

# Cyber Risks

in European Business Today

Conducted by StrategicRISK for ACE European Group

AUGUST 2006

Strategic**RISK**





# Contents

Executive Summary.....	04
Respondent Profile.....	06
Identifying and Mitigating Risks.....	09
Prevalent Losses and Disruptions.....	18
Overall Effectiveness.....	21

## Contact



Newsquest Specialist Media Business Intelligence, is a unit of Newsquest Specialist Media, providing customised market research for the financial & business community.  
Newsquest Specialist Media – a Gannett company



The mission of StrategicRISK is to deliver the latest risk and corporate governance solutions to key decision-takers in UK and European companies.

Peter Joy, Head of Research  
Tel: +44 (0)20 7618 3481 / [peter.joy@newsquestspecialistmedia.com](mailto:peter.joy@newsquestspecialistmedia.com)

Max Clapham, Head of Business Development  
Tel: +44 (0)20 7618 3411 / [max.clapham@newsquestspecialistmedia.com](mailto:max.clapham@newsquestspecialistmedia.com)

Tim Whitehouse, Managing Director  
Tel: +44 (0)20 7618 3469 / [tim.whitehouse@newsquestspecialistmedia.com](mailto:tim.whitehouse@newsquestspecialistmedia.com)

Suzanne Hirst, Publishing Director  
Tel: +44 (0)20 7618 3403 / [suzanne.hirst@strategicrisk.co.uk](mailto:suzanne.hirst@strategicrisk.co.uk)

Sue Copeman, Editor  
Tel: +44 (0)1787 237 446 / [sue.copeman@strategicrisk.co.uk](mailto:sue.copeman@strategicrisk.co.uk)

Tricia McBride, Group Production Manager  
Tel: +44 (0)20 7618 3425 / [tricia.mcbride@newsquestspecialistmedia.com](mailto:tricia.mcbride@newsquestspecialistmedia.com)

Graham Williams, Design / Workflow  
Tel: +44 (0)20 7618 3088 / [graham.williams@newsquestspecialistmedia.com](mailto:graham.williams@newsquestspecialistmedia.com)

# Executive Summary

During late July and August of 2006, Strategic RISK's research team conducted structured interviews with 50 individuals concerned with IT and/ or risk management in 48 companies and public sector organisations in Europe. The aim was to understand organisations' views of the external and internal IT-related threats they face and to discover the solidity of their defences against these threats.

What did we learn?

By no means have all companies - even the largest - got to grips with their IT risks. Sixteen per cent, including several multinationals, believe their organisations have only partly identified the IT-related threats they face. But a lot of effort is going into this task. Thanks to rapid changes in technology - and, to some extent, mergers and acquisition - risk mapping is widely viewed as a continuous process. While IT and Risk Managers do most of the work of identifying IT-related risks there is considerable input from other people within organisations.

## Risk Perception and Reality

What are the real threats? Most companies see viruses as the main external IT risk, with the risk of data theft or misuse a close second. Other key external threats are public disclosure of private information, and hackers. Extortion against data or systems is the area of least concern. But IT risks arising from physical disasters such as fire, flood, burglary, hardware failure and mainframe outages are viewed as real dangers.

As for internal IT threats, human error tops the table, with employee theft or misuse of data a very close second. The risk of a departing employee taking information and misusing it is a particularly widespread concern.

Companies are particularly vulnerable in some areas. Most prevention or mitigation of external risks centres around viruses, hackers and external electrical outages. Less emphasis is placed on denial of

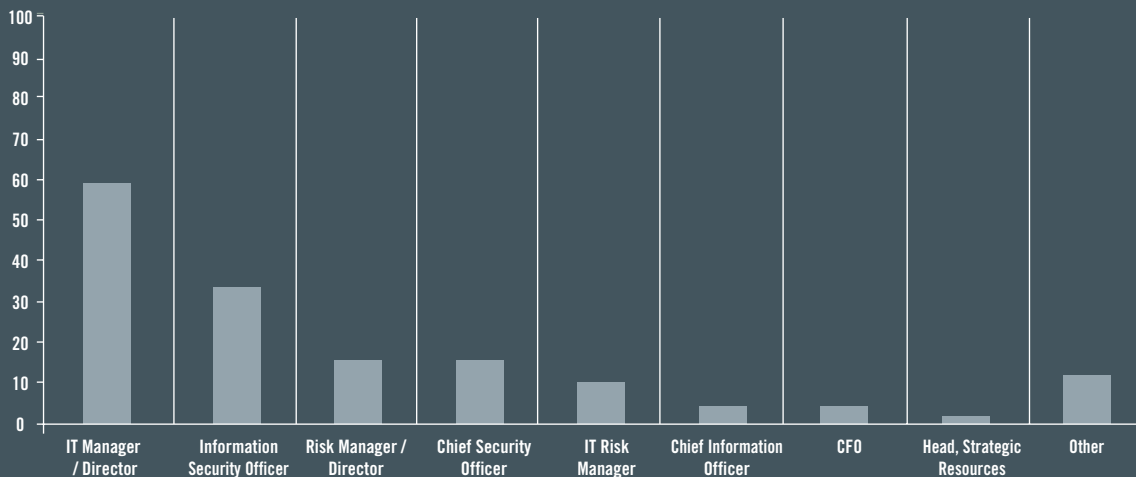
service attacks, defamation or copyright infringement issues, and disclosure of private information. Defences for extortion against data or systems, other malicious attacks and data theft or misuse appear to be even weaker. But the most vulnerable areas for most organisations are the non-electronic theft of passwords, third party fraud and - above all - the failure of IT partners or suppliers to manage their own risks. Some organisations have no controls at all in these areas.

*(see graph below)*

As regards internal risks, most businesses focus on controlling the effects of an internal electrical outage and preventing employee fraud. But fewer believe they have full controls in place for data processing errors, employee malicious attacks, theft or misuse of data, loss of or damage to physical equipment and human error.

*(see graph p5)*

### IT Managers and Info Security Officers commonly bear responsibility for IT security

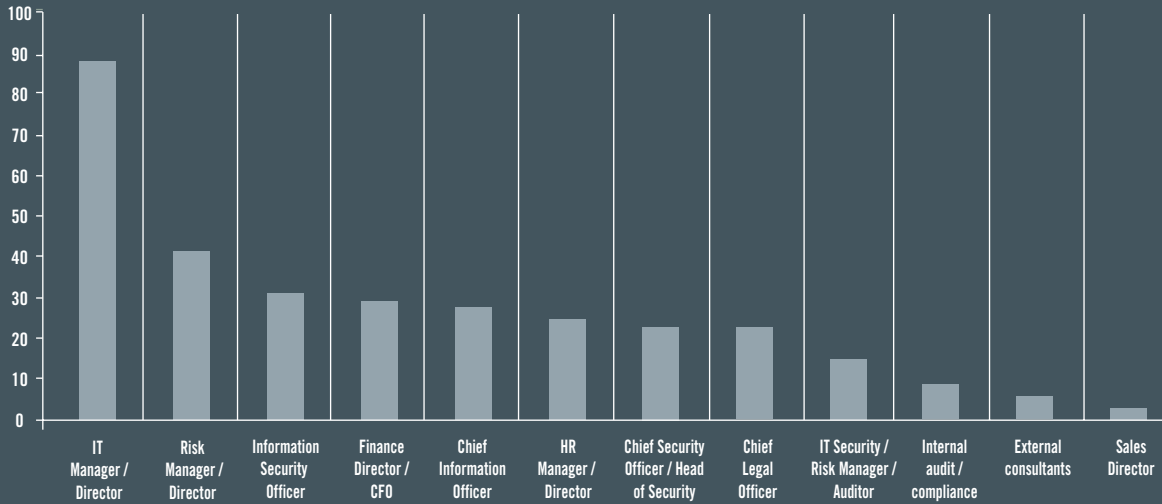


#### Who has DIRECT responsibility for IT security?

IT Manager/ Director	59%	Chief Information Officer	4%	CFO	4%
Information Security Officer	33%	Chief Security Officer	16%	Head, Strategic Resources	2%
Risk Manager/ Director	16%	IT Security/ IT Risk Manager	10%	Other	12%

Note: percentages do not total 100% as respondents could give more than one answer

IT and Risk Managers do most of the work of identifying IT-related risks



Who has been involved in identifying these (IT) risks?

IT Manager/ Director	88%	Chief Information Officer	27%	IT Security/ Risk Manager/ Auditor	14%
Risk Manager/ Director	41%	HR Manager/ Director	24%	Internal audit/ compliance	8%
Information Security Officer	31%	Chief Security Officer/ Head of Security	22%	External consultants	6%
Finance Director/ CFO	29%	Chief Legal Officer	22%	Sales Director	2%

Note: percentages do not add up to 100 as respondents could give multiple answers.

Organisations have a variety of strategies and tactics for limiting the impact of individual dishonesty, carelessness, incompetence or malice. But those in organisations with particularly serious security concerns tend to have robust vetting procedures - including criminal records checks - plus stringent training and monitoring systems.

In practice - it emerged - the most common cause of actual disruption to IT systems in the past 12 months had been human error. External electrical outage had been the next most common cause of disruption.

**Remote Access, Fraud and Insurance**

Most companies allow certain staff to access their servers from outside the company offices. But remote access is viewed as requiring tight security. Most larger organisations are already enforcing that security. But some smaller, or more old-fashioned businesses look very vulnerable to

unauthorised remote access. Remote access is often not limited to senior management, but also includes IT staff, middle management and front-line staff logging in from the field.

Computer fraud losses remain a problem. One respondent in seven stated that they had experienced a material case of computer fraud in the past 12 months. Three of the cases mentioned each involved less than €500,000, but the other four each involved losses of between €1 million and €5 million.

On insurance, it is relatively rare for a risk to be covered by a distinct, IT-specific insurance policy. Companies tend to look to their general commercial material damage and business interruption policies to include some cover for IT-related risks. Several respondents expressed a wish for more clarity, information and advice on this subject.

