PRICEWATERHOUSECOOPERS

dti

information **security** breaches survey 2006

technical report

in association with:

Microsoft

CLEARSWIFT
Simplifying content security

Entrust
Securing Digital Identities & Information

symantec.

Facial recognition technology is a biometric technique which measures for a match between facial models.

Facial recognition devices build up a model of the scanned person's face which is then matched with a database of known images.

2D devices commonly use a technique known as "eigenfaces" whereby the face is sliced into hundreds of distinct layers which are then matched with the models in the database.

3D devices work with 3D face models and are known to be much faster and more accurate than 2D devices. These are typically neural network based, enabling them to learn and cope better with the issues of ageing, glasses, facial hair and poor lighting conditions that can often reduce the accuracy of 2D devices.

DTI recommends

- Draw on the **right expertise** and **international standards** to understand the security threats you face and your legal responsibilities.
- Integrate security into **normal business practice,** through a clear security policy and staff education.
- Use **risk assessment** to target your **investment** in security controls at the areas of maximum business benefit.
- Make sure your key **security defences** are **up to date** and **integrated**, and address **emerging technologies** you are exposed to (such as spyware, instant messaging, Voice over IP, etc.).
- Develop **contingency plans** so that you can respond to any security incidents efficiently and **minimise business disruption**.

For more information, please see
www.dti.gov.uk/industries/information_security
and
www.getsafeonline.org

Preface

ISBS 2006

Alun Michael MP
Minister of State for
Industry and the Regions

Since 1991, the Department of Trade and Industry has sponsored research into information security breaches to help UK businesses better understand the risks they face. The Information Security Breaches Survey 2006 (ISBS 2006), is the eighth such survey, and has been managed by PricewaterhouseCoopers.

The survey results show that the UK continues to embrace the Internet, with the vast majority of even small businesses enjoying the benefits of broadband connections. Unfortunately, the last decade has shown that this new business environment is accompanied by new security threats. It is encouraging that the steep rise in the number of businesses affected by security incidents seen over the last few surveys appears to be levelling off. Underpinning this has been the step change in investment by UK companies in their security defences over the last two years.

This is certainly not a time for complacency. While the number of companies affected has dropped slightly since two years ago, it is still twice the level seen a decade ago. In addition, the total cost of security incidents is up on two years ago, with small businesses particularly hard hit.

Access to security expertise continues to pose an issue for the UK business community so the launch earlier this year of the UK Institute of Information Security Professionals is very welcome. The big increase seen in the use of external guidance and specialists to supplement in-house capability is also encouraging. Promotion of international security standards and raising awareness of effective information security management techniques will continue to be priorities for my Department in the future.

Introduction

Chris Potter
Information Security
Assurance Partner
PricewaterhouseCoopers LLP

In some senses, security awareness in the UK business community has never been better. For example, 98% of companies have anti-virus software in place, and three-quarters of businesses believe that security is a high priority to their senior management or board.

However, the gap between the companies that are focused on information security and those that are not is widening. Roughly half of all UK businesses have security policies, carry out risk assessment and spend at benchmark levels on information security. The other half, while they may have anti-virus protection, typically lack basic security disciplines and may be over-confident about the effectiveness of their security controls.

Large businesses continue to be more security-conscious, having been hit by more security incidents in the past. Their focus on security seems to be paying off, with the total cost of their incidents dropping significantly over the last two years. The opportunity is there for small businesses to learn from the experience of those on the front line; failure to do so is likely to result in the overall cost of security to continue its upward rise.

Nowhere is this more important than in the area of emerging technology. Spyware, instant messaging, identity theft, Voice over IP telephony, and even MP3 players pose new security threats for UK businesses. Evaluating the risks, educating staff about them and implementing appropriate technical controls are all vital for success in tomorrow's security landscape.

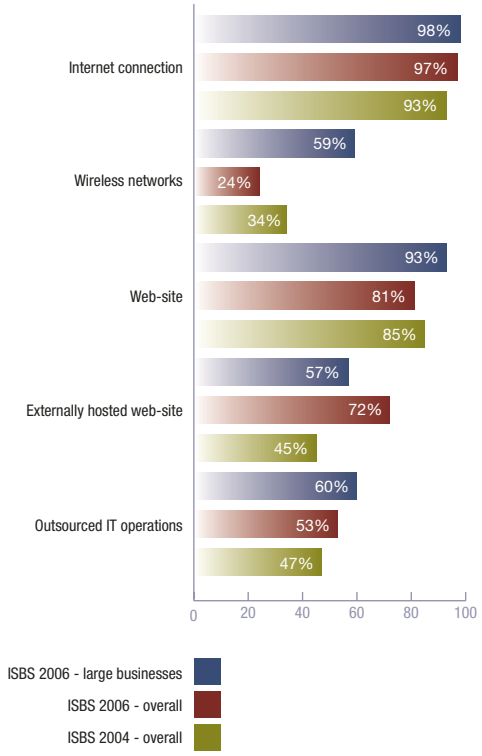
Andrew Beard
Information Security
Advisory Director
PricewaterhouseCoopers LLP

We thank all the sponsors and independent reviewers that worked on this survey with us. Together, these organisations represent an unparalleled source of knowledge and experience in the information security field. Their variety of perspectives has helped us keep the survey focused on the areas of greatest relevance to UK businesses today, and the analysis of the results as balanced and objective as possible.

Headline News

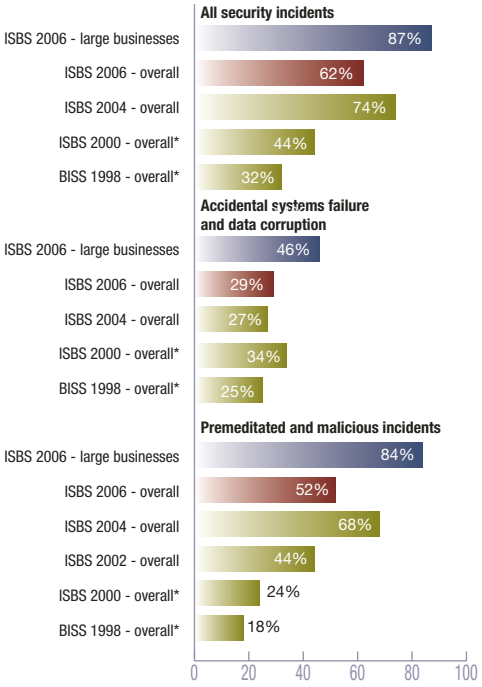
How has the business environment changed over the last two years?

Figure 1



What proportion of UK businesses had a security incident in the last year?

Figure 2



*The 2000 and 1998 DTI survey figures were based on the preceding two years rather than the last year. In addition, they included operator user errors as a security incident; these have been stripped out of the totals to present on a like for like basis. ISBS 2002 did not cover accidental systems failure.

IT systems in general, and the Internet in particular, are increasingly important to business operations. Given this, the priority attached to information security remains high:

- Nearly every UK business makes use of the Internet; 97% have an Internet connection and 88% of these are broadband.
- 81% of companies have a web-site, with 89% of these being externally hosted.
- Dependence on IT continues to grow – only one in six small companies could operate their business without IT.
- Over half of all businesses outsource some of their IT operations. Offshoring is growing, particularly in larger companies.
- Three-quarters of UK businesses rate security as a high or very high priority to their senior management or board of directors. The priority is consistent across all sizes of company.
- The main drivers for information security expenditure remain confidentiality, integrity and availability; nine-tenths of businesses rate these as important. Enabling business opportunities and improving efficiency tend to be less significant, with only two-thirds considering these as important.

The priority given to security has translated into action. Security controls have improved and confidence in those controls is high:

- The number of companies with a formal security policy has never been higher. Nearly three times as many have a security policy as did six years ago.
- Almost every UK business makes use of external guidance or expertise to supplement its in-house security capability.
- The average UK company now spends 4-5% of its IT budget on information security.
- Almost every organisation backs up its critical data and three-quarters store these backups offsite.
- 98% of businesses have anti-virus software, 80% update anti-virus signatures within a day and 88% install critical operating system patches within a week.
- 86% of companies filter incoming e-mail for unsolicited messages (spam).
- Three-quarters of UK businesses are confident or very confident that they have identified all significant security breaches in the last year.

The improved controls appear to be having an effect. After big rises since the mid-1990s, the number of companies affected by security incidents appears to have stabilised. The cost, however, remains considerable:

- 62% of UK companies had a security incident in the last year, down from 74% two years ago.
- The median number of incidents suffered is roughly eight a year. This has increased significantly compared with two years ago.
- The average cost of a UK company's worst security incident of the year was roughly £12,000 (up from £10,000 two years ago).
- Large businesses are more likely to have security incidents (87%), tend to have more of them (median of 19 per year) and their breaches tend to be more expensive (£90,000 on average for the worst incident). However, all three of these statistics are down on two years ago.
- Overall, the cost of security breaches to UK plc is up by roughly 50% since two years ago, and is of the order of ten billion pounds per annum.

Many UK businesses are a long way from having a security-aware culture. Their expenditure on security is either low or not targeted at the important risks:

- Roughly two-fifths of businesses spend less than 1% of their IT budget on information security.
- Only 44% of companies have carried out any security risk assessment in the last year. This is a small increase on six years ago. Those that assess the risks tend to spend more on security, suggesting the others are under-investing.
- There is still a shortage of security qualified staff; only one in eight companies has any.
- Three-fifths of UK businesses are still without an overall security policy, though a third of these have defined an acceptable usage policy for the Internet.
- Recruitment processes at a quarter of companies do not include any background checks; 19% of companies that believe security is a very high priority fail to check the background of their staff.
- One in eight organisations does nothing to educate their staff about their security responsibilities.
- The penetration of BS 7799 into UK businesses remains disappointing, with only one in ten aware of its contents.
- Only a quarter of UK companies have tested their disaster recovery plans in the last year.

New technologies pose a particular security threat for the future:

- A quarter of UK businesses are not protected against spyware.
- UK companies are poorly placed to deal with identity theft; only 1% have a comprehensive approach for identity management (authentication, access control and user provisioning). 84% say there is no business requirement to improve this.
- Three-fifths of companies that allow remote access do not encrypt their transmissions; businesses that allow remote access are more likely to have their networks penetrated.
- Three-fifths of companies do not block staff access to inappropriate web-sites and only one in six scans outgoing e-mail for inappropriate content.
- 30% of transactional web-sites do not encrypt the transactions that pass over the Internet.
- One in five wireless networks is completely unprotected, while a further one in five is not encrypted. Two-fifths of companies that allow staff to connect via public wireless hotspots do not encrypt the transmissions.
- 55% of firms have taken no steps to protect themselves against the threat posed by removable media devices (e.g. USB tokens).
- Two-fifths of companies that allow instant messaging have no controls in place over its use.
- Only half of the companies that have implemented Voice over IP telephony evaluated the security risks before doing so.

Despite high levels of confidence about today's security, UK companies are more concerned about tomorrow than ever:

- Nearly two-thirds expect there will be more security incidents in the next year than in the last.
- Three-fifths of companies believe it will be harder to detect security breaches in the future.

Headline News

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

Figure 3

	ISBS 2006 - overall	ISBS 2006 - large businesses
Business disruption	£6,000 - £12,000 *over 1-2 days*	£50,000 - £100,000 *over 1-2 days*
Time spent responding to incident	£600 - £1,200 *2-4 man-days*	£1,750 - £3,500 *5-10 man-days*
Direct cash spent responding to incident	£1,000 - £2,000	£5,000 - £10,000
Direct financial loss (e.g. loss of assets, fines etc.)	£500 - £1,000	£3,500 - £5,000
Damage to reputation	£100 - £400	£5,000 - £10,000
Total cost of worst incident on average	£8,000 - £17,000	£65,000 - £130,000

How has the overall cost of security incidents to UK plc changed since 2004?

Figure 4

	Overall	Large businesses
Number of companies affected	↓ 20%	↓ 10%
Average (median) number of incidents suffered by affected companies	↑ 50%	↓ 30%
Average cost of each incident	↑ 20%	↓ 10%
Total cost of security incidents	↑ 50%	↓ 50%

Given the inherent issues with extrapolation, the overall trends should be treated as indicative. Accordingly, the percentages have been rounded to avoid spurious accuracy.

How much progress has been made against the five recommendations made two years ago?

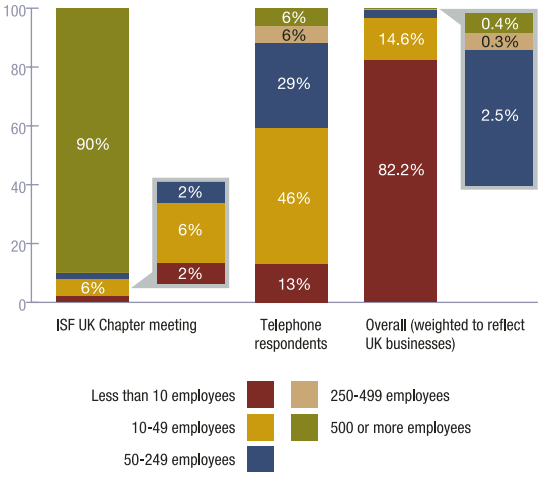
Figure 5

	Status	Trend since 2004
Draw on the right expertise		↑
Set clear policy and educate staff		↑
Invest in security		↑
Keep security defences up to date		↑
Respond to security incidents		↑

Methodology

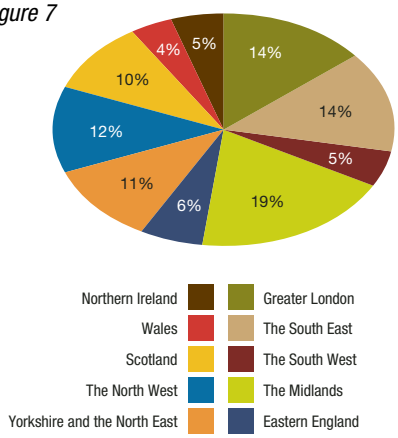
How many staff did each respondent employ in the UK?

Figure 6



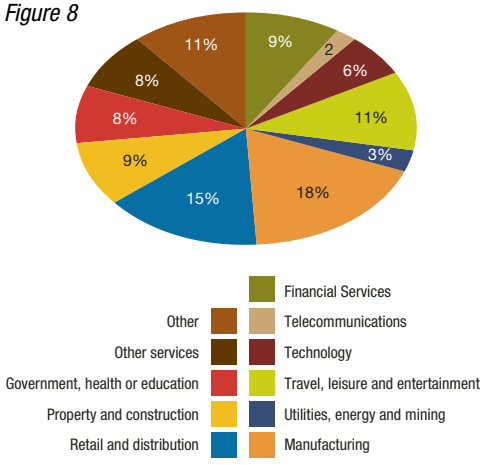
In what region were each respondent's main business operations located?

Figure 7



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

Figure 8



The core research for ISBS 2006 was a quantitative telephone survey using a structured questionnaire. We picked the sample randomly from a register of UK businesses. In each case, we contacted the person identified as responsible for information security. In total, we completed 1,001 computer-assisted telephone interviews, each lasting on average 30 minutes. The interviews took place between October 2005 and January 2006.

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 had 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.

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 example, we estimate that 98% +/- 1% of UK companies have anti-virus software.
- 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 no more than +/- 9%.

In addition to sampling error, question wording and practical difficulties in conducting surveys can introduce error or bias into the findings.

The response rate was similar to 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. Where appropriate, we have rebased the comparatives from the 2004 survey so they are on the same basis. 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). 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. In addition, we ran the survey interactively with the Mid-Yorkshire Chamber of Commerce. Finally, we issued an e-mail poll to Infosecurity Europe subscribers. These provided us with additional anecdotal data.

Attitudes to information security

Over the last two years, dependence on IT has continued to grow for companies of all sizes. The larger the business, the greater the reliance. Only one in twenty large respondents (and no very large ones) could operate their businesses without their IT systems. This rises to one in six small companies that could continue business without their IT.

The financial services, health and education sectors are most likely to hold highly confidential data. Travel, leisure and entertainment companies are least likely. Over the last two years, there has been a big rise in the proportion of manufacturing companies that hold sensitive data; nearly two-thirds now do this, compared with less than half in 2004. With the Inland Revenue encouraging online submissions of PAYE, this is perhaps unsurprising.

Data corruption and availability of IT systems were important across all sectors. Two-thirds of UK businesses would suffer significant business disruption if their critical data were corrupted.

Given this, the priority given to information security remains high across all sizes of company. Three-quarters of UK businesses rate security as a high or very high priority.

Companies that are heavily dependent on their IT are nearly twice as likely to assign a high priority to information security as those that are not. However, 5% of heavily dependent businesses do not see security as a priority.

Information security is most likely to be on the Board's agenda in financial services companies. 72% of them said it was a very high priority, whereas only 1% said it was a low priority. At the other end of the spectrum, retailers continue to be the least concerned. However, even here, only 15% felt that security was of low or no priority to their senior management.

There are some interesting variations by region. For example, the North West and Northern Ireland have a similar dependence on IT; however, companies in the North West were twice as likely to give a low priority to security as those in Northern Ireland. The South West and Scotland are the regions that depend most on IT, but both are average in the priority they give to security.

Confidence in security controls remains high across all sizes of company. There has been a big rise in the proportion of UK businesses that are very confident that they have caught all significant security breaches that occurred in their organisations in the last year.

Confidence levels are broadly similar among different sizes of organisation. However, one in six very large businesses were not very confident that they had picked up everything.

