BERR | Department for Business
Enterprise & Regulatory Reform

**2008 INFORMATION SECURITY
BREACHES SURVEY**

Technical report

SURVEY CONDUCTED BY

PRICEWATERHOUSECOOPERS

IN ASSOCIATION WITH

symantec.

hp®

THE
SECURITY
COMPANY
INTERNATIONAL

SPONSORING ORGANISATIONS

The following organisations have contributed to the development of this report, both financially and through their knowledge of information security management:

BERR | Department for Business Enterprise & Regulatory Reform

The **Department for Business, Enterprise & Regulatory Reform (BERR)** helps ensure business success in an increasingly competitive world. BERR is the voice for business across Government.

BERR works with industry to raise awareness of information security issues, to provide guidance on best practice and to promote the development of solutions. It also represents the information security interests of business at UK and international level.

For further information, see www.berr.gov.uk/sectors/infosec.

PRICEWATERHOUSECOOPERS

The member firms of the **PricewaterhouseCoopers (PwC)** network provide industry-focused assurance, tax and advisory services to build public trust and enhance value for its clients and their stakeholders. More than 146,000 people in 150 countries across our network share their thinking, experience and solutions to develop fresh perspectives and practical advice.

For PwC's security solutions, see www.pwc.com/security.

symantec.

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information and interactions by delivering software and services that address risks to security, availability, compliance and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries.

More information is available at http://www.symantec.com/en/uk/business/

hp

HP is a technology solutions provider to consumers, businesses and institutions globally. The company's offerings span IT infrastructure, personal computing and access devices, global services and imaging and printing for consumers, enterprises and small and medium businesses. For more than 25 years, HP has developed security technologies and services that help companies around the world protect their sensitive business data and resources.

For details about HP's security offerings, visit www.hp.com/go/security.

THE SECURITY COMPANY INTERNATIONAL | i-wareness
Creative Awareness Solutions

The Security Company (International) Limited is a global leader in the field of employee security awareness and compliance solutions. Applied and trusted by many of the world's leading organisations, our recognised and award-winning i-wareness® suite promotes long-term positive behavioural change amongst staff of all roles and across all levels of an organisation. We take the hard work out of implementing regulations and policies, and help ensure that organisations stay safe, legal and compliant.

For more information, see http://www.thesecurityco.com.

BERR ISBS 2008

Preface

This is the ninth Information Security Breaches Survey. The Department for Business, Enterprise & Regulatory Reform (and its predecessor, the Department of Trade and Industry) has sponsored research into information security breaches since 1991, to help UK businesses better understand the risks they face.

The survey results show that UK businesses continue to innovate, using the Internet to reach their customers better and improve the efficiency of their operations. The business environment is now very different from that of a decade ago.

It is encouraging to see that information security incidents are causing less disruption to companies' operations than two years ago. Firms of all sizes clearly understand that security is important and the vast majority have invested in security defences.

However, it is clear that the security battle is not over. While the total cost of security breaches has dropped over the last two years, it is still significantly higher than a decade ago. The Survey shows that considerable challenges still lie ahead for business.

Twice as many UK companies are aware of the international standard on information security management as two years ago. Those that are aware are rapidly deriving benefits from implementing the standard, either piecemeal or wholesale, across their businesses. The Department remains committed to encouraging the sharing of effective information security management techniques across UK businesses, so that the UK maintains its competitive edge.

Shriti Vadera,
Parliamentary Under Secretary
of State for Business and
Competitiveness

Introduction

Throughout history, the sea has been the lifeblood of commerce. Today, the Internet is the modern sea, carrying electronic commerce and communications around the world. Since the turn of the century, that sea has been rough, with wave after wave of viruses and hacking attacks crashing into the cyber ports. Over time, the harbour defences have improved, and now within those firewalls, the waters appear calmer.

Yet, there remain some fundamental contradictions. 79% of businesses believe they have a clear understanding of the security risks they face, but only 48% formally assess those risks. 88% are confident that they have caught all significant security breaches, but only 56% have procedures to log and respond to incidents. 81% believe security is a high priority to their board, but only 55% have a security policy. 77% say protecting customer information is very important, but only 11% prevent it walking out of the door on USB sticks. 71% have procedures to comply with the Data Protection Act, but only 8% encrypt laptop hard drives.

So, has the storm passed? Is information security yesterday's news? A better way of thinking is, perhaps, that high tide has passed and the waves receded a bit. Now is the time to make sure the defences are strong, before the next tide brings the waves again. Every sailor knows that you cannot have the sea without the waves. Similarly, we cannot enjoy the benefits that the Internet brings without acknowledging its darker side. Each of us needs to ensure that we understand those risks and have defended ourselves against them.
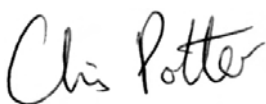
We thank all the sponsors and independent reviewers that worked on this survey with us. Together, these organisations have deep knowledge and wide experience in the information security field. They have helped us keep the survey focused on the areas that are most relevant to UK businesses today, and the analysis as balanced and objective as possible.

Chris Potter
Information Security
Assurance Partner
PricewaterhouseCoopers LLP

Andrew Beard
Information Security
Advisory Director
PricewaterhouseCoopers LLP

EXECUTIVE SUMMARY

As dependency grows, ….

UK businesses continue to grasp the opportunities provided by new technology. The broadband revolution has allowed companies to increasingly use the Internet to reach their customers and enable their staff to be more mobile. Their IT activities now extend beyond traditional physical network boundaries.

97%	have a broadband connection to the Internet.
93%	have a corporate website.
54%	allow staff to access their systems remotely.
42%	use a wireless network.
17%	use Voice over IP telephony.
5%	have moved some of their IT operations offshore.

The larger the company, the more likely it is to have adopted these business practices. For example, six out of seven very large businesses now offshore some IT operations.

All of these practices have increased significantly since two years ago. This trend is likely to continue. For example, 30% of companies will be using Voice over IP telephony by the end of 2008.

As a result, IT systems and information security are more important to UK companies than ever before. For the first time, small businesses believe security is as high a priority for them as large companies.

84%	are heavily dependent on their IT systems.
81%	believe their board gives a high or very high priority to information security.
77%	see protecting customer data as a very important driver of their expenditure.

Controls are improving, ….

This is translating into real improvements in controls, particularly in basic disciplines such as anti-virus and backups.

99%	back up their critical systems and data.
98%	have software that scans for spyware.
97%	filter incoming email for spam.
97%	protect their website with a firewall.
95%	scan incoming email for viruses.
94%	encrypt their wireless network transmissions.

It is not just technical controls that have improved. Companies increasingly realise that their people, while their greatest asset, can be their greatest vulnerability, and so need to be educated on security risks. Businesses are investing more in their security, especially those that think hardest about where to spend their money. The general level of awareness is rising, and the focus now needs to be on changing and measuring actual behaviour. With increasing awareness comes a move away from the traditional user ID and password and towards stronger authentication techniques such as smart cards or biometrics.

Over the last six years, the security landscape has changed dramatically.

2002	2008	
27%	55%	have a documented security policy.
2%	7%	of IT budget spent on security (on average).
20%	40%	provide ongoing security awareness training to staff.
5%	14%	use strong (i.e. multi-factor) authentication.
5%	11%	have implemented BS 7799/ISO 27001.

BS 7799 is the British information security management standard that formed the basis of, and is equivalent to, the ISO 27000 series of international standards.

EXECUTIVE SUMMARY

Leading to fewer reported incidents, ….

After the peak in 2004, the number of companies reporting a security breach has returned to roughly the level seen in 2002. However, attitudes and controls in some companies mean that incident statistics are probably understated. For example, companies that carry out risk assessment are four times as likely to detect identity theft as those that do not. In addition the average seriousness of incidents has increased, so roughly a quarter of companies had a serious breach, the same as in 2006.

	Small (<50 staff)	Large (>250 staff)	Very Large (>500 staff)
Companies that had a security incident in the last year	45%	72%	96%
Average number of incidents, median (mean)	6 *(100)*	15 *(200)*	>400 *(>1,300)*
Average cost of worst incident in year	£10k to £20k	£90k to £170k	£1m to £2m

The most striking feature is the decline in reported virus infections. Virus infection has dropped from the largest cause of security incidents (which it has been for the last decade) to fourth place out of five. The number of companies infected has fallen back to levels last seen in 2000. In contrast, unauthorised access by outsiders is not declining and remains at four times the level seen in 2000.

	Overall	Large businesses
Number of companies affected	↓ 25%	↓ 20%
Average (median) number of incidents suffered by affected companies	↓ 30%	↓ 20%
Average cost of each incident	↑ 25%	↑ 30%
Total cost of security incidents	↓ 35%	↓ 20%

The total cost to UK plc has dropped by roughly a third compared with two years ago, returning to the levels seen in 2004. An indicative estimate of the overall cost is in the order of several billion pounds a year. Companies are generally pessimistic, with only 17% expecting fewer security incidents next year.

But some big exposures remain.

Confidential information is increasingly at risk, especially in large businesses, where:

13%	have detected unauthorised outsiders within their network.
9%	had fake (phishing) emails sent asking their customers for data.
9%	had customers impersonated (e.g. after identity theft).
6%	have suffered a confidentiality breach.

Many companies are not doing enough to protect themselves and their customers' information.

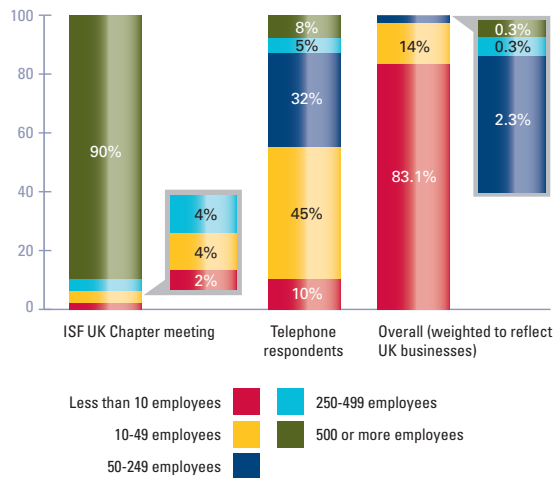|	
10%	of websites that accept payment details do not encrypt them.
21%	spend less than 1% of their IT budget on information security.
35%	have no controls over staff use of Instant Messaging.
48%	of disaster recovery plans have not been tested in the last year.
52%	do not carry out any formal security risk assessment.
67%	do nothing to prevent confidential data leaving on USB sticks, etc.
78%	of companies that had computers stolen did not encrypt hard discs.
79%	are not aware of the contents of BS 7799/ISO 27001.
84%	of companies do not scan outgoing email for confidential data.

To protect your business in this changing world:

1. **Understand the security threats you face, by drawing on the right knowledge sources.**

2. **Use risk assessment to target your security investment at the most beneficial areas.**

3. **Integrate security into normal business behaviour, through clear policy and staff education.**

4. **Deploy integrated technical controls and keep them up to date.**

5. **Respond quickly and effectively to breaches, e.g. by planning ahead for contingencies.**
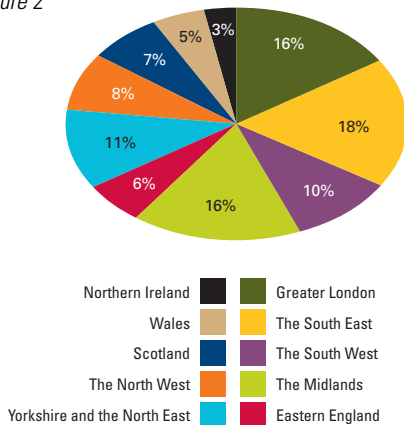
METHODOLOGY
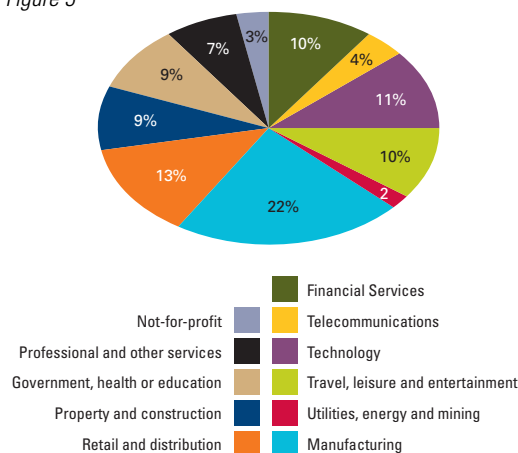
How many staff did each respondent employ in the UK?

Figure 1

- Less than 10 employees
- 10-49 employees
- 50-249 employees
- 250-499 employees
- 500 or more employees

In what region were each respondent's main business operations located?

Figure 2

Northern Ireland	Greater London
Wales	The South East
Scotland	The South West
The North West	The Midlands
Yorkshire and the North East	Eastern England

In what sector was each respondent's main business activity?

Figure 3

Not-for-profit	Financial Services
Professional and other services	Telecommunications
Government, health or education	Technology
Property and construction	Travel, leisure and entertainment
Retail and distribution	Utilities, energy and mining
	Manufacturing

Survey approach

The core research for the Information Security Breaches Survey (ISBS) 2008 was a quantitative telephone survey using a structured questionnaire. We picked the sample randomly from a register of UK businesses, ensuring that we had an appropriate mix of respondents to reflect the nature of UK businesses. In each case, we contacted the person identified as responsible for information security. In total, we completed 1,007 computer-assisted telephone interviews, each lasting on average 20 minutes. The interviews took place between October 2007 and January 2008.

Businesses of different sizes tend to exhibit different security profiles. A representative sample of UK businesses would be predominantly sole traders and small SMEs. To make sure we have meaningful findings for larger companies as well, we boosted the sample for this group. We then weighted the overall results, using number of employees as the weighting matrix, to reflect the actual distribution of companies in the UK (excluding sole traders). Where the results for large companies are significantly different from the overall result, we have quoted these separately.

To minimise the burden on respondents, we asked half the respondents the questions on security strategy (pages 5-13) and the other half the questions on security controls (pages 14-21). We asked all the respondents the questions on security breaches (pages 22-32).

Based on the total sample in this survey, we are 95% confident that the margin of error for our sampling procedure and its results is no more than +/- 3%. As is normal with surveys, the margin of error varies with individual statistics:

- With extreme results (towards 0% or 100%), the margin of error is reduced.
- For the questions on security strategy and controls, the number of respondents is smaller and so the margin of error is up to +/- 5%.
- Where results are analysed for a sub-sample, the margin of error is greater. For example, large company statistics have a margin of error of up to +/- 9%.

In addition to sampling error, question wording and practical difficulties in conducting surveys can introduce error or bias into the findings. We have sought to minimise this by keeping question wording consistent with past surveys for the majority of questions asked.

The response rate was slightly higher than two years ago. To reduce the risk of bias, we used the same sample selection techniques as two years ago. Our sample included appropriate representation by size, industry sector and region. We then weighted the results accordingly.

As with any in-depth survey of this kind, we would not necessarily expect every respondent to know the answers to every question. For presentation of percentages, we have consistently stripped out the Don't Knows. If the proportion of Don't Knows was significant, we have referred to this in the text.

To supplement the telephone interviews, we ran the survey interactively at a meeting of the Information Security Forum (ISF) UK Chapter. The ISF population provided an insight into the security practices that operate in very large businesses with a strong security culture. Accordingly, we have provided these statistics in several places in the report. The margin of error on the very large business population is +/- 14%.

We also carried out face-to-face in-depth interviews with information security officers and issued an email poll to Infosecurity Europe subscribers. These provided us with additional anecdotal data.

SECURITY STRATEGY

Attitudes to information security

The UK business community continues to grasp the opportunities provided by new technology. UK companies have now fully embraced the broadband revolution, with 97% having a broadband connection (up from 85% two years ago). Broadband penetration is fairly evenly distributed across the country, varying from 93% in East Anglia to 100% in Northern Ireland.

Dependence on IT systems remains high, at similar levels to those seen two years ago - only one in six small companies would be able to continue their businesses without IT. On average, companies in East Anglia are least dependent on their IT, and those in Greater London and Scotland most dependent.

As in previous surveys, the financial services, health and education sectors, particularly those based in London and the South-West, are likeliest to hold highly confidential data. Retail and leisure companies are least likely, but even here three-fifths keep sensitive information in electronic form. The continued push towards electronic submission of PAYE data is a big driver here.

Financial services, telecommunications and energy companies are most concerned about corruption of records since their turnover is largely dependent on electronic records. Availability is a significant concern to most sectors, though not-for-profit organisations are least concerned about outages. The North-East and Wales are least likely to suffer business disruption from the temporary loss of their computer systems; however, a one day outage would still significantly disrupt over half of these companies.

The increasing dependence on IT systems means the importance of information security has never been higher. Four-fifths of respondents believe that information security is a high or very high priority to their senior management (up from three-quarters two years ago). For the first time, small companies are now giving a higher priority to security than large ones. This priority is greatest in the professional services and not-for-profit sectors. The respondents that believe security is not a priority at all are in the technology, leisure, manufacturing and retail sectors.

A pharmacy chain used to rely on paper-based security procedures, since the pharmacists gained the patient's consent to holding data through physical signature. The increasing use of electronic records is causing the organisation to put more emphasis on information security.

Examples of positive behaviours showing a high priority include IT literacy at the board level, insistence on effective backup and access control processes, willingness to spend money and regular engagement on security issues. Behaviours that convey a low priority include wanting protection without being prepared to pay for it, lack of action after a security breach, poor understanding of technical issues and too little attention to raising staff awareness.

Companies in Greater London are likeliest to give a high priority to security, with nearly two-thirds doing so. In contrast, only a third of companies in Northern Ireland do so.

In some businesses, there is a clear gap between the good intentions of senior management and the actions taken. A third of companies that believe they give a high or very high priority to security don't even have a security policy.

The security officer at a retail bank commented that information security has senior management's ear but middle management, who are responsible for implementation, are much less convinced. Information security is one person's enabler and another's cost of doing business.
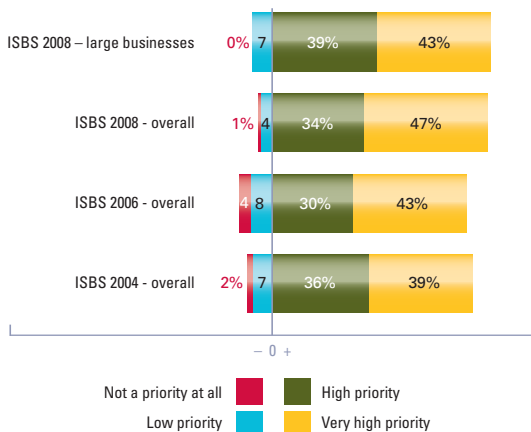
**How many UK businesses have information that:**

Figure 4

ISBS 2008 - large businesses / ISBS 2008 - overall / ISBS 2006 - overall / ISBS 2004 - overall
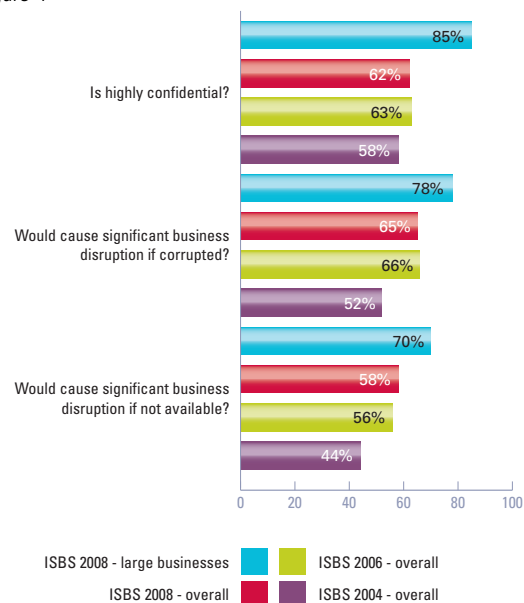
How high a priority is information security to top management or director groups?

Figure 5

Not a priority at all / Low priority / High priority / Very high priority

How clearly do top management or director groups understand the information security risks their businesses face?

Figure 6
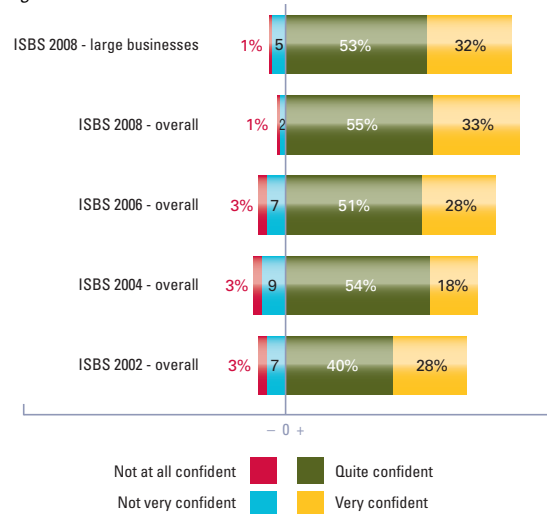

Very poorly / Quite poorly / Quite clearly / Very clearly
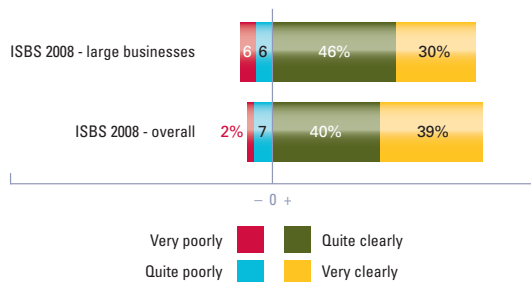
SECURITY STRATEGY

How confident are UK businesses that they have caught all significant breaches that occured in the last year?
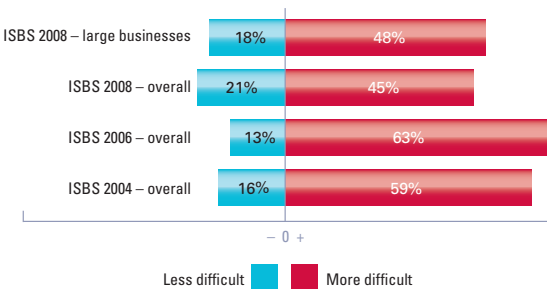
Figure 7

	Not at all confident	Quite confident
Not very confident		Very confident

How many security incidents do UK businesses expect next year compared with last?