Overall, only a quarter of companies rated their IT risk management and business

continuity planning as 'fully effective'. Most of the rest rated them 'fairly effective'. But six per cent considered their IT risk management to be 'fairly ineffective'. - and ten per cent viewed their IT business continuity planning as 'fairly ineffective'.

In many companies, IT risk management and business continuity planning are hot issues. Many interviewees - several of them relatively new appointees - were conscious of just how much work needed to be done throughout their organisations to catch up to satisfactory standards of protection.

# Respondent Profile

## The Interviewees

During late July and August of 2006, we interviewed 50 individuals concerned with IT and/or risk management in 48 companies and public sector organisations. Interviewees were taken through a structured questionnaire with frequent opportunities for comment and discussion. A small number who were too busy to be interviewed completed the questionnaire online. The full list of respondents is as follows:

Adrian Clements	Insurance Risk Manager	Arcelor
Daniel Bertaux	Senior Risk Manager	Arcelor
Peter Versloot	Head of Global Controls	ABN AMRO Asset Management
Colin Campbell	Head of Risk Management	Arcadia Group
Ralf Mareczek	Senior Director	Bertelsmann AG
Keith Labbett	Head of Audit	British Waterways
David Whitham	IT Manager	Brown & Newirth Ltd
Kip Berkeley-Herring	Group Risk Manager	BT plc
Bob Nowill	Director of Information & Network Security	BT plc
Jean-Michel Paris	Corporate Risk Manager	Bureau Veritas
Steven Jones	Partner with Responsibility for IT	BWCI Group
Barry Ryder	Corporate Risk Manager	Camden Council
David Ketley	Insurance Manager	Europe and Asia Pacific, Cargill Inc.
Ben Jones	Insurance Manager	Comet
Jeremy Gumbley	Chief Security Officer	CreditCall
Peter Berring	Director of Group Risk	De La Rue
Julia Graham	Chief Risk Officer	DLA Piper Rudnick Gray Cary
Michael Lewis	Group Risk Director	EMI Group
Richard Kavanagh	ICT Manager	ENCAMS
Brendan McCullagh	Group Insurance Manager	ESB
Terry Cunningham	Director of Group Risk Management	Euronext
Hugh Rees	Head of Internal Audit	Eurotunnel
Ian Sirrs	Director of Risk and Assurance	Experian
Kirsten Vej	Risk Management Consultant	H. Lundbeck A/S
Joerg Hempelmann	Group IT Risk Manager	Ikea
Stephen Hart	Managing Director	Intersys Micronics
George Kyriazis	IT Manager	Mvision
Paul Goulding	Risk & Insurance Manager	News International
Tony Troy	Head of Information Security Assurance Unit	Metropolitan Police
Graham Hodgson	Group IT Director	Newsquest Media Group Ltd
Russell Cosway	ICT Business Manager & Info Security Officer	North Cornwall DC
Andrew Bye	Head of Risk Management	O2
Chris Halliday	IT Manager (Contract Services)	Peterborough City Council
Rafal Rudnicki	IT Manager	Raben Group
Tatiana Shemyakina	Executive Director	Russian Risk Management Society
George Haitsh	Vice President	Corporate Risk Management, SAP
Stefan Bauhofer	Risk Manager	Schindler
Kenneth Miger	Group Risk & Insurance Manager	Securitas
Frank Bär	Insurance Manager	Solvay S.A.
Jose Fonseca	Insurance Manager	Sonae
Paul Herbert	Senior Technical Specialist	States of Jersey
Phil Stunell	Managing Director	Stunell Technology
Keith Faulkner	European Business Support Manager	Thermo Electron
Nick Avery	Chief Risk Officer	Tote
Paul Jarvis	Health & Safety Advisor	Turning Point
Bridget Kenyon	Information Security Officer	University of Warwick
Jason Giller	Director	Veritas IT
Christian Scott	Head of IT & Communications	Ware Anthony Rust
Iain MacKay	VP of Information Services	Wolfson Microelectronics
Colin Weddell	Head of Technology	Wood Mackenzie

### Business Sectors

The largest group of respondents - 16 per cent - described their organisation's business as being professional or business services. Financial services, manufacturing and engineering and the media each accounted for 12 per cent of responses, with the public sector accounting for a further 10 per cent and retailing and leisure eight per cent. The remainder of respondents were spread across telecoms, transport, pharmaceuticals, IT, food production, energy, construction, education and the charitable sector.

*(see right)*

### Respondent Organisations' Size and Turnover

The numbers employed by respondent organisations range from less than 100 to tens of thousands. The majority employed at least 5,000 people.

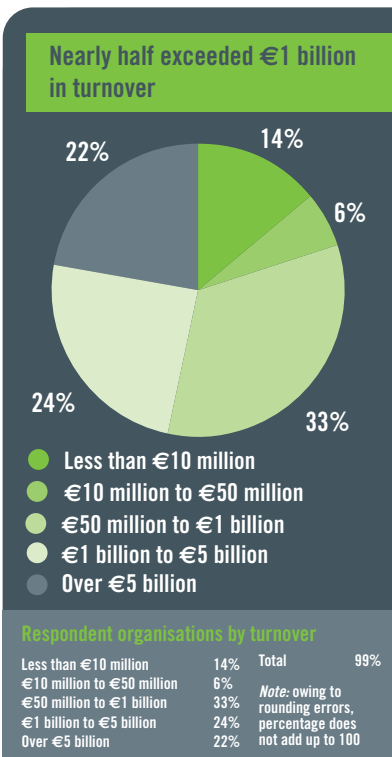
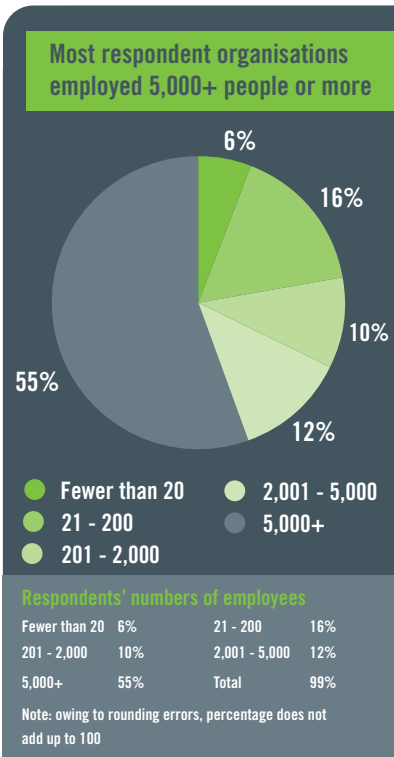
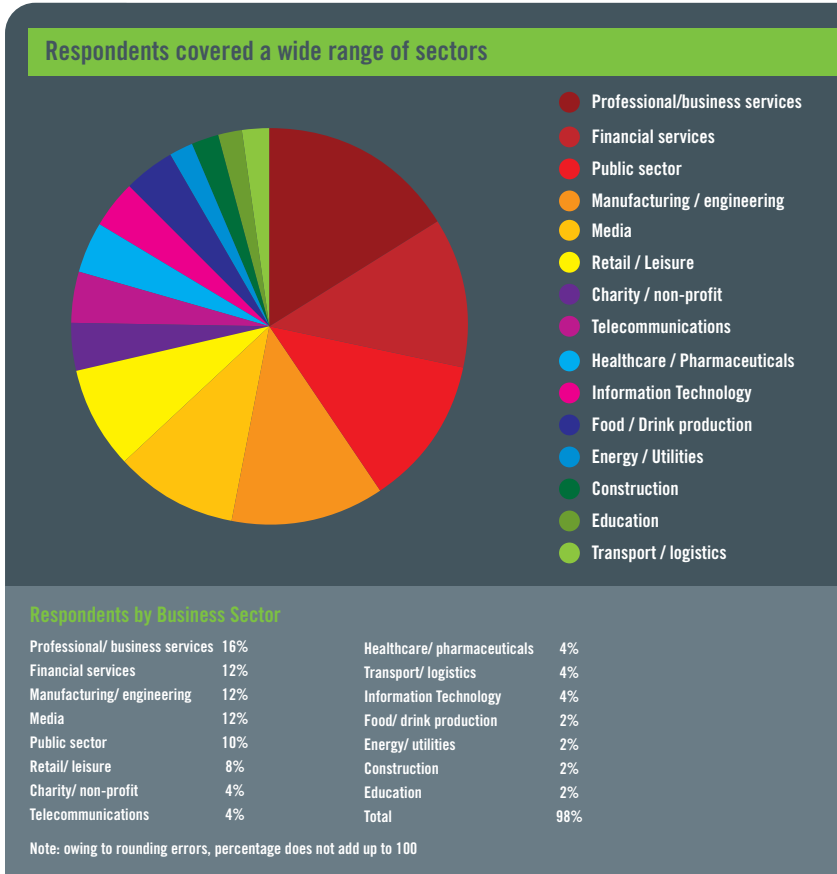
*(see bottom left)*

In terms of turnover, the largest group of respondents - 33 per cent - was in the €50 million to €1 billion band, but 46 per cent had a turnover in excess of €1 billion and 22 per cent exceeded €5 billion in turnover. A few companies were involved in financial or payment services, security, credit information or digital content and therefore enforced extremely high security standards, employing scores or even hundreds of staff in their IT security function. But for most, IT security was more an adjunct to routine business.

*(see bottom right)*

### Do you sell goods or services through a website trading platform?

We asked interviewees whether they sold goods or services through a website trading platform. Fifty-two per cent said they did. Eliminating the five public sector bodies raised this percentage, but only to 53 per cent, as - perhaps surprisingly - two of these bodies claimed to sell goods or services in this way.