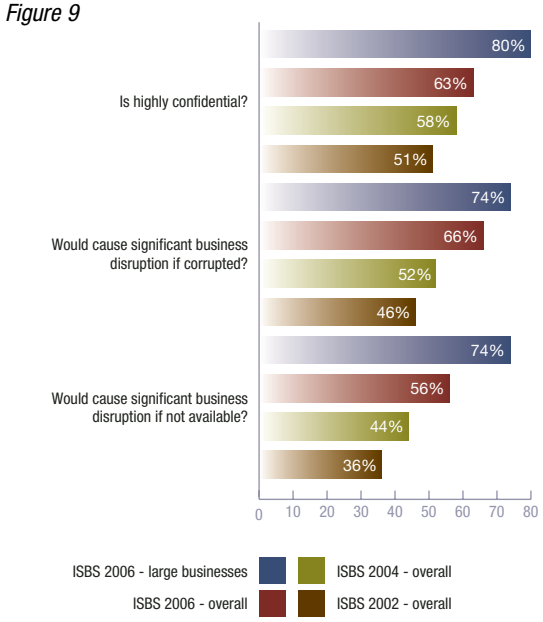
Confidence was highest in the technology sector, reflecting a relatively high priority given to technical security defences. In contrast, one in seven utilities and energy companies were not very confident; this sector was least likely to have data protection procedures in place, so this may have contributed to the concerns.

As always, it is important that confidence does not lead to complacency. There is a danger of undetected breaches, particularly with emerging threats such as spyware.

Security Strategy

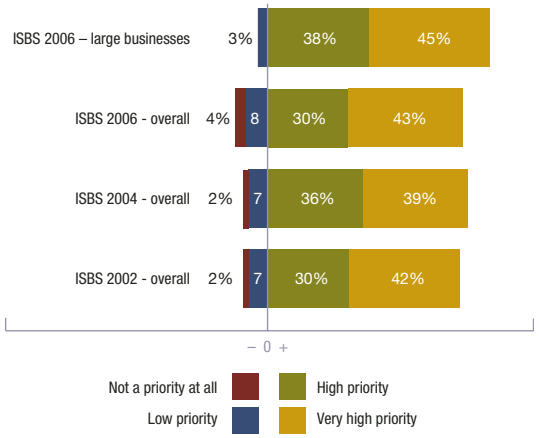
How many UK businesses have information that:

Figure 9



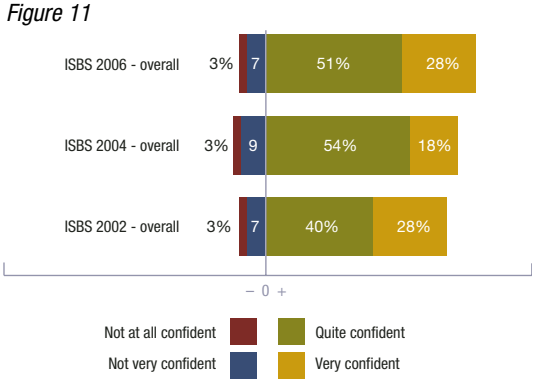
How high a priority is information security to top management or director groups?

Figure 10



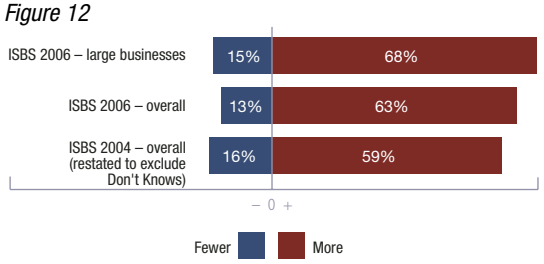
How confident are UK businesses that they have caught all significant breaches that occured in the last year?

Figure 11



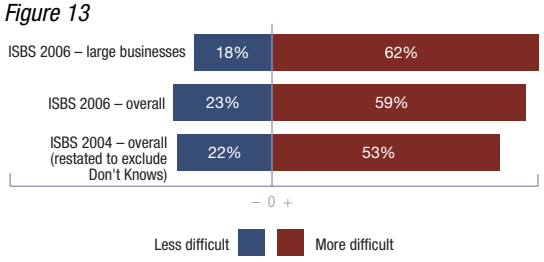
How many security incidents do UK businesses expect next year compared with last?

Figure 12



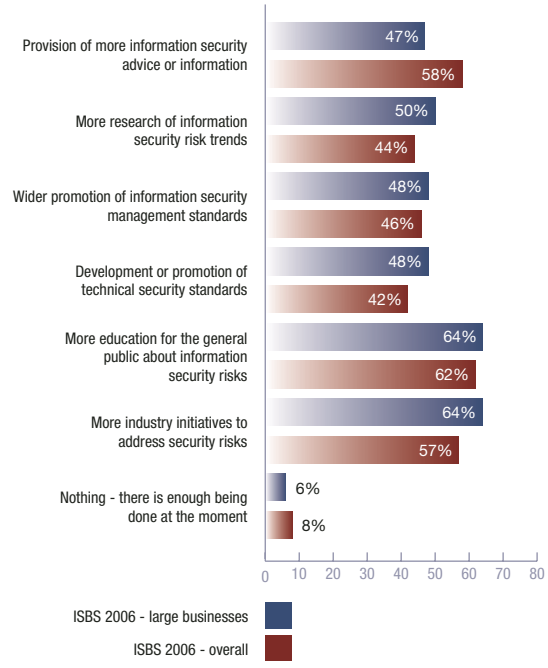
Will it be more or less difficult to catch security incidents next year?

Figure 13



What would most help UK businesses manage their risks in the future?

Figure 14



Future outlook

Despite the high levels of confidence about today, UK businesses are more concerned about tomorrow than ever. Levels of pessimism have increased for the third consecutive survey. Nearly two-thirds of companies think there will be more security incidents in the next year than in the last. This compares with only about a third who thought so four years ago.

Large businesses have historically been even more pessimistic. In 2004, over three-quarters thought there would be more incidents. 2006 shows a small glimmer of hope, in that large companies are slightly less pessimistic now than they were two years ago. There is now not much difference between different sizes of company.

There is some sector variation. Financial services companies are most pessimistic; three-quarters expect more incidents and only one in ten predicts fewer in future. The most optimistic are service companies, but, even there, twice as many predict more incidents as expect a decrease.

Businesses continue to be concerned about the nature of future incidents as well. Over half believe that they will be harder to catch in future. This is slightly worse than two years ago.

There is again not much variation by size of company. Very large businesses are the least pessimistic. Roughly half of them think it will be harder to catch security incidents, whereas nearly a quarter think it will become easier.

The most pessimistic sectors here are government, health and education; two-thirds of these think it will be more difficult to catch incidents. In contrast, nearly as many technology companies believe it will be easier to catch future incidents as think it will be harder. Interestingly, technology companies are also the most confident about their defences today. Looking across sectors, companies that were least confident about their current security controls tended to be the most pessimistic about the future.

Given the future outlook, UK businesses want more to be done to help them in this area. There appears to be a demand for a wide range of different activities.

Three-fifths of UK businesses believe that more public education about security risks would help them. A similar proportion would value more information security advice or information aimed at them. Since the start of the survey, the Get Safe Online campaign (www.getsafeonline.org) has launched. This provides individuals and small businesses with simple guidance on how to protect their IT activities.

Nearly half of all companies want wider promotion of information security management standards (such as BS 7799). Interestingly, the respondent's personal awareness of BS 7799 is not the determining factor here.

Over a half of all UK businesses would value more industry initiatives to address security risks. Demand was strong across all sectors for this, with utilities, energy and financial services companies particularly keen.

Security awareness

Basic security disciplines have spread within UK businesses over the last two years. Defining the security rules that staff must follow is the foundation of good security management. These rules, when written down, become the company's information security policy.

The number of companies with a formal security policy in place has never been higher. Nearly three times as many have a security policy as did six years ago. There is still, however, plenty of room for improvement. Three-fifths of UK businesses are still without such a policy. This seems surprising given the apparent priority given at board level to security.

Examining the data in more depth, there is a correlation between the priority that top management gives to information security and likelihood that the business has a security policy. 55% of companies that give a high or very high priority to security have a policy. In contrast, only 13% of those that treat security as low or no priority have one.

Larger companies remain more likely to have a security policy; roughly three-quarters now have one. This has steadily risen over the last few years. All of the very large respondents had a security policy.

Five out of six government, health and education respondents have a security policy. In contrast, only a quarter of retailers do. Companies in Greater London are one and a half times as likely to have a security policy as those in the North West.

A security policy in isolation is of limited use. It is important to link the policy to underlying technical standards and procedures. Risk assessment is an effective way of doing this. Assessing the threats and vulnerabilities that the business faces enables controls to be targeted to mitigate the exposure. Without a risk-based approach, a company can waste time and effort controlling the wrong things.

44% of UK businesses have carried out a security risk assessment in the last year. This is a small increase on the 37% reported in the survey six years ago. Large companies are more likely to assess risks. Two-thirds of them have done so in the last year. Roughly nine-tenths of the very large respondents had done so.

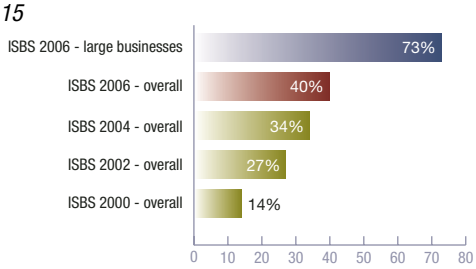
It is encouraging that the number of companies assessing security risks is rising. However, the practice is not yet fully embedded in the culture of UK businesses.

Organisations that have a security policy are more than twice as likely to have assessed their security risks in the last year as those without a policy. 57% of businesses that give a high or very high priority to security have assessed risks in the last year, compared with only 16% of those that treat security as low or no priority. Companies in Greater London are one and a half times as likely to have assessed their security risks as those in Eastern England and Scotland.

As in previous years, the vast majority of UK businesses take some steps to make their staff aware of their security responsibilities. Compared with two years ago, companies are doing more to educate their staff. Most large businesses include security responsibilities in their staff handbook and train new employees in security.

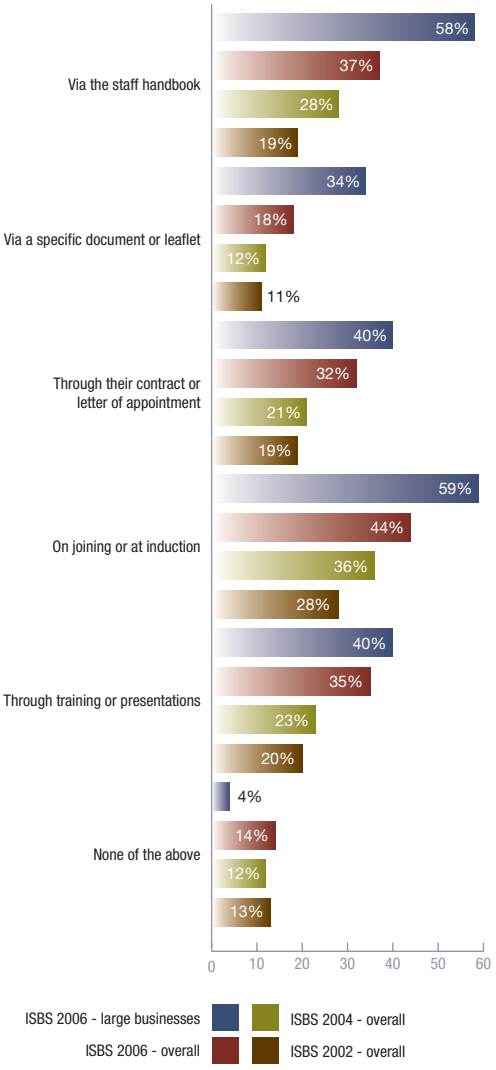
How many UK businesses have a formally documented and defined information security policy?

Figure 15



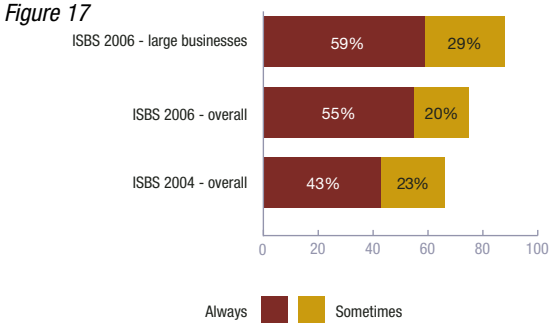
How do UK businesses make their staff aware of their obligations regarding security issues?

Figure 16



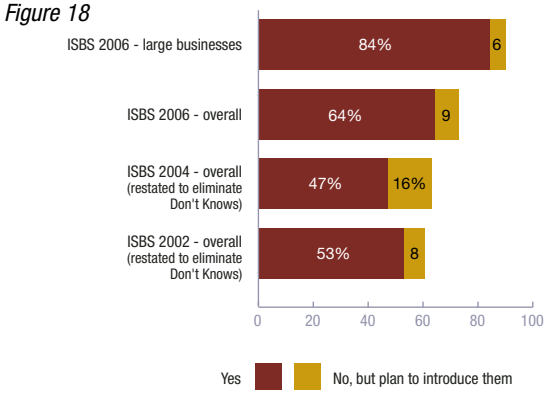
How often do UK businesses carry out background checks on staff and potential staff?

Figure 17



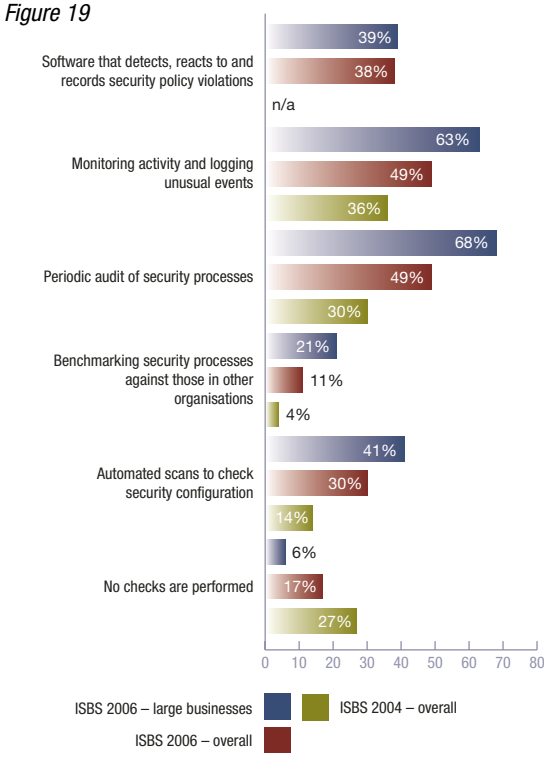
Do UK businesses have documented procedures to ensure compliance with the Data Protection Act?

Figure 18



How do UK businesses monitor compliance with their security policy?

Figure 19



Almost every company with a security policy takes steps to educate its employees about their security responsibilities. A third of those without a formal security policy refer to security in their staff handbook, and two-fifths include it in induction training; however, one in six does nothing to educate their staff.

The higher the priority that information security is to senior management, the more likely the company is to educate its staff. For example, only half of those for whom security is not a priority at all have taken any steps to raise awareness.

While education is important, it also helps if companies take steps to reduce the risk of employing dishonest staff. The number of UK companies ackground checks on staff has increased; three-quarters now do some form of checking, though the degree of checks can vary considerably. Large companies tend to be more rigorous, but struggle with consistency, in particular with checks on temporary staff and contractors.

There is some correlation between the priority given to security and background checking, but perhaps not as much as one might expect. 19% of companies that believe security is a very high priority do not carry out any background checks on their staff. Meanwhile, 42% of those for whom security is not a priority at all always carry out background checks.

Compliance with the Data Protection Act is seen as increasingly important by UK businesses. There has been a significant increase in the number of companies that have formal procedures in place to ensure compliance; two-thirds of UK businesses now do so. It appears that those who were planning to introduce procedures two years ago have done so.

There is a strong correlation between the priority given to security by senior management and whether Data Protection procedures are in place. Four-fifths of companies that give a very high priority to security have them, whereas only a third of companies where security is not a priority do so.

Businesses in the government, education and health sectors are most likely to have procedures to comply with the Data Protection Act; nine-tenths of them do this. In contrast, roughly half of all retailers and utilities companies do not have formal procedures for Data Protection compliance.

More companies are taking steps to monitor compliance with their security policy. Large companies are more likely to do this. However, many smaller companies appear to be changing their behaviour. The number using automated scans (such as penetration testing) has doubled over the last two years.

Interestingly, companies in the government sector are least likely to monitor compliance with their security policy. At the other end of the scale, telecoms providers do the most monitoring. Welsh businesses with a security policy are three times as likely not to monitor compliance with it as their equivalents in the South East of England.

One large bank had suffered incidents with staff misusing e-mail and web access in the past. The bank improved its processes for monitoring compliance with its acceptable usage policy and for following up breaches with disciplinary action. It has also carried out more ongoing education of its staff about the policy. As a result, the number of incidents in the last year has fallen.

BS 7799 adoption

The British Standards on information security (the 7799 standards) have existed for several years. The original BS 7799 comprised two parts: a code of practice (Part 1) and a specification for an information security management system (Part 2), the latter being the part against which an organisation could seek accredited certification. The standards are widely acknowledged as an important framework for security, both in the UK and overseas. BS 7799 Part 1 became ISO 17799 in 2000; BS 7799 Part 2 became ISO 27001 in 2005. ISO plans are to build on these to create a family of international standards on information security, all in the 27000 series. Overseas companies are increasingly using the ISO standards to structure their security processes.

Given this, the penetration of BS 7799 into UK businesses remains disappointing. Among people responsible for information security in their organisations, only one in ten is aware of the contents of the standard. This is not statistically different from the level of awareness four years ago.

Large businesses are more likely to be aware, but even here fewer than half the respondents were aware of the standard's contents. Awareness was greatest in the technology and government sectors, and lowest in retail, property and construction companies.

The survey separately asked respondents what would most help them manage their security risks in the future; roughly half of those that were not aware of the standard's contents wanted wider promotion of information security management standards. It seems that there is a wide potential audience for BS 7799, but that the pricing and distribution of the standard is acting as a barrier, in particular to small businesses. Roughly half of those that are aware of BS 7799 would also welcome wider promotion of the standard.

Adoption continues to rise among those who are aware of BS 7799. Over half have fully or partially implemented the standard within their organisation. Adoption is anything but static; 47% of adopters said they had moved to compliance with BS 7799 in the last year. Overall, technology companies were four times as likely to be compliant with BS 7799 as property and construction companies.