Figure 8

Fewer · More
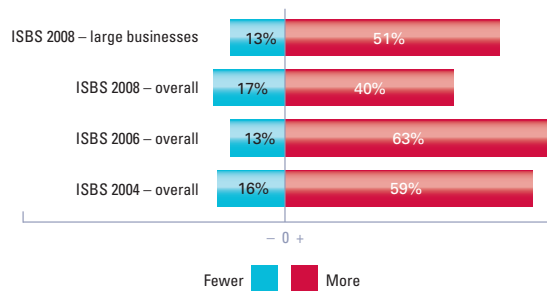
Will it be more or less difficult to catch security incidents next year?

Figure 9

Less difficult · More difficult

Confidence

In previous years, there has been a contrast between the high level of confidence UK businesses have in their controls and the actual controls in place. Over the last two years, both confidence and the quality of controls have improved. However, it still appears that confidence is derived from having very basic controls in place rather than from in-depth risk assessment. Some organisations still appear to have a tick-box mentality to their security.

Confidence is highest in financial services and lowest in the property and construction sector. It is greatest in the South-West and lowest in Northern Ireland. Interestingly, neither the extent to which companies have experienced security breaches during the year, nor the nature of those incidents, appears to affect their level of confidence.

Adopting basic security disciplines does seem to increase confidence. Companies that have a security policy are slightly more confident than those that do not. Two-fifths of companies with a security policy are very confident about their security processes, compared with one fifth of those without. On the other hand, the more people know about security, sometimes the less confident they are. Smaller companies are more confident about their security than very large ones where awareness is greater.

In some cases, senior management may not understand the security issues their business is facing. Certainly, the level of understanding appears to be lower than the priority given to security. If senior management does not realise that backups and anti-virus alone are not enough, it makes it very hard for the right security controls to filter down the organisation.

Understanding of security issues at the board level varies considerably between companies within the same sector. Overall, senior management in the energy sector appear to have the best understanding. Understanding also appears to vary significantly by region. Nearly half of companies in Greater London report that their senior management have a very clear understanding; in Northern Ireland, only 6% do.

There is a clear correlation between carrying out a formal risk assessment and the clarity of senior management's understanding. Two-fifths of senior management had a very clear understanding in businesses that had assessed the risks, compared with only a quarter in those who had not. Risk assessment helps people understand the commercial implications of their security decisions.

Senior management at a medium-sized financial services provider in London do not have a good understanding of security issues. However, they are clear that security is a very high priority to the business. A formal process for assessing risks coupled with a regular audit process gives senior management the assurance they want.

In the past, respondents have been very pessimistic about the future. The mood has improved, but remains downbeat. Telecoms providers are the most pessimistic about the future number of incidents. At the other extreme, energy companies are more neutral, with most expecting the same number as this year. While all sectors felt that incidents would be harder to detect than in the past, a large minority in the technology and retail sectors felt they would be easier to detect. Companies in Northern Ireland are particularly concerned that breaches will be harder to detect in the future. Companies, whose worst incident of the year was a computer fraud or hacking attack, tend to be more pessimistic about the future than those that suffered other incident types.

Nearly two-thirds of very large companies would welcome more education for the general public about information security risks and more industry initiatives to address security risks. More than half would appreciate provision of more information security advice and wider promotion of existing information security standards.

SECURITY STRATEGY

Security awareness

Basic security disciplines continue to propagate across UK businesses. The proportion of companies that have an information security policy has quadrupled over the last eight years. Large businesses remain more likely to have a security policy; seven out of eight do so, and some of the 12% that do not have a security policy have an integrated overall set of business policies that include information security. It is clear that the term security policy has different meanings to different companies, varying from a one page overall policy to many hundreds of pages of detailed standards.

Over three-quarters of not-for-profit organisations and financial services companies have a security policy in place. In contrast, manufacturing, travel, leisure and entertainment companies are least likely to have a security policy. There is also some regional variation, with Greater London and Scotland the best; three-quarters of companies based there have a security policy in place.

Previous surveys have shown a strong correlation between the priority given to security and whether basic disciplines, such as having a security policy, are in place. This seems to have weakened, as basic disciplines continue to be adopted by UK plc. 68% of companies that give a high or very high priority to security have a security policy (up from 55% in 2006) compared with 64% of those that treat security as low or no priority (up massively from 13% in 2006).

There is some correlation between how clearly senior management understand security issues and whether a security policy is in place. However, even when senior management have a very poor understanding, 56% have a security policy. The biggest correlation is between security policy and risk assessment; companies that carry out risk assessment are twice as likely to have a security policy in place as those that do not, and vice versa.

Of course, having a security policy alone does not magically improve security awareness among staff. The overwhelming majority of companies take some steps to raise awareness. The priority given by senior management makes a difference in the extent to which security awareness is drilled into all areas of the organisation. Only one in five companies for whom security is not a priority at all, takes any steps to raise the security awareness of their staff.
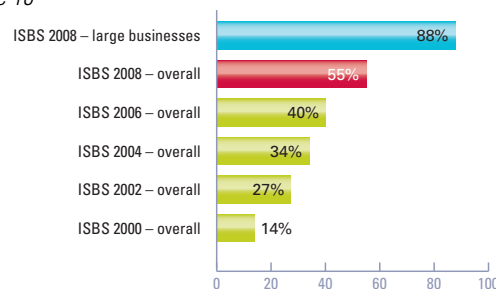
The staff handbook is most commonly used in financial services, with more than three-quarters using this as a way of communicating the security policy. Separate documents outlining the security policy are most favoured in the energy, government, health and education sectors, with two-fifths of respondents doing this. Technology and professional services companies are likeliest to include security obligations in employment contracts; two-fifths of them do this, compared with only 12% of telecoms providers. Three-fifths of professional services companies include security in induction training for their staff, and half give face-to-face training to existing staff on security matters. Computer-based training (CBT) is commonest in the energy sector, where two-fifths use it to get security messages across to staff; companies in Scotland are more than twice as likely to use CBT as those in Northern Ireland. The vast majority of very large businesses use a combination of CBT and face-to-face training to get security messages across. The more senior management understand security, the more likely they are to sponsor CBT. Overall, retailers, and companies in East Anglia and Wales, are least likely to take any steps to educate staff.

Increasingly, companies realise that what they need to do is to change their staff's behaviour rather than just increase awareness and skills. A "click mentality" has grown up - users do what expedites their activity rather than what they know they ought to. Only when behaviour changes, do businesses realise the benefits of a security-aware culture.

One bank found that bringing humour into awareness training has generated more interest and better results. People are much more positive about the training and the messages have stuck better.
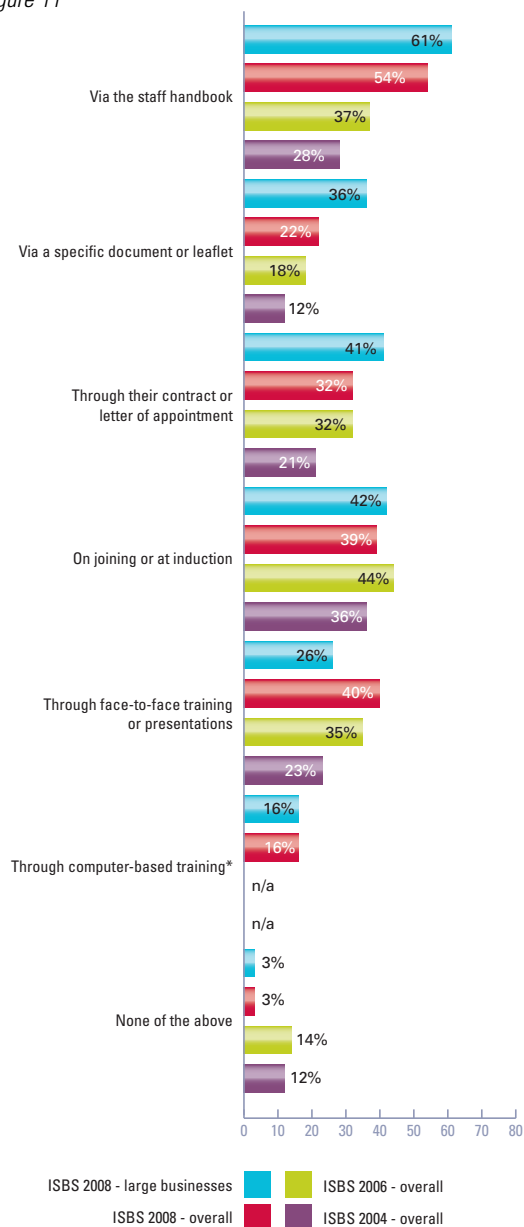
How many UK businesses have a formally documented and defined information security policy?

Figure 10

ISBS 2008 – large businesses	88%
ISBS 2008 – overall	55%
ISBS 2006 – overall	40%
ISBS 2004 – overall	34%
ISBS 2002 – overall	27%
ISBS 2000 – overall	14%

How do UK businesses make their staff aware of their obligations regarding security issues?

Figure 11

Via the staff handbook	61% / 54% / 37% / 28%
Via a specific document or leaflet	36% / 22% / 18% / 12%
Through their contract or letter of appointment	41% / 32% / 32% / 21%
On joining or at induction	42% / 39% / 44% / 36%
Through face-to-face training or presentations	26% / 40% / 35% / 23%
Through computer-based training*	16% / 16% / n/a / n/a
None of the above	3% / 3% / 14% / 12%

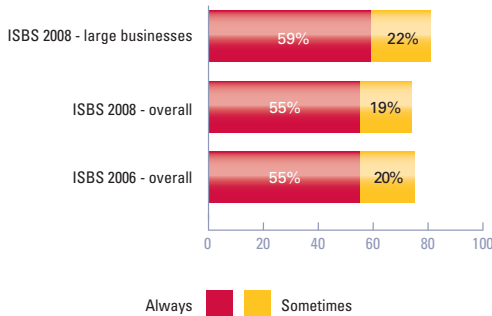|	
ISBS 2008 - large businesses	ISBS 2006 - overall
ISBS 2008 - overall	ISBS 2004 - overall

* New question in the 2008 survey

7

SECURITY STRATEGY

How often do UK businesses carry out background checks on staff and potential staff?
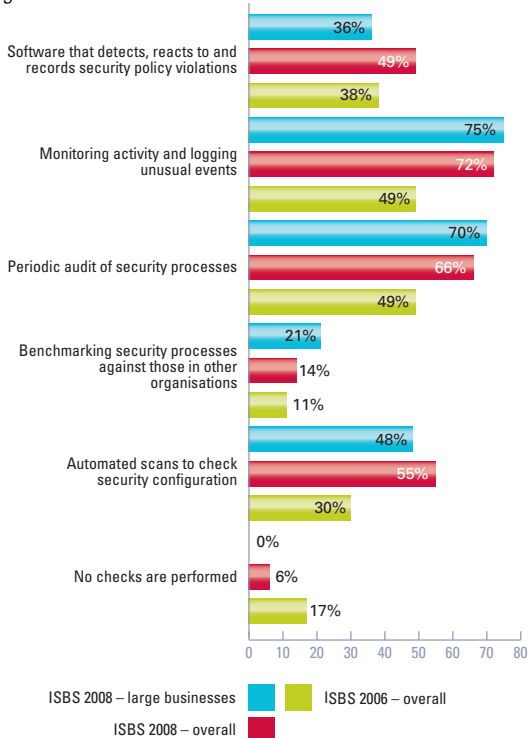
Figure 12

	Always	Sometimes
ISBS 2008 - large businesses	59%	22%
ISBS 2008 - overall	55%	19%
ISBS 2006 - overall	55%	20%

Always ▮ Sometimes ▮

Do UK businesses have documented procedures to ensure compliance with the Data Protection Act?

Figure 13

	Yes	No, but plan to introduce them
ISBS 2008 - large businesses	91%	3
ISBS 2008 - overall	71%	11%
ISBS 2006 - overall	64%	9%

Yes ▮ No, but plan to introduce them ▮
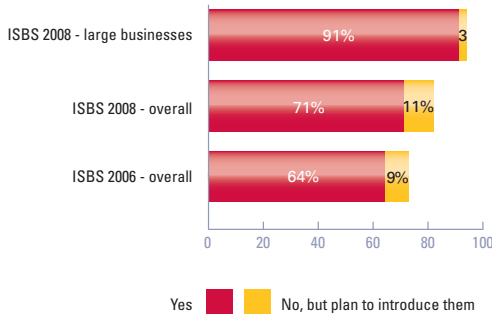
How do UK businesses monitor compliance with their security policy?

Figure 14

	ISBS 2008 – large businesses	ISBS 2008 – overall	ISBS 2006 – overall
Software that detects, reacts to and records security policy violations	36%	49%	38%
Monitoring activity and logging unusual events	75%	72%	49%
Periodic audit of security processes	70%	66%	49%
Benchmarking security processes against those in other organisations	21%	14%	11%
Automated scans to check security configuration	48%	55%	30%
No checks are performed	0%	6%	17%

ISBS 2008 – large businesses ▮ ISBS 2006 – overall ▮
ISBS 2008 – overall ▮

Risk assessment and compliance

Increasingly, security is part of a company's overall governance, risk management and compliance structure. Security risk assessment has increased since 2006, largely among companies where security has not historically been a high priority. Three times as many of these carry out risk assessment as two years ago. Now, 48% of UK companies have a security risk assessment process, rising to 77% of large businesses.

At a large professional services firm, the IT director sits on the main board and so helps the company translate their strong desire for security into action. There is a formal risk assessment process led by the internal security team with support from their external auditors.

The nature and extent of risk assessments vary considerably. Some companies have a complex approach following a formal methodology, typically involving analysing data from a wide variety of sources. In others, there is an informal discussion or the security manager presents his/her views to the board. Many firms use a third party to carry out a periodic risk assessment.

Nearly three-quarters of financial services providers carry out a formal assessment of their security risks, the highest of any sector. Companies in the travel, leisure and entertainment sector are least likely to have assessed their security risks. Companies in Greater London are likeliest to have carried out a security risk assessment; those in Northern Ireland are least likely.

Companies that carry out formal risk assessment are twice as likely to detect unauthorised access by staff or attacks on network traffic and nearly four times as likely to detect identity theft as those that do not.

One of the main risk management precautions is to carry out background checks on potential recruits. The more senior management understand about security and the greater the priority they give to it, the more likely background checks are to happen. Two-thirds of businesses where boards have a very clear understanding of security issues always carry out background checks on staff. In contrast, when the understanding is very poor, two-thirds never carry out any background checks. Similarly, when security is a very high priority, 62% always carry out background checks on staff, compared with only 27% where security is seen as low or no priority. Few companies appear to be using the BS 7858 code of practice on security screening.

Three-quarters of not-for-profit and financial services organisations always carry out background checks. In contrast, manufacturers are least likely to carry out checks. Two-thirds of companies in Greater London always carry out background checks, versus only a third in the North-East.

Compliance with the Data Protection Act 1998 (DPA) continues to improve. Senior management priority makes a big difference. 82% of companies that give a very high priority to security have data protection procedures, versus 42% of those where security is low or no priority. Worryingly, 25% of companies that say they hold highly confidential electronic information lack procedures to comply with the DPA.

Financial services companies are most likely to have documented procedures to ensure compliance with the DPA; 96% have procedures and the remainder plan to implement them in the next year. The energy sector has the lowest current rate, but manufacturers are most likely to have no current procedures and no plans to implement any.

A formal data protection process yields real benefits. Companies with documented procedures to ensure compliance with the DPA are half as likely to experience data protection infringements, unauthorised access or confidentiality breaches by staff as those that do not.

SECURITY STRATEGY

BS 7799 (ISO 27000) adoption

The British Standards on information security (the 7799 standards) have existed for over a decade and formed the basis of the international ISO 27000 family of standards. The original BS 7799 comprised two parts: a code of practice (Part 1, which now forms ISO 27002) and a specification for an information security management system (Part 2, now ISO 27001) against which an organisation can seek accredited certification. Companies around the world are increasingly using the ISO standards to structure their security processes.

The globalisation of the standard appears to be helping raise awareness in the UK. Awareness of the ISO 27000 standards amongst companies has doubled in the last two years. Awareness is highest in the financial services, telecommunications, technology and retail sectors. It is weakest in the property, travel, leisure and entertainment sectors. Interestingly, the more aware a sector is, the more likely the aware companies in the sector are to implement the standards.

Awareness of the standards is greatest among those companies who give a very high priority to security, but even here only 30% are aware of what the standards recommend. Companies that give a high or very high priority to security are more likely to have implemented the standards than those who do not.

Companies with a very clear understanding of their security issues are nearly three times as likely to be aware of what the standards say as those where understanding is very poor.

Awareness of the ISO 27000 standards is greatest amongst respondents who hold a security qualification - they are three times as likely to be familiar with the contents of the standard as unqualified respondents.

The number of companies that have implemented the ISO 27000 series of standards is up by 60% compared with two years ago. More than half of those that are aware of the contents of the standards have used them in the last year to help ensure appropriate security processes are in place. Half have already implemented the standards in at least part of their organisation, and a further quarter plan to do so in the next year. All the organisations that have implemented the standards have achieved benefits from doing so, but the benefits vary considerably between different companies. Implementation tends to raise the security baseline, by ensuring that a minimum level of control is adopted in all areas of security management.

The culture at one distribution company has changed over the last five years. The company invested in ISO 27001 certification several years ago. However, the business viewed security as an inhibitor to business, a particular bugbear being the removal of shared IDs. Increasingly, customers are now focusing on information security in their tender processes. The ISO 27001 certification is helping to win business; this has changed management's perception considerably.

ISO adoption strengthens companies' processes to check compliance with their security policy. Overall, all forms of compliance checks have become more popular since 2006, but adoption rates vary by sector. Nearly three-quarters of technology companies use software to detect security violations. A third of energy companies commission benchmarking, versus only 4% of professional services firms. Retailers are most likely to not carry out any checks.

While penetration testing is a condition of some specialist cybercrime insurance policies, the rise in uptake is not confined solely to those with such policies. Indeed, companies without are slightly more likely to commission tests than those with policies.

Security is a very high priority at a medium-sized telecoms company. The board gives the IT function a large budget and allows it to do what is needed to get the job done. This includes hiring ethical hackers to try to break into the company's systems.
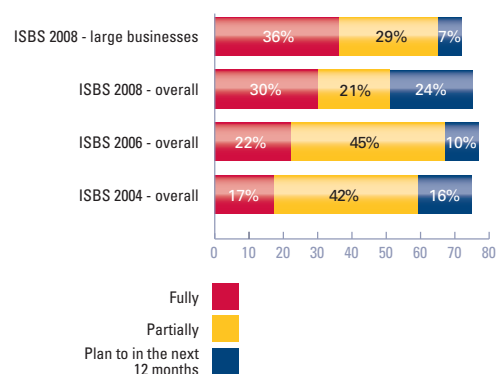
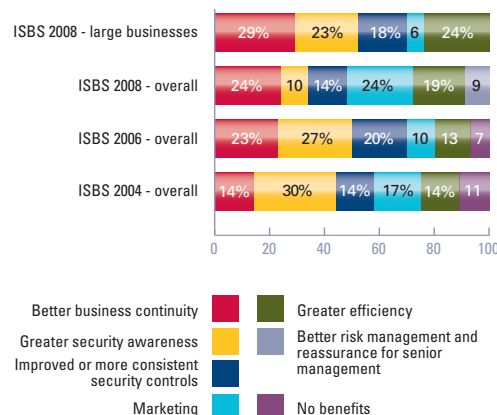**What proportion of UK businesses are aware of the contents of BS 7799?**

Figure 15
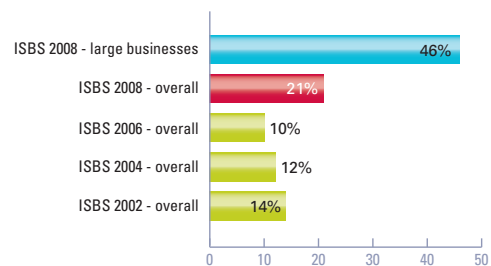
How many UK businesses that are aware of BS 7799 have implemented it?

