Brussels
+32 2 516 9711 tel
+32 2 513 0884 fax

Denmark

Regus House
Larsbjørnsstræde 3
Postboks 1009
DK-1006 København
+45 33 13 55 33 tel
+45 33 13 23 49 fax

Finland

Mannerheimintie 12 B
FI-00100 Helsinki
+358 9 2512 2626 tel
+358 9 2512 2627 fax

France

Le Colisée
8 Avenue de l'Arche
92419 Courbevoie Cedex
Paris
+33 1 5591 4545 tel
+33 1 4788 4510 fax

Germany

Lurgiallee 10
60439 Frankfurt
+49 69 756 130 tel
+49 69 746 193 fax

Gibraltar

Suite 825
Europort
+350 75122 tel
+350 75129 fax

Ireland

2nd Floor
5 George's Dock, IFSC
Dublin 1
+353 1 440 1700 tel
+353 1 440 1701 fax

Italy

Viale Monza, 258
20128 Milan
+39 02 27095-1 tel
+39 02 27095-333 fax

Netherlands

Marten Meesweg 8-10
3068 AV Rotterdam
+31 10 289 3500 tel
+31 10 289 3599 fax

Norway

Stortorvet 3
NO-0155 Oslo
+47 23 31 5440 tel
+47 23 31 5441 fax

Poland

ul. Chmielna 85/87
00-805 Warsaw
+48 22 581 07 50 tel
+48 22 581 11 33 fax

Russia

CJSC ACE Insurance
Turchaninov per, 6-2
119034 Moscow
+7 495 727 42 45 tel
+7 495 727 42 46 fax

Spain

Francisco Gervás, No.13
Madrid 28020
+34 91 837-4977 tel
+34 91 837-6776 fax

Sweden

Klarabergsviadukten 90
SE-101 37 Stockholm
+46 8 692 5400 tel
+46 8 692 5410 fax

Switzerland

Mainaustrasse 30
CH-8008 Zurich
+41 43 456 7600 tel
+41 43 456 7601 fax