Implementing BS 7799 normally changes attitudes to security and procedures. 31% of small businesses implementing it experienced a significant change, and a further 34% changed somewhat. For larger businesses, it tends more to be minor tightening up of processes rather than wholesale change; 20% changed significantly and 53% changed somewhat.

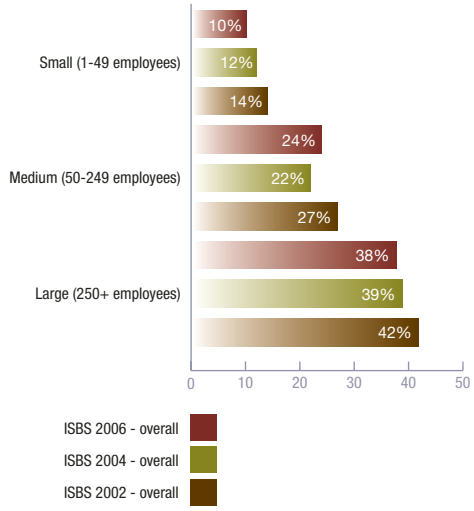
Nine-tenths of businesses that have implemented BS 7799 believe that they obtain benefits from it. The most common benefits are raising staff awareness and pushing security higher up the management agenda. Nearly a quarter of large businesses cited better business continuity as the biggest benefit. Formal accreditation and marketing was not normally the main benefit, except in very large companies. This may explain why formal accreditation rates remain very low in the UK compared with some other countries.

One medium-sized company commented that BS 7799 adoption had helped them become more commercially acceptable to the public sector. A financial services provider commented that, while parts of its business were BS 7799 accredited, other areas were finding the benefits came from adoption without formal accreditation.

Since ISO 27001 was launched, the number of accredited certificates issued has increased significantly. UK companies appear to value the international status of the standard. The greatest uptake has been in the telecoms, financial services and electronics sectors.

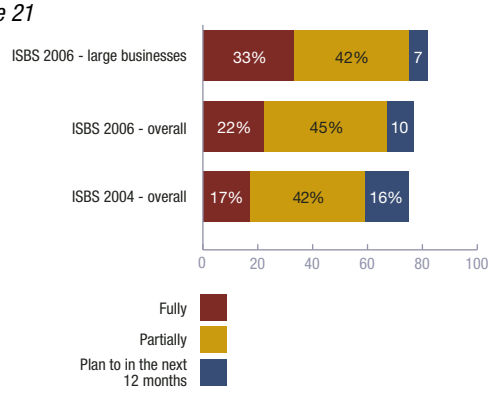
What proportion of UK businesses are aware of the contents of BS 7799?

Figure 20



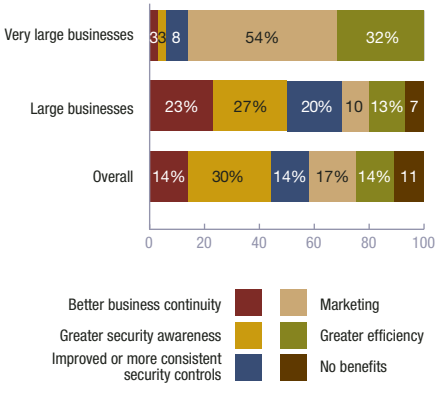
How many UK businesses that are aware of BS 7799 have implemented it?

Figure 21



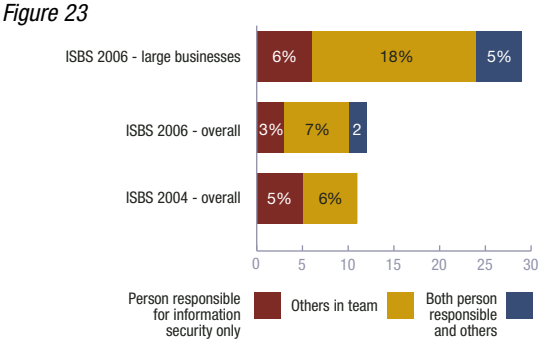
What was the biggest benefit from implementing BS 7799?

Figure 22



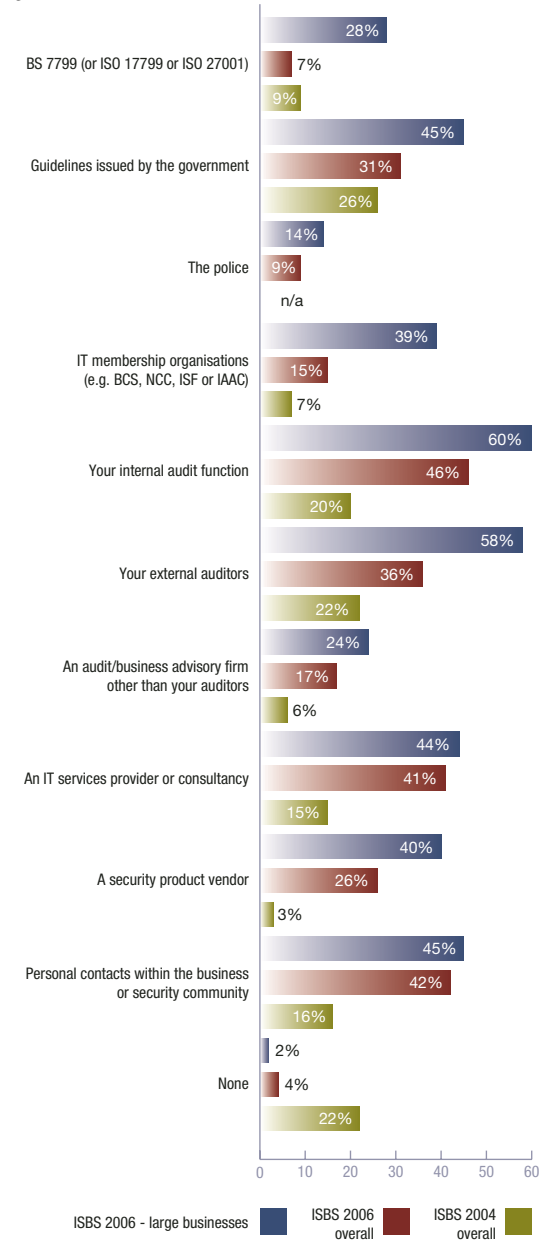
Does the team responsible for information security have any formal security qualifications?

Figure 23



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

Figure 24



Security skills and expertise

Security qualifications are becoming increasingly important in the information security community. The number of graduates obtaining MSc qualifications in information security has steadily increased over the last decade. Internationally, the CISSP qualification, which recognises technical security knowledge, has been supplemented by a new CISM qualification, focused on information security management. A new UK body, the Institute of Information Security Professionals, was launched in February 2006.

The number of qualified security professionals in the UK, while rising, remains low compared to the total number of businesses. Unsurprisingly, therefore, small businesses remain very unlikely to have anyone qualified in-house.

However, there is increasing penetration of security skills into large businesses, which can afford the specialist skills. For example, nine-tenths of very large respondents had someone in the organisation with a formal security qualification. Technology companies were most likely to have security qualified staff; retailers were least likely. There also seems to be some regional variation; companies in the South East were more than three times as likely to have security qualified staff as those in the North West.

Security qualified staff were much more likely to be aware of the contents of the British Standard for information security management (BS 7799) than others; 53% responded positively to this (versus 10% overall). Put another way, though, nearly half of all security qualified respondents were not aware of the standard's contents. This illustrates the range of skills and knowledge among information security professionals in the UK; businesses cannot simply rely on the qualification when hiring someone.

Security qualified staff were more likely to have carried out security risk assessments than others; 75% responded positively to this (versus 44% overall). Risk assessment is at the heart of most information security management approaches, so one might expect even more to do this.

A concern expressed in previous surveys was that the high levels of confidence shown by respondents might be due to lack of knowledge about the security risks. This year's survey shows that security qualified staff show similar levels of confidence as non-security qualified staff. They do, however, appear to have a sounder basis for that confidence.

Interestingly, the priority given to information security by senior management does not appear to have much correlation with whether the organisation has qualified staff. Roughly five-sixths of all companies that give a very high priority to information security do not have any security qualified staff.

Many small businesses cannot afford to hire full-time security professionals, and so lack the in-house knowledge to deal with today's security issues. It is encouraging, therefore, to see that almost every UK business makes use of external guidance or expertise to supplement their in-house capability. There has been a significant rise in the amount of external guidance that UK businesses have consulted compared with two years ago. Most businesses use a wide variety of sources of guidance, with auditors, IT vendors and personal contacts particularly popular. Sharing actual experience is often seen as more valuable than detailed technical standards and theoretical vulnerabilities.

Investment in security

Investment in security is a very strange insurance premium; the benefits (such as preventing incidents that would otherwise have occured) are often invisible and, however much is spent, there is no guarantee of safety. Spending the right amount on information security continues to challenge UK businesses. Over-expenditure reduces profitability, while under-investment can leave the business exposed. Two years ago, the survey results suggested that most UK businesses were spending too little on their security. This year's results indicate that most companies have taken this message on board.

Expenditure on information security continues to increase, especially among larger businesses. The rate of increase is slightly more than observed two years ago. Other surveys around the world have shown a similar pattern; the Internet has made security a worldwide issue.

The proportion of IT budget that UK companies spend on information security has risen significantly. The average UK company now spends 4-5% of its IT budget this way, and for 28% it consumes 6% or more of their IT budget. Large companies spend roughly 6-8%, with this dropping back towards 5% in very large companies. The average expenditure is now broadly in line with that in other countries.

While the average figures paint a rosy picture, a significant number of UK businesses are still not spending very much on information security. Roughly two-fifths of companies spend less than 1% of their IT budget on information security. It seems likely that some of these organisations are exposed to security threats.

As one might expect, there is a strong correlation between the amount that a business spends on information security and the priority its senior management places on it. Companies that give a very high priority to information security spend 7% of their IT budget on average. In contrast, 85% of those for whom it is not a priority spend less than 1% of their IT budget on it.

Interestingly also there is a correlation between carrying out a security risk assessment and spending on security. On average, those who carried out a risk assessment spent roughly 7% of their IT budget on security. The average expenditure for those that had not was only 4%. It seems likely, therefore, that those that have not assessed the risks are under-investing in their security.

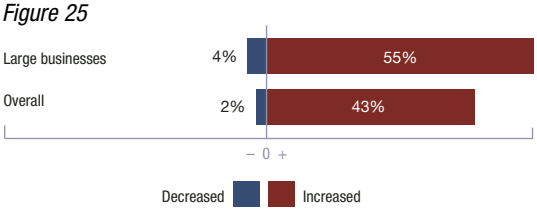
One financial services provider commented that, whilst there is strong support for security-related projects, demonstrating the direct business benefit of any security spend is more important than ever.

Organisations tend to spend more on information security if they have experienced incidents. 67% of those that spend 6% or more on their IT budget had at least one security incident in the last year, compared with only 42% of those that spend 1% or less on security. Put another way, those with incidents spend on average roughly 5% of their IT budget on security; those without spend a third less on average.

Businesses whose worst incident involved staff misuse are the most likely to spend on security, averaging 8% of their IT budget. In contrast, those whose worst incident was accidental systems failure do not spend any more on average than those that did not have any incidents at all.

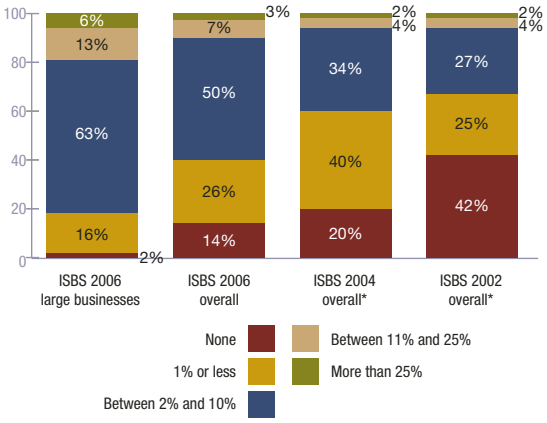
Has information security expenditure increased or decreased over the last year?

Figure 25



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

Figure 26



* 2004 and 2002 figures restated to eliminate don't knows, and so place on a consistent basis with other statistics quoted in the survey

Which sectors spend most on security?

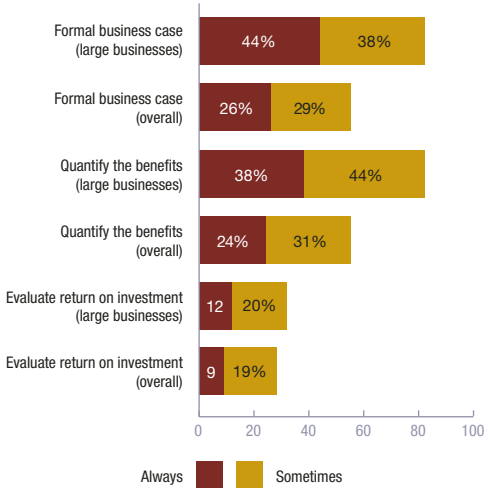
Figure 27

Average rate of increase (net number of companies reporting increase)	Average current security spend (as % of IT spend)		
	Below Average (Less than 4.5%)	Average (4.5% to 5.5%)	Above Average (More than 5.5%)
High (more than +50%)	-	Technology	Financial services, Other services
Average (between +35% and +50%)	Retail, Travel, Leisure and Entertainment	Telecommunications	Manufacturing
Low (less than +35%)	-	Property and Construction	Utilities, Energy and Mining

Security Strategy

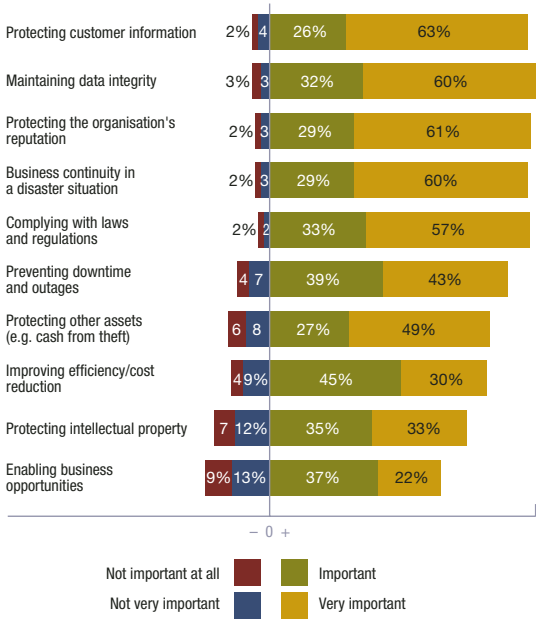
How do UK businesses decide what to spend on information security?

Figure 28



What drives information security expenditure?

Figure 29



Two years ago, most companies treated security expenditure as an overhead rather than an investment. This appeared to be one of the root causes of under-investment in security.

Return on investment (ROI) is one technique that business management use to decide whether to invest in an area of the business. However, formal ROI calculation for security expenditure remains rare. Less than a third of UK businesses ever apply ROI to their information security spend. There has been a slight increase over the last four years; in 2002, only 22% evaluated ROI on security expenditure sometimes or always. However, most businesses seem to continue to treat security as an overhead rather than an investment.

ROI adoption varies considerably by sector. Half of all technology companies evaluate ROI on security, versus only one in five property or construction companies. There is less variation by region; however, businesses in the South West appear most likely to use ROI and those in the North West least likely.

While formal ROI calculation remains rare, most UK businesses make formal business cases and attempt to quantify the benefits for their security expenditure. This is especially true in large companies. 98% of very large respondents prepare business cases for at least some of their security spend.

Companies where information security is a high priority to senior management tend to require more justification for information security expenditure than others. For example, only 23% of companies where security is not a priority have ever prepared a formal business case for any security expenditure. In addition, companies that carry out risk assessment are more likely to quantify the benefits from security expenditure than others. Companies that prepare formal business cases are likely to also quantify the benefits of that expenditure and vice versa; roughly three quarters of those that never prepare business cases also never quantify the benefits.

The main drivers for information security expenditure are to protect the organisation's information and reputation. Most UK businesses also think it is important to invest in information security to enable business opportunities and improve efficiency.

One large retail bank commented that their business expects strong security without being inconvenienced by it. As a result, the information security function needs to demonstrate business efficiency as well as higher levels of security.

The larger the company, the more important it seems to protect customer information and the organisation's reputation; nearly three quarters of large businesses rate these as very important. The more important protecting customer information is, the more likely the organisation is to have procedures for complying with the Data Protection Act. However, over half of the respondents for whom protecting customer information is important lack such procedures.

Different sectors tend to have different priorities. For telecoms providers, preventing downtime is the most important driver. Technology companies are most concerned about protecting intellectual property. Businesses in the financial services and government sectors are focused on protecting customer information, maintaining data integrity and regulatory compliance.

Outsourcing and offshoring

Outsourcing of IT activities is commonplace with over half of all UK companies now outsourcing some of their IT operations. Areas that are outsourced include application development and support, systems administration, web-site hosting and help-desk operation.

Government and service providers are most likely to outsource their IT operations. Technology companies are least likely, although even here two-fifths do.

Offshoring (to countries such as India and China) has become commonplace in very large companies; four-fifths of very large respondents have offshored some of their IT operations. Offshoring is now starting to emerge in smaller businesses too.

Service level agreements (SLAs) remain commonplace for outsourced IT operations. This is particularly true for large businesses. As in 2004, the vast majority of SLAs include security provisions, which is encouraging.

Surprisingly, BS 7799 compliant organisations are no more likely to have SLAs in place than the average. However, their SLAs almost always include appropriate security provisions. Both ISO 20000 on IT service management and ISO 17799 on security management provide good guidance in this area; balancing service objectives and security measures is critical to successful outsourcing.

Outsource providers overwhelmingly follow the customer's security policy. 91% follow the customer's security policy versus 7% that follow their own security policy instead.

A financial services provider has outsourced much of its IT. The company is careful to retain overall responsibility for security; a small in-house team is responsible for checking that the outsource providers meet their security policy.