Figure 16
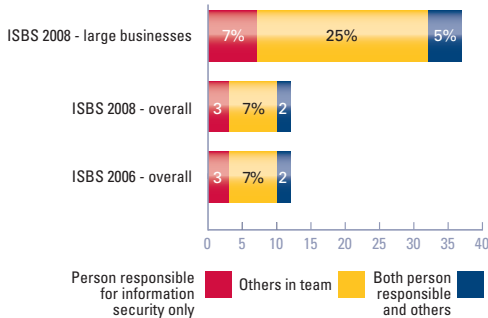

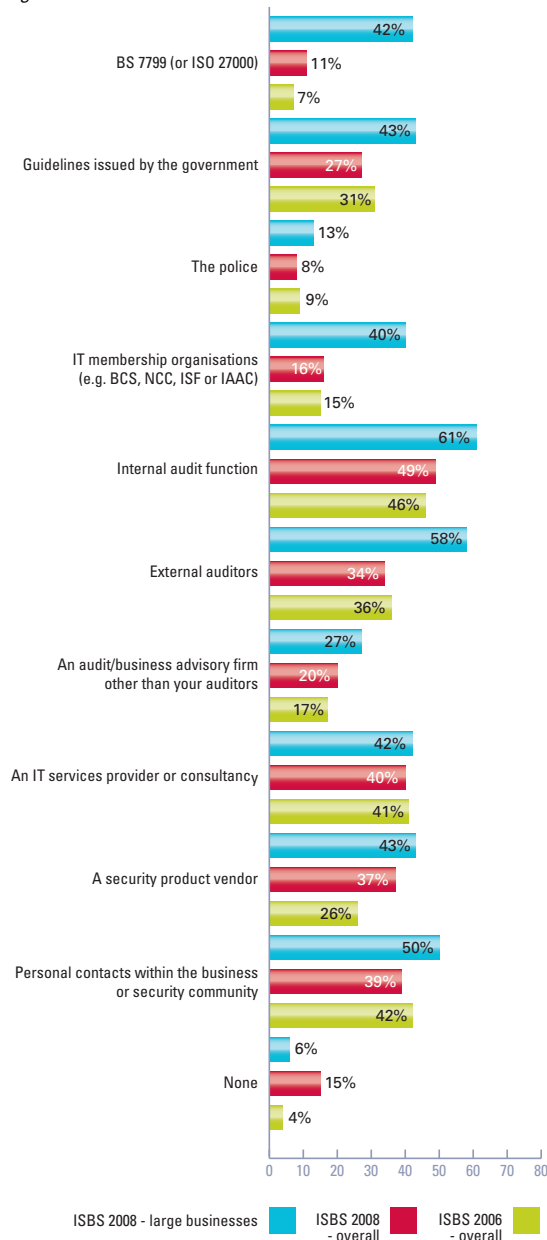**What was the biggest benefit from implementing BS 7799?**

Figure 17

9

SECURITY STRATEGY

Does the team responsible for information security have any formal security qualifications?

Figure 18

	Person responsible for information security only	Others in team	Both person responsible and others
ISBS 2008 - large businesses	7%	25%	5%
ISBS 2008 - overall	3	7%	2
ISBS 2006 - overall	3	7%	2

What external security guidance and expertise have UK businesses drawn on in the last year?

Figure 19

	ISBS 2008 - large businesses	ISBS 2008 - overall	ISBS 2006 - overall
BS 7799 (or ISO 27000)	42%	11%	7%
Guidelines issued by the government	43%	27%	31%
The police	13%	8%	9%
IT membership organisations (e.g. BCS, NCC, ISF or IAAC)	40%	16%	15%
Internal audit function	61%	49%	46%
External auditors	58%	34%	36%
An audit/business advisory firm other than your auditors	27%	20%	17%
An IT services provider or consultancy	42%	40%	41%
A security product vendor	43%	37%	26%
Personal contacts within the business or security community	50%	39%	42%
None	6%	15%	4%

Security skills and expertise

There has been an increased emphasis on security qualifications in the UK following the formation of the Institute of Information Security Professionals in 2006. It is, therefore, pleasing to see that, among large businesses at least, security qualifications are becoming more common. 98% of very large businesses now have qualified staff.

Companies where security is a very high or high priority are more than twice as likely to have qualified staff as those where security is low or no priority. However, qualifications remain rare in small businesses; even among those where security is a very high priority, only one in five has qualified staff. When the person responsible for information security has a security qualification, the company is three times as likely to have other security qualified staff as well. This suggests that the value of such qualifications is most apparent to those who have them.

Security qualifications are commonest in the technology sector, where roughly a third of companies have some qualified staff. Manufacturers are least likely to have qualified staff. Two-fifths of companies in Greater London have qualified staff, but they are found in fewer than one in ten businesses in Northern Ireland, East Anglia and the North-East.

Companies that employ security qualified staff tend to have a better understanding of the security issues they face. Two-thirds say their management have a very clear understanding, compared with only 30% of companies without qualified staff. In addition, the emphasis that qualifications give to risk assessment appears to pay off - three-quarters of qualified respondents carry out risk assessment, compared with only half of unqualified ones. As a result, qualified respondents are more likely to have strong views on whether their security controls are adequate.

A distribution company commented that it is hard to find skilled people in the marketplace. People need to have more than technical skills. They also need to be able to communicate technical issues to management in a way they will understand. Both internally and externally, such people are a scarce and valued resource.

To supplement their own personal knowledge, the vast majority of companies draw on security guidance and expertise from outside their organisation. Most use multiple sources of advice. Companies in the North-West and East Anglia are least likely to use external security guidance and expertise; companies in Greater London, Scotland and Wales are most likely.

Standards and guidelines are generally seen as a useful reference point. However, the standards alone appear unlikely to solve people's security issues. Only about 10% of the respondents who consult one of these sources cite them as the most useful external source of guidance. IT service providers, personal contacts, security vendors and external auditors are most likely to have provided the most helpful guidance. The main attributes that companies look for when seeking external guidance are technical expertise and comprehensive advice. Reliability and existing knowledge of the organisation are also seen as very helpful.

The nature of the business seems to influence what sources of external advice companies use. Professional services companies and those that work in the public sector are most likely to consult government guidelines. More than a quarter of telecoms providers have consulted the police, while very few manufacturers and not-for-profit organisations have. Professional services firms are most likely to use IT membership organisations, while manufacturers are least likely. Financial services companies are twice as likely to consult their external auditors on security matters as energy companies. Professional services firms tend to favour IT consultants, while technology companies tend to prefer specialist security product vendors. Not-for-profit organisations are least likely to consult personal contacts in the business or security community.

SECURITY STRATEGY

Investment in security

The average expenditure on information security continues to rise, though the rate of increase now appears to be slowing slightly. Small companies now spend on average 7% of their IT budget on security (significantly up from 4-5% in 2006). Average expenditure in large businesses is relatively static, at roughly 6% of IT budget (up slightly in absolute terms but down slightly as a % of IT budget). As in the past, very large businesses, where IT budgets are correspondingly higher, spend a smaller proportion of those budgets (an average of 4%) on security.

Companies differ in their views on what constitutes information security expenditure, and many do not track it in a separate budget. Any benchmarks in this area should, therefore, always be treated as indicative rather than absolute.

There remains a correlation between the priority senior management give to security and expenditure on it. For example, companies for whom security is not a priority at all spend less than 1% of their IT budget on security on average. However, even companies where security is a low priority are now devoting 6% of their IT budget to it. Companies where security is a medium priority have increased their expenditure most; they now spend as much as those where it is a very high priority.

Companies where senior management have a clear understanding of the security issues spend more on security, but also are more demanding about the business case justifying that expenditure. However, even companies where understanding is very poor still spend 4-5% of their IT spend on average on security.

Companies that carry out risk assessment spend more on security (8% of IT budget on average) than those that do not (who spend 6% of IT budget on average). However, this gap has narrowed since two years ago, when the respective figures were 7% and 4%. They are also more likely to demand a business case to support this expenditure.

Companies that outsource some of their IT services tend to spend slightly more on their security (8% of IT budget on average) than those that don't (6% of IT budget). This may be because outsourcing tends to lead to more detailed categorisation of IT spending.

While the averages look good, a small but significant proportion of companies spend very little on security; between a fifth and a quarter continue to spend less than 1% of their IT budget on security. This is, however, down from the two-fifths seen two years ago.
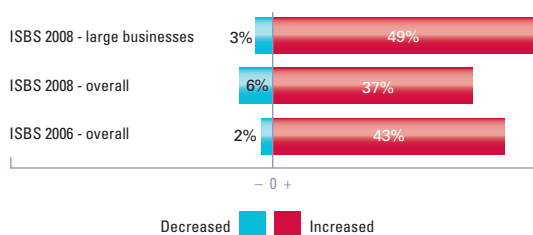
A medium-sized retailer in the Midlands commented that their senior management have a poor understanding of information security issues and so give it a low priority. The board wants protection without being prepared to spend what is required. To overcome this, the company uses its external systems auditors to assess the security risks and consults widely with personal contacts in the business and security community.

Telecoms, technology and property companies now spend the greatest proportion of their IT budget on security on average (8-10%); these have all jumped considerably since two years ago. Travel, leisure, entertainment and energy companies spend the least on average (4-5%); security spending at energy companies appears to have dropped since 2006. By region, Scottish and Welsh companies spend the most on security (9%); companies in East Anglia spend the least (5%).

Security expenditure is increasing most in the financial services, professional services and not-for-profit sectors. The lowest rate of increase is in the energy, manufacturing and retail sectors, but even in these sectors only about 5% say their security expenditure is decreasing. Security expenditure is increasing most in Greater London and the Midlands. It is growing least in the South-West.
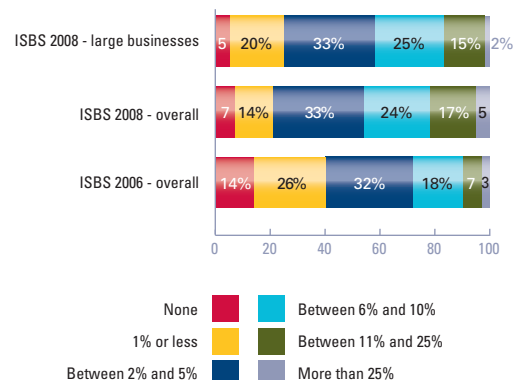
Has information security expenditure increased or decreased over the last year?

Figure 20

	Decreased	Increased
ISBS 2008 - large businesses	3%	49%
ISBS 2008 - overall	6%	37%
ISBS 2006 - overall	2%	43%

– 0 +

Decreased   Increased

What percentage of IT budget was spent on information security, if any?

Figure 21

	None	1% or less	Between 2% and 5%	Between 6% and 10%	Between 11% and 25%	More than 25%
ISBS 2008 - large businesses	5	20%	33%	25%	15%	2%
ISBS 2008 - overall	7	14%	33%	24%	17%	5
ISBS 2006 - overall	14%	26%	32%	18%	7	3

None
1% or less
Between 2% and 5%
Between 6% and 10%
Between 11% and 25%
More than 25%

Which sectors spend most on security?

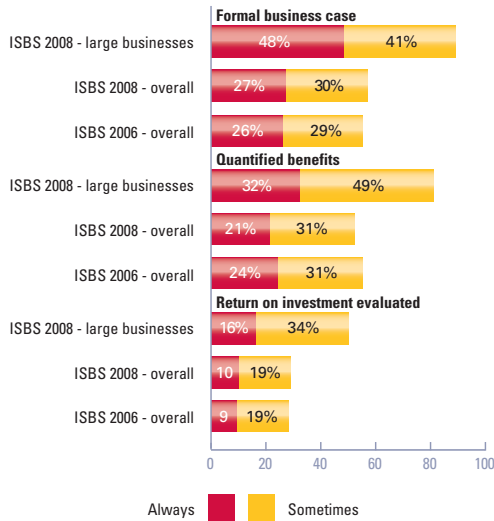*Figure 22*

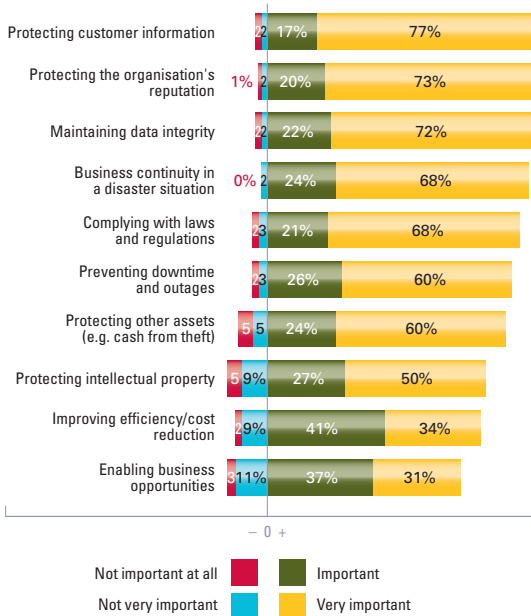| Average rate of increase (net number of companies reporting increase)	Average current security spend (as % of IT spend)		
	Below Average (Less than 6%)	**Average** (6% to 8%)	**Above Average** (more than 8%)
High (more than +40%)	Not-for-profit	Financial services, Professional services	-
Average (between +30% and +40%)	-	Government, health and education	Technology, Property and construction
Low (less than +30%)	Travel, leisure and entertainment, Utilities, energy and mining	Manufacturing, Retail and distribution	Telecommunications

11

SECURITY STRATEGY

How do UK businesses decide what to spend on information security?

Figure 23

Formal business case
- ISBS 2008 - large businesses: 48% / 41%
- ISBS 2008 - overall: 27% / 30%
- ISBS 2006 - overall: 26% / 29%

Quantified benefits
- ISBS 2008 - large businesses: 32% / 49%
- ISBS 2008 - overall: 21% / 31%
- ISBS 2006 - overall: 24% / 31%

Return on investment evaluated
- ISBS 2008 - large businesses: 16% / 34%
- ISBS 2008 - overall: 10 / 19%
- ISBS 2006 - overall: 9 / 19%

Always ■   Sometimes ■

What drives information security expenditure?

Figure 24

- Protecting customer information: 2/2 / 17% / 77%
- Protecting the organisation's reputation: 1% / 2 / 20% / 73%
- Maintaining data integrity: 2/2 / 22% / 72%
- Business continuity in a disaster situation: 0% / 2 / 24% / 68%
- Complying with laws and regulations: 2/3 / 21% / 68%
- Preventing downtime and outages: 2/3 / 26% / 60%
- Protecting other assets (e.g. cash from theft): 5 / 5 / 24% / 60%
- Protecting intellectual property: 5 / 9% / 27% / 50%
- Improving efficiency/cost reduction: 2/9% / 41% / 34%
- Enabling business opportunities: 3/11% / 37% / 31%

Not important at all ■   Important ■
Not very important ■   Very important ■

Business case for security expenditure

While security expenditure has increased over the last two years, the techniques used to justify it have barely changed. Practices vary considerably from one company to another. Telecoms and technology companies are most likely to make formal business cases. However, in all sectors there are many companies that never do this. Telecoms providers are also most likely to quantify the benefits and to evaluate return on investment (ROI). While most financial services companies make business cases, very few evaluate ROI, possibly because their reputation is their greatest asset and it is hard to quantify this.

More than half of the companies that always prepare a formal business case also always quantify the benefits, compared with one in ten of those that never prepare a formal business case. However, 22% of companies that always prepare formal business cases never quantify the benefits. Quantification is particularly rare in Northern Ireland.

These disciplines do pay off. Companies that always make a formal business case for security expenditure tend to spend a greater proportion of their IT budget (9-10% on average) than those that never make a formal business case (5% on average).

Budget approval at a manufacturer for tangible, physically visible items has never been a problem. Expenditure on intangible, hidden IT assets is subject to more scrutiny. This normally means emphasising the non-security business benefits; the recent business case for a network storage device stressed its storage and disaster recovery benefits rather than the extra security it brings.

All the drivers for expenditure on information security have increased in importance over the last two years. The biggest increases were in two of the relatively lowly rated drivers: protecting intellectual property and enabling business opportunities. The smallest increases were in improving efficiency/cost reduction and complying with laws and regulations.

The relative importance of different drivers for expenditure on information security is remarkably consistent with the pattern two years ago. There are only two movements in the list. Reputation has overtaken data integrity in the number two spot. Intellectual property has risen in importance, overtaking improving efficiency and cost reduction.

Preventing outages is most important in technology and energy companies and in businesses that depend heavily on systems availability. Intellectual property is most important in the financial services and technology sectors and least important for not-for-profit organisations. Protecting customer information is paramount in financial and professional services, with the energy sector least concerned. Protecting hard assets from theft is a very strong driver in the energy, travel, leisure and entertainment sectors.

Data integrity is important across all sectors. Data protection compliance is most important in heavily regulated sectors, such as financial services, but interestingly is least important among telecoms providers; the extent to which confidential data is actually handled also seems to have little effect on it. The energy sector is most concerned about business continuity in a disaster situation. Reputation is most important in the energy, not-for-profit and professional services sectors, and least important in the telecoms, government, health and education sectors. Technology and property companies are keenest on security as an enabler of business opportunities, while manufacturers and those in the government, health and education sectors are least likely to be motivated by this. Retailers are enthused by efficiency and cost reduction, while this is least likely to drive security expenditure in the telecoms sector.

If senior management understand security issues very clearly, customer information, reputation and compliance are clearly the biggest drivers; more than four-fifths rate each one as being a very important driver. If senior management have a very poor understanding of security issues, maintaining data integrity and business continuity appear more important.

SECURITY STRATEGY

Outsourcing and offshoring

Outsourcing remains common with over half of respondents having outsourced some of their IT operations (similar levels to two years ago). Areas that are commonly outsourced include application development and support, systems administration, website hosting and help-desk operation.

Not-for-profit organisations are most likely to outsource their IT operations; telecoms providers are least likely. Outsourcing is most common in Greater London, where two-thirds of companies outsource some of their IT operations; in contrast, only a third of East Anglian companies do so.

Senior management at a medium-sized property company in the North-West meet regularly to discuss security issues and compliance with policies. These discussions are underpinned by a formal risk assessment, facilitated by their external auditors. Because IT is outsourced, specialist technical consultancy is brought in as required.

Most companies that outsource now recognise that they cannot outsource the responsibility and oversight of the operations. Three-quarters now have formal service level agreements (SLAs) in place. The vast majority of these SLAs now include security. The larger the company outsourcing its IT operations, the more likely it is to have SLAs in place. Financial services, professional services and not-for-profit organisations are most likely to have SLAs that adequately cover security concerns. Energy companies seem to struggle most with this.

A large financial services company had outsourced their customer relationship management system (CRM). Unfortunately, one of the outsource provider's laptops had a virus containing a key logger. This enabled an attacker to capture one of the outsource team's user ID and password. The attacker then used these to access customer details and launch phishing attacks against customers registered in the CRM system.

While the proportion of companies outsourcing their IT operations has remained static over the last two years, there is a clear trend towards some of those operations being carried out offshore (e.g. in India and China). The number of companies offshoring some of the IT operations has doubled since 2006, and has quadrupled for large businesses. Six out of seven very large businesses now offshore some of their IT operations. Financial services, professional services and energy companies are most likely to have offshored some of their operations; property companies are least likely.

The first wave of offshorers tended to visit the offshore facilities to gain comfort firsthand. For small businesses, this is very expensive and has declined in popularity. Instead, increasingly the offshoring company is demanding from the service provider an independent auditor's report (typically prepared in accordance with the SAS 70 standard).

An insurance company has offshored some of its processing. To mitigate the security risks, the company applies the same control requirements on the outsourced operations as it would if they were in-house. Critically, there are people on-site in the overseas location whose job it is to monitor and supervise the offshored activities.

Outsourcing does not seem to drive the priority that senior management give to information security. However, 91% of companies that give a very high priority to security have service level agreements in place for their outsourced operations, compared with only 50% of those for whom security is low or no priority. For offshored operations, companies where security is a very high priority tend to restrict access and tie down data protection procedures; those where security is a medium to high priority are more likely to rely on an independent audit.
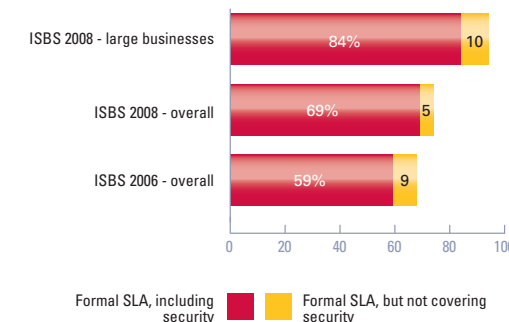
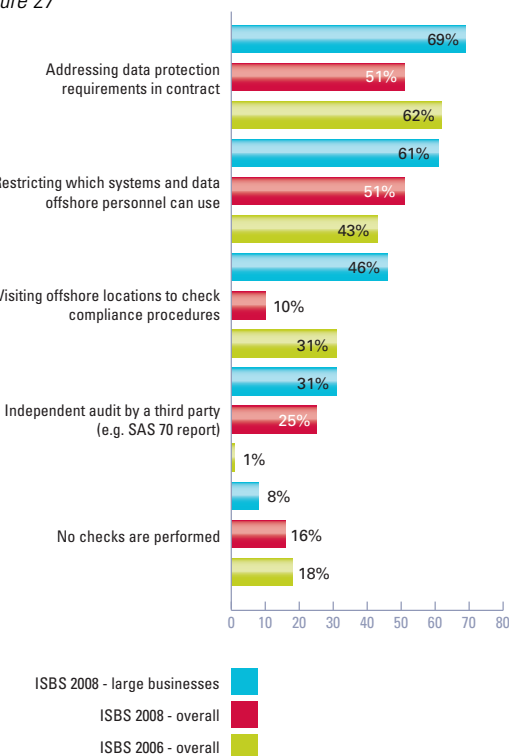**How many UK businesses have outsourced any of their IT operations?**

Figure 25
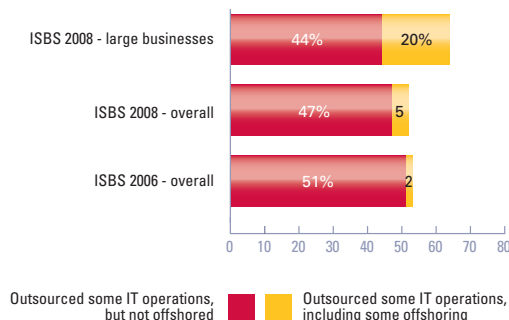
How many outsource arrangements have Service Level Agreements in place?