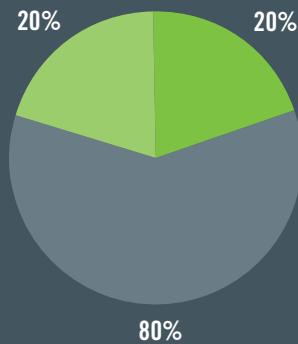
**Do you sell goods or services through a website trading platform?**

Yes	52%
No	48%
Total	100%

**If yes, is this business to business, business to retail consumer, or both?**

Of the 25 respondent organisations that did sell goods or services through a website trading platform, five did so only to other businesses, while five did so only to consumers. The remaining 15 - 60 per cent - sold to both.

**Six of every ten web trading platforms were both B2B and B2C**



- Business to Business
- Business to retail consumer
- Both

**Is this business to business, business to retail consumer, or both?**

Business to business	20%
Business to retail consumer	20%
Both	60%
Total	100%

**Does your website have facilities for receiving personal information from visitors, such as credit card or address details?**

Although only 52 per cent of respondent organisations sold goods or services through a website trading platform, 59 per cent had

facilities for receiving personal information from visitors, such as credit card or address details, on their websites. In some cases, this was as elementary as a sign-up process for newsletters or the facility to upload CVs or register for a course or conference.

**Does your website have facilities for receiving personal information from visitors, such as credit card or address details?**

Yes	59%
No	41%
Total	100%

**Does your company or organisation have an intranet and/ or an extranet and do they use company laptops for mobile working?**

Ninety-four per cent of the respondent companies interviewed said they had an intranet. Only six per cent - three companies - said they did not. All three were small

companies with fewer than 200 employees; two of them employed fewer than 20.

As for extranets, two thirds of respondent organisations used them. Those that did not use extranets included 80 per cent of public sector bodies - but only 13 per cent of the organisations with over €1 billion in turnover.

Laptops and other portable electronic devices are now practically ubiquitous in business - and as we shall see, they raise distinct security issues. At one respondent's business, a third of the workforce normally worked remotely from customers' premises. "We have 60 offices in 23 countries and employees can go to any of them, plug in and go." Of all the respondent organisations, only one said that no staff used company laptops for mobile working.

*(see graph below)*

**IT Managers and Info Security Officers commonly bear responsibility for IT security**



**Who has DIRECT responsibility for IT security?**

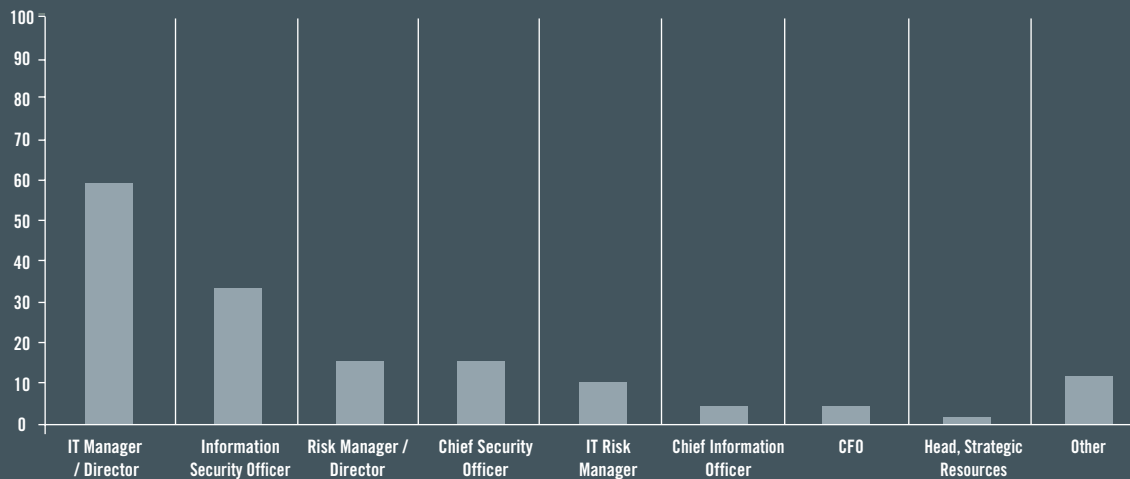
IT Manager/ Director	59%	Chief Information Officer	4%	CFO	4%
Information Security Officer	33%	Chief Security Officer	16%	Head, Strategic Resources	2%
Risk Manager/ Director	16%	IT Security/ IT Risk Manager	10%	Other	12%

Note: percentages do not total 100% as respondents could give more than one answer



# Identifying and Mitigating Risks

## IT Managers and Info Security Officers commonly bear responsibility for IT security



### Who has DIRECT responsibility for IT security?

IT Manager/ Director	59%	Chief Information Officer	4%	CFO	4%
Information Security Officer	33%	Chief Security Officer	16%	Head, Strategic Resources	2%
Risk Manager/ Director	16%	IT Security/ IT Risk Manager	10%	Other	12%

Note: percentages do not total 100% as respondents could give more than one answer

## Who in your organisation has direct responsibility for IT security?

Given a range of seven choices (Information Security Officer, Risk Manager/ Director, Chief Security Officer/ Head of Security, IT Manager/ Director, HR Manager/ Director, Finance Director/ CFO and Other - Please Specify) our 48 organisations gave 76 answers - an average of one to two individuals in each organisation.

(see graph above)

It will come as no surprise that IT Managers have direct responsibility for IT security in six organisations out of ten. In organisations where they did not, there tended to be one or more specialised individuals typically who took primary responsibility - an Information Security Officer, Chief Security Officer, or, as ten per cent of interviewees mentioned of their own accord, an IT Security Manager or IT Risk Manager.

One interviewee, for example, had individual responsibility for developing security policy and procedures, but worked in conjunction

with a multi-departmental security group that agreed policies. Current policies and procedures, though compliant to BS7799, had not been developed using a risk assessment-based approach - an approach to which the company was now moving. Another respondent described his firm's approach as being "led by the security function, but consulting finance, HR and legal".

The Information Security Officer figure includes one company that devolved responsibility to numerous Information Security Officers across its operations. Another described the role of its Information Security Officer as being "to identify risks and solutions, make recommendations and suggest policies, manage incidents and otherwise advise information owners - but not to implement solutions. It is information owners - such as heads of department - who have direct responsibility for IT security in their business areas."

'Other' responses (not including IT Security or IT Risk Manager) included: a risk

management team and committee reporting to the Finance Director; information owners ('typically heads of departments'); an Infrastructure Manager; a Head of Strategic Resources; and a dedicated IT risk committee. Other respondents said responsibility was diffused along business lines.

Many respondents pointed out that IT security is, to some extent, the responsibility of all. "Ultimately everyone in the organisation is expected to take responsibility - and signs up to protecting the network," said one senior manager in a professional services firm.

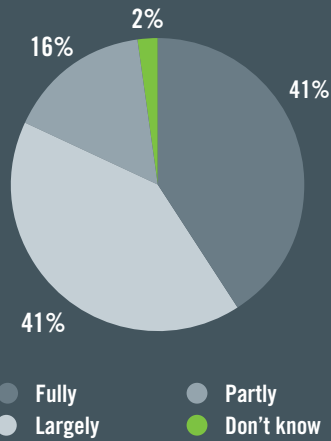
## In your view, has the organisation identified (mapped) its key IT risks?

Interviewees had a choice of 'Fully', 'Largely', 'Partly' and 'Hardly at all', plus 'Don't know', though only one respondent chose the latter response. No one said that their organisation had hardly identified its key risks at all.

(see graph on p10)



**Eighty-two per cent reckoned they had fully or largely mapped their IT risks**



**Has your organisation identified (mapped) its key IT risks**

Fully	41%	Largely	41%
Partly	16%	Hardly at all	0%
Don't know	2%	Total	100%

Forty one per cent said their IT risks had been fully mapped. The same again believed the job was largely complete. Sixteen per cent, however, said that their organisation had only partly identified the IT-related threats it faced.

What sort of firms were these? Of these eight organisations, one was a charity and another was a small business services firm. The other six, however, were all large organisations with over 5,000 staff. Several were multinational operations and several were in fact currently engaged in efforts to review and improve IT risk management processes. One IT Security Manager flagged up the influence of "residual elements of risk" in acquisitions, which can require fresh updates of risk maps.

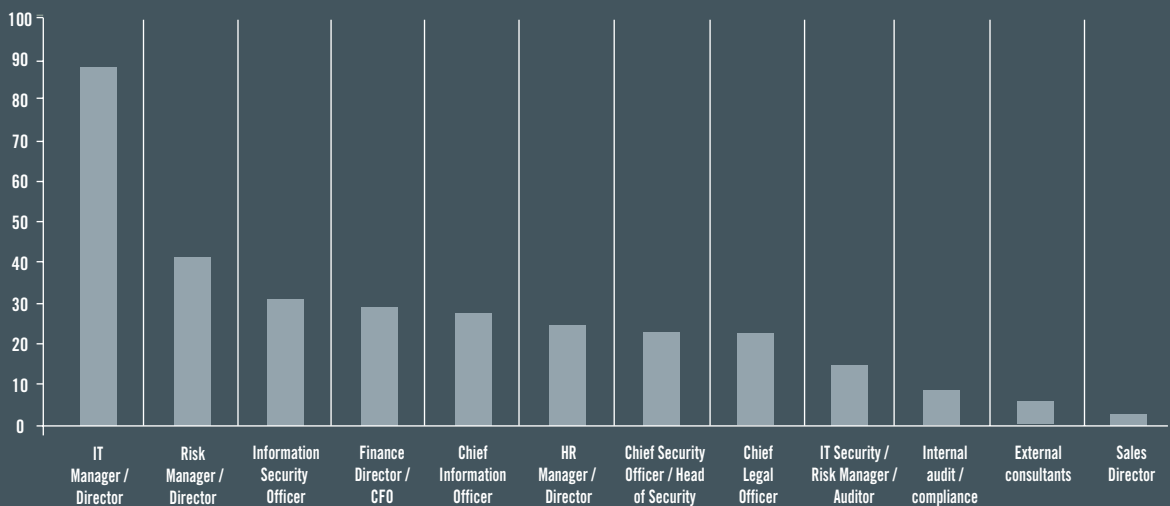
There was a common recognition that risk mapping has to be a continuous process. As one senior IT manager in a large and sophisticated FTSE 100 company put it: "Have we mapped our key IT risks? Yes for today's risks - less so for tomorrow's."