Most companies that have offshored IT operations have taken steps to ensure the security of the operations. However, small businesses seem to place over-reliance on the contract; only a third have actually visited the offshore facilities.

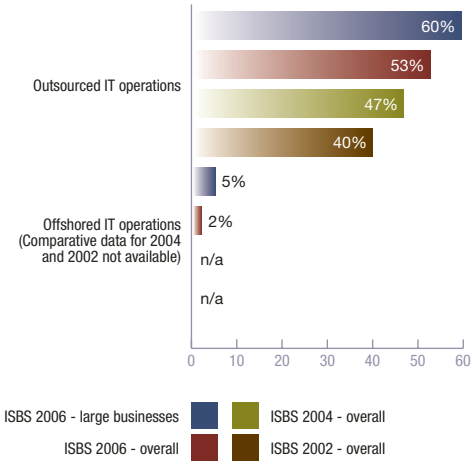
A large pharmaceutical company has offshored code development. To control this, they have established strong network restrictions limiting developers' access to specific servers. In addition, they plan to deploy terminal servers to grant greater access to offshore workers in a controlled fashion. This approach has built trust in the offshore workforce, helped transfer skills to them and ensured there is a strong security culture.

Increasingly, companies that have offshored significant processes are looking for a regular audit of the controls operated offshore. SAS 70 reviews (or equivalent independent audits) now take place in over a third of the major offshored activities. They are particularly common where the company offshoring is an SEC registrant (and so subject to section 404 of the Sarbanes-Oxley Act).

A financial services provider not directly affected by Sarbanes-Oxley commented that Sarbanes-Oxley and other regulation has made the company more aware of the need to have a strong risk management framework over all of its security activities (including those that are outsourced).

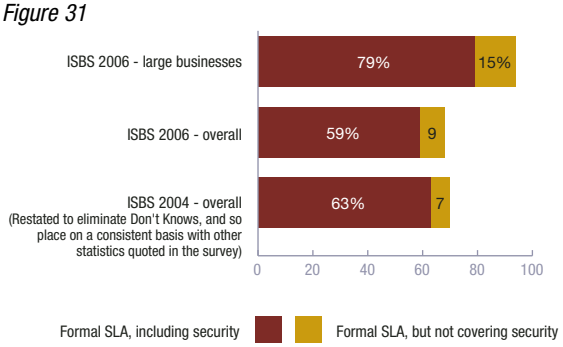
How many UK businesses have outsourced any of their IT operations?

Figure 30



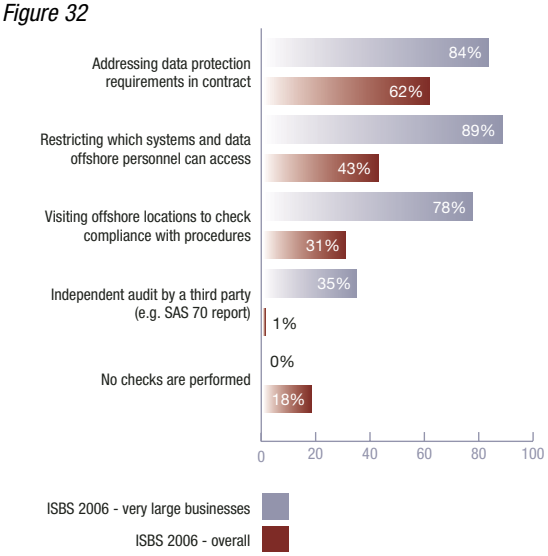
How many outsource arrangements have Service Level Agreements in place?

Figure 31



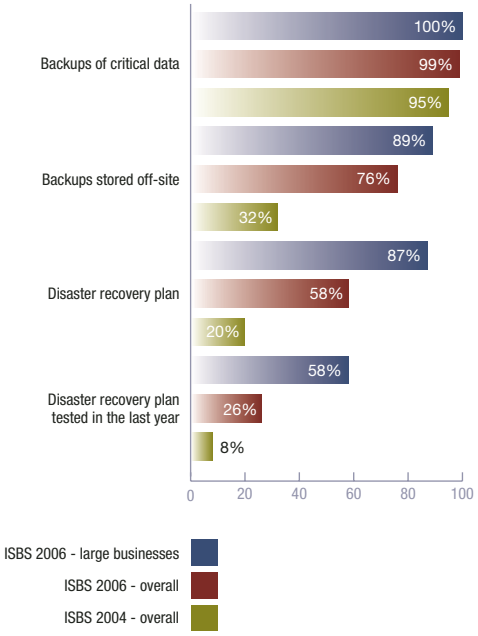
How do UK businesses that have offshored IT activities ensure thay are secure?

Figure 32



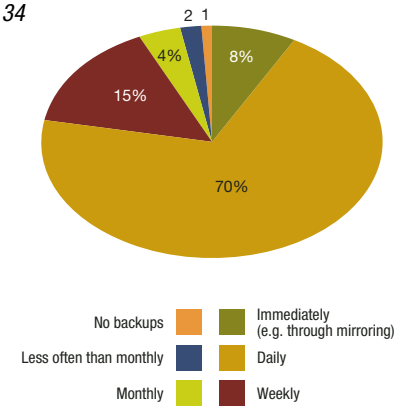
What precautions do UK businesses take against disasters?

Figure 33



How frequently do UK businesses back up their critical data?

Figure 34



Preparing for the worst

Over the last decade, natural disasters such as flooding and storms have been on the increase in the UK. Gloomy forecasts about climate change suggest that this trend is unlikely to reverse in the short term. In addition, since 9/11, there has been a heightened threat of terrorism, as illustrated by the bombings in London last July.

It is encouraging, therefore, that UK businesses appear better protected against disasters than two years ago. The number of companies storing backups off-site has doubled. There has been a threefold increase in the number of companies with disaster recovery plans.

However, the picture is not all rosy. A quarter of UK businesses do not store any backups off-site. Two-fifths do not have a disaster recovery plan in place. Of those that do, less than half of the plans have been tested in the last year.

A subsidiary of a food and drink group had a hardware fault that rendered their core business and finance (ERP) system unavailable for three days; this sharply highlighted the need for end-to-end disaster and business continuity testing. The company had regularly tested individual systems, but it was the links between individual subsystems that took most time to reinstate. The estimated recovery schedule had been far too optimistic.

Companies that are heavily dependent on the availability or integrity of their systems are more likely to have disaster recovery plans. However, this is not as pronounced as one might expect. Almost a third of companies that believe unavailability of information for a day will cause them significant business disruption do not have a disaster recovery plan in place. A similar pattern emerges for those where data corruption might cause them significant business disruption.

As one might expect, there is a significant correlation between backup discipline and disaster recovery planning. 72% of companies that store backups off-site also have a disaster recovery plan.

Most UK businesses back up their data daily. Among large businesses, this is more pronounced, with 97% backing up at least daily and the remainder at least weekly.

Frequency of backup is fairly consistent across industries. Telecoms providers are the most likely to use real-time mirroring of data. Travel and leisure companies are least likely to make daily backups, and are also markedly worse than other sectors at storing backups off-site. Financial services providers are most likely to have a disaster recovery plan, though they are only average at testing those plans. Property and construction companies are least likely to have a disaster recovery plan and are relatively poor at testing those plans.

There are some interesting regional variations. One in twenty Welsh businesses does not back up its critical data. Scottish companies are significantly worse than average at storing backups off-site. Organisations in London are most likely to have a disaster recovery plan (presumably due to the terrorist threat), one and a half times as likely as those in East Anglia for instance.

Encouragingly, businesses do not appear to wait for an incident before implementing backups. The frequency of backup is not significantly different between companies that have experienced accidental systems failure or data corruption in the last year and those that have not.

Physical security

48% of UK businesses (and 88% of large ones) keep their main computers in a dedicated computer room or data centre. Technology companies are most likely to do this and those in the property and construction sector are least likely to do so.

Access to most major computing facilities is restricted, for example through locks. Access to roughly half of them is also monitored, for example through logs or video surveillance. As one might expect, facilities with restricted access are more likely to be monitored, though 5% of facilities have unrestricted but monitored access. Nine-tenths of very large respondents have logging and monitoring over their data centre. Technology companies are nearly twice as likely to monitor access as utilities providers. Scottish businesses are least likely to monitor access.

Environmental and fire suppression controls, such as air conditioning and halon gas, are present in just under a half of these facilities. The larger the company the more likely these controls are to be in place. For example, 96% of very large respondents have such controls. Telecoms providers are most likely to protect the environment, as one might expect from their focus on availability. Companies in London are twice as likely to have environmental controls as those in East Anglia.

Almost all UK businesses (92% overall and 98% of large businesses) have some computers (e.g. desktop PCs and laptops) that are not within the main data centre or computer room.

Half of these rely solely on the physical security of their premises to protect these computers. Many of these have sophisticated security alarms, swipe cards, CCTV and 24 hour security. Others, though, rely principally on the locks on their windows and doors. Retailers are most likely to be in this position and financial services providers least likely.

Tagging equipment is the most popular additional security precaution, in place in a quarter of UK businesses. This involves marking equipment so that, if it is stolen and subsequently recovered, the police can identify its rightful owner. Tagging techniques in use include electronic tags, barcodes, ultraviolet ink and smart water. Large businesses are more likely to tag equipment than small ones. 52% of very large companies mark their PCs in this way. Roughly two-fifths of respondents in the government, health and education sectors also do this.

Physically securing PCs is the next most common precaution, particularly favoured in the utilities sector. Nearly one in six businesses overall does this. Common techniques include lock leads and cages (that secure PCs to desks) and secure physical storage of laptops overnight. Some larger businesses have implemented equipment alarms that go off if the equipment is disconnected.

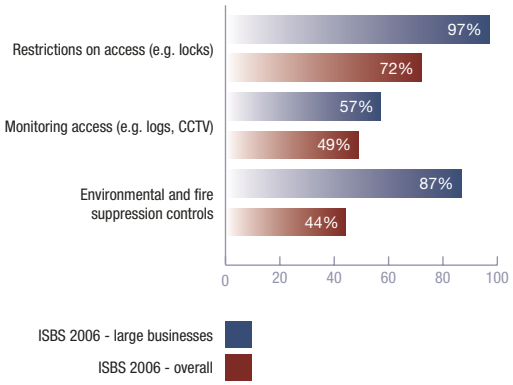
It is rarer to find the data on the hard discs protected, for example through encryption. This is surprising given the number of cases of laptops being mislaid. Encryption is particularly rare in East Anglia, where only 4% do this. Very large organisations are much more likely to encrypt laptop drives; 54% do so. Those that do not encrypt rely on educating their staff to reduce loss levels.

After a spate of laptop losses and thefts, a publishing company now charges laptop costs directly to the managers responsible for that area of the business.

Security Controls

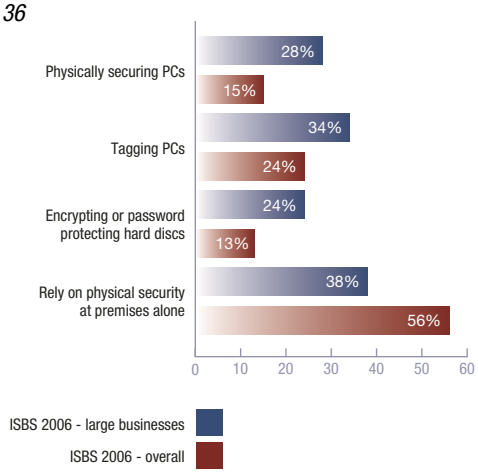
How do UK businesses with a data centre or computer room protect it?

Figure 35



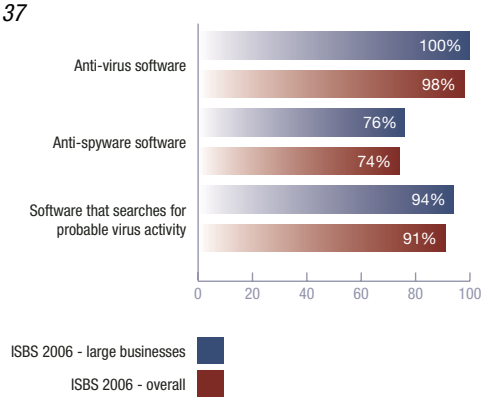
How do UK businesses protect their desktop PCs and laptops?

Figure 36



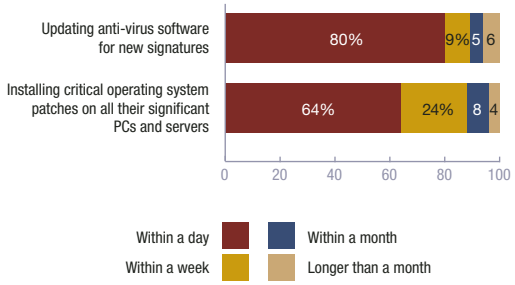
What precautions do UK businesses have in place to protect themselves against viruses and malicious software?

Figure 37



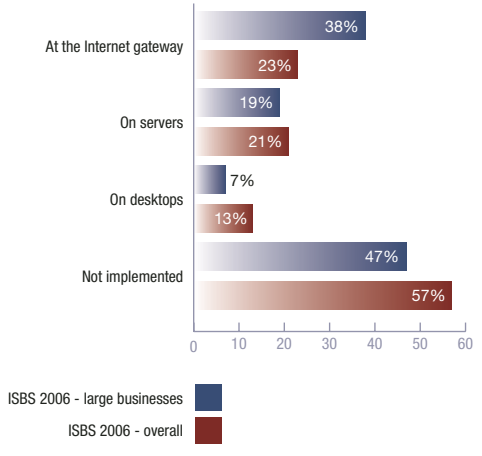
How quickly do UK businesses update their anti-virus defences?

Figure 38



Where have UK businesses implemented intrusion detection or prevention software?

Figure 39



Viruses and malicious software

UK businesses are only too aware of the threat that malicious code (viruses, worms and Trojans) poses to their operations. Almost every company irrespective of size installs anti-virus software on its computers.

Companies without anti-virus software did not report many infections. Organisations that suffer virus infection tend to install anti-virus software afterwards. In addition, the nature of the virus risk has changed. Virus outbreaks that blatantly disable their target's network are less common. Today's viruses are more subtle. Their stealth techniques mean that some businesses without anti-virus software may not realise that a virus has infected them. Worryingly, a quarter of UK businesses are not protected against the threat from spyware.

Most UK businesses now realise that installing anti-virus software is not enough. Four-fifths of companies update their anti-virus signature files at least daily, an improvement on two years ago.

Organisations that update their anti-virus software immediately seem slightly less likely to have infections than those that do not. One might expect a bigger difference. However, anti-virus software is becoming more sophisticated. Some packages don't just scan for viruses they know, but also try to spot probable virus activity (through so-called heuristic logic). Most UK businesses have this kind of software and so depend less on signature file updates.

Nearly nine in ten UK businesses now apply new operating system security updates within a week of their release. Large companies tend to be slower than smaller ones. Testing that new patches do not affect critical applications often takes time, as does manual patching across a large number of servers.

Patching discipline seems to pay off. Companies that install critical patches within a day of the patch being released report fewer virus infections than those that wait even a week. Even those patching within a day still suffered a significant number of infections, so patching alone is not enough. A multi-layer defence of patching, anti-virus software and intrusion detection software offers the best protection.

A large pharmaceutical company does not feel a single product provides full coverage, so uses multi-layered virus, spam and spyware filtering at the firewall, mail server and client level. Their security team views spyware as its biggest current challenge.

An increasing number of companies are implementing intrusion detection or prevention software. Nine in ten very large organisations do this. The Internet gateway remains the most popular place to install this software. Increasingly, personal firewalls installed on individual PCs now include some intrusion detection capability.

Interestingly, companies with intrusion detection or prevention reported more virus infections than those without. One possible explanation is that those without such software may not be detecting all the attacks. Another is that those with the greatest exposure (e.g. with broadband links to the Internet) tend to be the ones that implement this defence.

For further information, see the separate fact sheet on Viruses and malicious software.

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. Strong authentication is becoming more common, particularly in large companies, with hardware tokens and biometrics seeming to give greater security benefits than software tokens. Almost always, strong authentication is targeted at specific applications rather than being enterprise-wide.

Why are UK businesses so dependent on user IDs and passwords? Quite simply, most do not see a business need to move to stronger authentication. Those that do are put off by cost and usability issues. Companies that suffer unauthorised staff access are more likely to see the business need for stronger authentication.

One large retailer that is a subsidiary of an overseas group commented that the corporate headquarters takes the decisions on what to implement.

The average user has to remember three different user IDs and passwords to do his/her job. In 2% of businesses, the average user has to remember more than ten different IDs and passwords. Large businesses tend to be slightly worse than small ones; only one in four has single sign-on (up slightly since two years ago). The more IDs and passwords users have to remember, the more likely the business is to have had unauthorised access.

Three in five UK businesses have a formal process for user access administration (up slightly on 2004). Most large companies use electronic access requests (e.g. e-mail or workflow). Automated user provisioning (where the authorisation of a user request triggers the automatic set-up of the required access rights) is up threefold on 2004. Companies that use electronic requests without automated user provisioning are most likely to have experienced unauthorised access.

Levels of remote access remain similar to those seen two years ago. Roughly 36% of UK businesses allow some staff to access their systems from a remote location (e.g. from home or via wireless hotspots). Four-fifths of large businesses allow this. Interestingly, respondents who allow remote access are twice as likely to have had an unauthorised outsider try to break into their network as those who do not; they are also more likely to have experienced an actual penetration incident.

The overwhelming majority (94%) of companies allowing remote access restrict either the staff who can do this or the systems they can access remotely. Those that do not are twice as likely to have had an outsider actually penetrate their network.

More businesses use Virtual Private Network (VPN) technology to encrypt their data than two years ago. All the very large respondents have additional controls over remote access. 94% use VPN and 84% have two-factor authentication for remote users. Companies without any additional controls over remote access are more than three times as likely to have suffered penetration by an outsider as those with controls.