Figure 26

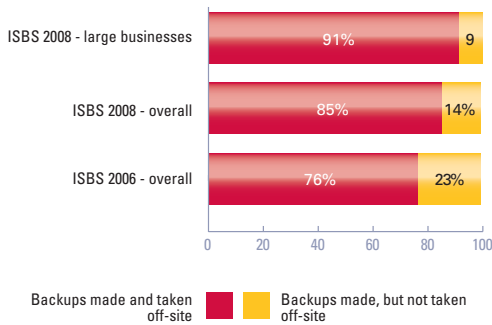**How do UK businesses that have offshored IT activities ensure they are secure?**
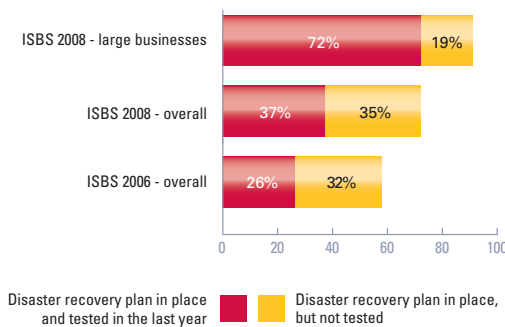
Figure 27

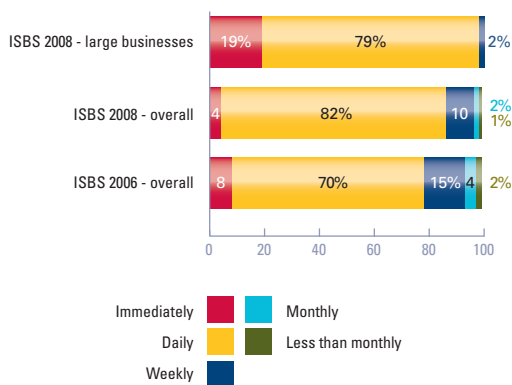# SECURITY CONTROLS

How many UK businesses back up their data?

Figure 28

ISBS 2008 - large businesses	91% / 9
ISBS 2008 - overall	85% / 14%
ISBS 2006 - overall	76% / 23%

Backups made and taken off-site | Backups made, but not taken off-site

How many UK businesses have disaster recovery plans?

Figure 29

ISBS 2008 - large businesses	72% / 19%
ISBS 2008 - overall	37% / 35%
ISBS 2006 - overall	26% / 32%

Disaster recovery plan in place and tested in the last year | Disaster recovery plan in place, but not tested

How frequently do UK businesses back up their critical data?

Figure 30

ISBS 2008 - large businesses	19% / 79% / 2%
ISBS 2008 - overall	4 / 82% / 10 / 2% / 1%
ISBS 2006 - overall	8 / 70% / 15% / 4 / 2%

Immediately | Monthly
Daily | Less than monthly
Weekly

Preparing for the worst

The severe floods in July 2007 highlighted the business continuity threats that UK companies face. It is encouraging to see that almost every UK business makes backups and the vast majority now take these backups off-site. The risks are well understood; it does not take an incident to raise awareness.

Financial services and professional services companies are most likely to have immediate backups of transaction data through replicating transactions.

In contrast, travel, leisure and entertainment companies tend to have the most relaxed attitude to backing up data. Companies in the South-West and North-West are the least likely to store their backups off-site.

Management at a Midlands-based SME insist on rigorous backup procedures being in place. Their security risk assessment processes include double-checking backup processes. They employ an IT consultancy to advise them; they find face-to-face contact with an expert invaluable.

Taking backups off-site poses its own security risks. Historically, backups have tended to be unencrypted to minimise the effort to restore data. More companies now consider whether they ought to be encrypting their backups.

A technology company nearly lost some confidential data when tapes were being transferred by a courier firm. By mistake, the delivery driver took the tapes to the next-door address, which was a building site. Rather than realising the error, the driver simply allowed a builder to sign for the tapes. Fortunately, they were recovered.

Disaster recovery plans, which focus on restoring IT systems after a disaster, and business continuity plans, which focus on maintaining business operations, are increasingly common. Disaster recovery plans are most common in the financial services and energy sectors; travel, leisure and entertainment companies are least likely to have a plan. Four-fifths of companies where outages would cause significant business disruption have plans.

Interestingly, 10% of companies with a disaster recovery plan do not store backups offsite, These are largely in the energy, government, health and education sectors. It is not clear how effective their plans would be if invoked.

Experience shows that plans are only effective if regularly tested. It is a concern that only half of plans have been tested in the last year. Financial services and telecoms providers are most likely to test their plans; not-for-profit organisations are least likely. The South-West has now overtaken London as the region with the most disaster recovery plans in place (possibly as a result of last year's floods), but fewer of these plans are tested than in other regions. Overall, Wales and Northern Ireland appear best prepared to recover from a sudden disaster.

A large financial services company highlighted the need for a full understanding of infrastructure components. They had two redundant power supplies and had successfully tested the failover. However, a previously unidentified electrical component failed and took out both of them. It took five minutes to restore power, but four hours to deal with the consequent disruption to IT systems.

A new British Standard (BS 25999) has been launched covering business continuity; it includes more detail than the existing section in ISO 27001. Companies can now have their business continuity management arrangements independently certified, to provide stakeholders, customers and insurers with assurance. Several companies have already done this.

SECURITY CONTROLS

Carried away

Recent press stories have highlighted how confidential data can become exposed when computer equipment is stolen. Yet, two-thirds of UK companies continue to rely solely on their premises' physical security to protect against this threat. Most thefts of computer equipment by outsiders appear to put confidential data at risk. Only 22% of companies experiencing theft of computer equipment by an outsider have encrypted the data on that equipment. Fewer companies appear to encrypt hard drives than two years ago.

A large multi-national started a project to encrypt all its laptops around the world. While, at the time, the UK subsidiary did not see this as necessary, it was in hindsight quite fortuitous; the project completed about the time that losses of unencrypted customer data on laptops hit the press.

Companies in the travel, leisure and entertainment sectors are least likely to have taken steps to protect confidential data held on PCs and laptops. Professional services firms are not much better, a major concern given the confidential nature of their work. Financial services, telecoms and not-for-profit organisations take more steps, but even here there are major concerns. Only 12% of financial services companies encrypt hard discs. Companies in Greater London are most likely to protect their computers from theft. In contrast, only a third of companies in Northern Ireland take any precautions.

It seems companies have to have a theft before they put controls in place. Three-quarters of companies that had computer equipment stolen by outsiders in the last year now have controls.

A medium-sized professional services business in London lost confidential data when some of its computer equipment was stolen. The data was not encrypted, but fortunately it was recovered within a week. Despite the near miss, the firm has not subsequently changed its controls.

Physical security and tagging may deter some thefts but they do not eliminate the need for encryption. Companies that experienced theft were actually more likely to have physical security and tagging in place than those who were not affected.

Removable media devices (such as MP3 players, USB data sticks, digital cameras and portable hard discs) potentially enable staff to extract large quantities of confidential data onto insecure and easily stolen media. Yet, two-thirds of UK businesses seem to be either unaware of the risks or unwilling to spend money on protecting themselves when other organisations do not.

Property, travel, leisure and entertainment companies and businesses in the North-East appear most relaxed about removable media devices; only a quarter have put any controls in place. In contrast, two-thirds of financial services providers have taken steps, and half have implemented technical controls to mitigate the risk.

Simply telling staff not to use removable media devices, a practice relied on by a fifth of firms, does not seem to make a major difference to the chances of having a confidentiality breach. Encryption of data alone does not seem to prevent all breaches, since some organisations that encrypt confidential data still report confidentiality breaches.

One medium-sized firm found it hard to persuade the board to deploy security over USB sticks, since the business was making widespread legitimate use of them. Recent high profile security breaches at other companies have helped the directors understand the potential for brand damage and compliance breaches. As a result, secure USB sticks with enforced encryption and complex passwords have been issued to the staff who need them and other devices have been blocked.
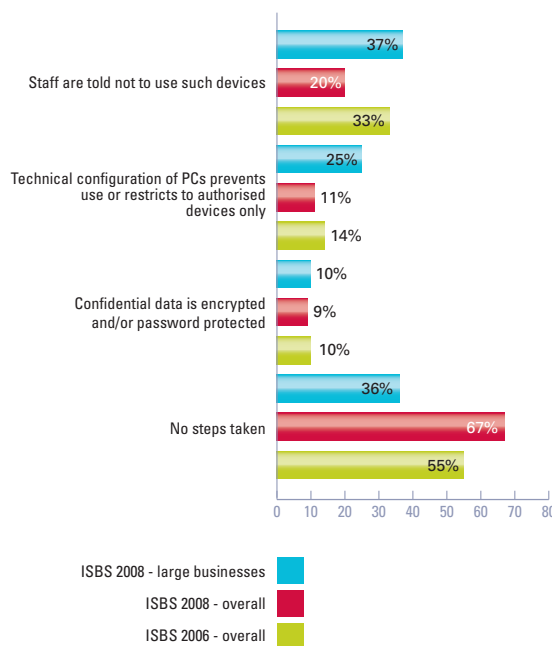
How do UK businesses protect their desktop PCs and laptops?

Figure 31

ISBS 2008 - large businesses		
ISBS 2008 - overall		
ISBS 2006 - overall		
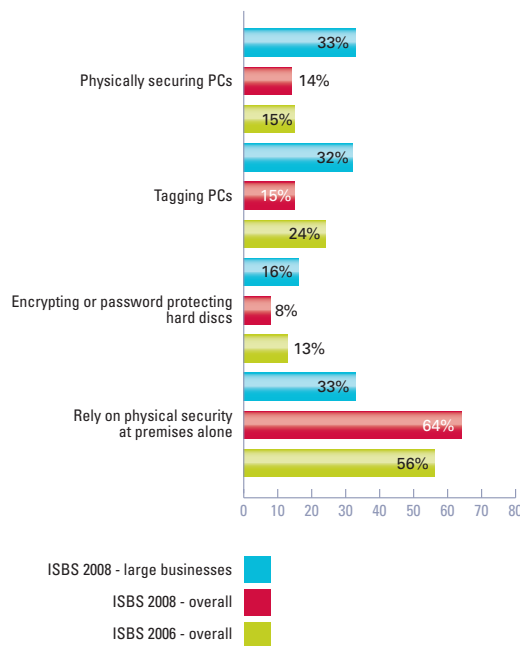
What precautions do UK businesses take over removable media devices?

Figure 32

ISBS 2008 - large businesses		
ISBS 2008 - overall		
ISBS 2006 - overall		

SECURITY CONTROLS

How do UK businesses protect themselves against malware?

Figure 33

Software that scans for possible spyware
- 97%
- 98%
- 74%

Automatic scanning of incoming email and web downloads for malware
- 98%
- 95%
- 94%

Automatic scanning of outgoing email for malware
- 85%
- 77%
- 70%

ISBS 2008 - large businesses
ISBS 2008 - overall
ISBS 2006 - overall
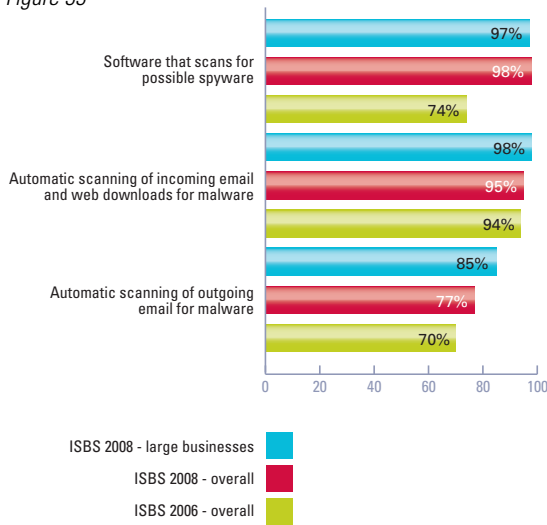
How quickly do UK businesses update anti-virus defences?

Figure 34

Updating anti-virus software for a new virus signature file
- 82% | 7 | 5 | 6

Installing critical operating system updates on all significant PCs and servers
- 33% | 16% | 18% | 33%

Within a day — Within a month
Within a week — Longer than a month
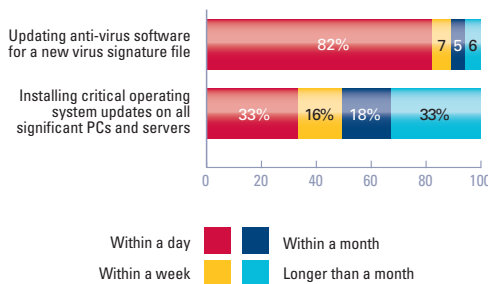
Where have UK businesses implemented intrusion detection or prevention software?

Figure 35

At the Internet gateway
- 43%
- 30%
- 23%

On servers
- 20%
- 24%
- 21%

On desktops
- 5%
- 12%
- 13%

Not implemented
- 47%
- 54%
- 57%

ISBS 2008 - large businesses
ISBS 2008 - overall
ISBS 2006 - overall
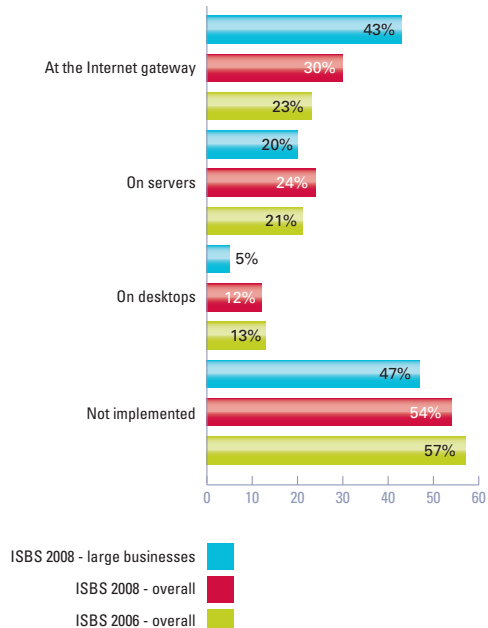
Anti-virus controls

Viruses, worms, Trojans and spyware, collectively known as malware, represent a clearly understood threat. Two years ago, almost every company irrespective of size installed anti-virus software, but there were some variations in the steps taken against spyware. The overwhelming majority of businesses now use anti-spyware scanning software as well as anti-virus software. This is one of the few areas where almost all companies, no matter what their size, sector or location, agree on the need for controls. Energy companies are least likely to be protected against spyware, but even here 91% have anti-spyware software in place. Interestingly, most of the companies without anti-spyware software are in the South-East.

One security officer summarised how malware has changed. Spyware and phishing attacks are becoming more of a concern. Other viruses and Trojans are no longer a big issue, since the company's anti-virus software and patching procedures screen these out.

Anti-virus and anti-spyware is only effective if it is kept up to date. New malware is emerging at a frightening rate. Recent research (published in the Symantec Internet Security Threat report) indicates there are over a thousand new malicious code threats coming out every day. Financial services and telecoms providers are the most rigorous at keeping their anti-virus software up to date; energy, property and leisure companies appear more relaxed, with one in five waiting a month or more before updating virus signatures. Companies that had a virus infection in the last year are slightly more likely to set their anti-virus software to update automatically.

Two years ago, there was a big improvement in the discipline with which operating system critical security updates were installed. Companies now seem to be slower to install patches than they were in 2006 (though a quarter of respondents were uncertain). There is a balance for companies to strike between the risk of being vulnerable to attack (if patches are not installed immediately) and the risk of systems instability (if a patch causes problems with the systems in use). As the memory of the major Internet worm attacks of 2003-4 recedes, companies seem to believe the balance of the risk has shifted. This is in marked contrast to anti-virus software updates, which companies are just as quick to install as they were two years ago.

There is a strong correlation between the speed with which new operating system patches are rolled out and the speed with which anti-virus software is updated. 98% of companies that set their computers to install critical operating system updates automatically also automatically install anti-virus updates. Very few businesses install patches faster than they implement anti-virus updates, but there is a significant number where patch rollout is significantly slower than anti-virus update. Only two-fifths of companies that automatically install anti-virus updates set their computers to automatically install critical operating system updates. Most prefer to have a testing window before patches are rolled out.

Management at a small Scottish financial services provider feel they have a very clear understanding of security issues and give security a very high priority. They continually apply the latest security updates to their systems.

Firms in Northern Ireland are particularly poor at updating their anti-virus software for new virus signatures; a third do this less often than once a month. It is also the weakest region when it comes to installing operating system patches - half do this less often than once a month. Finally, Northern Ireland has the lowest use of intrusion detection software, adopted by just over a quarter of businesses based there. There is also some sector variation. Nearly four-fifths of telecoms providers have implemented intrusion detection or prevention software. In contrast, only a third of property companies have done so.

SECURITY CONTROLS

Email and web usage

Restricting which staff have access to the Internet used to be quite common, but has dropped significantly over the last two years as companies' dependence on web-based applications continues to grow. 9% of UK companies do not give any staff access (roughly the same as in 2006), but, among those that do, the proportion restricting access to some staff only has nearly halved (from 42% to 24%). In this changing environment, defences need to adapt accordingly.

An acceptable usage policy is almost a pre-requisite to the implementation of other controls to prevent or detect staff misuse of the Internet. Nine-tenths of companies that implement other controls also have an acceptable usage policy. Companies in Greater London and Scotland are most likely to give staff Internet access, but also to have an acceptable usage policy. Nearly every not-for-profit organisation has one. Companies with an acceptable usage policy are between three and eight times as likely to report staff misuse as those without. Those without such a policy tend not to have a clear corporate view on what constitutes misuse, so do not pick up all incidents.

More than two-thirds of those that block inappropriate sites also log and monitor usage, and vice versa. The property, government, health and education sectors favour blocking access; financial services and telecoms providers, and companies in Scotland and Northern Ireland, tend to focus slightly more on monitoring usage. Companies that block web access or log and monitor it are still twice as likely to report incidents as those that do not. It is very hard to detect abuse without these techniques.

An IT department piloted software to monitor web usage. The Head of IT explained to the team how their activity would be monitored and the disciplinary consequences of inappropriate usage. Unfortunately, this was not enough to change all the behaviour. The software identified a number of individuals in IT abusing access; one was ultimately fired and others formally disciplined.

Filtering incoming email to strip out unsolicited junk emails ("spam") has now become virtually universally adopted by UK businesses. Given that other research shows that spam volume has roughly doubled in the last two years and that spam messages now make up nearly three-quarters of all email messages, this is not surprising. Other scans on incoming email remain common.

A medium-sized business installed software to scan incoming email for profanity. Unfortunately, the scanner blocked a number of legitimate messages from their business partners in Sweden. It turned out that a common Swedish word is spelt the same way as an English profanity.

Three-fifths of large businesses enable staff to encrypt the emails they exchange with business partners, up from a third in 2006. This capability is taking longer to reach smaller businesses. A third can now do this, versus a quarter in 2006. It is most common in the financial services sector and in the Midlands.

The number of companies scanning outgoing email has gone up. Over half of large businesses and a quarter of small ones now scan for inappropriate content such as swear words in their outgoing email, an increase of about 50% over the last two years. However, only one in six businesses checks for confidential data leaving by email. Companies that do scan outgoing email had fewer confidentiality breaches on average.

A call centre employee used their work email to ask an external party whether they wanted to acquire customer data. The email stated that if the person was interested in acquiring the data they could contact the employee on their work phone number.
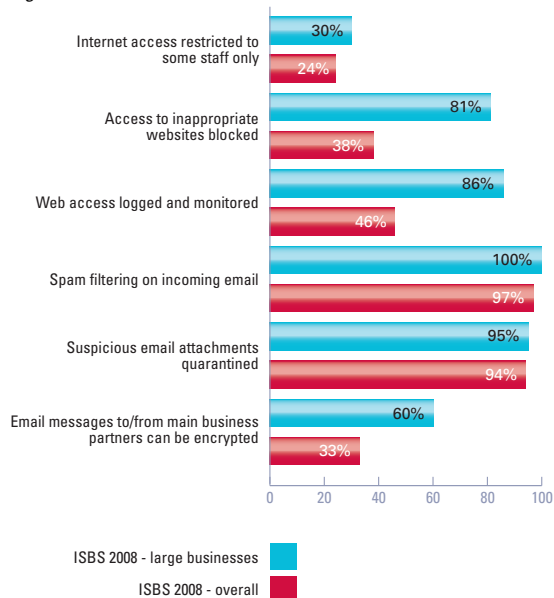
How many UK businesses that give staff Internet access have an acceptable usage policy?
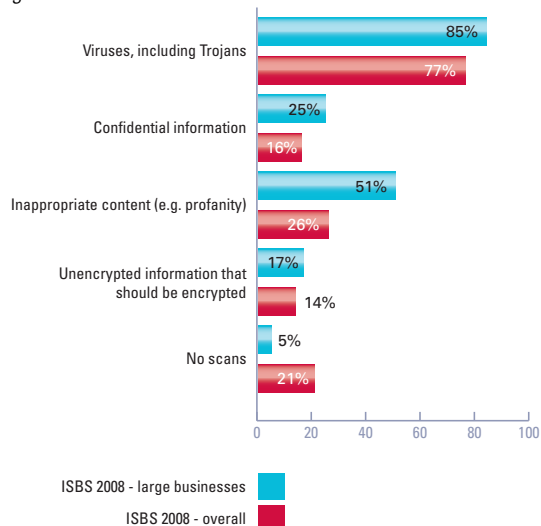
Figure 36
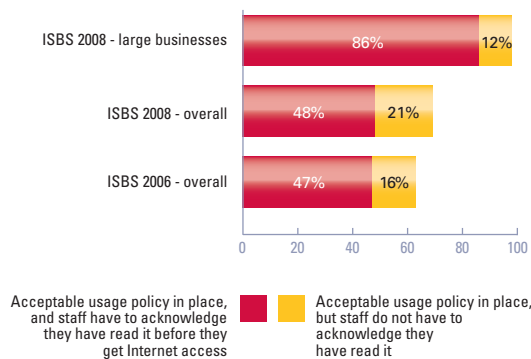
How is staff access to the Internet controlled?