**Who has been involved in identifying these risks?**

Who actually gets involved in identifying the IT risks that organisations face? We offered interviewees nine options (IT Manager/ Director, Risk Manager/ Director, Information Security Officer, Chief Information Officer, Finance Director/ CFO, HR Manager/ Director, Chief Security Officer/ Head of Security, Chief Legal Officer, and Other - please specify). (see graph below)

No surprise that nearly nine out of ten respondents cited the organisation's IT Manager or Director as having been involved in identifying their organisation's IT risks. Forty-one per cent said their Risk Manager or Director had been involved, while 31 per cent cited an Information Security Officer or similar and 29 per cent, the Finance Director or CFO. One institution currently had an Information Security Officer busy interviewing all senior administrative, professional, technical and operational staff to identify risks. Twenty-seven per cent mentioned a Chief Information Officer, 24

**IT and Risk Managers do most of the work of identifying IT-related risks**



**Who has been involved in identifying these (IT) risks?**

IT Manager/ Director	88%	Chief Information Officer	27%	IT Security/ Risk Manager/ Auditor	14%
Risk Manager/ Director	41%	HR Manager/ Director	24%	Internal audit/ compliance	8%
Information Security Officer	31%	Chief Security Officer/ Head of Security	22%	External consultants	6%
Finance Director/ CFO	29%	Chief Legal Officer	22%	Sales Director	2%

Note: percentages do not add up to 100 as respondents could give multiple answers.



per cent an HR Manager or Director, 22 per cent a Head of Security and 22 per cent a Head of Legal.

Respondents also mentioned several other species of manager. Fourteen per cent cited an IT Security Officer, IT Risk Manager or IT Audit Officer as being involved in identifying IT risks. A further eight per cent mentioned the role of their internal audit function, while six per cent made reference to external consultants.

Is it a case of the more contributors to the process, the better? "We are in a fast-moving, dynamic environment," said a Risk Director in a multinational financial services operation. "Openness and transparency help to proactively identify risks."

One respondent from a large multinational described how their IT Security Manager had been leading a fresh risk mapping effort with the aim of getting "a more granular approach to their risk catalogue - looking in more detail and breaking it down into

subsidiary risks which we will have more ability to manage." Consultants were helping too. They had recently appointed - for the first time - a Technology Security Officer and a Chief Information Officer to whom the IT Security Manager reported.

### Which of the following do you consider to be key external IT risks for your company?

What are businesses' real external IT risks? We offered interviewees the choice of a dozen threats and the opportunity to volunteer any other key threats they perceived.

While most firms considered most of the threat-list to be genuine risks, that did not necessarily make them *key* risks. The figures below deal with risks interviewees specifically regarded as key risks.

*(see graph above)*

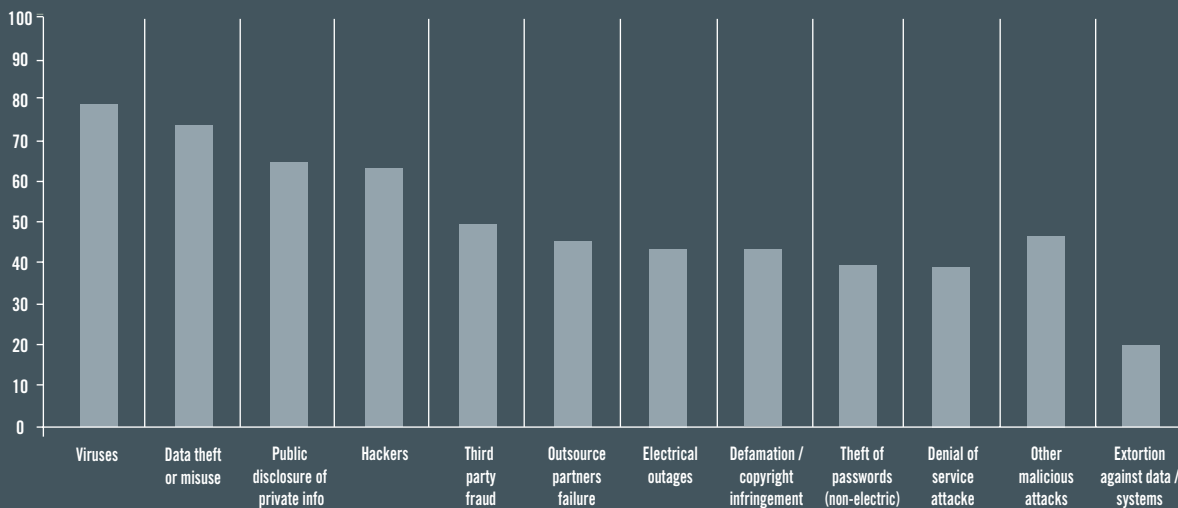
Seventy-eight per cent saw viruses as a key external risk, while 73 per cent were concerned at the risk of data theft or misuse. At an increasing number of organisations, of course, the whole business

hangs on data and its confidentiality. A further 65 per cent saw public disclosure of private information as a key threat. Hackers were a key risk for 63 per cent, while third party fraud, outsourced IT partners' failings, electrical outages and defamation or copyright infringement all registered as key risks with 40 to 50 per cent of respondents. Third party fraud was perhaps less of a risk for interviewees from regulated professional firms than in other businesses, owing to the stringent 'know your customer' enquiries they are obliged to conduct.

Theft of passwords and denial of service attacks were a key concern for 39 per cent, while other malicious attacks - i.e. ones other than those already mentioned above - were a key concern for 47 per cent. One professional services firm had experienced a denial of service attack just weeks earlier - though it was alerted almost instantly and was able to stop it within three minutes.

Extortion against data or systems was the area of least concern: just one respondent in

## Viruses and data theft or misuse topped the table as key external IT risks



Viruses	78%	Third party fraud	49%	Theft of passwords (non-electronic)	39%
Data theft or misuse	73%	Outsource partners' failure to manage risk	45%	Denial of service attacks	39%
Public disclosure of private information	65%	Electrical outages	43%	Other malicious attacks	47%
Hackers	63%	Defamation/ copyright infringement	43%	Extortion against data/ systems	20%

Note: percentages do not add up to 100 as respondents could give multiple answers.



five considered it a key external risk. One respondent from a large and sophisticated business said that: 'Extortion is a key risk, though we don't get much of it.' On hacking, the same interviewee remarked that they "care about some kinds: we're less concerned by schoolboys in their bedrooms than by organised criminals with serious resources behind them." One public sector organisation mentioned applying BS7799 on external risks.

Perceptions of what was a 'key risk' quite often depended on the nature of the respondent's business and many saw plenty of risks, but relatively few 'key' risks. Some privately owned businesses, probably valuing their financial privacy, seemed particularly concerned about public disclosure of private information. Companies heavily dependent on their intellectual property were naturally very concerned to keep it secure.

Interviewees offered a few specific key external risks of their own. These included:

spyware; Trojans and 'phishing' expeditions; loss of laptops and any critical data on them; and access granted to mobile users being compromised in some way.

One IT specialist in a large public sector organisation observed that while denial of service attacks are common, they are no longer much of a threat to his organisation. Another risk manager reckoned that the threat from viruses had declined substantially within the past 12 months. One risk manager in a large professional services firm made a point of ensuring that all '501' scams were quarantined in a central location - less to protect the firm's finances than its reputation.

Negative feedback at external sites was another concern volunteered by interviewees. For a large business, this is probably as unavoidable as the weather. Smaller firms, however, seem to genuinely fear a material impact on their business from such comment. Another point raised

was the carelessness of corporate foot-soldiers - "users who don't know what they're doing, who are exposing systems to external risk," as one Information Security Officer put it. Changes in technology - including upgrades - were also seen as exposing organisations to many species of risk.

The key external IT risk interviewees most commonly raised of their own accord was that of physical disaster: fire, flood, burglary, hardware failure and mainframe outages. "A true physical disaster to a main platform would be a major problem for us," explained one risk manager, who was in the midst of a major review of IT risks in his large multinational company. "We have mirroring and backups, but these have never been tested in anger."

Another stated it even more plainly. "The main risk for our 130,000-employee group remains the loss of one of the two main computer centres."

### Human error and employee theft or misuse were the two most-identified key internal risks



#### Which are key internal IT risks for your company?

Human error	69%	Employee fraud	39%
Employee theft or misuse of data	65%	Internal electrical outage	37%
Data processing error	47%	Employee loss or damage of physical equipment	33%
Employee malicious attack	45%		

Note: percentages do not add up to 100 as respondents could give multiple answers.



### Which of the following do you consider to be the key internal IT risks for your company?

What about the threat within? Interviewees were offered a choice of seven potential internal IT risks (Human error, Employee theft or misuse of data, Employee malicious attack, Data processing error, Employee fraud, Internal electrical outage and Employee loss or damage of physical equipment) and were asked which were the key concerns for their organisation. They also had the opportunity to volunteer others. Again, the focus was not on risks in general, but on 'key risks' to the interviewee's own organisation.

*(see graph on p12)*

Simple human error topped the key internal IT risks table; 69 per cent of respondents identified it as a key risk. But employee theft or misuse of data came a very close second. The risk of a departing employee taking information with them and misusing it is a particularly widespread concern. "Employee theft or misuse of data is our single greatest concern," said one senior figure in a

professional services firm. An IT Security Manager in a major retail group agreed: "The main threat is intentional or unintentional release of customer data. Identity theft and the security of credit card information are serious concerns." Another respondent remarked on the fact that their confidential price lists commonly reached their competitors.