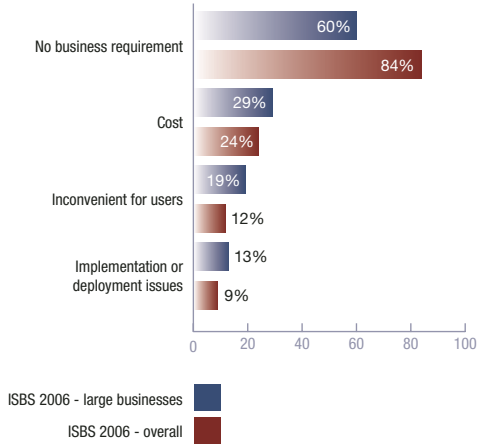
Among large companies, views on federated security models varied. There was, however, a strong consensus that technology alone will not solve identity and access management issues.

For further information, see the separate fact sheet on Identity and access management.

Security Controls

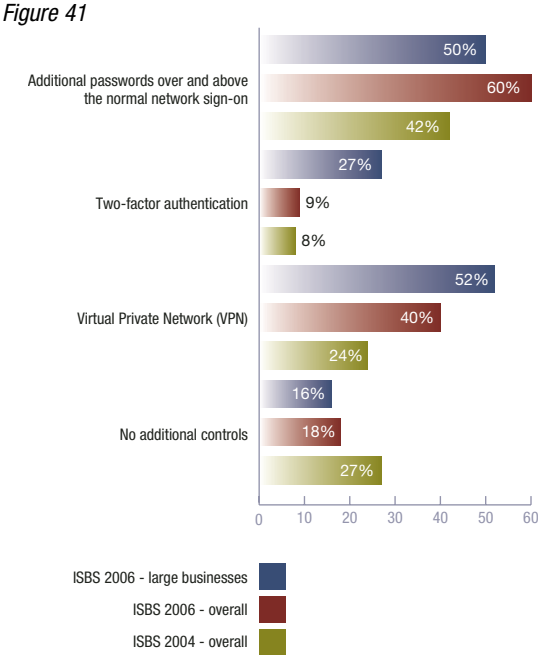
Why do UK businesses with weak authentication not implement stronger authentication?

Figure 40



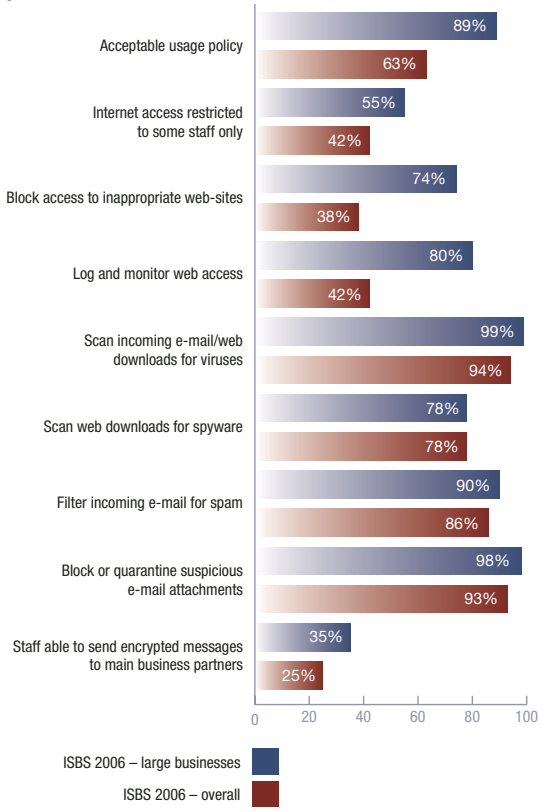
What additional security controls are deployed by UK businesses that allow remote access?

Figure 41



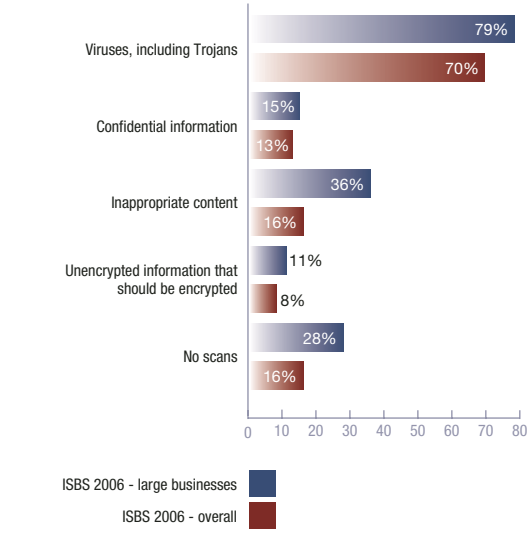
How do UK businesses with Internet access control their staff's usage?

Figure 42



What scans do UK businesses carry out on outgoing e-mail?

Figure 43



E-mail and web usage

97% of UK companies now have an Internet connection and 88% of these are broadband. With broadband, the Internet is only a click away. Increasingly, businesses recognise the temptation this poses to their staff. More companies have an acceptable usage policy for the Internet than have an overall information security policy. The dip in controls seen two years ago has reversed as late adopters have implemented better controls.

Companies with a policy are nearly three times as likely to have reported staff misuse as those without. Those without tend not to have a clear corporate view on what constitutes misuse, so do not pick up all incidents.

Three-quarters of companies with an acceptable usage policy require staff to acknowledge that they have read it before they can access the Internet. This has grown over the last four years, particularly in small companies.

Companies that have experienced staff misuse in the past are most likely to restrict Internet access. Companies that block access to certain web-sites also tend to log and monitor access, and vice versa. Companies that log and monitor web access report more incidents than those that do not; content security tools play a key role in detecting abuse.

One publishing company takes a pragmatic approach to web-site access. Because its staff may need to access a wide range of web-sites, it does not block at the proxy server. Instead, all access is logged and line managers monitor staff access.

Scanning incoming e-mail and web downloads has become common, especially in large companies. Four times as many UK businesses filter incoming e-mail for unsolicited messages ("spam") as did two years ago. Two-thirds of the businesses that do not scan incoming e-mail for viruses do filter for spam and block suspicious attachments.

Mass-mailing viruses have made UK companies recognise the danger of e-mailing a virus to their customers. As well as their reputation suffering, litigation could follow. Two thirds, therefore, scan outgoing e-mail for viruses. Generally, the companies scanning outgoing messages are a subset of those that scan incoming ones.

A company's reputation can also suffer if its staff (either deliberately or by mistake) send offensive correspondence to customers. This is especially true if the media report the story, as has happened in several recent cases. It is surprising that only one in six UK companies scans outgoing e-mail for inappropriate content.

Unsurprisingly, companies that scan outgoing e-mail for inappropriate content (such as profanity) are nearly three times as likely to detect incidents of staff misuse. The worry for the others is what is slipping through the net.

Protecting confidential information sent by e-mail as it passes across the Internet is still rare. In only a quarter of UK businesses can staff send encrypted e-mail to the company's main business partners. Only a third of these scans outgoing e-mail for unencrypted information that should be encrypted.

For further information, see the separate fact sheet on E-mail and web usage.

Network and web-site security

UK businesses have similar levels of web presence as two years ago; 81% (and 93% of large companies) have a web-site.

89% of these web-sites are externally hosted. Large businesses tend to host more internally, but even here 61% are externally hosted. Most people who host their web-site externally do not know what security controls their external service provider has over their web-site. Only 29% knew these. In large businesses, this is better, but still 55% are unaware.

Firewalls remain the main defence for web-sites; the web-sites without firewalls tended to be externally hosted.

Intrusion detection software is much more common than it was two years ago. A surprisingly high number of companies say they have intrusion prevention software. This may indicate some confusion between intrusion detection and prevention, especially in small businesses. Only 36% of very large companies (who tend to implement new technology first) say they have intrusion prevention software.

In contrast, the proportion of web-sites that automatically switch over to a backup site if the primary web-site fails is very similar to that observed four years ago.

The 2004 survey saw a large rise in the number of web-sites that would accept orders online (up to 73% overall). This year's survey clarified that, while most web-sites will accept orders (e.g. through e-mail or simple forms), relatively few web-sites take financial transactions online. Only 13% overall do this. The larger the business, the more likely its web-site is to accept financial transactions; one in five large businesses and two-thirds of very large businesses do this. The sites that do not take financial data online are either static information sites or use an online payment services provider to capture the financial data from their customers.

The number of transactional web-sites that encrypt transaction information using Secure Sockets Layer (SSL) has increased over the last four years, and most now do this. However, 30% overall (and 22% of large company web-sites) do not encrypt data transmissions, leaving private customer information exposed as it travels across the Internet. In contrast, every transactional web-site run by a very large respondent used encryption.

24% of UK businesses (and 59% of large ones) have now implemented wireless networks. These are similar levels of adoption as two years ago, in marked contrast to the massive increase seen in the two years before that.

There has been a big improvement in the adoption of security controls over wireless networks. The number of unprotected networks has more than halved. However, one in five wireless networks remains completely unprotected. In addition, another one in five is not encrypting its transmissions.

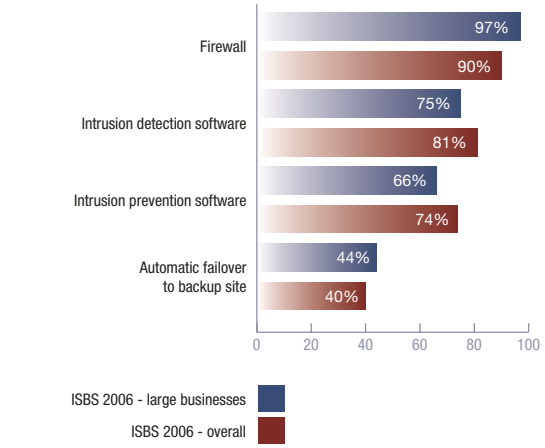
Very few businesses (only 12%) claim to allow their staff to access their systems via public wireless hotspots. Large businesses are twice as likely to allow this. Most businesses (59%) that allow access via public wireless hotspots encrypt those wireless transmissions (e.g. through VPN software). 86% of large businesses do this.

For further information, see the separate fact sheet on Trustworthy networking.

Security Controls

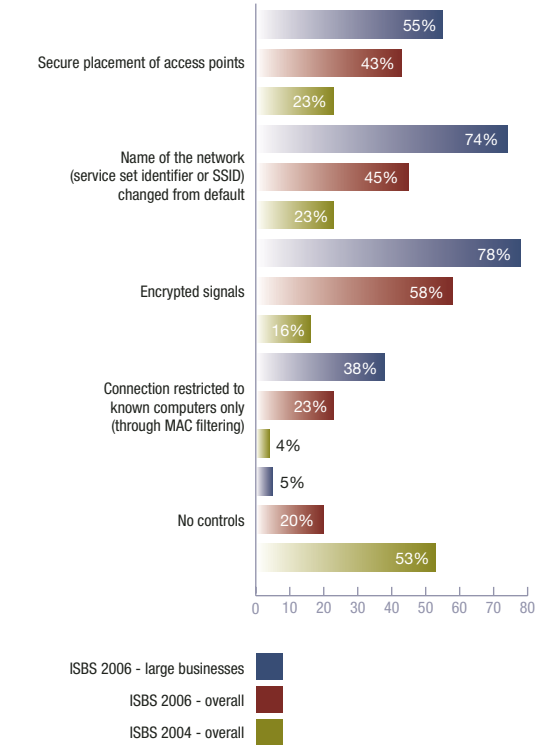
How do UK businesses protect their web-sites?

Figure 44



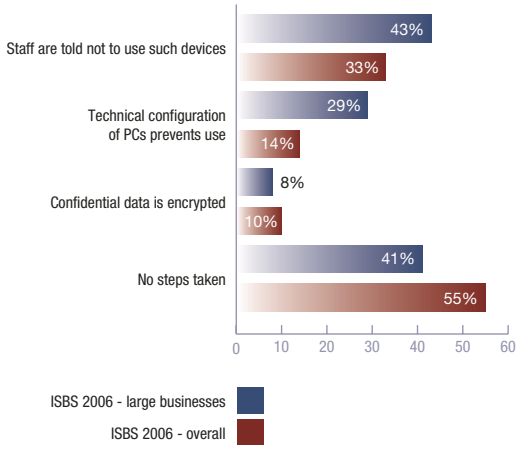
How do UK businesses protect their wireless networks?

Figure 45



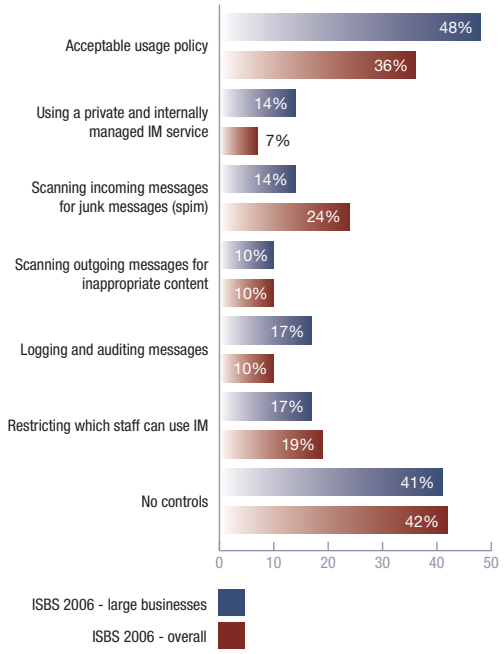
What precautions do UK businesses take over removable media devices?

Figure 46



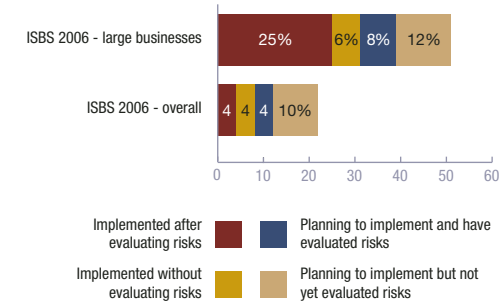
What precautions do UK businesses that allow instant messaging (IM) take over its use?

Figure 47



How many UK businesses are implementing Voice over IP telephony?

Figure 48



Emerging technologies

Removable media devices are becoming smaller, more common and more powerful. MP3 players, USB data keys, digital cameras and portable hard discs all pose a potential security threat, since staff could download confidential data onto them and then remove it from the organisation. However, over half of all UK businesses are taking no steps to protect themselves against this threat.

The most common step taken is to tell staff not to use such devices (e.g. through an IT usage policy) and then to rely on normal disciplinary procedures. Changing PC configuration to prevent use of USB devices and encrypting confidential data are both relatively rare.

Respondents in government, health and education are most likely to have controls; even here, two-fifths have taken no precautions. In contrast two-thirds of property and construction firms have not implemented controls. Scottish businesses are one and a half times as likely to lack controls as those in the South West of England.

One company whose business is to sell information takes the threat from portable storage devices very seriously. The steps it has taken include ensuring all information resides on servers wherever possible; downloads to the desktop occur only when absolutely required.

Just as e-mail provided a faster, less formal alternative to written letters, instant messaging (IM) offers an even quicker, less structured way to communicate. 42% of UK businesses now allow IM across the Internet (e.g. through AOL, MSN Messenger or Yahoo! Messenger). Fewer large companies (roughly one in four) do so.

Two-fifths of the companies that allow IM have no controls in place over its use. Very large businesses tend to have better controls; three-quarters use a private internally managed service and four-fifths have an acceptable usage policy.

Telecoms and technology businesses are most likely to use IM; roughly two-thirds do so. Technology companies are relatively well-controlled, with only one in five having no controls in place. In contrast, utilities companies are least likely to allow usage, but those that do tend to have poor controls. IM use is twice as common in Wales as in the North West of England.

Voice over IP (VoIP) technology is set to transform telephony over the next few years as voice and data traffic merge. 8% of UK businesses (and 31% of large ones) have implemented VoIP so far; the early adopters tend to be in the technology and telecoms sectors. A similar number plans to implement VoIP over the next year. Two-thirds of technology companies say they will use VoIP by 2007.

Roughly half the companies that have implemented VoIP evaluated the security risks associated with it before implementation. Two-thirds of those planning to implement VoIP have not yet evaluated the risks. Large companies are twice as likely to have evaluated the security risks as small businesses.

One financial services provider has adopted VoIP in some parts of the business. They try to assess the security implications before deploying new technology, but sometimes implementation deadlines make this difficult.

Incidence of security breaches

After the steady rise in security breaches seen over the last decade ISBS 2006 records a small drop in the number of UK businesses affected. Roughly three-fifths had a security incident in the last year. Of those firms that reported incidents, fewer reported serious breaches i.e. breaches that adversely impact on business.

Just as malicious breaches were responsible for the large rise in incidents in 2004, they now account for the reduction seen in 2006. The previous three ISBS surveys had all shown sharp increases in malicious incidents. The 2006 figures still remain higher than 2002 levels, so it is too early to assume the reduction represents a longer term downward trend.

Overall, accidental incidents remain at the same levels as 2004; there has, however, been a small increase among larger organisations.

Large businesses are most likely to suffer security incidents. In the last year, approximately nine-tenths of large organisations had at least one incident, and every very large respondent reported at least one security incident.

Why are large businesses more likely to suffer? 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.

Despite having a higher risk profile, large firms appear better equipped to repel attacks. Large companies are more likely to have intrusion detection and other monitoring techniques in place. This makes them more likely to identify security incidents. On average, large firms detect more network probes than small businesses, yet they suffer fewer penetrations by outsiders. Overall, one probe in a hundred resulted in a breach; for large firms, it was less than one in a thousand.

The actual number of reported incidents is up from 2004. On average, every UK company now suffers several security incidents a day (up from roughly one a month in 2004); large businesses report many incidents a day (up from roughly one a week in 2004). Small numbers of organisations, reporting hundreds of attacks on a daily basis are responsible for this increase.

More representative of the overall picture is the median number of incidents, i.e. the number of incidents experienced by the mid-point companies. These figures show an increase in the number of incidents suffered by firms overall, but a drop in the numbers for large businesses.