Figure 37

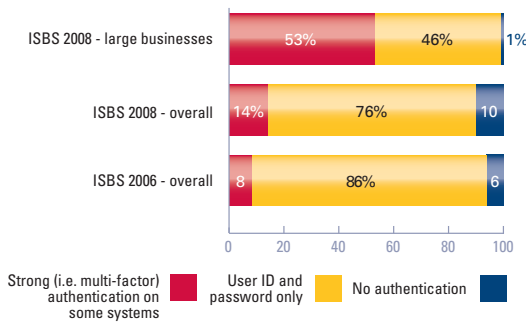**What scans do UK businesses carry out on outgoing email?**
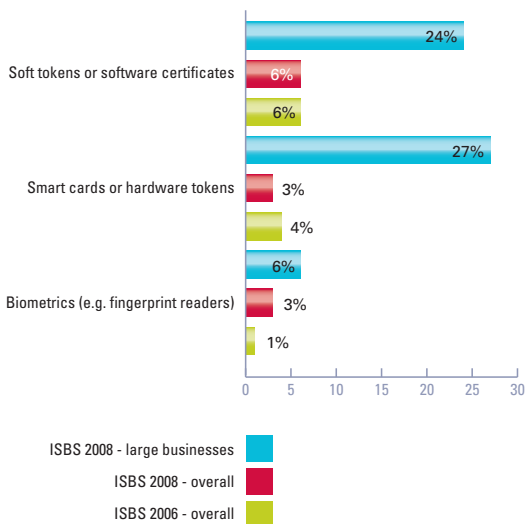
Figure 38

SECURITY CONTROLS

What techniques are used to authenticate users?
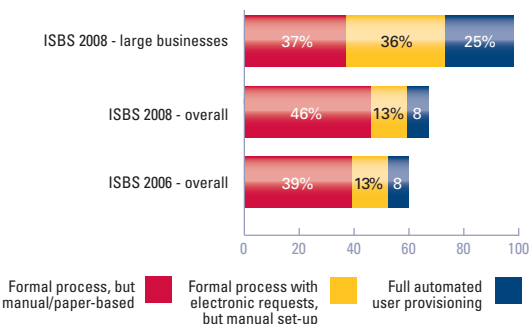
Figure 39

ISBS 2008 - large businesses	53% / 46% / 1%
ISBS 2008 - overall	14% / 76% / 10
ISBS 2006 - overall	8 / 86% / 6

Strong (i.e. multi-factor) authentication on some systems
User ID and password only
No authentication

What strong authentication techniques are used?

Figure 40

Soft tokens or software certificates	24% / 6% / 6%
Smart cards or hardware tokens	27% / 3% / 4%
Biometrics (e.g. fingerprint readers)	6% / 3% / 1%

ISBS 2008 - large businesses
ISBS 2008 - overall
ISBS 2006 - overall

How do UK businesses set up user access on their systems?

Figure 41

ISBS 2008 - large businesses	37% / 36% / 25%
ISBS 2008 - overall	46% / 13% / 8
ISBS 2006 - overall	39% / 13% / 8

Formal process, but manual/paper-based
Formal process with electronic requests, but manual set-up
Full automated user provisioning

Identity and access management

UK businesses still overwhelmingly depend on user IDs and passwords to check the identity of users attempting to access their systems. However, there is a small minority of companies in virtually every sector that do not require their users to authenticate their identity on login. This is most common among property companies and in Northern Ireland. The number of companies with no authentication has actually gone up over the last two years.

The use of strong (i.e. multi-factor) authentication has nearly doubled since 2006. It is most common in the telecoms, technology and professional services sectors. It is least common in not-for-profit organisations. Professional services firms tend to use software tokens, financial services favour smart cards or hardware tokens, and biometrics appear most in the telecoms sector. Over a third of Welsh firms use some strong authentication; Northern Ireland is at the other end of the scale.

A small Scottish leisure company has a strong focus on information security from the top down. While they don't formally assess risks, they have introduced biometric system access controls.

The growth in remote access is one of the drivers for greater adoption, but does not explain the whole picture. Only two-fifths of companies that use strong authentication apply it to remote access. Instead, companies appear to implement strong authentication in response to incidents involving unauthorised access, confidentiality breaches or impersonation of customers. Companies that had at least one such incident in the year are between two and three times as likely to have implemented strong authentication. It would, however, be a mistake to believe that technology alone will eliminate breaches.

A company in the Midlands implemented tokens to make user authentication more secure. Unfortunately, a number of users simply attached a post-it with their user ID and PIN number on the back of their tokens. This somewhat defeated the purpose.

Granting the right access to staff is just as important as authentication. Companies with a formal process for authorising access rights are twice as likely to detect unauthorised access as those without. 88% of financial services companies have a formal process for authorising and granting access to systems. Companies in the travel, leisure and entertainment sectors are least likely to have a formal authorisation process. Small businesses continue to lag behind large companies in this area.

One educational organisation gave a temporary member of staff a removable hard drive and access to sensitive information via a generic account, without a second thought to security. There were no checks, safeguards or encryption in place.

Removal of access rights on a timely basis is also vital. A contractor in the South-West had access to schedule emails to be sent out to groups of staff. He used this access to send out a leaving message to the entire business on the day after he had left the organisation. The message contained a video clip of inappropriate material. This not only caused business interruption (due to the amount of email traffic generated) but also offended several employees.

Manual processes for user access administration tend to be expensive and error-prone. Over half of companies in Greater London use electronic user access requests. Automated user provisioning (where the authorisation of a request automatically sets up the correct access rights) is used in most sectors, but is most common in financial services, adopted by 22% of companies.

The administrator at a medium-sized property company made a mistake when updating access rights in the personnel system. Suddenly, everyone could see everyone else's staff records.

SECURITY CONTROLS

The extending network

UK companies continue to open their systems to access from outside their physical network boundaries. This exposes them to attacks that tunnel through or bypass traditional perimeters.

With increasing staff mobility and changing work patterns, 54% of UK companies now allow staff to access their systems remotely (up from 36% in 2006); every very large business gives remote access to at least some staff. Energy, technology, professional services and not-for-profit firms are the most likely to grant remote access; about four-fifths do so. In contrast, only about a third of travel, leisure and entertainment companies do so. Four-fifths of companies in Greater London allow remote access, but less than half do so in Wales and East Anglia.

Enabling remote access potentially opens up the core network to unauthorised outsiders. Two-thirds of companies that allow remote access recognise this and have some form of additional authentication. There is also an eavesdropping risk as transmissions pass over the Internet. This is less recognised, with less than half using Virtual Private Networks (VPNs). Among very large companies, however, VPN adoption is almost universal. Technology companies are most likely to have additional security over their remote access; travel, leisure, entertainment and not-for-profit organisations are least likely. VPNs are most common in the technology and not-for-profit sectors.

A manufacturer found there was a spike in their VPN usage overnight. On investigation, it turned out that one of their IT staff was using the company's systems remotely to download MP3 tracks. The individual has now left the organisation.

42% of companies now use a wireless network (up from a quarter two years ago). Encouragingly, use of encryption has increased dramatically from 58% in 2006 to 94% in 2008. This is possibly due to the way that manufacturers now supply preconfigured routers or simple set-up wizards. Over half the companies that do not encrypt their wireless networks do not have any other security controls over them.

Telecoms and technology companies are most likely to have wireless networks. They are twice as likely as the most cautious sector, financial services. Two-thirds of companies in Greater London use a wireless network. Financial services companies are most likely to have implemented WPA (Wi-Fi Protected Access) or stronger encryption over their wireless transmissions; travel, leisure and entertainment companies are most likely to transmit unencrypted data. All very large companies protect their wireless networks, and none rely on the weaker WEP (Wired Equivalent Privacy).
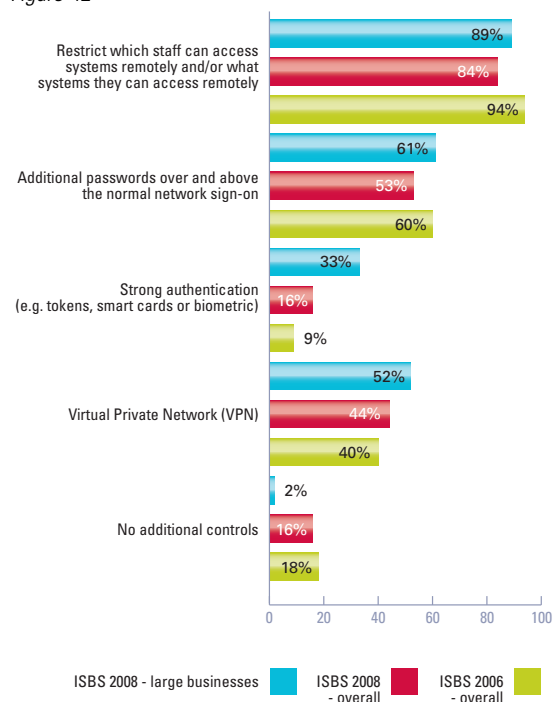
A company was proud of its network security, and hired security consultants to test it. They found an unsecured wireless access point that had been connected to the core network.

The more network connections that a company has, the more ways there are for an outsider to attack the company's network. Use of remote access, Voice over IP and wireless networks all increase the threat. Companies that use any one of these are twice as likely to have detected attempts to break into their network as those that do not. It is less clear how extending the network perimeter increases the likelihood of an outsider actually penetrating a company's network.

Public wireless hotspots pose a particular risk. 28% of businesses (and three-quarters of very large ones) allow staff with laptops to access systems through hotspots. These companies are twice as likely to have eavesdropping of network traffic as those that do not allow staff to access hotspots. It is small wonder then that two-thirds of them, and 93% of the very large companies, encrypt such transmissions using VPNs.
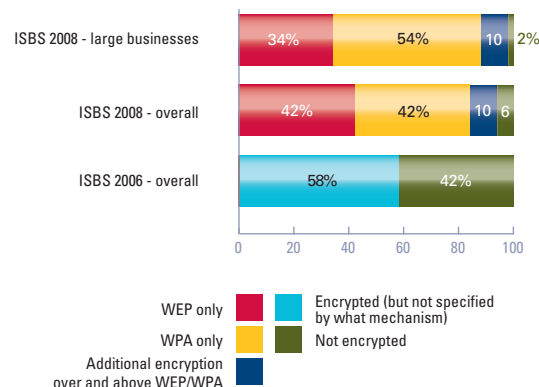
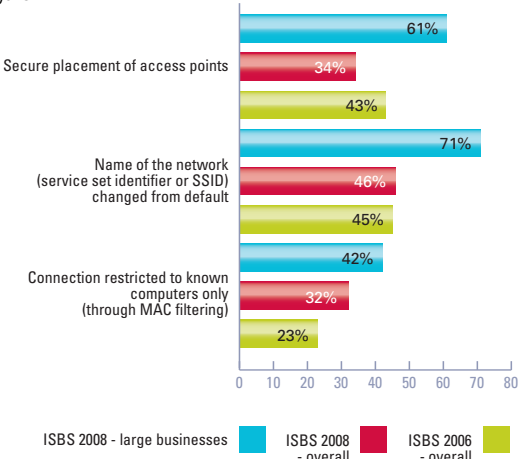### How is remote access secured?

Figure 42

	ISBS 2008 - large businesses	ISBS 2008 - overall	ISBS 2006 - overall
Restrict which staff can access systems remotely and/or what systems they can access remotely	89%	84%	94%
Additional passwords over and above the normal network sign-on	61%	53%	60%
Strong authentication (e.g. tokens, smart cards or biometric)	33%	16%	9%
Virtual Private Network (VPN)	52%	44%	40%
No additional controls	2%	16%	18%

How are wireless networks encrypted?

Figure 43

ISBS 2008 - large businesses: WEP only 34%, WPA only 54%, Additional encryption over and above WEP/WPA 10, Not encrypted 2%

ISBS 2008 - overall: WEP only 42%, WPA only 42%, Additional encryption over and above WEP/WPA 10, Not encrypted 6

ISBS 2006 - overall: Encrypted (but not specified by what mechanism) 58%, Not encrypted 42%

WEP only

WPA only

Additional encryption over and above WEP/WPA

Encrypted (but not specified by what mechanism)

Not encrypted

How else are wireless networks protected?

Figure 44

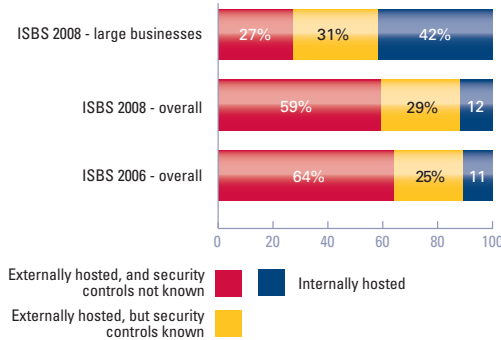|	ISBS 2008 - large businesses	ISBS 2008 - overall	ISBS 2006 - overall
Secure placement of access points	61%	34%	43%
Name of the network (service set identifier or SSID) changed from default	71%	46%	45%
Connection restricted to known computers only (through MAC filtering)	42%	32%	23%

SECURITY CONTROLS

Are websites internally or externally hosted?
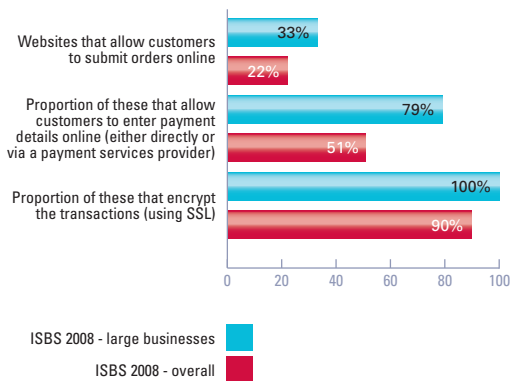
Figure 45

How do UK businesses protect their website?

Figure 46
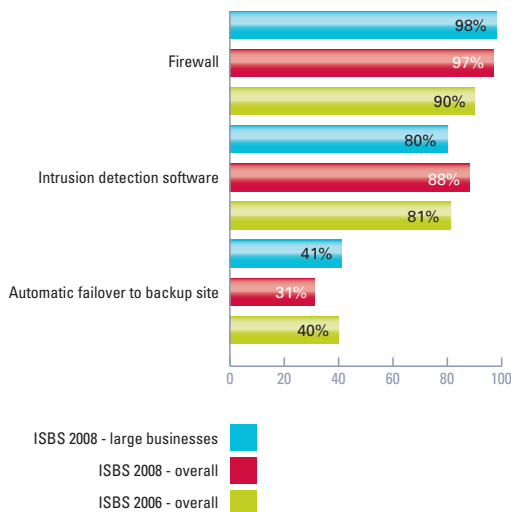
How many UK websites allow customers to transact online?

Figure 47

Website security

The proportion of websites that are hosted externally has not changed much since 2006, but companies are getting better at understanding the controls their hosting provider has. The sectors that are least likely to use an external website hosting provider are government, health and education (because of the sensitivity of the data held) and technology (because they have the best in-house capability).

Telecoms companies have the best knowledge of the controls operated by their hosting provider, while companies in the travel, leisure and entertainment sector show relatively little interest.

The firewall is now regarded as a basic security discipline for websites. 96% of companies whose website is externally hosted know whether their site is protected by a firewall. For intrusion detection, this drops to 88% and only 76% know whether fall-back facilities are in place. Where respondents know, almost every externally hosted website is behind a firewall and 94% are protected by IDS (Intrusion Detection Software). Only 42% of websites automatically transfer traffic to a fall-back site in the event the primary site cannot handle all the incoming traffic.

Internally hosted websites tend to be less well protected than externally hosted ones. 94% are behind a firewall, but only 67% have IDS and 27% automatic fail-over. A firewall appears to be the basic pre-requisite for other security mechanisms; websites without a firewall generally lack any other protection. The websites without firewalls are in the retail and manufacturing sectors. Energy websites are most likely to have IDS and automatic fail-over; property and not-for-profit websites are least likely.

A large financial services provider suffered a denial of service attack on its website, which disrupted Internet traffic for a day. Fortunately, effective defences and a contingency plan were in place, so the disruption was minimised.

Companies that host their websites in-house are more than twice as likely to report attempts by outsiders to break into their network as those whose websites are externally hosted. In many cases, ISPs do not report this kind of information to their customers.

All the companies that reported actual penetration into their networks had firewalls and four-fifths had IDS. Those without such defences may simply not detect such unauthorised access.

One company bought an IDS and installed it on the network; however, they have not had the resource or budget to tune and monitor it. Therefore, they are not getting any real value from it.

Retailers and telecoms providers are most likely to let customers submit orders online through their websites; energy companies are least likely. All of the websites that allow customers to submit orders online are behind a firewall. However, 13% of them are not protected by IDS.

95% of websites that collect credit or debit card information, either directly or via a payment services provider, encrypt this data using secure-sockets layer (SSL). However, only half of the companies that collect direct debit details on their website appear to encrypt this information.

The companies that do not encrypt payment transactions taken through their website are in the telecoms, technology, travel, leisure and entertainment sectors. None of the companies that reported eavesdropping attacks currently take credit card transactions over the Internet.

SECURITY CONTROLS

Emerging technologies

Instant messaging (IM) services provide a fast, informal way for people to communicate with others over the Internet. IM exposes companies to the same confidentiality and reputation risks as email, but controls over IM in most UK businesses are worse than those over email.

The apparent increasing use of IM is partly explained by a change in the way survey questions are asked. In 2006, respondents were asked whether they allowed staff to use IM; in 2008, they were asked whether they blocked access to it. Some of the 2006 respondents shown as blocking access probably had instructed staff not to use IM but had not actually blocked the service.

An acceptable usage policy is normally a pre-requisite for implementing other IM controls. Four-fifths of companies that scan incoming or outgoing messages, and 94% of those that log and audit messages, have a policy. The exception to this is restricting which staff can use IM. Many companies do this without having an acceptable usage policy. Most companies that scan messages also log and audit them, and vice versa. Implementing these controls does appear to have an impact. On average, companies with IM controls had fewer confidentiality breaches.

Financial services companies tend to take the most steps to mitigate IM risks. However, even here, a third have taken no steps. Companies in Northern Ireland are half as likely as the national average to block IM, and most do not control their staff's access. In contrast, more than half of Welsh companies block IM, and nine-tenths of those that allow it control its usage.

Until recently, a travel company allowed staff non-business use of the Internet as long as the use remained reasonable and during the employee's lunch hour. However, monitoring of usage statistics showed increasing productivity loss during work hours, for example through IM and accessing social networks. The policy has now changed; little Internet use is now permitted and IM and social networks have been blocked.

The number of companies that have implemented Voice over IP telephony (VoIP) has doubled since 2006. It is expected that, by the end of 2008, nearly a third of companies will be using VoIP. Companies in Scotland, Greater London and East Anglia lead VoIP adoption. It is most common in the technology and telecommunications sectors, with roughly 45% penetration. The travel, leisure and entertainment sectors are the slowest adopters.

The security risks posed by VoIP depend on whether it is being used for internal or external communication. It is important that these risks are evaluated before implementation. In practice, 70% of companies that have implemented VoIP have evaluated the security risks of doing so. 40% of those that plan to implement it over the next year have already evaluated the security risks. Financial services companies are most likely to evaluate the risks before implementation.

A further emerging area is the use of social networking sites (such as MySpace, Facebook and Bebo). Many of these sites can provide legitimate business benefits (e.g. through sharing experience and best practice with other businesses). However, many companies have found that the habitual nature of these sites can adversely affect staff productivity. In addition, businesses are becoming increasingly concerned about what is being said about them on these sites, and some have experienced loss of confidential information.