"Bungs for information are a concern," said one respondent. "Fifty thousand staff are, in effect, the main threat to security." There, an automatic auditing system with deterrent sanctions offsets temptation.

Nearly half of respondents saw data processing errors as a key internal risk. It seems curious that more respondents (45 per cent) were concerned by the threat of malicious attack by an employee than by a fraud by one (39 per cent), though many did mention having tight anti-fraud procedures in place. Internal electrical outage and employees' loss of or damage to physical equipment were seen as key risks by 37 per cent and 33 per cent respectively.

One senior risk manager offered some worthwhile insights into the implications of outsourcing and contracting. "With partners and contractors, the distinction between employees - insiders versus outsiders - has become blurred," he said. "You don't know whether they're loyal to us or someone else. That blurring (and hence the 'internal' risk) is increasing rather than decreasing. With 'people risks' - such as disclosure of information or defamation - it is harder to put controls in place because people's motives are harder to control."

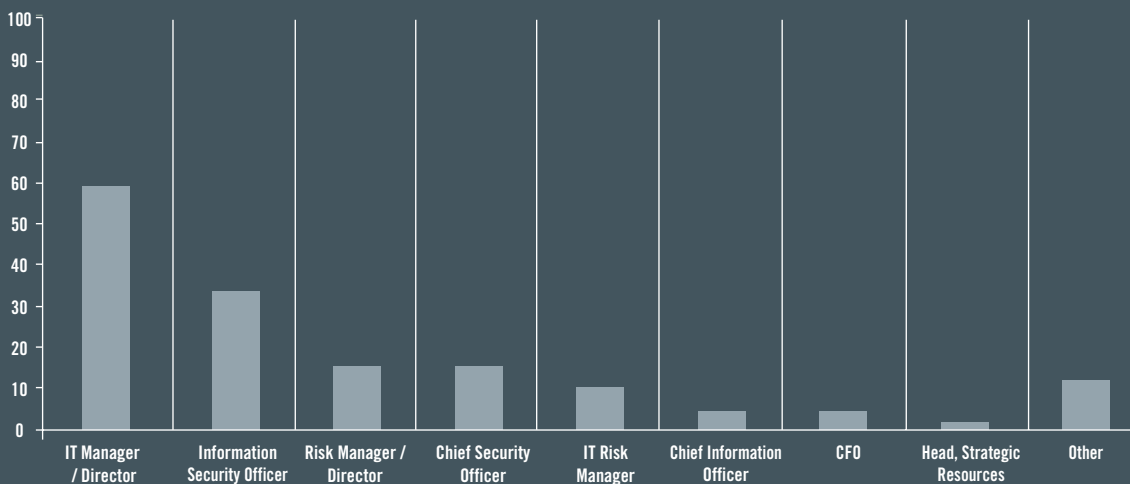
### To what extent does your company have controls and processes in place to prevent or mitigate the following external risks?

We asked interviewees to what extent they had processes or controls in place to mitigate or prevent a range of a dozen different external risks: 'complete controls', 'partial controls' or 'no controls'. The few 'don't knows' were excluded.

*(see graph below)*



### IT Managers and Info Security Officers commonly bear responsibility for IT security



#### Who has DIRECT responsibility for IT security?

IT Manager/ Director	59%	Chief Information Officer	4%	CFO	4%
Information Security Officer	33%	Chief Security Officer	16%	Head, Strategic Resources	2%
Risk Manager/ Director	16%	IT Security/ IT Risk Manager	10%	Other	12%

Note: percentages do not total 100% as respondents could give more than one answer

Seventy-two per cent reckoned they had complete controls in place for viruses, while 56 per cent said they had complete controls for hackers and 43 per cent for external electrical outages. On denial of service attacks, defamation or copyright infringement issues and disclosure of private information, they were less confident: in each case, around 45 per cent of respondents believed they had complete controls.

Many had a due sense of caution, however. As one interviewee said: "We can never rest on our laurels. We never feel 'we have this one licked'." Another commented: "These issues are far more complex than the question suggests. Anyone who answers 'full controls' to most of these questions is deluding themselves."

Defences for extortion against data or systems, other malicious attacks and data theft or misuse appear to be even weaker: just 35-37 per cent of respondents reported complete controls in these areas. But the most vulnerable areas for most

organisations, it appears, are the non-electronic theft of passwords, third party fraud and - above all - the failure of IT partners or suppliers to manage their own risks. On each of these fronts, less than one third of respondents reported having complete controls in place.

What about situations where organisations admit to having no controls in place at all? A full 20 per cent of respondents said their firms had no controls in place for extortion against data or systems. Double-digit percentages also admitted to having no controls for defamation or copyright infringement, public disclosure of private information or failure of outsourced IT suppliers' or partners' risk management.

### To what extent does your company have controls and processes in place to prevent or mitigate the following internal risks?

We then asked much the same question for internal controls. Interviewees had a list of

seven IT-related risks of internal origin and were asked to state the extent of the controls they had in place to deal with them. A small handful of 'don't knows' have been excluded from calculations.

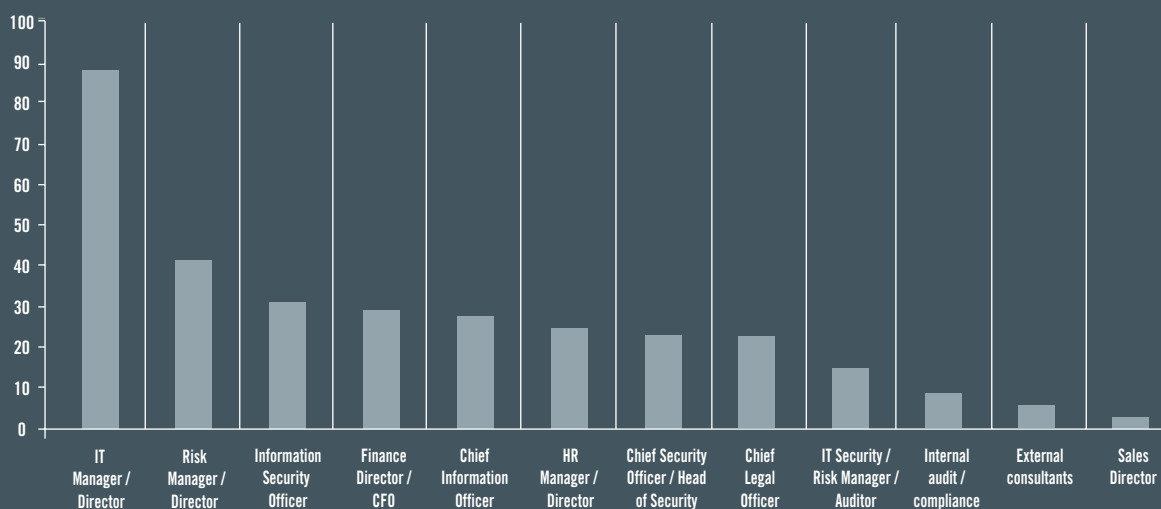
*(see graph below)*

Nearly three-quarters of businesses said they had full controls in place to cope with an internal electrical outage. Forty-eight per cent of interviewees said they had full controls in place for employee fraud, with another 50 per cent saying they had partial controls here.

In all other areas, however - data processing errors, employee malicious attacks, theft or misuse of data and loss of or damage to physical equipment and human error - the proportion of organisations believing they had full controls in place ranged from 32 per cent right down to a paltry 18 per cent.

Where malicious attack, theft or misuse of data and human error by employees was concerned, nine per cent of interviewees

### IT and Risk Managers do most of the work of identifying IT-related risks



#### Who has been involved in identifying these (IT) risks?

IT Manager / Director	88%	Chief Information Officer	27%	IT Security / Risk Manager / Auditor	14%
Risk Manager / Director	41%	HR Manager / Director	24%	Internal audit / compliance	8%
Information Security Officer	31%	Chief Security Officer / Head of Security	22%	External consultants	6%
Finance Director / CFO	29%	Chief Legal Officer	22%	Sales Director	2%

Note: percentages do not add up to 100 as respondents could give multiple answers.



admitted to having no controls in place at all. For loss or theft of physical equipment by employees, the figure was 13 per cent.

### What form, in general, do these controls and processes take?

We asked interviewees to talk us through the nature of their controls against external and internal IT risks. Naturally there were huge variations in the technologies, systems and controls that organisations had in place. What is practicable or relevant for a financial services company with 100,000 staff in 50 countries may well not be for a 100-person media business. Even so, the amount of comment was broadly in line with the level of concern interviewees had about various issues - and some interesting points emerged regarding the risk control methods different organisations are applying.

### External Risks

On external risks, respondents cited a range of policies, technological defences and back-up procedures. Dealing first with viruses, one interviewee from a large financial group spoke of the need for an "industry wide effort to batten down the hatches", and the need to implement a "secondary defence regime, with all virus patches, firewalls and intruder detection systems." Another respondent listed his company's robust anti-virus protections on servers and desktops and its security measures on downloads and e-mails - but confessed that anti-virus software was lacking on company PDAs, Blackberries and smartphones. These devices, it seems, are a growing security issue. So, according to one respondent, is VOIP technology.

Where hackers are concerned, a large part of many companies' defence strategy consists of having tough enough defences to move the perpetrator on to someone more vulnerable. Many now had intrusion detection systems and where the business justifies it, some were investing serious money in penetration-testing. On denial of service attacks, smaller organisations with limited resources are tending to rely on their ISP for protection. One respondent mentioned his

organisation having been used on several occasions as a way station to attack other systems.

People had little to say about extortion, but one large company mentioned having been the subject of 'phishing' attacks where scammers had targeted customers with fake versions of its websites. A couple of interviewees saw the shift to electronic banking and billing as a source of risk, but far more made mention of the controls they had in place to prevent third party fraud. One respondent mentioned conducting careful checks when signing up customers and suppliers for accounts, while another mentioned audit controls and policies on segregation of duties to prevent collusion between employees, or employees and outsiders. Many felt third party fraud to be a particular concern when it involved overseas contractors.