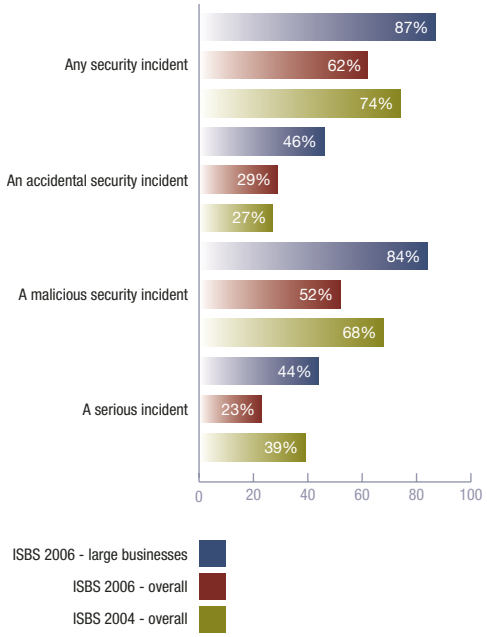
Telecoms companies are the most likely to have suffered a security breach; eight out of ten companies reported one or more incidents. In contrast, only half of travel and retail companies had breaches, making them the least affected sectors.

Curiously, Welsh companies are least likely to have suffered security breaches; only two-fifths had one. This is the most distinctive regional variation. At the other end of the spectrum, Northern Irish businesses are most likely to report breaches, with two-thirds affected.

Security Breaches

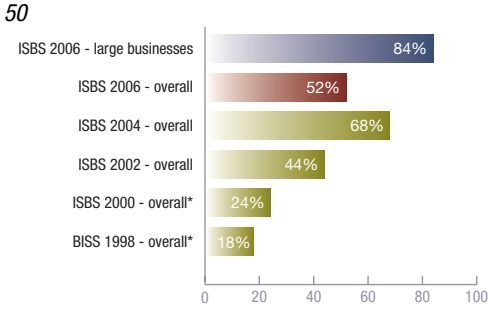
What proportion of UK businesses had a security incident last year?

Figure 49



What proportion of UK businesses had a malicious security incident last year?

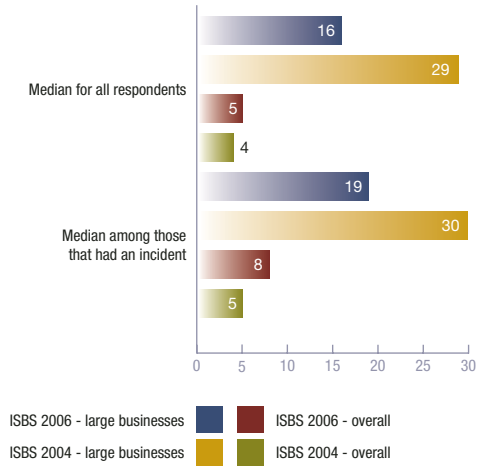
Figure 50



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

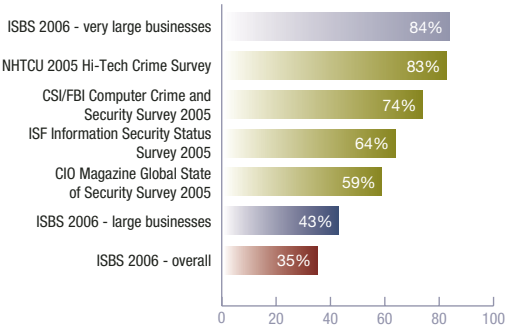
What is the median number of malicious incidents in the last year?

Figure 51



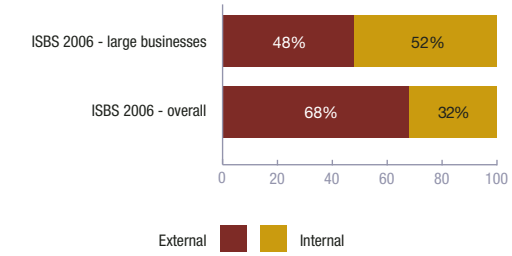
How do the levels of malicious code infections reported in ISBS 2006 compare with those in other similar surveys?

Figure 52



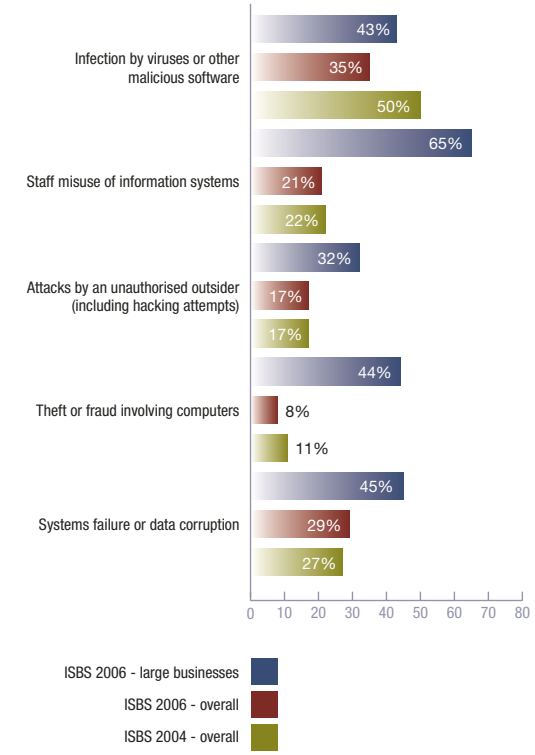
Was the cause of the worst incident internal or external?

Figure 53



What type of breaches did UK businesses suffer?

Figure 54



Comparison with other security surveys

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 National High Tech Crime Unit (NHTCU) 2005 Hi-Tech Crime Survey. National Opinion Polls (NOP), who carried out the survey, interviewed 200 respondents, representing a range of UK firms with 100 or more employees.
- The Information Security Forum (ISF) also conducted a survey in 2005; it comprised responses from its member firms, typically businesses with 500 or more staff. 18% were from the UK; the rest represented Europe, North America and South Africa. The survey is a benchmarking exercise against the ISF Standard of Good Practice (which is publicly available on the ISF web-site).
- The CIO Magazine Global State of Security Survey was an online survey, managed by PricewaterhouseCoopers, which gathered information from 8,200 companies in 60 countries. Two-thirds of the respondents had an annual turnover of over $100m.
- The CSI/FBI Computer Crime and Security survey is the longest running computer survey in the USA. In 2005, it received responses from 700 computer security practitioners working for US businesses and government. 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 2006 for large to very large businesses are broadly consistent with those shown in other surveys. This is illustrated by malicious code infections, where the percentage of respondents affected in the other four surveys all fall between the ISBS 2006 figures for large and very large respondents.

The other surveys all show either no change or a small drop in the number of respondents having security incidents. This is again broadly consistent with the trends observed in ISBS 2006.

Most of the other surveys show a steep rise in the average number of incidents each affected company suffers. This is consistent with the mean number of breaches in ISBS 2006, but, as seen earlier, the median shows a more complex picture, with most large UK companies having fewer incidents.

ISBS 2002 identified a major change from the conventional view that the majority of security breaches were internal. This picture has remained largely unchanged over the last four years. In 2006, roughly twice as many of the worst incidents reported by small businesses had an external, as opposed to internal, cause. For large companies, the split is more even i.e. roughly half internal and half external. This picture is generally consistent with the ratios reported in other surveys.

Looking forward, the boundary between internal and external is increasingly blurred; firms need to make sure they target their security expenditure at the areas of greatest risk, regardless of their origin.

Type of security incidents

Viruses continue to be the single largest cause of security breaches for UK businesses. However, there has been a significant drop in the number of affected firms. Less than half of large companies had infections; this contrasts with 68% in 2004. Despite this, the median number of infections has actually risen since 2004.

The number of firms reporting other types of malicious or accidental incidents has stayed at similar levels to 2004.

The number of companies reporting staff misuse of information systems has levelled off after the big rise seen in 2004. However, the average number of incidents reported by affected businesses continues to climb. Staff misuse is the largest cause of incidents for large businesses; large firms are three times more likely to report staff misuse than small ones.

Attacks by outsiders affected roughly the same number of UK businesses as in 2004. Large firms were nearly twice as likely to report attacks of this type. A third of large firms, and nearly all of the very large respondents, had suffered unauthorised access attempts by outsiders. However, the number of significant attacks reported by affected firms has dropped sharply; most organisations now consider port and network vulnerability scans as routine rather than significant.

Reported levels of incidents of theft or fraud involving computers have dropped slightly since 2004. Three-quarters of businesses affected by physical theft or computer fraud cited it as their worst security incident of the year. Large businesses are five times as likely to have had incidents of this type as small ones; criminals tend to target them more.

Firms reporting systems failure or data corruption are at similar levels to 2004 and previous surveys. This applies equally to businesses overall and large businesses. However, the impact of these incidents has changed; nearly twice as many firms now report this as the source of their worst incident.

Large businesses continue to be more likely to suffer all categories of security breaches than small ones. They are also more likely to have had repeated instances of incidents; the median number of incidents for large firms is more than twice that for small firms.

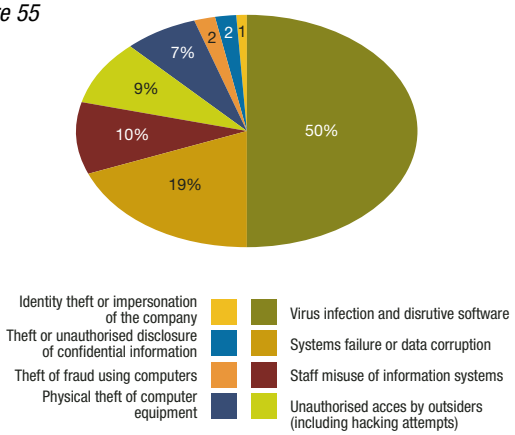
Interestingly, however, the gap has narrowed over the last two years; small businesses are reporting more incidents on average, while large ones are reporting fewer. Large companies have tended to invest more in security in the past; it could be that this investment is now paying off.

Very large businesses had the most incidents on average. Over half of them reported hundreds of attempts to break into their networks every day. The median number of staff misuse incidents in very large businesses equates to several breaches a day. Virus infections, phishing attacks and physical thefts also led to a significant number of incidents.

Security Breaches

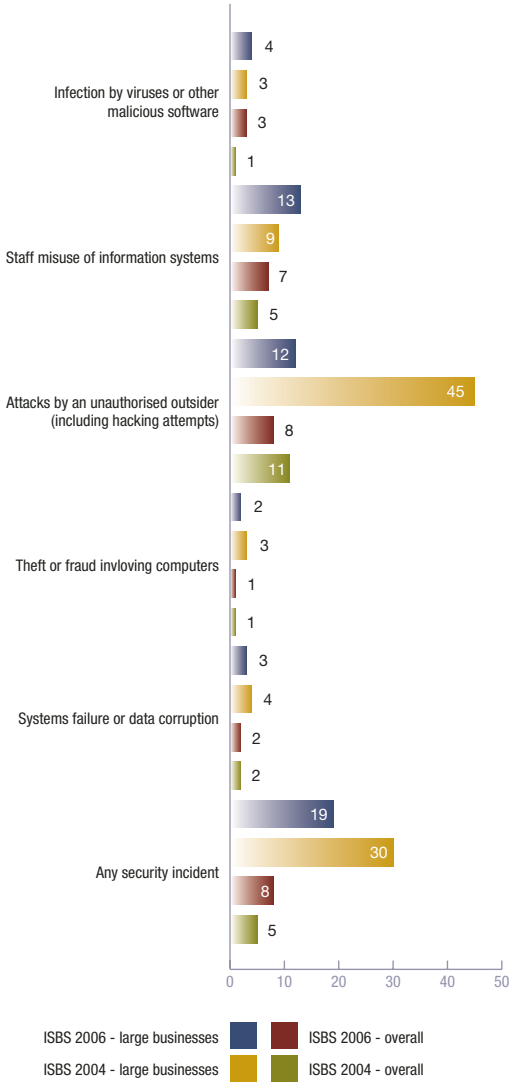
What was the worst security incident faced by UK businesses?

Figure 55



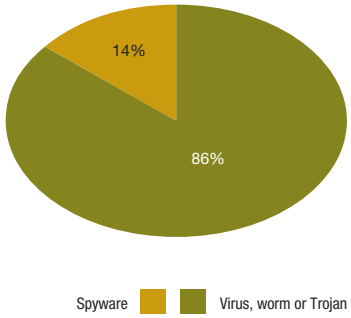
What was the median number of breaches suffered by affected UK businesses in the last year?

Figure 56



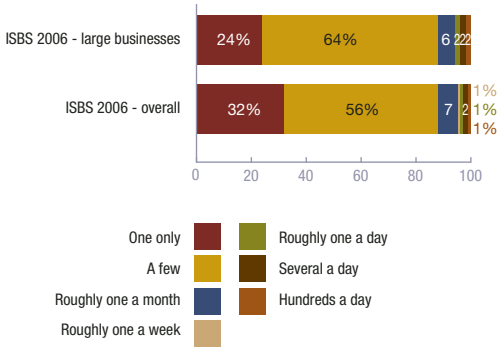
What was the source of the worst malicious software incident?

Figure 57



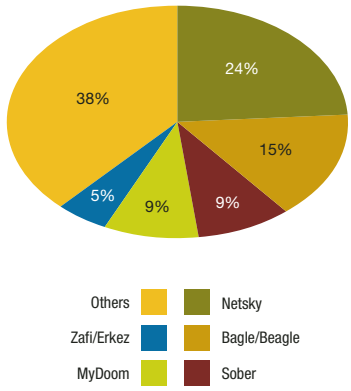
How many infections did the affected businesses suffer in the last year?

Figure 58



What caused the worst virus infections?

Figure 59



Infection by viruses and malicious software

Viruses and malicious software continue to be the most common cause of security incidents. Over a third of firms suffered a virus or disruptive software incident. However, this figure is a reduction from 50% in 2004.

Infection by malicious software also accounted for half of the worst incidents suffered. This is less than in 2004 but more than in 2002.

Viruses, worms and Trojans continue to dominate malicious software incidents, causing six out of seven of the worst incidents.

However, the virus landscape has changed since ISBS 2004. In 2004 a single worm, Blaster, was responsible for more than half the worst incidents in large businesses. No single virus or worm has caused such disruption during the last year. Survey responses reflect this; three-fifths of respondents were unable to report which virus caused their worst incident. Virus infection is not restricted to direct attacks on businesses; the increase in remote working has made organisations' perimeters more difficult to define and defend.

An employee at a medium-sized travel company had used his laptop at home. The machine developed problems. When the IT department connected the machine to the network to diagnose the problem, it unintentionally infected all their systems. It took three days to disinfect all the firm's computers.

One in seven of the worst breaches involved spyware. This is software that is downloaded without the users' knowledge and used to record and transmit their activity. Given the publicity surrounding spyware in the last year, it is perhaps surprising that this figure is not higher. A possible explanation is that, due to the stealth techniques employed by spyware, firms may not always be aware that they have been infected.

One respondent described how spyware had infected their system and caused it to 'crash'. They had anti-virus software but this had not identified the spyware. Recovery of the affected system was time consuming. After the incident, the business invested in some anti-spyware software.

The average number of malicious software infections has risen slightly compared with 2004 as businesses are bombarded by a multitude of virus variants. However, most affected companies still have only a few virus infections a year.

A virus disrupted a manufacturer's systems. As a result, the company had to upgrade its anti-virus software and pay an expert to resolve the problem.

Emerging technologies pose a new virus challenge for companies. In 2005, Comwarrior became one of the first rudimentary viruses to infect mobile phones. Earlier this year, computer science researchers demonstrated that even radio frequency identification (RFID) tags (used to identify goods) may be vulnerable to virus infection.

A medium-sized technology company had anti-virus software in place and scanned incoming e-mail and web downloads. Unfortunately, one of its staff plugged in a removable storage device that was infected and managed to bypass the anti-virus scanner.

For additional information and analysis, see the fact sheet on Viruses and malicious software.

Staff misuse of information systems

UK businesses report roughly similar levels of misuse of information systems as two years ago. Large firms are three times more likely to report misuse than small ones. Approximately two-thirds of large businesses are affected, and every very large business had at least one incident in the last year.

As well as having more staff, large firms are more likely to have an acceptable usage policy and to monitor compliance with that policy. This, combined with more dedicated security staff, may explain why more large firms report these incidents.

A small firm deployed web and e-mail monitoring software which captured many more instances of misuse. As a result, they have fine-tuned the monitoring software. This has helped prioritise which incidents to follow up.

Staff misuse strikes small businesses disproportionately hard. Roughly half of those affected cited a staff misuse incident as their worst security incident of the year. In contrast, while more large companies reported staff misuse as their worst incident, only a quarter of those that suffered misuse did so.

Misuse of web access is the most common form of misuse; this affects over half of large firms. Most companies that suffer any staff misuse have incidents involving web usage. Web misuse accounts for roughly three-quarters of the worst incidents of staff misuse; these were split fairly evenly between access to inappropriate web-sites and excessive web surfing.

Misuse of e-mail access also affects many businesses. One in ten firms reported one or more instances. E-mails containing inappropriate content (e.g. profanity or harassment) were the biggest offenders. Large companies were also troubled by confidential information leaving the organisation via e-mail. Small businesses were more concerned with excessive personal e-mail.

A manufacturer in the North East of England had a serious incident when one of its staff e-mailed its customer information to a competitor.

Telecoms companies are the most likely to have suffered misuse of web or e-mail access; one in three reported such incidents. Technology companies had the most confidentiality breaches, four times as many as the overall level. Intellectual property is important to these firms, so this represents a serious threat to their business.

One firm described its worst incident as staff accessing inappropriate web-sites. This became a serious incident when, due to the content downloaded, other staff complained.