IT staff at an insurance company used an Internet chat room to help them solve technical issues. However, this resulted in them inadvertently disclosing the company's security set-up and configuration in a public forum.
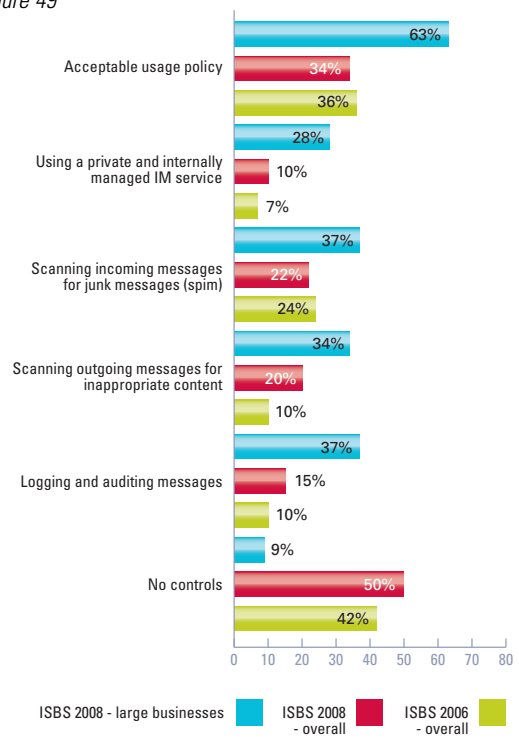
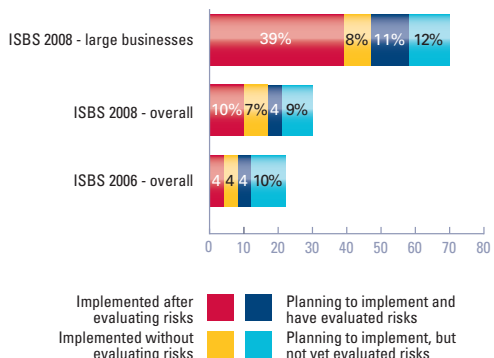**How many UK businesses allow staff to send instant messages (IM) across the Internet?**

Figure 48
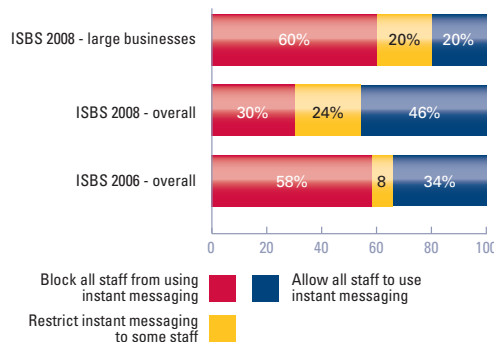
What precautions do UK businesses that allow IM take over its use?

Figure 49

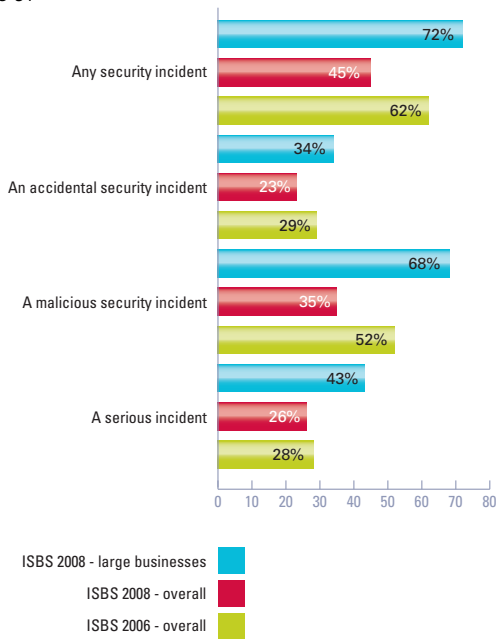**How many UK businesses are implementing Voice over IP telephony?**
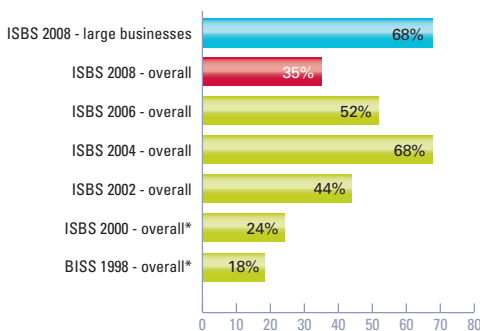
Figure 50

SECURITY BREACHES

In the last year, how many UK businesses had...

Figure 51

Any security incident — 72%, 45%, 62%

An accidental security incident — 34%, 23%, 29%

A malicious security incident — 68%, 35%, 52%

A serious incident — 43%, 26%, 28%

ISBS 2008 - large businesses
ISBS 2008 - overall
ISBS 2006 - overall

How many UK businesses had a malicious security incident last year?

Figure 52

ISBS 2008 - large businesses — 68%
ISBS 2008 - overall — 35%
ISBS 2006 - overall — 52%
ISBS 2004 - overall — 68%
ISBS 2002 - overall — 44%
ISBS 2000 - overall* — 24%
BISS 1998 - overall* — 18%

* The 1998 and 2000 DTI survey figures were based on the preceding two years rather than last year

What is the median number of malicious incidents in the last year?

Figure 53

Median for all respondents — 10, 2, 5

Median among those that had an incident — 15, 6, 8

ISBS 2008 - large businesses
ISBS 2008 - overall
ISBS 2006 - overall
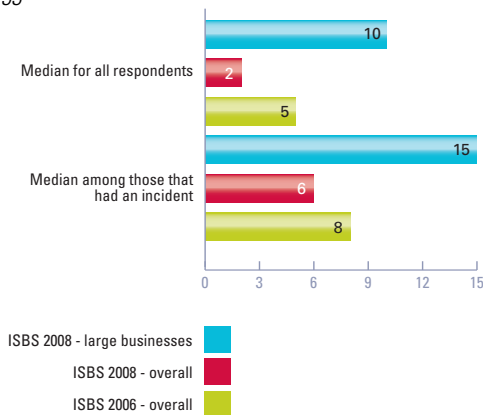
Incidence of security breaches

Fewer companies had a security incident in the last year than two years ago. After the peak in 2004, the number of companies affected by security breaches has returned to the level seen in 2002. Overall, just under half of UK businesses experienced a security incident. However, the average seriousness of incidents increased, so the number having a serious breach has stayed constant at about a quarter.

Overall, companies in Northern Ireland, the South-West and the North-East are least likely to report a security incident, with only a third affected. In contrast, over half of the companies in Greater London report incidents. Telecoms providers are likeliest to have had a security incident, with more than half affected. In contrast, only a third of companies in the travel, leisure and entertainment sectors had a breach.

While the good news is welcome, it is important to remember that these statistics under-estimate the actual experience for the following reasons:
- There is some evidence that management is becoming desensitised to minor incidents in well-understood areas, such as systems failure and virus infection. Companies no longer regard these as security breaches, but as routine events swept up by business-as-usual controls without needing to be logged;
- In some areas, such as network penetration and staff misuse, many companies still lack the controls that would enable them to detect all incidents. According to the hacking community, only a tiny proportion of actual penetrations are detected by network owners;
- Many firms do not fully appreciate the risks posed by newer technologies (such as USB sticks, Voice over IP, instant messaging and social networking) and so are not aware of breaches involving them;
- Many companies do not log security incidents, and so are likely to under-report the number of incidents; and
- Some small businesses were so badly affected by the flooding in summer 2007 that they have ceased trading. Since this Survey is compiled via a telephone interview, these incidents will not be picked up (since there is no-one at those businesses to speak with).

Large businesses are still likeliest to report security incidents. The number of large companies affected has dropped, but by slightly less than for small businesses. Nearly three-quarters of large businesses had a breach in the last year. The bigger the organisation the likelier it is to have a breach. 94% of very large companies had an incident, of which 76% had at least one serious incident.

The reasons for large companies reporting more breaches remain the same. Firstly, they have more staff, so the likelihood of some internal misuse increases. Secondly, their size and typical presence on the Internet makes them a more attractive target for external attackers. Thirdly, they have better tools and procedures to detect breaches.

The average number of incidents per company affected is down slightly from the last survey in 2006. The mean number of breaches is roughly two per week (down from one per day) and roughly one per day for large businesses (down from several per day). As in 2006, the median number of breaches (6 overall and 15 for large companies) gives a more representative picture, since the mean is distorted by a small number of companies that have hundreds of breaches per day.

Incidents tend to be considered serious if they involve major business disruption, more than 10 man-days of staff time fixing the problem, more than £10,000 cash costs, disciplinary action against staff and/or media coverage. The factors that seem to have least influence are the duration of disruption and whether there are customer complaints. The seriousness of most incident types varied widely; for example, while 13% of the worst systems failures were not at all serious, 10% were considered extremely serious. However, all incidents involving infringement of laws were rated as serious or very serious.

SECURITY BREACHES

Comparison with other security surveys

It is useful to examine how the results of ISBS 2008 compare with other security surveys around the world. This can shed light on trends that are international rather than local to the UK. In addition, because different questions are asked in different surveys, comparison can yield richer interpretation of what the ISBS 2008 results mean.

Most other security surveys around the world operate on a self-select basis. As a result, they tend to be biased towards large and very large organisations, rather than being representative of the whole business community. Comparison with other surveys is, therefore, particularly relevant to the larger UK businesses.

Among the most respected security surveys from around the world are:
- The Information Security Forum (ISF) conducted a survey in 2007; it comprised responses from 91 of its member firms, typically businesses with 500 or more staff. 20% were from the UK; the rest were principally from Europe and North America. The survey is a benchmarking exercise against the ISF Standard of Good Practice (which is publicly available on the ISF web-site).
- The Global State of Security Survey is an annual online survey, managed by PricewaterhouseCoopers in conjunction with CIO Magazine and CSO Magazine. The fifth such survey, conducted in 2007, gathered information from 7,200 companies in more than 100 countries. More than half the respondents had an annual turnover of over $100m.
- The annual Computer Security Institute (CSI) Computer Crime and Security Survey is the longest running computer survey in the USA. In 2007, the twelfth such survey received responses from 500 computer security practitioners working for US businesses and government. Roughly half of their organisations had more than 1,500 staff.

While definitions vary from survey to survey, the levels of security breaches seen in ISBS 2008 for large to very large businesses are broadly consistent with those shown in other surveys. This is illustrated by serious incidents, where the percentage of respondents affected in the other three surveys all fall between the ISBS 2008 figures for large and very large respondents. Other figures are also similar; for example, 13% of CSI respondents report that their systems were penetrated by hackers, identical to the large business ISBS 2008 statistic.

ISBS 2008 shows a significant swing from external to internal threat; nearly two-thirds of the worst incidents have an internal cause, reversing the trend of previous years. The Global State of Security Survey shows a similar pattern; for the first time in its nine year history, employees are now considered the single most likely cause of a security incident. On the surface, the CSI survey shows a very different picture; 62% felt that less than 20% of their losses were due to insiders. The explanation is that most internal incidents cost less to deal with than external attacks.

The most common breach types are similar around the world. The top three incident types in the CSI survey are insider abuse of Net access, viruses and laptop/mobile device theft, all experienced by more than half of respondents. Four-fifths of ISF members experienced external attack (mostly viruses, spam and malicious probes), theft and internal misuse/abuse.

Finally, investment in security seems fairly consistent around the world. According to the CSI survey, average expenditure is roughly 5% of the IT budget, increasing slowly in absolute terms but largely static as a % of IT spend. Among ISF members, the average spend is 3.5% of the IT budget. However, the biggest driver for security expenditure, according to the Global State of Security Survey, is business continuity, whereas protecting the company's reputation and customer data take precedence in the ISBS 2008.
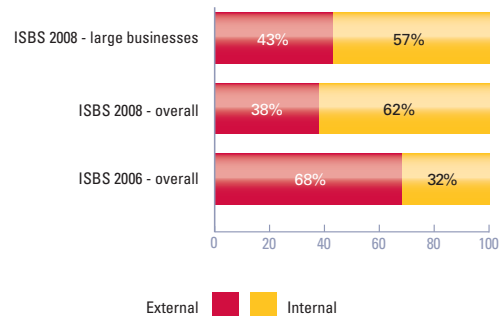
How do the levels of serious incidents reported in ISBS 2008 compare with those for other similar surveys?
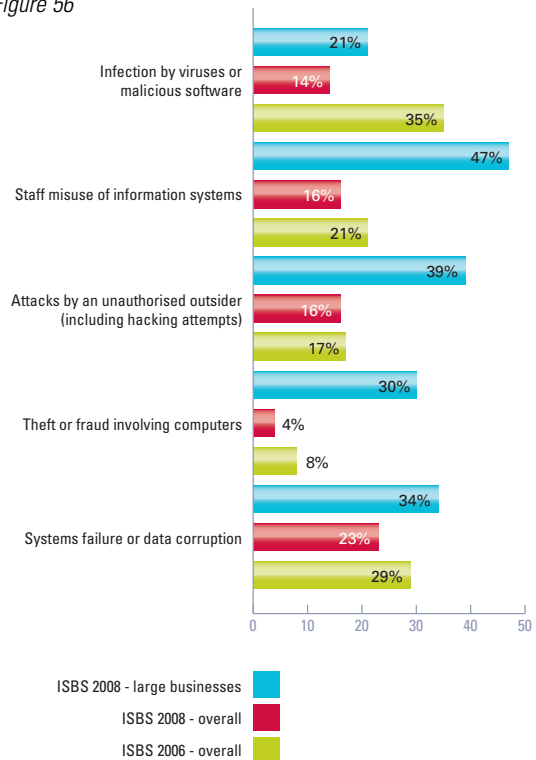
Figure 54
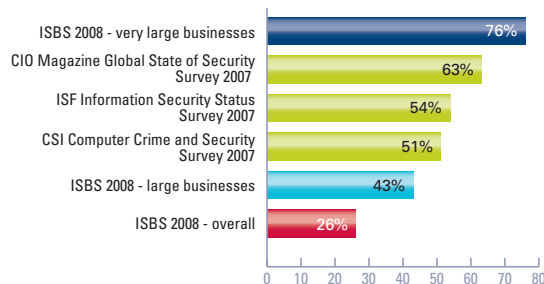
Was the cause of the worst incident internal or external?
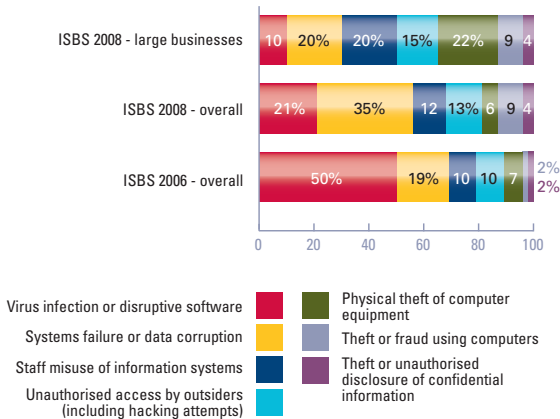
Figure 55

What type of breaches did UK businesss suffer?

Figure 56

SECURITY BREACHES

What was the worst security incident faced by UK businesses?

Figure 57

Virus infection or disruptive software

Systems failure or data corruption

Staff misuse of information systems

Unauthorised access by outsiders (including hacking attempts)

Physical theft of computer equipment

Theft or fraud using computers

Theft or unauthorised disclosure of confidential information

What is the median number of breaches suffered by the affected companies in the last year?

Figure 58

ISBS 2008 - large businesses

ISBS 2006 - large businesses

ISBS 2008 - overall

ISBS 2006 - overall
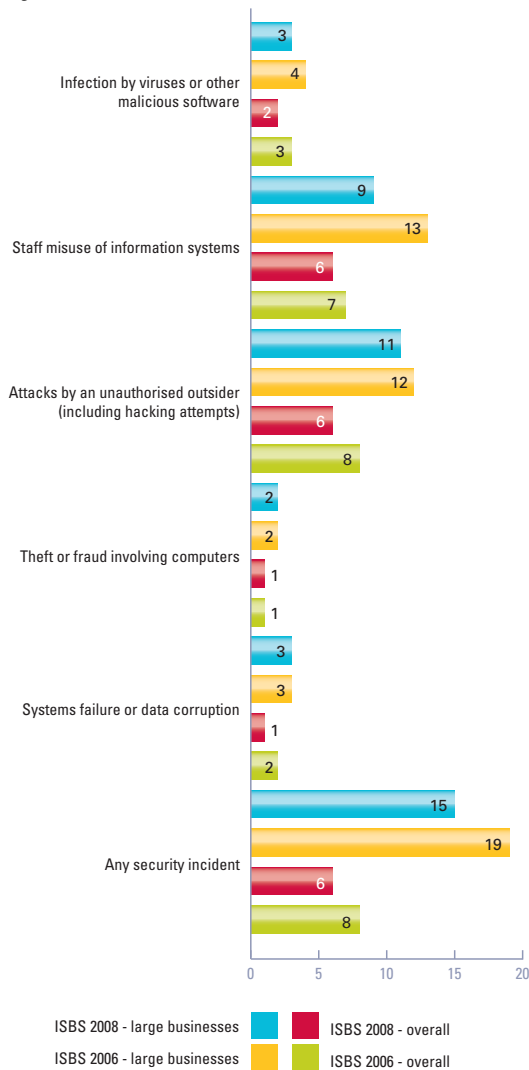
Type of security incidents

The most striking feature of ISBS 2008 is the decline in reported virus infections.

For the last decade, virus infection was the largest cause of security incidents. Indeed, in 2006, virus infection accounted for half of the worst security incidents suffered by UK businesses. Two years on, virus infection has dropped to being the fourth most common type of security incident. The number of companies affected has fallen to levels last seen in 2000.

Levels of staff misuse of systems and theft are also lower than two years ago. Outsider attacks, however, remain at roughly the same levels as seen in 2006 overall, and are on the increase for large businesses.

Staff misuse, outsider attack and theft are all areas where large companies are much more likely to have incidents than small businesses. Of very large companies, 91% suffered staff misuse, 85% had detected significant attempts to break into their networks (28% had detected actual penetration) and 54% experienced computer fraud.

No sector is immune from incidents of staff misuse. The retail and distribution sector seems to suffer most, with nearly a third having incidents. The least affected is the energy and utilities sector, but even here 20% of companies have reported incidents. Companies in Greater London are most likely to report staff misuse, with a third affected, while companies in Northern Ireland are least likely, with only one in seven affected. One reason for this is that more large companies are based in London and large companies have more issues with staff misuse than small businesses.

Outsider attacks vary quite markedly by sector. Telecoms providers suffer most, with nearly two-fifths having incidents. At the other end of the spectrum, only one in seven firms in the leisure sector report incidents. Interestingly, relatively few financial services providers (only one in six) report attacks by an outsider. Companies in Greater London are twice as likely to report attacks by an outsider as those in the South-West.

Theft and fraud are commonest in the not-for-profit, government, health and education sectors, with one in six reporting incidents. In contrast, only one in twenty in the telecoms, energy and retail sectors reports such breaches. Wales and East Anglia have the lowest incidence of theft or fraud - companies in Greater London are eight times as likely to report theft or fraud as those in Wales.

Not-for-profit organisations report the most accidental systems failures, with one in three affected. They are more than twice as likely to have problems of this kind as the least affected sector, the travel, entertainment and leisure sector. Companies in the North-West report the fewest incidents of accidental systems failure, half the rate reported in Greater London.

The average number of breaches suffered by affected companies is down across all types of incident and sizes of company. The biggest reductions for small businesses are in virus infections and systems failures. Large companies have made good progress in reducing staff misuse but remain subject to a large volume of external attacks. Very large companies remain the main target for hackers and 20% detect hundreds of significant attempts to break into their network every day.

Relative to their size, small businesses continue to bear the brunt of security incidents. While six breaches a year may not seem a lot, for a business of fewer than ten employees, security incidents remain a significant drain on time and resources.

SECURITY BREACHES

Infection by viruses and malicious software

Viruses, worms, Trojans and spyware (collectively known as malware) caused massive business disruption in the early years of this decade. Now, it is clear that malware causes much less direct damage than in the past. Only 14% of UK companies had a malware infection last year, down from 35% two years ago. Even among very large businesses, less than half had an infection last year.

It appears that there are three main reasons why fewer malware infections are being reported:

- Corporate anti-virus defences have significantly improved;
- Most minor virus infections no longer register in the same way as they did. They are no longer considered security breaches but as events dealt with by routine controls; and
- Malware itself and the motivation of its writers have changed. Law enforcement in this area has improved around the world. As a result, the kudos derived from writing a disruptive worm is outweighed by the personal consequences. Instead, virus writers are increasingly employed by organised crime to write stealthy code that seeks to obtain confidential data or open holes in security for hackers to exploit. Spyware now accounts for one in six of the worst infections. Malware infection used to be the end goal; now, it is merely the first step, enabling other more lucrative attacks.

A virus bypassed security systems at a medium-sized business in the North-East, opening up the email system for hackers to use as a spam relay. The consequences for the business were very serious - their email domain became blacklisted, causing their legitimate email to be treated as spam by recipients.

Companies providing services to the public sector and telecoms providers are most likely to have had virus infection; in contrast, not-for-profit organisations report very few infections. The companies with the greatest number of incidents are in the entertainment, property and public sectors. Companies in the North-West were least affected by virus infection; Greater London and the Midlands had the worst experience.

Despite the lower levels of infection, it would be a mistake, however, to assume that the malware threat is extinguished. For two-thirds of companies that had a virus infection, it was their worst security incident of the year. Malware infections were particularly damaging in the telecommunications sector.

A small manufacturer in London suffered when a virus bypassed its security systems. The infection caused major disruption to its computer systems for several days. Following the incident, policies and procedures were changed to prevent a similar outbreak in the future.

The fragmentation trend observed in the last Survey has continued. In 2004, a few viruses (Blaster, Sobig, Bugbear) dominated the statistics and 57% of respondents could name the virus that caused their worst incident. In 2006, this fell to 38%, and this year only 27% could name the virus that caused their worst incident. The reality is that companies are being bombarded by an enormous number of viruses and variants; individual pieces of malware no longer stand out like their predecessors, such as Melissa, the Lovebug or Blaster. As before, many of these exploit human weaknesses to bypass defences.