Fraudsters cannot get a toehold without information. "One can avoid third party fraud by simply never giving any information to third parties," said one interviewee.

The process of implementing new systems and software was also felt to present an opportunity to attackers. Interviews gave the impression that not all organisations are as rigorous as they could be on security-testing internal applications before deploying them.

On mitigating the risk of password theft, one respondent mentioned how his firm used a three-factor authentication system. Sensible access controls, of course, can minimise the potential damage from the loss of a password.

Judging by the interviews, the gold standard of protection on electrical outage is to have multiple feeds from utilities, plus UPS on critical systems at least. But mitigating electrical outages is seen as expensive. Investing in resilience at data centres - and requiring the same from one's ISP - were also mentioned.

Copyright infringement was a key issue for

relatively few companies, but the businesses we spoke to included several to whom protection of copyrighted material was fundamental. These had strict and sophisticated controls to prevent customers, for example, transmitting downloaded content onwards for sharing.

As for IT partners' failure to manage key risks, most saw a combination of detailed contractual controls and vigilant supervision as the key - including checklists of standards and requirements for suppliers to comply with their organisation's own security policies. "We ensure that outsourced providers' risk practices and controls are aligned to our company, fully vet and test their risk management and BCP and do regular switch tests to confirm their capability," said one fairly typical large-company respondent.

With outsourced services now absolutely integral to many businesses' operations, many large companies treat this issue with the utmost seriousness, monitoring it at Board level. "If outsourced IT people fail to manage their key risks, we see that as our failure to quality check and manage the outsourcers properly," said one interviewee.

Set up properly, however, outsourced services can perform at least as well as in-house operations. "Our servers are maintained by a third party," said one respondent from a retail business. "Following a power outage at one site, the contractor simply switched to their backup site and systems - so we were affected only temporarily and in a minor way."

One IT Security Manager in a huge worldwide business made an interesting point on the way in which the ground is shifting under corporate risk managers' feet. The need to protect information is balanced against a growing need to share it. "Extranets and external suppliers and more developed CRM mean that we are merging more of our businesses into the corporate world," he said. "Boundaries disappear and maintaining security is a constant challenge."



## Remote Access

Remote access a boon to business. But it is also a hot security issue and there was a clear sense among interviewees that such access needs to be firmly governed. In the larger organisations, access tended already to be pretty tightly managed. "Those with laptops have to be granted specific permission," said one Financial Director. "Access is not by default. Remote access is given to key staff at all levels in the organisation and numbers are increasing, but it would never be given to all 30,000 staff."

Others took a similar line. "External access to servers is limited to certain people and to a varying extent," said one IT Manager from the business services field. "It is almost always simply e-mail rather than access to data-based systems." Another said: "Anyone who has remote access to systems has to be authorised by the chief officer in their business area. It has to be justified at that level."

Were there any interesting technical innovations? Firewalls, of course, are vital to a mobile working strategy. Among the tightest-run organisations was one whose home-working policy transformed laptops into dumb terminals the moment their users dial in. In several cases, remote users were required to connect through an additional bolt-on security device, to prevent hackers breaking in. One local authority mentioned the use of remote access keys, while another public body was considering bringing in mobile boot-up disks, which can provide secure web-mail via users' home PCs.

One financial services group requires users to be onsite to access anything on its systems. "We have no remote dial in, which eliminates a lot of issues."

But some smaller businesses are wide open to unauthorised remote access. "A concern is staff failing to log off completely from public terminals, such as in airport lounges," said one respondent from a middling-sized,

growing business. "The next user could then access our company systems."

## Internal Risks

On risks of internal origin, the human factor is paramount. Interviewees mentioned a variety of strategies and tactics for limiting the impact of individual dishonesty, carelessness, incompetence or malice. "In most large organisations, it is acknowledged that insiders are more likely to compromise security than external attackers," said one respondent. This view was the norm.

Smaller, closer-knit businesses tended to be more relaxed. "All our staff have longevity within the businesses and we trust them implicitly," said the MD of one IT firm. "But appropriate checks and internal procedures are in place."

Some organisations see value in a daily restatement of employees' duties. "Staff are made very aware of our policies and their responsibilities," said one local authority IT Manager. "They can't dial into the system in the morning without agreeing to them." Internet and e-mail acceptable use policies and email content screening were common.

Many respondents, particularly those in large organisations and/ or those with particularly serious security concerns, outlined vetting procedures - including criminal records checks - plus training and monitoring systems. Sensible access controls are also crucial. "It's partly down to trust though," said one. "A disgruntled employee may well know how to get round technical controls."

Another explained: "We place great emphasis on vetting and monitoring staff behaviour (e.g. by comprehensive audit logs) and ensuring that they are aware of their responsibilities and that firm sanctions are in place for misuse of information systems. In terms of technical security, we're now doing about as much as can reasonably be expected given the availability requirements for our information." Too much logging and controlling can impact on a system's practical usability. Prevalent issues? One firm mentioned the

high turnover of staff in its Eastern European operations as creating internal security problems.

Most large organisations have a mix of policies and technical controls to monitor activity and prevent, or at least alert managers to, access breaches and attempts to transfer data externally by email. Some respondents also mentioned bans on employees attaching their own devices to company hardware. But these can be hard to enforce - and stopping people printing material onto paper and physically removing it can be a lot more difficult.

Several respondents mentioned checks and procedures on systems to mitigate data processing errors. Data processing errors predate computers, however, and automation probably does more to reduce than to increase this problem.

Employee fraud? For most organisations it seems to be more of a matter for the audit and finance departments, and the policies and procedures they put in place, than for IT. Interestingly, though, one large company did mention having a whistleblowers' line on which people could report fraud and an ethics policy "to encourage honest behaviours".

Theft of laptops, one respondent said, "tends to go in bursts where a particular department will get lax in its approach - and then lose ten in a month as part of a systematic raid." Others then tighten up, for a while. But staff in some organisations seem to be much more prone to leaving their company laptops behind or unattended than those in others. One large multinational with a turnover in the tens of billions reported having lost just three laptops in three years.

Perhaps the best summary of the internal threat was this, from a Risk Manager in a large, hi-tech company: "The modern management challenge is how to put the right controls on people. IT opens up new security challenges - but the counterpart is



that following an audit trail to dodgy employees is now so much easier."

### Conclusion

For the most sophisticated firms, IT risk - whether internal or external in origin - is today an accepted part of day-to-day operations. "We've been looking at this issue for 15 years," said one interviewee in a FTSE 100 company. "It is all business as usual for us."

"People need to remember that paper and other physical media have risks too," said one IT manager in a European healthcare company. "Information security is not just about IT," said another interviewee. "There is plenty of printed documentation, hardware and knowledge in people's heads that we should be concerned about securing." ■



# Prevalent Losses and Disruptions

## Which of the following staff can connect to your servers remotely (i.e. dial up from home or the field)?

As we've already seen, company laptops are in use almost everywhere now. Many people are able to log in to company servers either from such laptops or from their own computers at home.

Which employees are connecting to company servers remotely? We offered interviewees six choices - 'senior management', 'middle management', 'IT support staff', 'field staff', 'ancillary staff' and 'all other permanent white-collar staff', plus 'none at all'.

*(see graph below)*

Nearly 90 per cent of organisations have senior management accessing their servers from outside the company offices. The figures for IT staff (84 per cent) and middle management (78 per cent) are almost as high, while 63 per cent now have front-line staff logging in from the field. Only two organisations had no employee remote access to their servers at all.

While the overall trend seems to be towards wider access, some firms are now tightening their approach. "At one time, we allowed all staff remote access," said a board member in a business services firm. "Now, after remote access was abused by an employee, it is limited to senior management and the longest-employed sales staff."

## To what extent has your company suffered from the following?

We asked interviewees how often their organisation suffered theft or loss of laptop computers, and from theft or misuse of data: routinely, frequently, occasionally, rarely or never. No one described the loss of either as 'routine' - though in one or two public sector organisations it seems to have been close to such a level in the past.

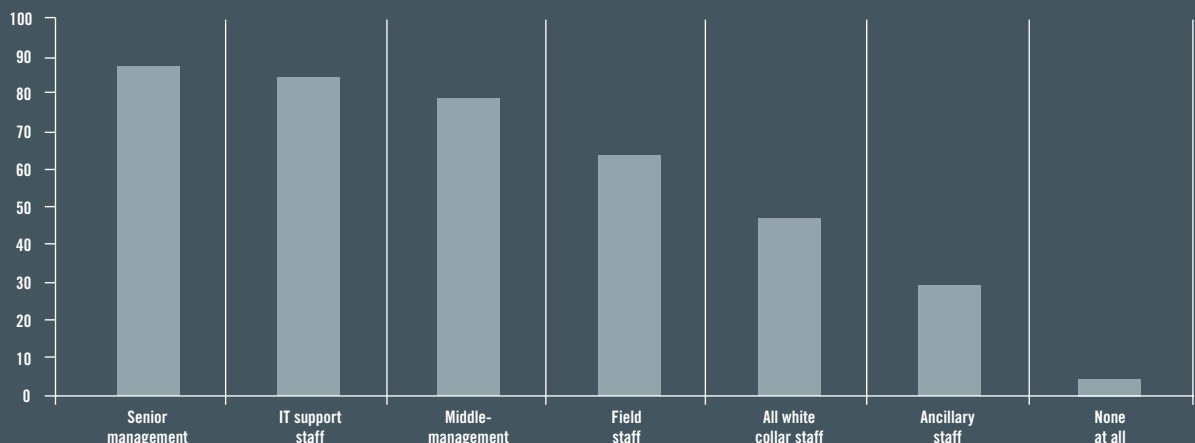
*(see graph on p19)*

Ten per cent said their organisation frequently suffered lost or stolen laptops, while a third described such losses as occasional and 42 per cent described them as rare. Fifteen per cent said their organisation had never lost a laptop.