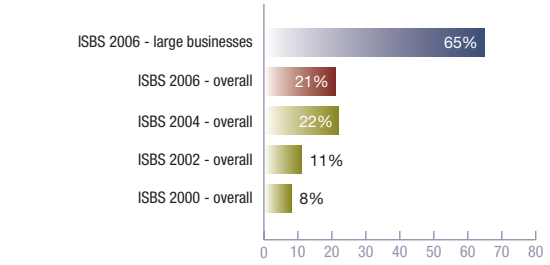
There has been an increase in the number of instances of staff misuse. This applies to both small and large businesses. Overall, the majority of firms are still suffering relatively few instances of staff misuse; the median is just a few instances a year. However, worryingly, 1% of businesses report e-mail misuse having occurred hundreds of times a day.

For further information see the separate fact sheet on E-mail and web usage.

Security Breaches

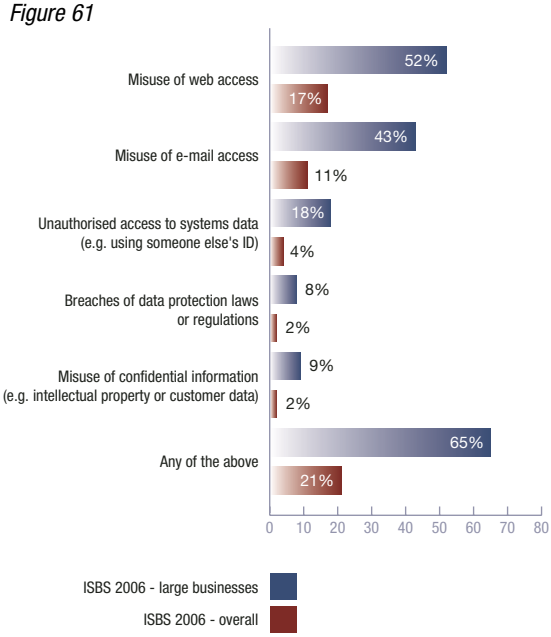
How many UK businesses have suffered from staff misuse of information systems?

Figure 60



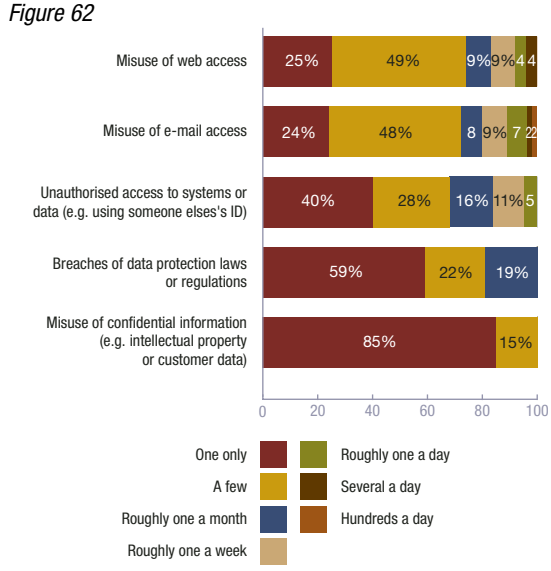
What type of staff misuse did UK businesses suffer?

Figure 61



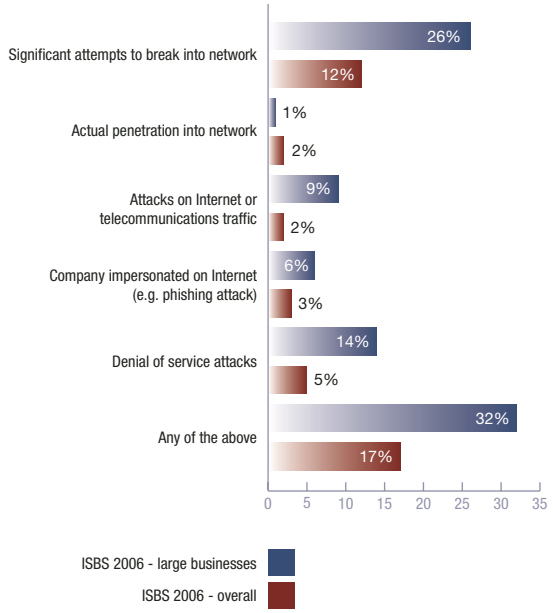
How many misuse incidents did affected UK businesses suffer?

Figure 62



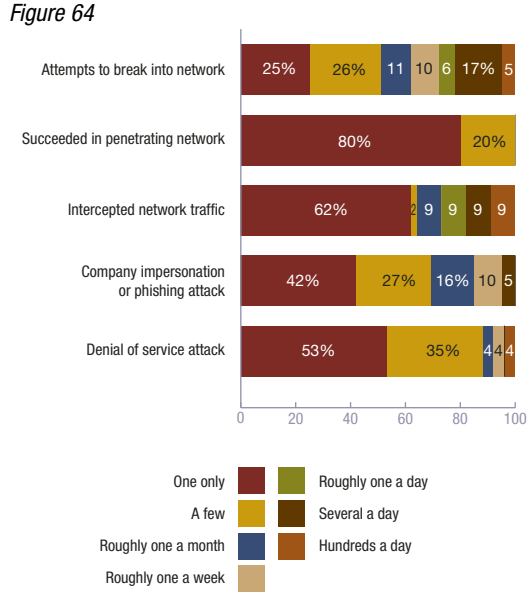
How many UK businesses were attacked by an unauthorised outsider in the last year?

Figure 63



How many attacks by unauthorised outsiders did affected UK businesses suffer?

Figure 64



Unauthorised access by outsiders

Record numbers of UK businesses have broadband connections to the Internet, increasing their exposure to attack. It is encouraging, therefore, that the number of companies reporting attempts to break into their networks (e.g. through significant probes of their Internet gateway) has not risen compared with two years ago. Indeed, the median number of attempts reported by affected companies has dropped from roughly one a week to roughly one a month.

Does this mean that the Internet is a safer place? Evidence from other sources (e.g. honeypot studies) suggests that unprotected computers attached to the Internet are attacked hundreds of times a day. The drop observed in this survey seems to reflect the changing perception of what constitutes a significant attempt to break into a network. Very few companies these days view simple port or network vulnerability scans as significant. Many simply screen out these relatively harmless attacks.

One organisation's firewalls were detecting hundreds of probes every day. After the company installed intrusion detection software, they could filter the data. As a result, they now review fewer alerts and feel they can now 'see the wood for the trees'.

Denial of service attacks (where one or more computers bombard a target with traffic until it becomes overloaded and unable to handle normal transactions) are the second most reported type of attack by an outsider. The number of affected organisations has not altered significantly over the last two years.

Attacks on Internet or telecommunications traffic, for example eavesdropping or interception, are not common. However, one in ten companies affected reports hundreds of attacks each day. This is a concern given the increasing volume of sensitive data (e.g. credit card and tax details) transmitted across the Internet. Adoption of new technologies, such as Voice over IP (VoIP), heightens this concern, especially as most firms have not assessed the associated security risks. The growth of wireless hotspots and the number of company authorised wireless connections is another potential area of exposure.

A large business reported the disclosure of sensitive company information as their worst security incident. Subsequent investigation suggested that the cause had been interception of unencrypted network traffic.

Technology and telecoms companies are most likely to be affected by attacks on Internet or telecommunications traffic. This could be the result of attackers targeting the medium over which sensitive data is transmitted, rather than where it is stored. Interestingly, financial services companies reported lower levels of interception attacks compared with other sectors.

The last few years have seen a new form of attack on the Internet, where perpetrators create a web-site that appears to be that of a legitimate organisation. They then lure that company's customers to the site (e.g. through spam e-mail) and then gather confidential information provided by the customers. These impersonation attacks are known as phishing. Overall, one in thirty companies was affected by impersonation or phishing. Telecoms providers were five times as likely to be affected. In contrast, retail and travel companies were the least likely to have incidents. Twice as many large companies reported impersonation or phishing attacks as small ones.

For further information and analysis, see the separate fact sheets on Trustworthy networking and Identity and access management.

Computer theft and fraud

Overall levels of theft and fraud appear to be down slightly on two years ago, with only one in twelve companies affected. The most common type of theft and fraud involving computers is the physical theft of computer equipment. The bigger the organisation, the more likely it is to have computer equipment stolen. Over a third of large businesses (and 82% of very large ones) reported theft of equipment by outsiders. Seven times as many firms suffered theft by outsiders as had thefts by their own staff. Large businesses have more thefts by staff, but even here it is still a three to one ratio.

The vast majority of thefts were isolated incidents. For 86% of firms, theft of computer equipment by outsiders was restricted to a single instance. No company reported more than a few thefts in the year, though roughly half of large firms did have a few incidents. Several respondents highlighted the challenge of securing laptop computers which are attractive to thieves.

One firm describing their worst incident said that a single laptop had been stolen from a desk during working hours. The theft appeared targeted since other laptops in the vicinity had been left untouched. Another small business traced a very serious confidentiality breach to the theft of one of its laptops.

Instances of computer fraud were low. However, their impact on businesses is significant; several small businesses reported losses of between £10,000 and £50,000 as the result of computer assisted fraud. In larger businesses, some losses ran into millions. Four-fifths of those affected by such incidents considered them serious, very serious or extremely serious. All of the organisations that had a computer fraud reported it as their worst security incident of the year.

An insurer reported how one of its staff tricked his manager into allowing him access under the manager's ID. An attempt to obtain information that could have been used to commit fraud followed.

Systems failure and data corruption

Accidental systems failure or data corruption affected three-tenths of UK businesses, the second highest incident type after virus infection. Roughly one in five firms reported it as the cause of their worst incident, again second only to malicious software.

Government, health and education and telecoms organisations are most likely to have experienced problems; 46% reported one or more incidents. In contrast, only a quarter of financial services organisations were affected. Sectors that are highly dependent on information systems tend to implement more resilient systems and change control processes; as a result, they typically have fewer incidents of this type.

A small retailer reported major disruption to its information systems after a disc drive crashed. Backups did exist, but it was two days before the systems were fully restored. A small amount of data was also lost as a result of the incident.

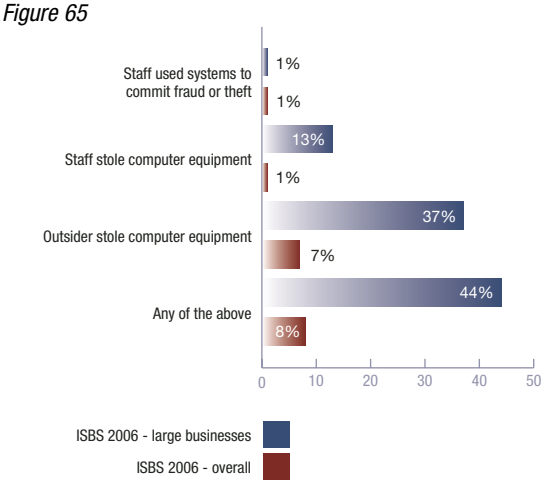
Hardware errors accounted for roughly half of systems failure and data corruption incidents. This echoes the results seen two years ago. Software bugs were the second most common cause.

A fifth of firms reported their systems failure or data corruption incidents as being very or extremely serious. In contrast, nearly half overall did not consider their incident to be serious.

The incidents were, on the whole, isolated. Roughly a third of firms suffered from systems failure or data corruption; of these only 3% had more than a few instances. Nearly half had only one such incident.

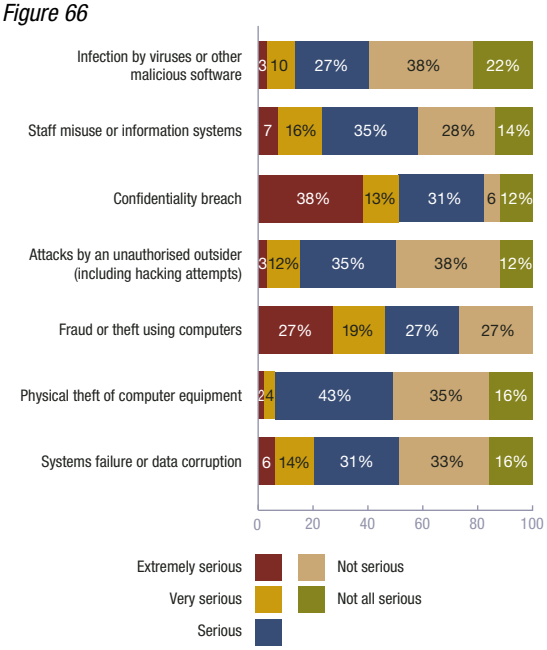
What type of theft and fraud did UK businesses suffer?

Figure 65



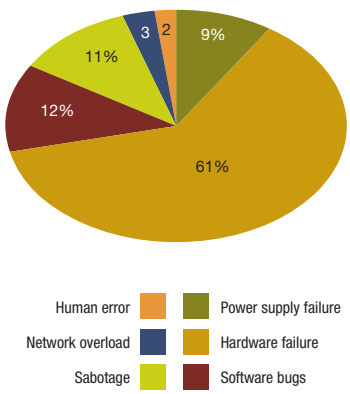
How serious were different types of incident?

Figure 66



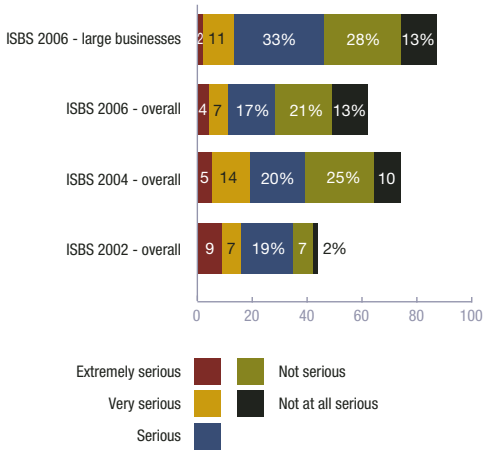
What caused system failure or data corruption?

Figure 67



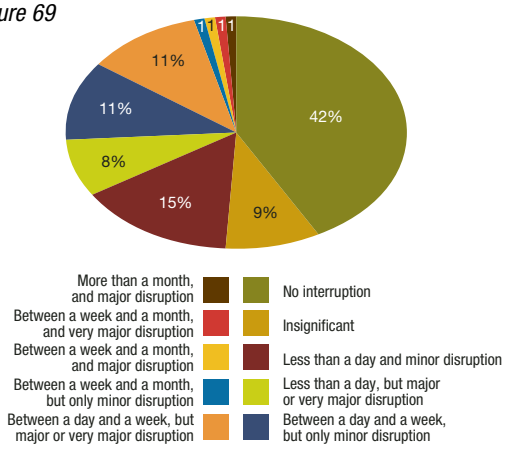
What proportion of UK businesses had a serious incident?

Figure 68



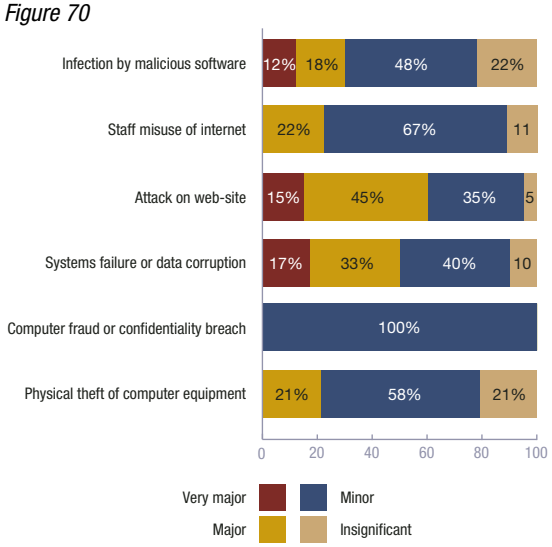
How much disruption to the business did the worst security incident cause?

Figure 69



What types of incidents were most disruptive to business?

Figure 70



Impact of breaches

It is important that firms understand the impact that security breaches have on their organisations; only by doing this can they effectively assess risks and prioritise actions.

42% of the UK businesses that reported security incidents considered their worst incident to be serious. A fifth described it as extremely or very serious.

The average seriousness of incidents has fallen since two years ago. The reduction was greatest among large businesses. In 2004, 37% of large businesses had at least one incident they rated as very or extremely serious. In 2006, this had fallen by two-thirds to only 13%.

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.

A very large technology company's worst security incident was when a competitor gained access to two key bid documents. While there was no direct financial loss (and only a few days of investigation time), the incident was very serious to the business since it had implications for the whole bid strategy.

Business disruption

The biggest single impact of security breaches continues to be business disruption. Three-fifths of organisations' worst incidents caused some interruption. Of these, just over a half caused more than a day's disruption, with some companies reporting more than a month of problems. These levels are similar to two years ago.

The most disruptive type of incident is an attack on a web-site or Internet gateway; when these attacks interrupt service, they tend now to cause major disruption to the business, illustrating how most businesses are increasingly dependent on the Internet. Roughly two-fifths of the worst systems failures also led to a major business disruption, with systems out for more than a day in about half of these.

One large firm had web-site problems that resulted in customers being unable to access the site for three days. The result was lost orders and, of greater concern, the possibility of lost customers.

Telecoms companies reported the greatest business disruption, 56% describing the disruption from their worst incident as major or very major. In contrast, financial services providers suffered the least disruption; for 81% of them, the disruption was minor or insignificant.

By making some assumptions about the impact of business disruption combined with average turnover figures, a crude estimate of the cost can be calculated. Based on this, worst incidents caused slightly more disruption to small businesses than in 2004, interrupting service for 1-2 days at an average cost of £6,000-£12,000. Large businesses suffered slightly less disruption than in 2004, with average interruption falling to 1-2 days (from 2-3 days) and the average cost of that interruption down to £50,000-£100,000.

Incident response costs

Even when the level of business disruption is low, organisations still incur the indirect cost of staff time responding to the incident.

Two-thirds of businesses are able to investigate and correct their worst incident with less than a man-day's effort. 97% of firms spent less than 10 man-days of investigation and remediation time on their worst incident. Despite their greater size and complexity, large firms achieved similar levels.

A small retailer infected by a virus estimated that a total of 25 man-days had been spent investigating and fully recovering from the incident. The organisation had only a handful of IT staff so the impact on other IT services was felt by users.