Systems at a medium-sized telecommunications provider were compromised after staff accessed and downloaded files from an inappropriate website, leading to a virus infection that bypassed the anti-virus defences. The resultant outage caused customer complaints, and the company has since updated its technical defences to prevent further incidents.
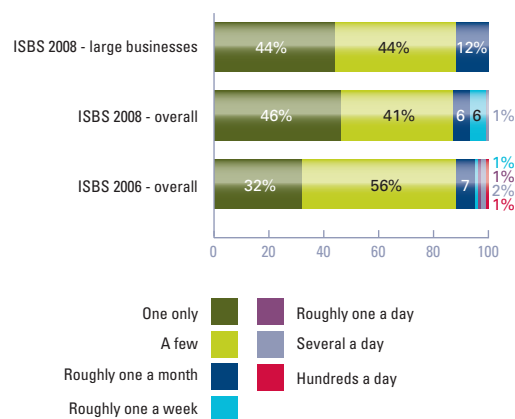
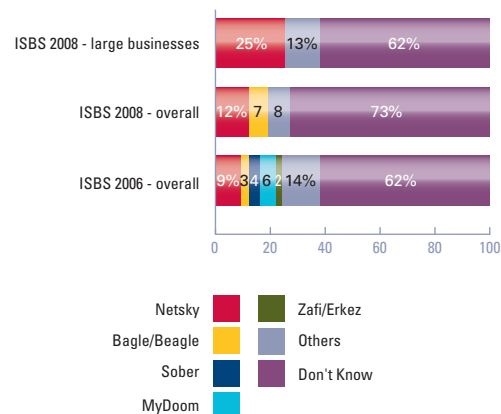**What was the source of the worst malicious software incident?**

Figure 59
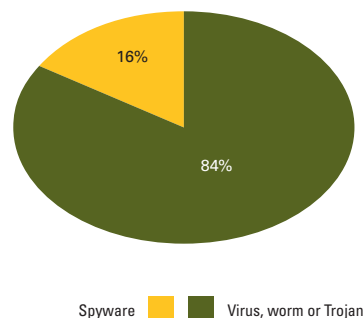
How many infections did the affected businesses suffer in the last year?

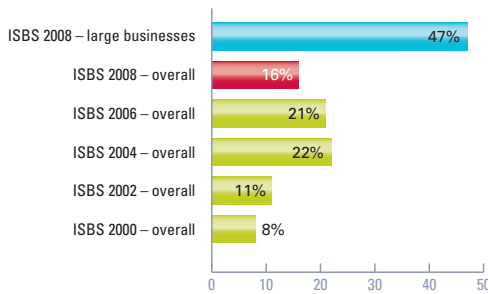*Figure 60*

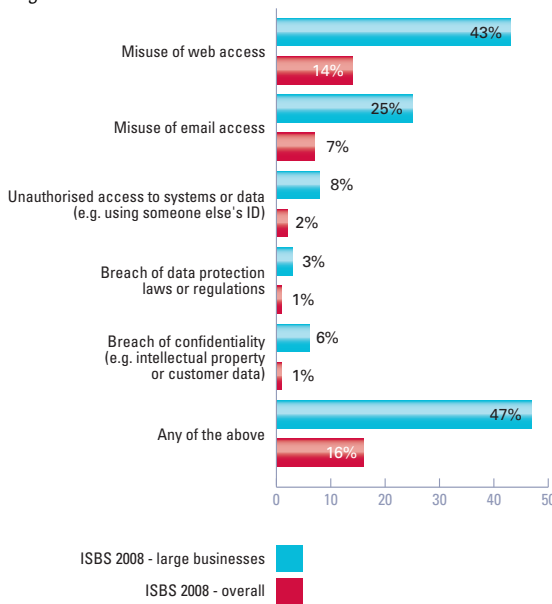**What caused the worst virus infections?**

Figure 61

SECURITY BREACHES

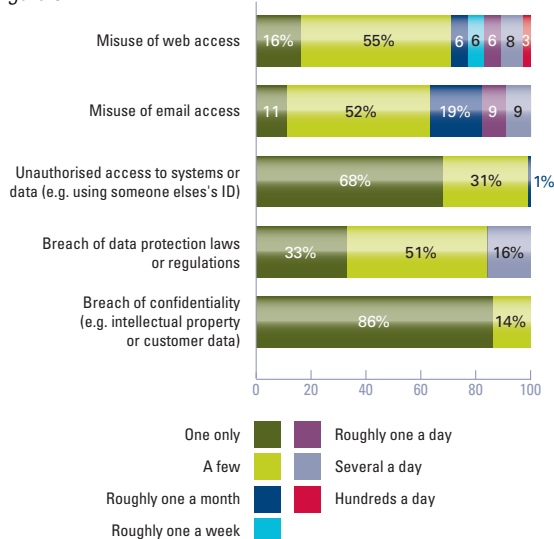**How many UK businesses suffered from staff misuse of information systems?**

Figure 62

ISBS 2008 – large businesses	47%
ISBS 2008 – overall	16%
ISBS 2006 – overall	21%
ISBS 2004 – overall	22%
ISBS 2002 – overall	11%
ISBS 2000 – overall	8%

What type of staff misuse did UK businesses suffer?

Figure 63

Misuse of web access	43% / 14%
Misuse of email access	25% / 7%
Unauthorised access to systems or data (e.g. using someone else's ID)	8% / 2%
Breach of data protection laws or regulations	3% / 1%
Breach of confidentiality (e.g. intellectual property or customer data)	6% / 1%
Any of the above	47% / 16%

ISBS 2008 - large businesses
ISBS 2008 - overall

How many misuse incidents did the affected businesses suffer in the last year?

Figure 64

Misuse of web access	16%	55%	6	6	6 8 3
Misuse of email access	11	52%	19%	9	9
Unauthorised access to systems or data (e.g. using someone elses's ID)	68%	31%	1%		
Breach of data protection laws or regulations	33%	51%	16%		
Breach of confidentiality (e.g. intellectual property or customer data)	86%	14%			

One only   Roughly one a day
A few   Several a day
Roughly one a month   Hundreds a day
Roughly one a week

Staff misuse of information systems

Levels of staff misuse of systems and data are lower now than the past two Surveys. The commonest forms are still visiting inappropriate websites, excessive browsing and sending inappropriate email.

The number of incidents reported could be understated, since some companies do not detect or record such breaches. Companies that log incidents are three times as likely to report unauthorised access by staff, twice as likely to report data protection breaches and ten times as likely to report confidentiality breaches as those that do not. Firms with a security policy are more than twice as likely to detect unauthorised access or confidentiality breaches as those without. Only companies that take steps to raise security awareness report any incidents.

Companies in the retail, travel, leisure and entertainment sectors are most likely to report web misuse, twice as likely as financial services providers. In contrast, the companies experiencing the greatest number of incidents per annum are in the financial services and technology sectors. The regions least affected are Scotland and Northern Ireland; Greater London and Wales had the worst experience.

Companies in the financial and professional services sectors rely heavily on email, and are most likely to have had staff misuse of email; professional services firms also report the greatest number of incidents. In contrast, not-for-profit organisations report very few incidents. The least affected regions are Wales and the South-West; Greater London had the worst experience.

Not-for-profit organisations are four times more likely to have staff gain unauthorised access to systems and data than the national average. The companies with the most incidents are in the financial services, manufacturing and not-for-profit sectors. Companies in Wales and Northern Ireland report no such incidents; Scotland had the worst experience, with 7% affected.

A large manufacturer had an extremely serious confidentiality breach when an employee sent some of its intellectual property externally. The contingency plan and controls enabled the company to detect this quickly; disciplinary and legal action was taken against those responsible.

The companies that report data protection infringements have mature security controls in place. They have security policies and carry out risk assessments, they check for compliance with their security policy, they include security in their staff handbook and they train staff on security matters. This suggests less diligent companies simply do not detect similar breaches. Not-for-profit organisations, telecoms providers and energy companies are most likely to report infringements. In contrast, no financial services, technology or retail companies had such breaches. Companies in Greater London report three times as many infringements as the national average.

Staff at a telecommunications company inadvertently breached the Data Protection Act by leaking confidential personal data. Fortunately, an effective contingency plan was to hand and consequently the matter was dealt with quickly and effectively. After the incident, staff received additional training to prevent similar incidents occurring in the future.

Companies in London, particularly in professional services and telecoms, are most likely to have lost confidential data, with professional firms reporting the most breaches. In contrast, no financial services, leisure or energy companies had such incidents. Confidentiality breaches were more likely to be the worst incident of the year in the not-for-profit sector than in other sectors.

A large technology company lost some sensitive data, when an employee left a laptop on the roof of their car and then drove off.

SECURITY BREACHES

Unauthorised access by outsiders

Unlike other types of incident, attacks by outsiders do not appear to be on the decline. One in ten small businesses reports attempts to break into its network, virtually the same proportion as in 2006. The bigger the company, the more attractive a target it is. 85% of very large businesses were attacked. Telecoms providers are most likely to be attacked, three times as likely as average; leisure and not-for-profit organisations are least likely. Greater London and the South-East are the worst affected regions, while East Anglia and Wales had fewest attacks.

A large telecoms provider had an extremely serious social engineering attack which led to theft of confidential data. The breach was reported in the media, but fortunately the contingency plan proved effective. After several man-weeks of investigation, legal action was taken against the perpetrators. After the incident, procedures were changed and additional staff training provided.

Companies that have procedures for logging and responding to security incidents are twice as likely to report attempts by outsiders to break into their network as those without. It seems that the incident statistics for companies without such procedures are understated.

Staff at one small business helped a young hacker to "penetration test" their network. Unfortunately, they had not checked the person's credentials first.

Hackers appear more successful at breaking into corporate networks than two years ago. One in twenty five small businesses had its network penetrated. The bigger the company, the more likely it is to have been penetrated; more than a quarter of very large companies were affected. Companies working in the government, health and education sector appear particularly susceptible, while hacking attacks on telecoms providers tended to have the biggest impact.

A security vulnerability in a server allowed hackers to break into an ISP that hosts personal and small business websites. Customer passwords were compromised. As a result, some websites were subject to unauthorised access and some email domains were used to send spam messages.

Telecoms providers are the main targets of attacks on Internet or telecommunications traffic, with one in eight affected. One in ten of them also suffered denial of service (DoS) attacks, twice the national average. However, some companies in every sector reported DoS attacks. Nine-tenths of companies that suffered a DoS attack were prepared for it, with intrusion detection systems in place; automatic failover to a fall-back site was much rarer.

Some companies in every sector reported that outsiders had sent emails pretending to be from them (known as phishing). One in ten not-for-profit organisations were impersonated, but very few property and retail companies were targeted. No companies in Northern Ireland were aware of such attacks. Companies that accept orders online are slightly more likely to be targeted by phishing; however, phishing is clearly not restricted to website logins, and 4% of companies that do not accept orders online report attacks.

Financial services, travel, leisure and entertainment companies, especially in Greater London, are most likely to report attempts to impersonate their customers (e.g. following identity theft). No such incidents were reported in energy and not-for-profit firms, nor in Northern Ireland.

A small company in the leisure sector lost tens of thousands of pounds after fraudsters purchased goods using stolen credit card details. After the incident, the company upgraded its systems, changed its processes and trained staff on how to spot such attacks in the future.
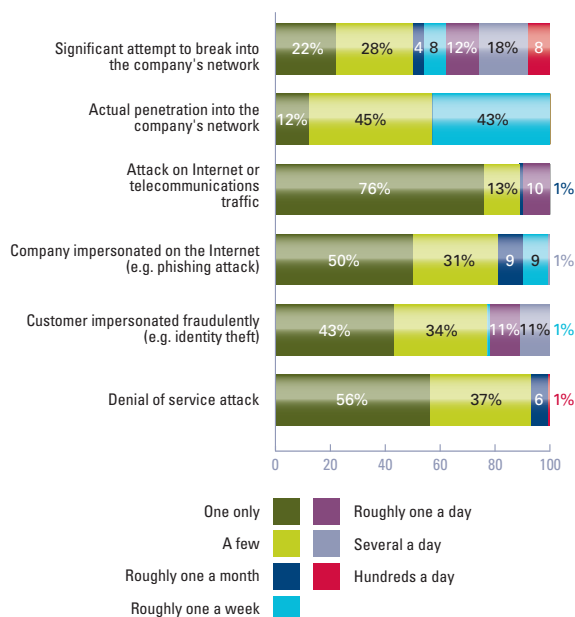
How many businesses were attacked by an unauthorised outsider in the last year?

Figure 65
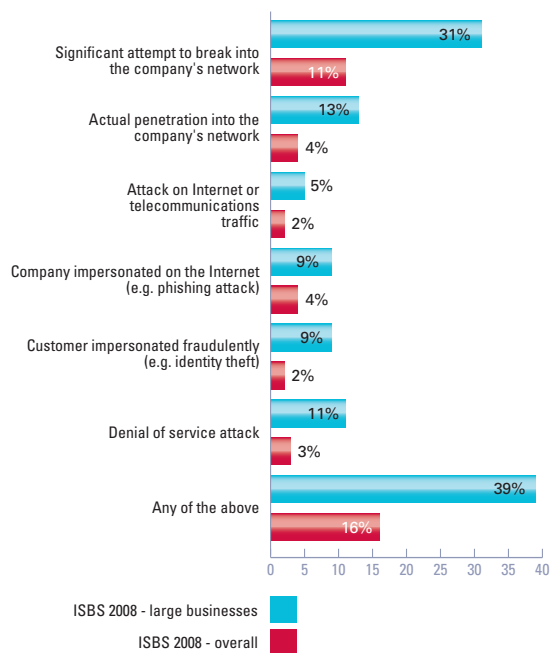
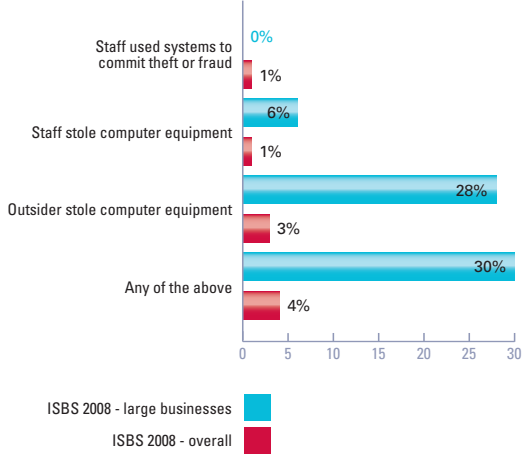**How many attacks by unauthorised outsiders did the affected businesses suffer in the last year?**
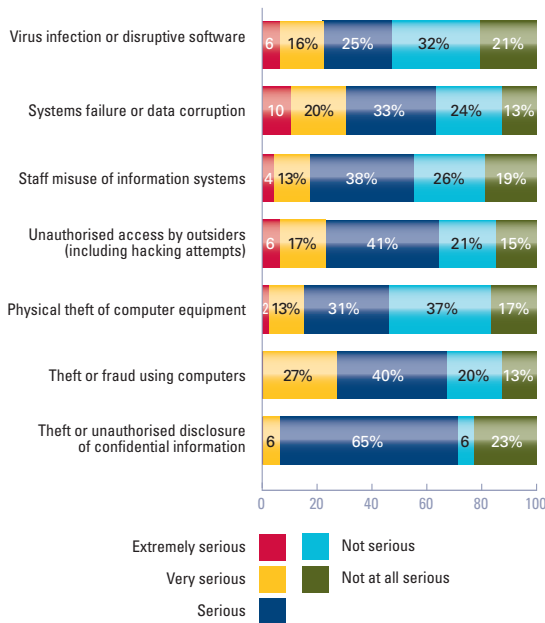
Figure 66

SECURITY BREACHES

What type of theft and fraud did UK businesses suffer?
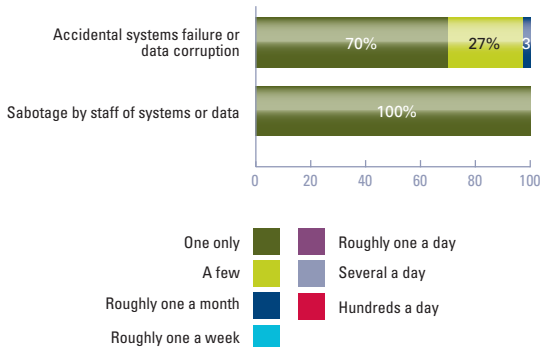
Figure 67

Staff used systems to commit theft or fraud	0% / 1%
Staff stole computer equipment	6% / 1%
Outsider stole computer equipment	28% / 3%
Any of the above	30% / 4%

ISBS 2008 - large businesses
ISBS 2008 - overall

How serious were different types of incident?

Figure 68

Virus infection or disruptive software	6 / 16% / 25% / 32% / 21%
Systems failure or data corruption	10 / 20% / 33% / 24% / 13%
Staff misuse of information systems	4 / 13% / 38% / 26% / 19%
Unauthorised access by outsiders (including hacking attempts)	6 / 17% / 41% / 21% / 15%
Physical theft of computer equipment	2 / 13% / 31% / 37% / 17%
Theft or fraud using computers	27% / 40% / 20% / 13%
Theft or unauthorised disclosure of confidential information	6 / 65% / 6 / 23%

Extremely serious   Not serious
Very serious   Not at all serious
Serious

How many systems failures or data corruptions did the affected businesses suffer in the last year?

Figure 69

Accidental systems failure or data corruption	70% / 27% / 3
Sabotage by staff of systems or data	100%

One only   Roughly one a day
A few   Several a day
Roughly one a month   Hundreds a day
Roughly one a week

Computer theft and fraud

The commonest type of theft remains physical theft of computer equipment. The level of theft in small companies is lower than two years ago, but this is still a major annoyance for large businesses. Thefts affected 28% of large businesses, typically several times a year. In contrast, no companies with fewer than 10 employees had any such incidents and the vast majority of small businesses affected had only one such theft.

Companies in greater London are more than five times as likely to have computer equipment stolen as those in Wales or Northern Ireland. Scotland also has a high theft rate, while East Anglia and the North-East are relatively safe. Government, health, education, professional services and not-for-profit organisations had the most incidents. They are five times as likely to have thefts as telecoms providers and retailers, who had the fewest incidents. Theft was most likely to be the worst incident of the year in the government, health and education sectors.

Staff at a medium-sized Welsh manufacturer failed to follow the correct procedures; as a result, computer equipment was stolen. The individuals were disciplined and legal action taken. After the incident, additional security technical controls were put in place and staff received extra training.

Staff at small businesses carried out very few computer frauds; these were largely in the manufacturing, telecommunications and retail sectors. In contrast, over half of very large businesses had a staff computer fraud in the last year. Companies in Northern Ireland were three times as likely to report computer fraud by staff as the national average. When companies have a computer fraud, this tends to be their worst security incident of the year.

An increasing trend is computer fraud by outsiders, which accounts for three-quarters of the worst frauds. Many of these frauds were in the travel, leisure and entertainment sector.

Systems failure and data corruption

Accidental systems failure or data corruption is now the commonest incident affecting small businesses. A quarter had incidents in the last year. Almost every very large business had some incidents. In contrast, staff sabotage remains rare, even in very large businesses.

One very large company had a major incident when its power supply failed. Due to its effective contingency plan, the power was restored in a few hours. However, in the meantime, staff could not work and the company suffered adverse media coverage as a result.

Not-for-profit organisations and telecoms providers are most affected, twice as likely to have an incident as companies in the travel, leisure and entertainment sectors. The companies with the greatest number of incidents are in the financial services and technology sectors. Greater London and Scotland are hit hardest, while systems in the North-West appear relatively robust.

Hardware failure at a small manufacturer in the South East took out its systems for more than a month. It took more than 100 man-days of effort to fix the problem. The company did not have a contingency plan in place; after the incident, it changed its backup procedures.

Accidental systems failures are likelier to be the worst incident of the year in the property sector than in other sectors.

Software at a small property company malfunctioned, disrupting operations for more than a week. This exposed weaknesses in the fall-back workaround procedures, which were later amended.

SECURITY BREACHES

Impact of breaches

Only by understanding the impact of security breaches on the business can UK companies effectively assess risks and prioritise actions.

The worst security incidents were more serious on average than two years ago. In 2006, 42% of the UK businesses that reported security incidents considered their worst incident to be serious; this has risen to 57%. A quarter had incidents they described as extremely or very serious. The telecommunications sector had the most extremely serious incidents.

However, since the number of companies affected by security incidents has dropped, the number of companies with serious incidents has stayed roughly the same as two years ago. It appears that the main reduction has been in the volume of minor incidents.

The impact of breaches can be measured in several ways. Relying on a single measurement, such as estimated cash cost, can be misleading. For many firms, the impact that an incident has on their reputation may be more important than financial loss. Other indirect costs such as investigation and remediation time also need to be considered. All of these aspects are tracked in this survey.

Business disruption

The biggest single impact of security breaches continues to be business disruption. Roughly half of the worst incidents reported caused disruption, slightly fewer than two years ago. However, there were more incidents causing very major disruption than in 2006.

A denial of service attack on a medium-sized financial services provider's online services had extremely serious consequences. The attack caused very major disruption for several days. There was a contingency plan for dealing with such attacks, but the plan proved ineffective in the event.

Companies in the South-West are most likely to suffer disruption from their security incidents. Welsh businesses had the least disruption from their incidents. In the manufacturing sector, business disruption tends to be particularly important.

Systems failure, infection by malicious software and attacks on websites are the incident types most likely to cause major disruption to services. Disruption from website attacks tends to be short-lived, while systems failure and malware can lead to longer interruptions in service.

A virus infection at a medium-sized property company in the South-East caused very major disruption for a week. It took more than 100 man-days of effort to eradicate the virus, despite an effective contingency plan. The company has since changed the configuration of its systems and deployed additional security technology to protect against future infections.