Where data was concerned, only four per cent - i.e. two respondents - considered theft or misuse of data from their organisation frequent, while 13 per cent described it as occasional, 48 per cent as rare and 35 per cent said they had never suffered the theft or misuse of data.

Without an objective standard for the terms 'routine', 'frequent', 'occasional' and 'rare', of course, it is not possible to put much weight on these responses. The loss of four per cent of a firm's laptops in 12 months might equate to alarmingly frequent losses for one manager. Another might accept such losses as relatively rare events. Isolated casual theft is not of course the whole story. One large firm mentioned incidences of whole offices being cleared by organised criminals. In any case, a large multinational company with 10,000 staff using laptops every day is invariably going to lose some every quarter, while a small firm could, with care, go years without such a loss. One large company had a pragmatic approach on this issue: "If someone loses a laptop it is paid for out of their departmental budget. But there is no provision for such losses in those budgets."

### Nearly two-thirds of organisations have non-management staff logging in from the field



### Which of the following staff can connect to your servers remotely (i.e. dial up from home or the field)?

Senior management	88%	Field staff	63%	None at all	4%
IT support staff	84%	All white collar staff	47%		
Middle-management	78%	Ancillary staff	29%		

Note: percentages do not add up to 100 as respondents could give multiple answers.



43 per cent - followed by external electrical outage, on 41 per cent. External viruses had disrupted 29 per cent. Twenty seven per cent had suffered disruption from a data processing error, while nearly a fifth had had their IT systems disrupted by employee loss of or damage to physical equipment. Several respondents mentioned the strain the 7th July 2005 London bomb attacks had placed on telecommunications networks. Most coped without significant disruption, but some did suffer outages of three hours or so. One company had been affected by the severing of a Pacific Ocean telecoms cable, while another had recently lost internet access for some hours owing to an electrical outage at their ISP - preventing its New York office from accessing any of the firm's systems, which were based on servers at the London office

Disruption from theft or misuse of data, denial of service attack, hackers and malicious employees was less common, though with anything from four to ten per cent of companies affected, such incidents were far from unknown. ▶▶▶

What this table does seem to tell us is that IT Managers and Risk Managers believe they are managing to keep a tighter grip on their data than on the company's laptops.

**Has your company or organisation experienced an incident of computer fraud in the past year - and if so, how large was the loss?**

Interviewees were asked whether their organisation had, to their knowledge - experienced a computer-related fraud in the past year. It is possible that one or two may have known of such frauds, but were understandably reticent to discuss them. Quite a few also alluded to petty cash frauds which were too small to be material and which in any case had nothing much to do with computers.

Still, one respondent in seven - 14 per cent - stated that yes, they had experienced a material case of computer fraud in the past 12 months. How big were these cases? Three each involved less than €500,000.

But four each involved sums of between €1 million and €5 million.

The victims seemed to be a cross-section of the interview sample, including as they did two media companies, a public sector body, a manufacturer, a retailer, a telecoms group and an IT firm. With one exception, all were large organisations with over 5,000 staff.

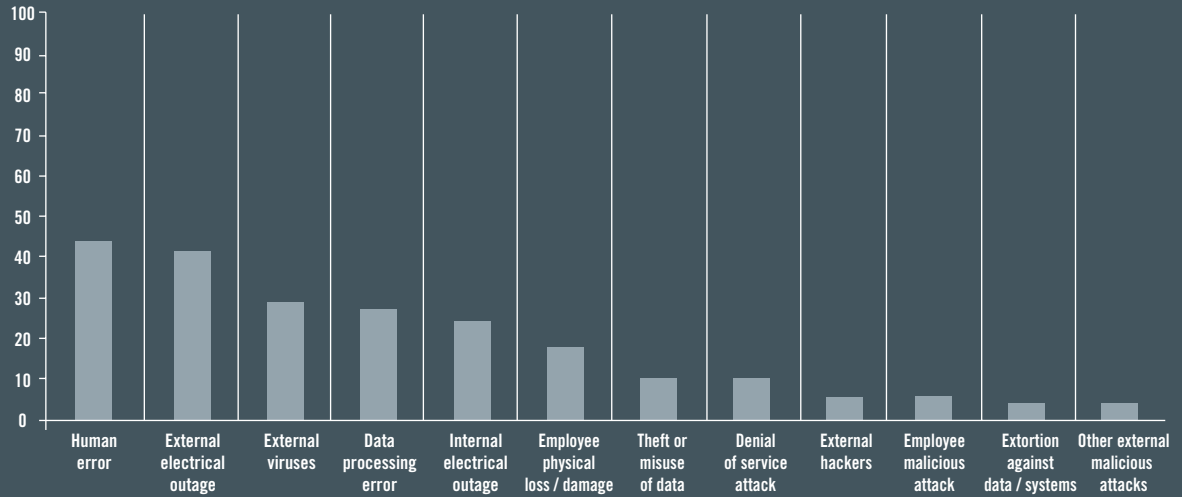
**Within the past 12 months, have your organisation's IT systems been disrupted by any of the following?**

Of all the potential threats to companies' IT systems, which ones had materialised to cause real disruption in the past year? We offered interviewees a dozen options and also invited them to mention any other problems that caused disruption to their IT systems within the past 12 months. Many had suffered some of these phenomena, but without disruption.

*(see graph on p20)*

Where actual disruption had occurred, human error was the problem most cited -

In the past year, denial of service attacks had disrupted the IT systems of one organisation in ten



Within the past 12 months, have any of the following disrupted your organisation's IT systems?

Human error	43%	Theft or misuse of data	10%
External electrical outage	41%	Denial of service attack	10%
External viruses	29%	External hackers	6%
Data processing error	27%	Employee malicious attack	6%
Internal electrical outage	24%	Extortion against data/ systems	4%
Employee physical loss/ damage	18%	Other external malicious attacks	4%

Note: percentages do not add up to 100 as respondents could give multiple answers.





# Overall Effectiveness

## Overall, how effective do you consider your IT risk management and IT business continuity planning to be?

We asked interviewees how effective they considered their general IT risk management and their IT-related business continuity planning to be - fully effective, fairly effective, or fairly ineffective.

(see graph below)

In both cases, around a quarter said 'fully effective', with another two thirds, give or take, describing it as 'fairly effective'. With some interviewees, the latter response equated to a genuine sense of vulnerabilities, known or as yet undiscovered. Others seemed to feel their IT risk management and BCP were about as sound as they could be - but that to describe any system or process as 'fully effective' was conduct unbecoming a risk manager. "It is impossible to consider that the risk controls in place are complete," said one. "Prevention or mitigation strategies may be 'state of the art' but they need to be continually reviewed and refreshed."

Be that as it may, six per cent of respondents described their IT risk management as 'fairly ineffective', while ten per cent put their organisation's IT-related business continuity planning in the same sorry category. What sort of organisations were these? The group included a fair cross section of respondents, though no public sector bodies were present. Several were small organisations of limited resources, but two or three were large, well-known organisations with turnovers in the billions.

"The effectiveness of our BCP plans depends on the severity of the incident," said an IT Manager in a middling-sized financial services firm. "We can restore from backups for individual servers quickly. But we would find it harder to recover from, say, a serious fire rendering our office unusable."

Bigger businesses whose revenues rely heavily on IT tended to be more able and willing to build in redundancy. "Our BCP is robust and we understand the value of redundancy," said a senior Risk Manager in a major telecoms group. "We can on-sell

that capability. With 25m customers, there is always a bit of the net down, but we can minimise this and we have fallbacks."

Judging by interviewees' comments, there is a good deal of work going on in many organisations, both on IT risk and BCP. "Even complete controls - the most robust you can implement - leave residual risks in today's environment," said one interviewee. "There is no room for complacency and the control environment must therefore be continuously reviewed and improved."

## Against which of any of the following risks does your organisation carry insurance policies?

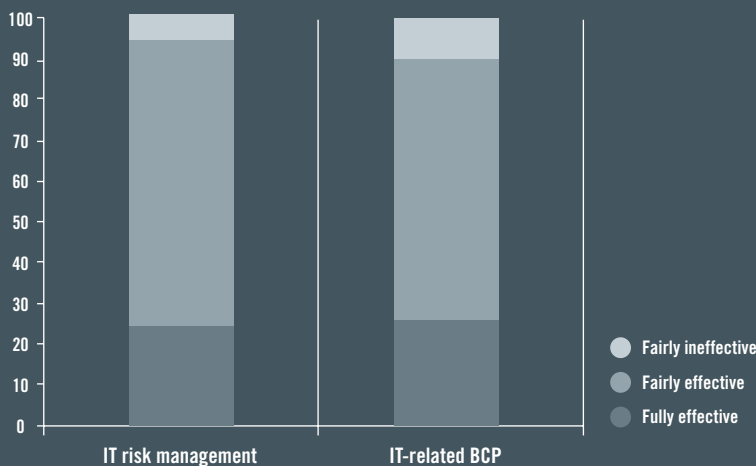
We asked interviewees against which IT-related risks they carried insurance policies. We offered a list of nine risks - internet media liability, network security liability, security and privacy liability, cyber extortion, cyber terrorism, information asset value, network business interruption, suppliers' service interruption and data corruption - and also invited them to mention any other IT-related insurance they carried.

(see graph on p22)

Many respondents were a little vague on the coverage they had. Often, coverage against IT risks was wrapped up in more general commercial policies, covering - depending on the nature of the business - physical loss or damage, fraud, breach of confidentiality, professional indemnity, extortion, defamation and of course business continuity. The cover tended to be seen largely in that context. It was relatively rare for a risk to be covered by a distinct, IT-specific policy.