Infection by malicious software and systems failure were the most labour intensive type of incident to resolve. A small number of companies had malicious software infections that took more than 100 man-days to investigate and remediate. Infringement of laws or regulations took the least effort; all such incidents were addressed with less than one man-day's work.

In addition to the staff costs, two-fifths of firms spent cash to recover from their worst incident. This is an increase from 2004, when the figure was 32%. Large firms spent slightly more than small businesses, also up on 2004. It is rare for any incident to require more than £10,000 to be spent on recovery. However, the very largest firms find it difficult to quantify the cash cost of recovery; 38% of them did not know how much cash had been spent.

Fraud or theft using computers tends to be the most costly type of incident. Such incidents often require technical and legal expertise which is not always readily available in-house, especially for small businesses.

A telecoms company had an extremely serious fraud involving several million pounds. It took more than 100 man-days and cost more than £500,000 to investigate. The company's contingency plans for this eventuality proved effective, the technical configuration was fixed to prevent any repeat, and the perpetrators were prosecuted.

On average, UK businesses spent between £1,000 and £2,000 cash costs recovering from their worst incident. The average large firm spent £5,000 to £10,000.

Direct financial loss

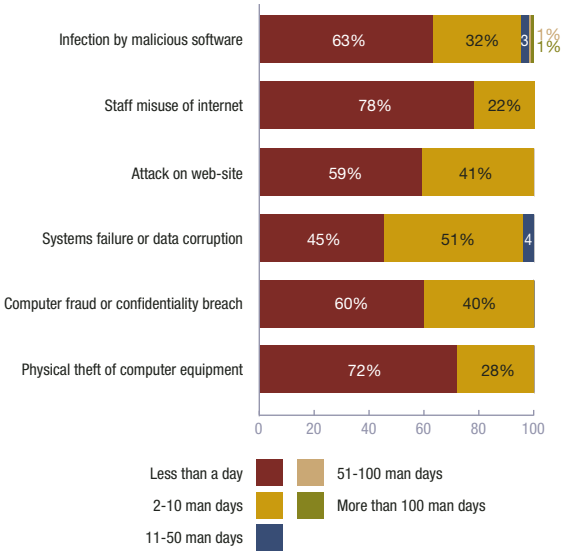
A security breach may also cause direct financial loss. As well as loss of assets, direct costs may include fines imposed by regulators or compensation payments to customers. Direct losses from security incidents are unusual; 85% of companies suffered no direct financial loss as a consequence of their worst incident.

Although direct losses remain low, they have increased. 2% of firms had direct financial losses of over £10,000, half of these over £50,000; in 2004, there were no reported losses over £10,000. 4% of very large firms reported losses of more than £500,000 as a direct result of their worst incident. These large losses were caused by frauds and confidentiality breaches.

Growing regulatory oversight and customer appetite for compensation could further increase the direct losses associated with security incidents. If levels of business conducted over the Internet continue to grow, more firms may be susceptible to direct losses.

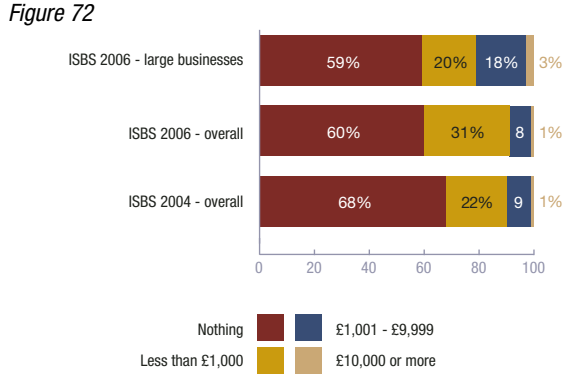
How much staff time was spent responding to the worst security incident?

Figure 71



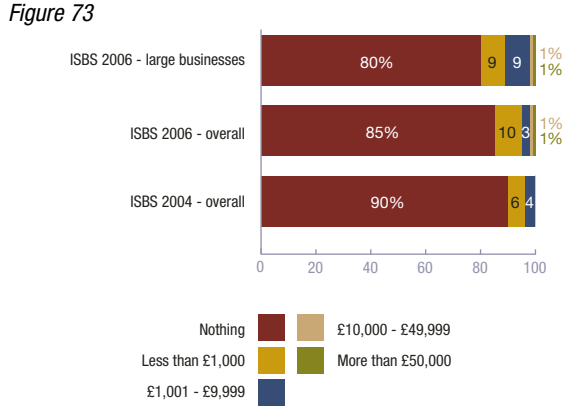
How much cash expenditure was required to recover from the worst incident?

Figure 72



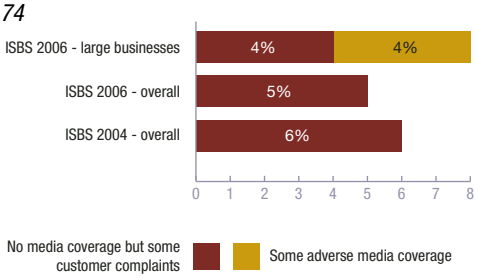
What was the direct financial loss associated with the worst incident?

Figure 73



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

Figure 74



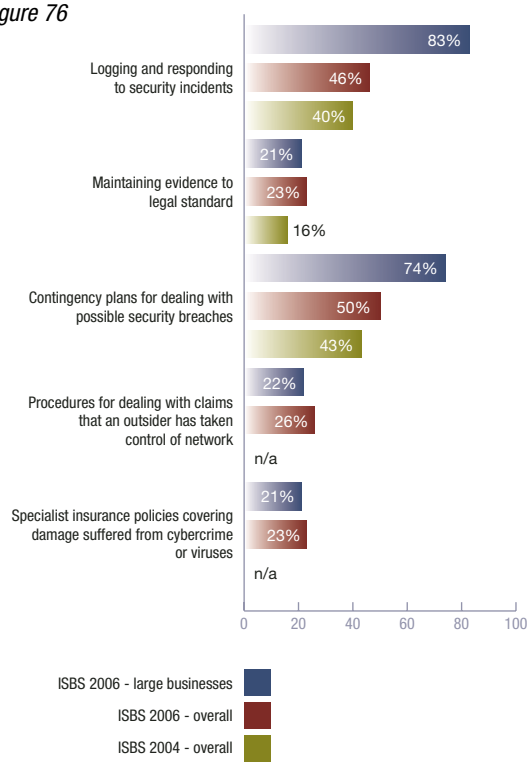
What was the overall cost of a company's worst incident in the last year?

Figure 75

	ISBS 2006 - overall	ISBS 2006 - large businesses
Business disruption	£6,000 - £12,000 *over 1-2 days*	£50,000 - £100,000 *over 1-2 days*
Time spent responding to incident	£600 - £1,200 *2-4 man-days*	£1,750 - £3,500 *5-10 man-days*
Direct cash spent responding to incident	£1,000 - £2,000	£5,000 - £10,000
Direct financial loss (e.g. loss of assets, fines etc.)	£500 - £1,000	£3,500 - £5,000
Damage to reputation	£100 - £400	£5,000 - £10,000
Total cost of worst incident on average	£8,000 - £17,000	£65,000 - £130,000

What procedures do UK businesses have in place to respond to security incidents?

Figure 76



Direct financial loss remains a small part of the overall cost of security incidents. UK businesses incurred losses of, on average, between £500 and £1,000 from their worst incident. For large firms, the average figure was between £3,500 and £5,000.

Damage to reputation

Damage to reputation can have more impact on a company's brand and can last longer than direct financial loss. Few firms, however, reported security incidents that damaged their reputation. Nine-tenths were able to contain knowledge of their worst security incident within their own organisation.

Some large businesses suffered from adverse media coverage; the number affected has quadrupled since 2004. The larger the business the more likely it is to have its reputation damaged; over a third of very large respondents could not prevent knowledge of the incident going outside their organisation. This is not surprising; newspapers and other media are most interested in household names. This interest, rather than necessarily the severity of the incident, may account for the higher impact on reputation suffered by the largest firms.

It is difficult to quantify the cost of damage to reputation, as the impact varies greatly. Given the low number of incidents causing external impact, the value (estimated on the same basis as 2004) is relatively low. The estimated average cost is between £100 and £400. Large firms incurred higher costs, on average £5,000 to £10,000.

A large manufacturer had a serious incident when one of its staff surfed child pornography. The subsequent investigation, disciplinary action and prosecution consumed man-months of effort. What made the incident particularly damaging was the adverse media coverage. The company did not have any contingency plan in place for how it would deal with this kind of incident.

Total cost of incidents

The average total cost of a UK company's worst incident, based on these different impacts, is in the range of £8,000 to £17,000. For large businesses, the average cost is between £65,000 and £130,000. For very large respondents, the average cost of the worst incident is correspondingly greater, averaging roughly £1 million, with business disruption again the largest component.

For firms overall, the cost is roughly 50% higher than two years ago. In contrast, large businesses have seen a 20% reduction in the average cost. A steep reduction in the cost associated with business disruption was the main reason for the lower figure.

Extrapolation of cost data across the whole business community should always be treated with caution. However, taking the number of companies affected, the average number of incidents suffered and the cost per incident into account, the overall cost of security breaches to UK plc has increased by roughly 50% over the last two years. An indicative figure for the overall cost to UK business is in the order of ten billion pounds per annum. The cost to large companies, however, has dropped by roughly 50%; it is small businesses that appear to be suffering the most

Businesses remain pessimistic about the level of security incidents expected in the next year. The majority also believe it will be more difficult to detect incidents. Businesses, therefore, need to follow the lead of the largest companies; only by continuing their investment in security controls can they make sure they reduce the number of incidents and their impact.

Incident reponse and contingency planning

There has been a rise in the number of businesses that have formal procedures in place to log and respond to security incidents when they arise. Roughly half of all UK businesses (and five-sixths of large ones) do this.

Half of the organisations that suffered a security incident said they had a contingency plan to deal with it; two-thirds of larger firms had plans. Organisations plan for some incidents better than others. More firms planned for systems failure or data corruption than for other incidents. The least planned for incidents were theft or unauthorised disclosure of confidential data (25%).

Interestingly the existence of contingency plans does not appear to depend on whether a business has security breaches or not. Overall, 50% have contingency plans; among those that had a breach, 52% had plans. In contrast, the priority that senior management places on security has a significant impact on the implementation of these practices. In companies where security is not a priority at all, only 17% log their security incidents and only 19% have any contingency plans for dealing with them.

The vast majority of plans were effective at dealing with the incident. 93% of companies said their plans dealt with malicious software effectively. In contrast, this figure fell to 84% for attacks on web-sites or Internet gateways.

Maintenance of evidence (to support possible legal proceedings) has improved. However, such forensic procedures remain rare, with only a quarter of UK businesses having them.

Nearly four-fifths of the firms that experienced a breach took specific actions after their worst security incident. Some took several actions; all were designed to reduce the likelihood of the security incident recurring. Firms respond to incidents with a mixture of technology, people and process changes.

There is a link between the actions taken after the worst incident and the type of incident. Fraud and theft drive the most change; on average, three different steps are taken in their wake. In contrast, systems failure or data corruption cause the least changes. Legal action has low scores regardless of incident type, but is most likely after fraud or confidentiality breaches. Interestingly, there were no cases of legal action being taken as the result of malicious software, web-site attacks or infringement of laws.

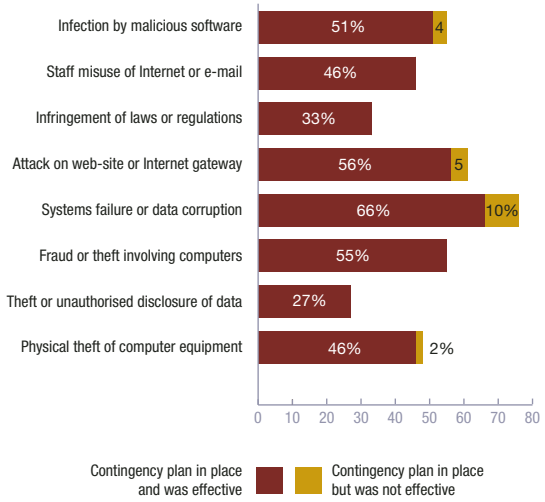
UK businesses now seem to have a more realistic view of the degree of coverage that their insurance policies provide against damage arising from security breaches and data loss; 20% think they have full cover, 44% partial cover and 36% no cover. However, a quarter of respondents (and nearly half of those from large companies) are unaware of what their insurance cover includes.

Nearly a quarter of small businesses claim to have taken out some form of cyber insurance policy; large businesses are less likely to do this (preferring to accept or self-insure the risk). Firms with specialist cyber insurance policies are most confident about their cover with 46% believing they were now fully covered. In contrast, only 10% of those without specialist policies think their normal insurance policies fully cover them for damage.

The larger the organisation, the more sceptical they are about their insurance cover; none of the very large respondents believe their insurance fully covers them for security breaches.

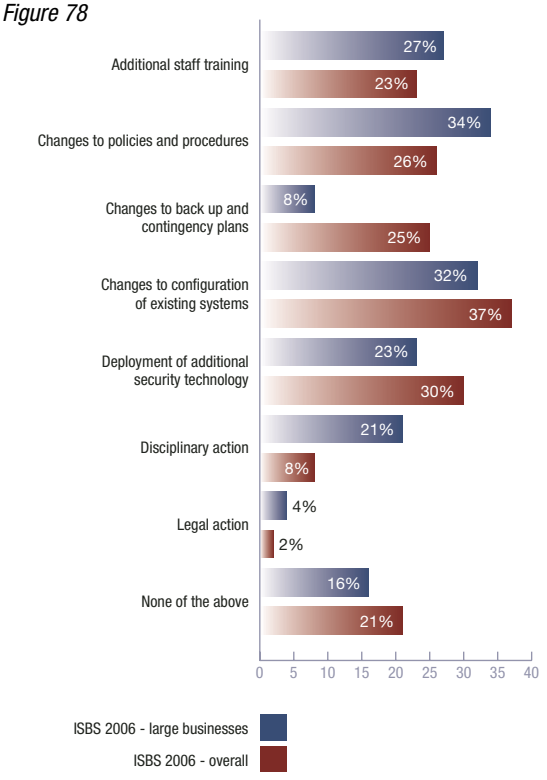
What type of security incidents do businesses plan for, and how effective are those contingency plans?

Figure 77



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

Figure 78



Sponsoring organisations

The **DTI**'s Information Security Policy Team 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.dti.gov.uk/industries/information_security.
For guidance on protecting your online business, see www.getsafeonline.org.

Founded in 1975, **Microsoft** (Nasdaq "MSFT") is the worldwide leader in software, services and solutions that help people and businesses realize their full potential. The security of customers' computers and networks is a top priority, and Microsoft are committed to building software and services to better help protect customers and the industry. For more information, see www.microsoft.com.

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability and integrity of their information. Its mission is to protect its customers' connected experiences – their identity, transactions, systems environment, stored data, as well as their ability to communicate safely and securely with business and personal contacts. Headquartered in Cupertino, California, USA, Symantec has operations in more than 40 countries with a UK base in Reading. For more information, see www.symantec.co.uk.

The member firms of the **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 130,000 people in 148 countries across our network work collaboratively using connected thinking to develop fresh perspectives and practical advice.
For PwC's security solutions, see www.pwc.com/security.

Clearswift simplifies content security. Our range of content filtering solutions makes it easy to deploy, manage and maintain no-compromise email and web security for both inbound and outbound traffic. Clearswift is the only vendor to offer comprehensive, policy-based content security in all three deployment methods: as software, as an appliance and as a managed service. Twenty years of experience across 15,000 organizations has helped us raise security standards while simplifying security management. For more information, see www.clearswift.co.uk.

Entrust, Inc. [Nasdaq: ENTU] is a leading provider of Identity and Access Management solutions, enabling businesses and governments to transform the way they conduct online transactions and manage relationships with customers, partners and employees. Entrust's solutions promote a proactive approach to security that provides accountability and privacy to online transactions and information. For more information, see www.entrust.com.

Independent reviewers

The **Information Assurance Advisory Council** is a unique partnership that brings together corporate leaders, public policy makers, law enforcement and the research community to address the challenges of information infrastructure protection. For more information, see www.iaac.org.uk.

The **Serious Organised Crime Agency (SOCA)** is a new law enforcement agency created to reduce the harm caused to people and communities in the UK by serious organised crime. For further information see www.soca.gov.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 **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.

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 **National Computing Centre** is the UK's foremost source of independent advice, guidance, networking and services for IT professionals. For more information, see www.nccmembership.co.uk.

The role of the **National Infrastructure Security Co-ordination Centre** is to minimise the risk to the Critical National Infrastructure from electronic attack. It is an inter-departmental centre drawing on contributions from Defence, Central Government Policy, Trade, the Intelligence Agencies and Law Enforcement.
For more information, see www.niscc.gov.uk.

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.

Other DTI Information Security Breaches Survey 2006 publications

In addition to this technical report, five other ISBS 2006 publications are also available. You can download electronic copies from www.security-survey.gov.uk. Alternatively, you can obtain printed copies from the DTI's Publications Unit at www.dti.gov.uk/publications (under "search") by quoting the Unique Reference Numbers (URNs) listed.

The 4 page **Executive summary** provides an overview of the results. It is aimed at senior business management who may not have time to read the full survey results. (DTI URN 06/802).

There are also four fact sheets, each of which analyses the results in a particular area and provides specific recommendations for addressing the associated risks.

Viruses and Malicious software
(URN 06/804) - 2 page fact sheet.

Produced in association with:

symantec.

www.symantec.com

Identity and access management
(URN 06/805) - 2 page fact sheet.

Produced in association with:

Entrust
Securing Digital Identities & Information

www.entrust.com

E-mail and web usage
(URN 06/806) - 2 page fact sheet.

Produced in association with:

CLEARSWIFT

www.clearswift.co.uk

Trustworthy networking
(URN 06/807) - 2 page fact sheet.

Produced in association with:

Microsoft

www.microsoft.com

This report is printed on Mega Matt paper which is made from 50% recycled and 50% chlorine-free pulp from countries that operate strict reforestation policies.

Department of Trade and Industry. April 2006. URN 06/803