By using similar techniques to previous surveys, an estimate of the cost of disruption from companies' worst incidents has been calculated. This shows a slight increase in service disruption experienced by small businesses, to 1-2 days at an average cost of £8,000-£15,000. Large businesses also suffered slightly more disruption than in 2006, with average interruption of 1-2 days and an average cost of £80,000-£130,000.

A hacking attack at a medium-sized technology company took systems out of action for more than a week, and lost data had to be recreated or restored. It took several man-weeks of effort to recover from the incident and a number of customers complained. There was a contingency plan in place but unfortunately this proved ineffective, prolonging the pain.
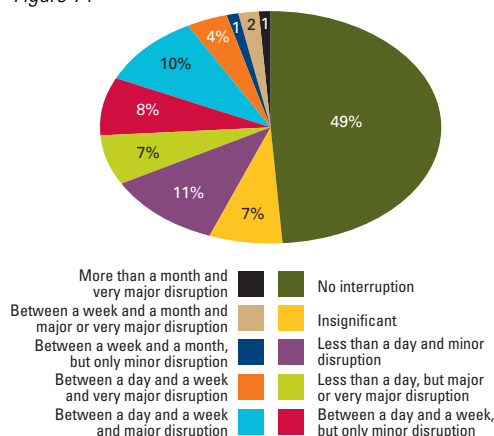
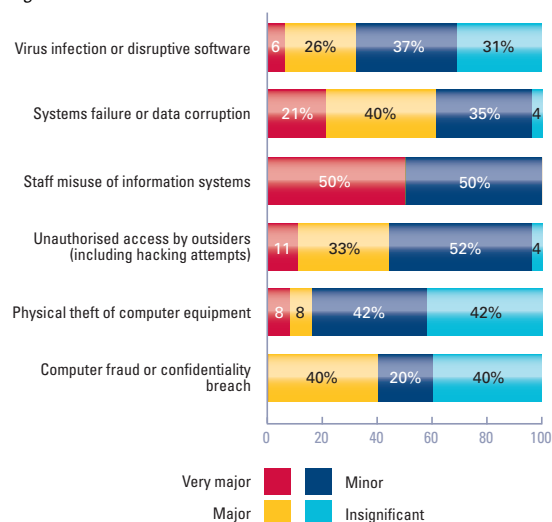**How many UK businesses had a serious incident?**

Figure 70
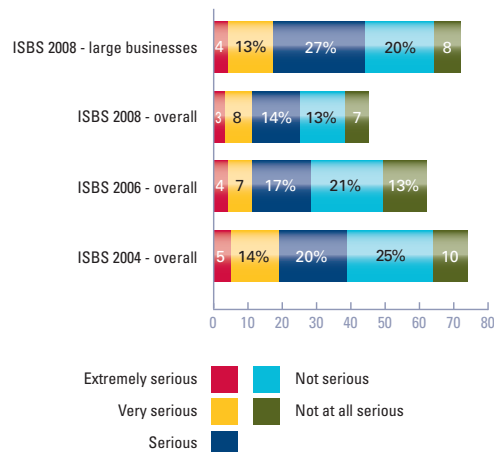
How much disruption to the business did the worst security incident cause?

Figure 71
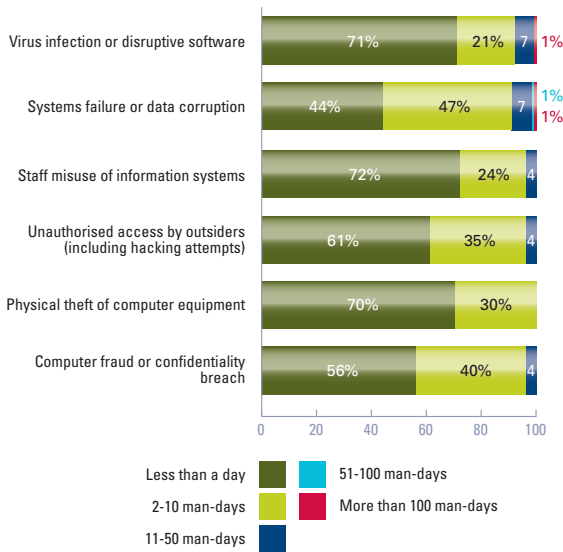

Which incidents were most disruptive to the business?
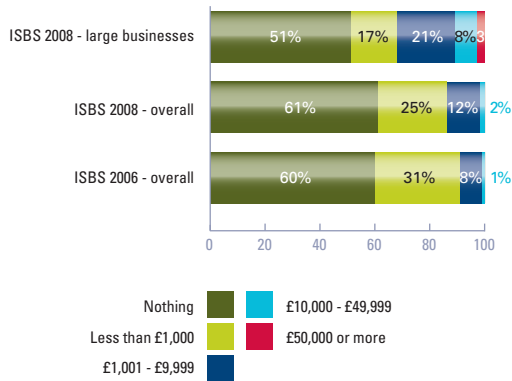
Figure 72

SECURITY BREACHES

How much staff time was spent responding to the worst security incident of the year?

Figure 73

	Less than a day	51-100 man-days
	2-10 man-days	More than 100 man-days
	11-50 man-days	

How much cash expenditure was required to recover from the worst security incident of the year?

Figure 74

	Nothing	£10,000 - £49,999
	Less than £1,000	£50,000 or more
	£1,001 - £9,999	

What was the direct financial loss associated with the worst security incident of the year?

Figure 75

	Nothing	£10,000 - £49,999
	Less than £1,000	£50,000 or more
	£1,001 - £9,999	

Incident response costs

Regardless of how much damage an incident causes, organisations still incur the indirect cost of staff time responding to it. For some incidents (such as staff misuse), this time is primarily the investigation of what went wrong and may include building up evidence to support disciplinary or legal proceedings. For others (such as accidental systems failure), more time tends to be spent restoring systems to operation and changing processes so that similar incidents do not recur.

As in the past, two-thirds of small businesses can investigate and correct their worst incident with under a man-day's effort, and 97% with fewer than 10 man-days. The position for large firms has deteriorated slightly since 2006; 14% of their worst incidents needed more than 10 man-days' effort. 15% of very large businesses had at least one incident that took more than 100 man-days to resolve. The costliest incidents reported were in the manufacturing, property and retail sectors.

Systems failure and infection by malicious software remain the incident types that require significant staff time investigating and fixing the problem; remedial action also sometimes involves cash costs. In contrast, physical theft of equipment tends to soak up only limited staff time, but usually requires cash expenditure to recover the situation.

In addition to the staff costs, two-fifths of firms spent cash to recover from their worst incident, a similar level to 2006. Large firms spent more than small businesses, with 11% having incidents that cost more than £10,000 in cash costs. However, as in the past, the very largest firms find it difficult to quantify the cash cost of recovery; 36% of them did not know how much cash had been spent.

Some staff at a large retailer based in the North-East were sending and receiving inappropriate emails, unrelated to their work. The subsequent investigation and remediation took several man-weeks and cost more than a quarter of a million pounds, partly because no contingency plan was in place. The incident forced a rethink of IT policies and a contingency plan is now in place.

On average, UK businesses spent between £1,000 and £2,000 cash costs recovering from their worst incident. The average large firm spent £4,000 to £8,000.

Direct financial loss

A security breach may also cause direct financial loss. As well as loss of assets, direct costs may include fines imposed by regulators or compensation payments to customers. Direct losses remain unusual; 88% of companies suffered no direct financial loss from their worst incident. Companies in the South-West are most likely to suffer direct financial loss from their security incidents; businesses in Northern Ireland are least likely.

A very large financial services provider had a very serious confidentiality breach that was covered in the media. The incident ended up costing more than half a million pounds in cash costs; it also led to extra training for staff and disciplinary action against the employee responsible.

The biggest direct costs come from staff misuse and confidentiality breaches. Most physical thefts involved losses of up to £10,000. Malware infection appears least likely to result in direct costs.

An employee at a medium-sized manufacturer based in East Anglia leaked confidential data. The losses incurred, together with the cost of the subsequent disciplinary and legal action, came to more than £100,000. The company subsequently revised its policies and invested in additional staff training to avoid any repeat.

SECURITY BREACHES

Damage to reputation

The two biggest drivers for security expenditure are protecting customer information and the company's reputation. Security breaches that become known outside the company are, therefore, management's greatest fear. Fortunately, these remain rare, with knowledge of 97% of the worst incidents contained within the organisation.

The incidents that appear most likely to cause customer complaints are infringing laws, website attacks and systems failures. In contrast, physical theft of computer equipment did not lead to a customer complaint, since customers were not aware of data being lost. This could change if UK legislators follow other countries and make the reporting of security breaches that expose customer data mandatory.

A large bank was replacing its data storage hardware. It sold off an old tape silo that it no longer needed. Unfortunately, this was still full of old tapes containing unencrypted customer data.

The bigger the organisation, the more likely its security breaches are to become reported in the media. One in six very large businesses had at least one security breach reported in this way.

A very large financial services provider had adverse media coverage after one of its laptops was stolen. Fortunately, because the laptop was encrypted, the impact on the company was minimised with the eventual cost only a few thousand pounds.

Interestingly, all of the small companies that had a confidentiality breach involving customer data had managed to contain knowledge of the breach within their organisation. This implies that, for every such incident that is reported in the press, many others go unreported. Given the number of data loss stories that have been in the news over the last year, this is of concern.

One very large government agency suffered from extensive adverse media coverage after it lost a large quantity of customer data. As well as the impact on its reputation, the investigation involved more than 100 man-days of effort and cost a considerable amount of money. After the incident, policies and procedures were changed and additional staff training provided. In addition, the configuration of systems was changed to prevent a repeat.

Sometimes, the best of intentions can lead to unforeseen and undesired consequences.

A conscientious member of staff at one large business started a system for recycling paper. Sadly, the risk of confidential documents being exposed on their way to recycling was not considered.

When incidents become known about externally, the damage to their reputation cost small businesses between £1,500 and £6,000, and large businesses between £30,000 and £250,000. Because very few incidents were known about externally, the overall average cost for small businesses has fallen to between £50 and £200. Large firms incurred costs on average of £2,000 to £15,000.

Total cost of incidents

The average total cost of a UK company's worst incident is between £10,000 and £20,000, up slightly on 2006. The cost increases with size of company; for large businesses, it is between £90,000 and £170,000, and for very large businesses, between £1 million and £2 million.

Extrapolation of cost data across the whole business community should always be treated with caution. However, the total cost of security incidents to UK plc appears to have dropped by roughly a third compared with two years ago, returning to the levels seen in 2004. An indicative estimate of the overall cost is in the order of several billion pounds a year.

**To what extent did the worst incident damage the reputation of the business?**

Figure 76
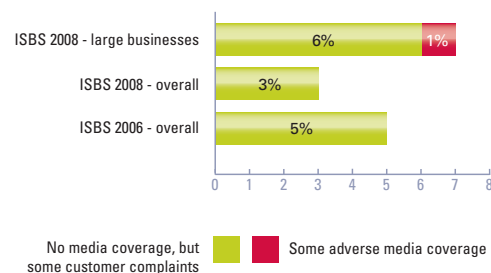
What was the overall cost of a company's worst incident in the last year?

Figure 77

	ISBS 2008 - overall	ISBS 2008 - large businesses
Business disruption	£8,000 - £15,000 *over 1-2 days*	£80,000 - £130,000 *over 1-2 days*
Time spent responding to incident	£600 - £1,200 *2-4 man-days*	£2,500 - £5,000 *6-13 man-days*
Direct cash spent responding to incident	£1,000 - £2,000	£4,000 - £8,000
Direct financial loss (e.g. loss of assets, fines etc.)	£500 - £1,000	£4,000 - £8,000
Damage to reputation	£50 - £200	£2,000 - £15,000
Total cost of worst incident on average	£10,000 - £20,000	£90,000 - £170,000
2006 comparative	*£8,000 - £17,000*	*£65,000 - £130,000*

What procedures do UK businesses have in place to respond to security incidents?
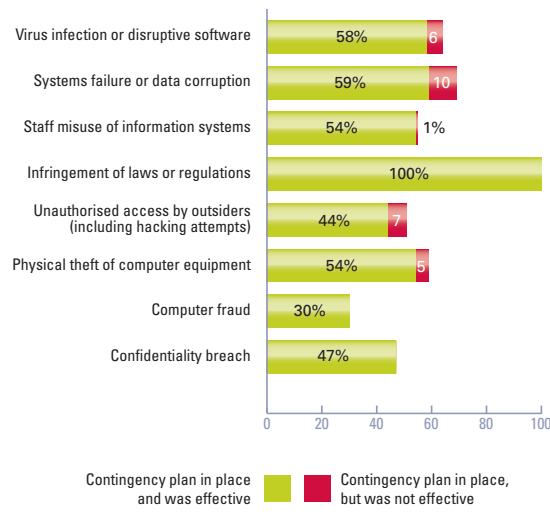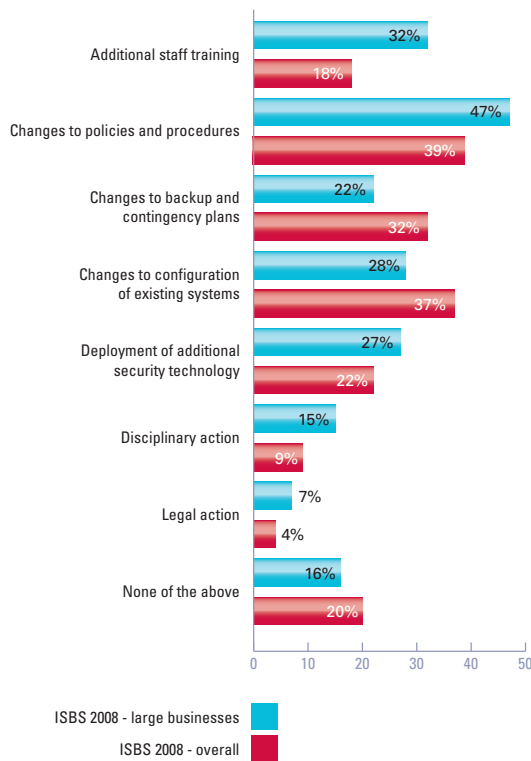
Figure 78
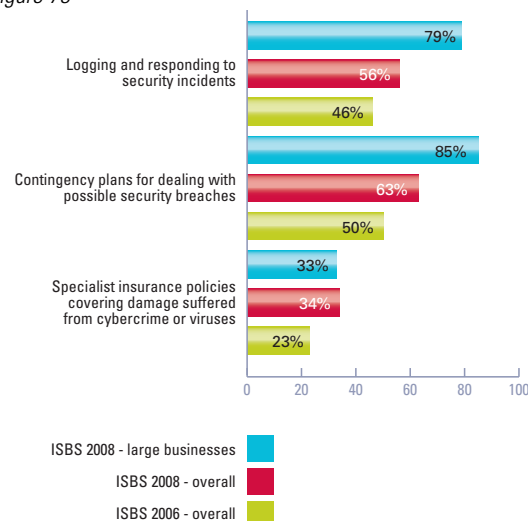
SECURITY BREACHES

What type of security incidents do businesses plan for, and how effective are those contingency plans?

Figure 79

Virus infection or disruptive software — 58% / 6
Systems failure or data corruption — 59% / 10
Staff misuse of information systems — 54% / 1%
Infringement of laws or regulations — 100%
Unauthorised access by outsiders (including hacking attempts) — 44% / 7
Physical theft of computer equipment — 54% / 5
Computer fraud — 30%
Confidentiality breach — 47%

Contingency plan in place and was effective | Contingency plan in place, but was not effective

How did UK businesses address the weakness that caused their worst incident?

Figure 80

Additional staff training — 32% / 18%
Changes to policies and procedures — 47% / 39%
Changes to backup and contingency plans — 22% / 32%
Changes to configuration of existing systems — 28% / 37%
Deployment of additional security technology — 27% / 22%
Disciplinary action — 15% / 9%
Legal action — 7% / 4%
None of the above — 16% / 20%

ISBS 2008 - large businesses
ISBS 2008 - overall

Incident response and contingency planning

More UK businesses have procedures to record and respond to security incidents, and contingency plans to address them, than two years ago. These exist in roughly three-fifths of small businesses and four-fifths of large ones. They are commonest in energy companies and least common in not-for-profit organisations. Companies that give a very high priority to security are twice as likely to record security incidents as those that give security a low or no priority. Companies in Greater London are particularly good at recording breaches, while those in Scotland are most likely to have contingency plans.

Senior management at a medium-sized telecommunications provider are IT-literate and have a pretty good understanding of security issues. However, they give a relatively low priority to security. For example, there is no formal security risk assessment. Instead, when an issue arises, management respond quickly to it.

Three-fifths of companies that had experienced a security breach during the year had a contingency plan in place to address it. Companies are most likely to have contingency plans in place to address systems failure, infection by malicious software and breaking the data protection law. In contrast, less than half of companies have contingency plans in place to deal with computer fraud and confidentiality breaches.

While contingency plans seem generally effective, plans to address systems failure, website attacks and malware infections appear the most likely to fail when put into practice.

The amount of action taken following the worst incident varies by sector. Professional services companies are least likely to take action, whilst not-for-profit organisations are most likely. The nature of the action varies as well. Companies in the travel, leisure and entertainment sector are most likely to invest in additional staff training after incidents. Not-for-profit, government, health and education organisations tend to change their policies and procedures. Retailers are the most likely to take disciplinary action, while energy companies are the most likely to take legal action.

The nature of the incident also strongly influences the follow-up actions. Additional staff training happens most after incidents involving staff misuse or breaches of laws or regulations. Changes to policies and procedures are commonest after staff misuse, computer fraud and confidentiality breaches. Backup and contingency plans typically change after accidental systems failures. Companies tend to change the configuration of their existing systems after website attacks, confidentiality breaches or malicious software infections. They are most likely to deploy additional security technology after a malicious software infection, and most likely to take disciplinary action after staff misuse. Legal action tends to occur after physical theft, computer fraud and confidentiality breaches.

Nearly a third of businesses claim to have some form of specialist insurance covering damage from cybercrime or viruses, though this falls to under one in ten very large businesses. Specialist insurance is found most often in the travel, leisure and entertainment sector, and least often among not-for-profit organisations. Four-fifths of companies in the North-East have cyber-insurance policies. Companies who have a poor understanding of security are very unlikely to have this insurance.

A large number of respondents were unable to say whether the company had specialist insurance policies. This suggests that, especially in large organisations, the security function and the staff responsible for insurance may not be fully aligned. Some large companies are also self-insuring these risks.

INDEPENDENT REVIEWERS

Eskenzi PR are a creative and strategic PR Consultancy that specialises in the hi-tech sector. Our objective is to be the best niche PR consultancy in IT/Comms with an unrivalled reputation with journalists and clients. For more information, see www.eskenzipr.com.

The European Information Society Group (EURIM) brings together politicians, officials and industry to help improve the quality of policy formation, consultation, scrutiny, implementation and monitoring in support of the creation of a globally competitive, socially inclusive and democratically accountable information society. For more information, see www.eurim.org.uk.

GetSafeOnline.org is a joint initiative between HM Government, the Serious Organised Crime Agency (SOCA) and leading businesses, which aims to help individuals and small businesses protect themselves against internet security risks. For more information, see www.getsafeonline.org.

The mission of the **Institute of Information Security Professionals (IISP)** is to be the authoritative body of information security professionals. For more information, see www.instisp.org.
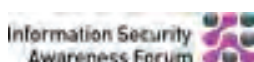
The **Information Security Awareness Forum** is an umbrella organisation incorporating the BCS, the CMA, Eurim, GetSafeOnline, ISC2, The Jericho Forum, SASIG and 10 other organisations. The aim of the forum is not to create new information security awareness material, but to coordinate the efforts of its member organisations in order to reduce overlap and identify gaps for member organisations to fill. For more information, see www.theisaf.org.

The **Information Security Forum (ISF)** is the world's leading independent authority on information security; its members include 50% of Fortune 100 companies. For more information, see www.securityforum.org.

With active participation from individuals and chapters all over the world, the **Information System Security Association (ISSA)** is the largest international, not-for-profit association for information security professionals. It provides educational forums, information resources, and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members. For more information, see www.issa.org.

Infosecurity Europe is Europe's number one dedicated Information Security event with the most comprehensive range of products & services from every segment of the global security industry together with an unrivalled education programme. For more information, see www.infosec.co.uk.

The **International Information Systems Security Certification Consortium,** Inc. is the internationally recognised *Gold Standard* for certifying information security professionals. Founded in 1989, (ISC)2 has certified over 58,000 information security professionals in 135 countries. For more information, see www.isc2.org.

The **Jericho Forum** is an international IT security thought-leadership group dedicated to defining ways to deliver effective IT security solutions that will match the increasing business demands for secure IT operations in our open, Internet-driven, globally networked world. For more information, see www.jerichoforum.org.

The **Mid Yorkshire Chamber of Commerce and Industry (MYCCI)** is committed to helping the region's businesses mitigate the risks posed by an information security threat. For more information, see www.mycci.co.uk.

The **National Computing Centre** is the single largest UK corporate membership body in the IT sector. NCC champions the effective deployment of IT to maximise the competitiveness of its members' business, and serves the corporate, vendor and government communities. For more information, see www.ncc.co.uk.

Royal Holloway is a multi-faculty College of the University of London. Its Information Security Group is recognised worldwide and in 1998 was awarded a Queen's Anniversary Prize. For more information, see www.isg.rhul.ac.uk.

The **UK ISO/IEC 27001 User Group** is the UK Chapter of the International ISMS User Group. It exists to promote awareness of and share good practice in relation to ISO/IEC 27001 and information security management systems. For more information, see http://www.iso27001usergroup.co.uk.