"Our insurance coverage wraps round all business activity, but supports our risk strategy to deliver an 'always on' business," said one Head of Risk Management in a large company. "We are focused on business continuity - not compensation for failure to trade as normal." Another respondent said: "On insurance, we need to have synergy with the business and match cover to level of risk perceptions."

### Only a quarter rated their IT risk management and BCP planning fully effective



### How effective is your organisation's IT risk management and IT BCP?

	IT risk magt	IT-related BCP
Fully effective	24%	27%
Fairly effective	71%	63%
Fairly ineffective	6%	10%
Total	101%	100%

Note: percentages may not add up to 100 owing to rounding errors



The limitations of insurance were a regular theme. Several commented on perceived high premiums, high deductibles and limited cover. "Insurance against network security liability and any kind of data insurance is very expensive - prohibitively so for us," said one senior manager. One interviewee from a very large commercial business commented: "We have often looked at bespoke wordings, but capacity has tended to be limited for an organisation like ours. None has sufficient capital. We have an element of IT cover in existing policies but any additional cover would really need to be for catastrophic situations."

A professional services firm told a similar story. "There's a high deductible so we also use our own insurance captive and a

separate one for PI too. Mainly we are insuring for the BCP recovery period, plus business interruption and hardware."

Still, some interviewees saw a valuable role for insurance - not just in terms of necessary coverage, but also for the insights that specialist brokers can bring to risk management: "Underwriters' interest in these risks often sharpens the mind."

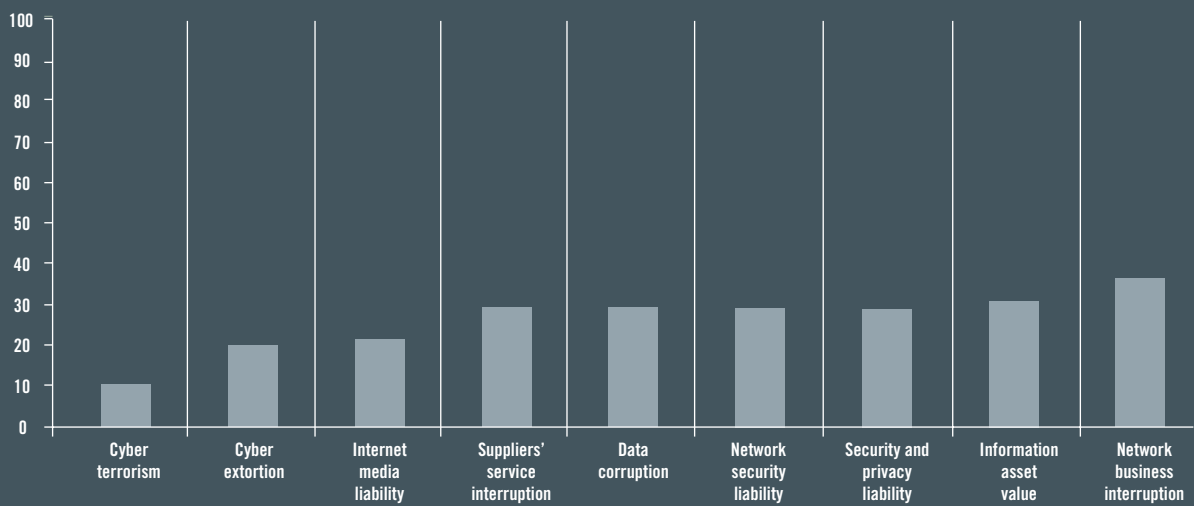
For several, this was a hot issue. "Our brokers are providing lots of information on cyber-risk insurance," said a Risk Director from a well-known global business.

"Our mapping of IT risks is under control - we think," said one UK-based interviewee, whose company had recently fired its

previous brokers. "But we have discussed in the last six months the fact that we are under-covered and are working with our new brokers on this."

But for many businesses, insurance against IT risks remains something of a grey area. As the Head of Insurance in one international business commented: "Many organisations are not aware of the risks to which they are exposed.... and covers available," he said. "There is a big gap between exposure and knowledge."

### Network business interruption was the risk commonly insured against



#### Against which risks does your organisation carry insurance policies?

Cyber terrorism	10%	Suppliers' service interruption	29%	Security and privacy liability	29%
Cyber extortion	20%	Data corruption	29%	Information asset value	31%
Internet media liability	22%	Network security liability	29%	Network business interruption	37%

Note: percentages do not add up to 100 as respondents could give multiple answers.





# The Questionnaire

## Main questionnaire

1. Do you sell goods or services through a website trading platform?
  - Yes/ No
  
2. If yes, is this business to business, business to retail consumer, or both?
  - Business to business
  - Business to retail consumer
  - Both
  
3. Does your website have facilities for receiving personal information from visitors, such as credit card or address details?
  - Yes/ No
  
4. Does your company or organisation have an intranet?
  - Yes/ No
  
5. Does your company or organisation have an extranet?
  - Yes/ No
  
6. Do members of staff use company laptops for mobile working?
  - Yes/ No
  
7. Who in your organisation has direct responsibility for IT security?
  - Please tick all that apply:
  - Information Security Officer
  - Risk Manager / Director
  - Chief Security Officer/ Head of Security
  - IT Manager / Director
  - HR Manager / Director
  - Finance Director/ CFO
  - Other - please specify.
  
8. In your view, has the organisation identified (mapped) its key IT risks?
  - Fully
  - Largely
  - Partly
  - Hardly at all
  
9. Who has been involved in identifying these risks?
  - Please tick all that apply:
  - IT Manager/ Director
  - Risk Manager/ Director
  - Information Security Officer
  - Chief Information Officer
  - Finance Director/ CFO
  - HR Manager/ Director
  - Chief Security Officer/ Head of Security
  - Chief Legal Officer
  - Other - please specify.
  
10. Which of the following do you consider to be key external IT risks for your company?
  - Please tick all that apply:
  - third party fraud
  - defamation and / or copyright infringement
  - data theft and misuse
  - outsourced IT partners' failing to manage key risks
  - denial of service attacks
  - external electrical outage
  - hackers
  - viruses
  - other malicious attacks
  - theft of passwords by non-electronic means
  - public disclosure of private information
  - extortion against data or systems
  - other - please specify.

11. Which of the following do you consider to be the key internal IT risks for your company?

Please tick all that apply:

- human error
- employee loss of or damage to physical equipment
- employee fraud
- employee theft or misuse of data
- data processing error; internal electrical outage
- employee malicious attack
- other - please specify.

12. To what extent does your company have controls and processes in place to prevent or mitigate the following external risks?

Please tick whichever applies -

Full Controls, Some Controls or No Controls

- for each of the following:

- viruses
- hackers
- denial of service attacks
- extortion against data or systems
- other malicious attacks
- third party fraud
- data theft or misuse
- theft of passwords by non-electronic means
- failure of IT partners / suppliers to manage key risks
- defamation and / or copyright infringement
- public disclosure of private information
- electrical outage.

13. To what extent does your company have controls and processes in place to prevent or mitigate the following internal risks?

Please tick whichever applies -

Full Controls, Some Controls or No Controls

- for each of the following:

- internal electrical outage
- employee loss of or damage to physical equipment
- data processing error
- employee theft or misuse of data
- employee fraud
- employee malicious attack
- human error.

14. What form, in general, do these controls and processes take?

Please answer in your own words.

15. Which of the following staff can connect to your servers remotely (i.e. dial up from home or the field)?

Please tick all that apply:

- senior management
- middle management
- IT support staff
- field staff
- ancillary staff
- all other permanent white-collar staff
- none at all.

16. To what extent has your company suffered from the following?

Please tick whichever applies

Routinely, Frequently, Occasionally, Rarely or Never -

for each of the following:

- loss or theft of laptops
- theft or misuse of data.

17. Has your company or organisation experienced an incident of computer fraud in the past year?

- Yes
- No
- not to my knowledge

18. If so, how large was the loss? (€1.00 currently equals about \$1.28, while £1 is worth about €1.44)

- Less than €500,000
- €500,001 to €1,000,000
- €1,000,001 to €5,000,000
- €5,000,001 to €10,000,000
- more than €10,000,000



19. Within the past 12 months, have your organisation's IT systems been disrupted by any of the following?

Please tick all that apply:

- external viruses
- external hackers
- denial of service attack
- external extortion against data or systems
- other external malicious attack
- external electrical outage
- internal electrical outage
- employee malicious attack
- physical loss or damage by employees
- human error
- data processing error
- theft or misuse of data
- other - please specify.

20. Overall, how effective do you consider your IT risk management to be?

- Fully effective • Fairly effective
- Fairly ineffective • Don't know

21. Overall, how would you rate your IT business continuity planning?

- Fully effective • Fairly effective
- Fairly ineffective • Don't know

22. Against which of any of the following risks does your organisation carry insurance policies?

Please tick all that apply:

- internet media liability
- network security liability
- cyber extortion
- cyber terrorism
- information asset value
- network business interruption
- suppliers' service interruption
- security and privacy liability
- data corruption
- other IT-related insurance - please specify.

23. Have you any further thoughts, comments or observations - general or specific - on the issue of IT risks affecting organisations such as yours and how to address them?

Please answer in your own words

## Background details

24. What is your name?

25. What is the name of your company/ organisation?

26. What is your job title?

27. What is the job title of the person to whom you report?

28. What is your company or organisation's main business sector?

Please tick one:

- telecommunications • professional or business services
- financial services • retail or leisure
- transport or logistics • media
- energy or utilities • manufacturing
- healthcare or pharmaceuticals • construction
- food or drink production • raw materials
- public sector • charity or non-profit
- other - please specify.

29. How many employees does it have?

Please tick one:

- 1-20 • 21-200 • 201-500
- 501-2,000 • 2,001-5,000 • 5,000 +

30. What is its approximate annual turnover?

Please tick one:

- Less than €10 million
- €10 million to €50 million
- €50 million to €1 billion
- €1 billion to €5 billion
- over €5 billion.

