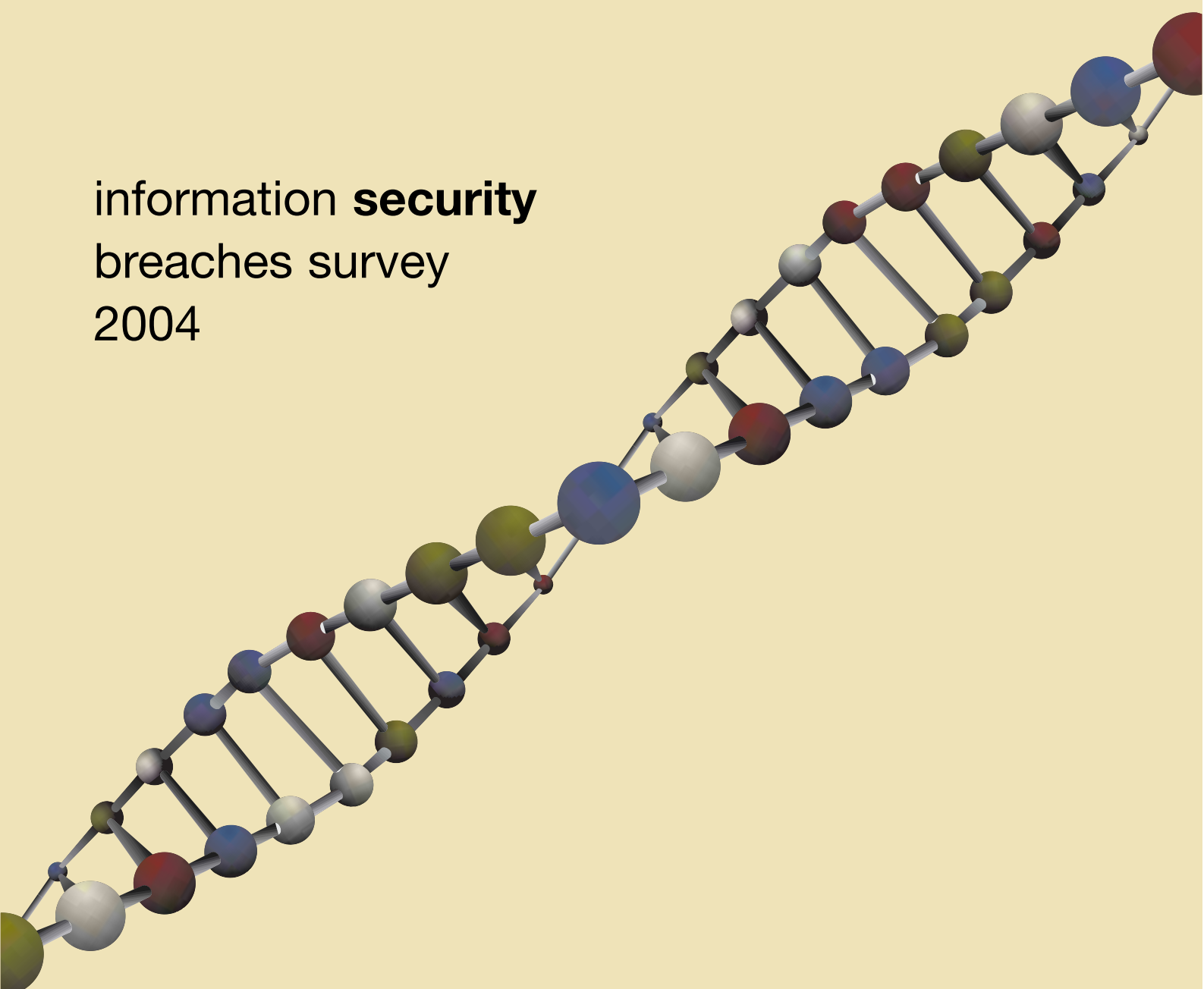


information **security**
breaches survey
2004



technical report

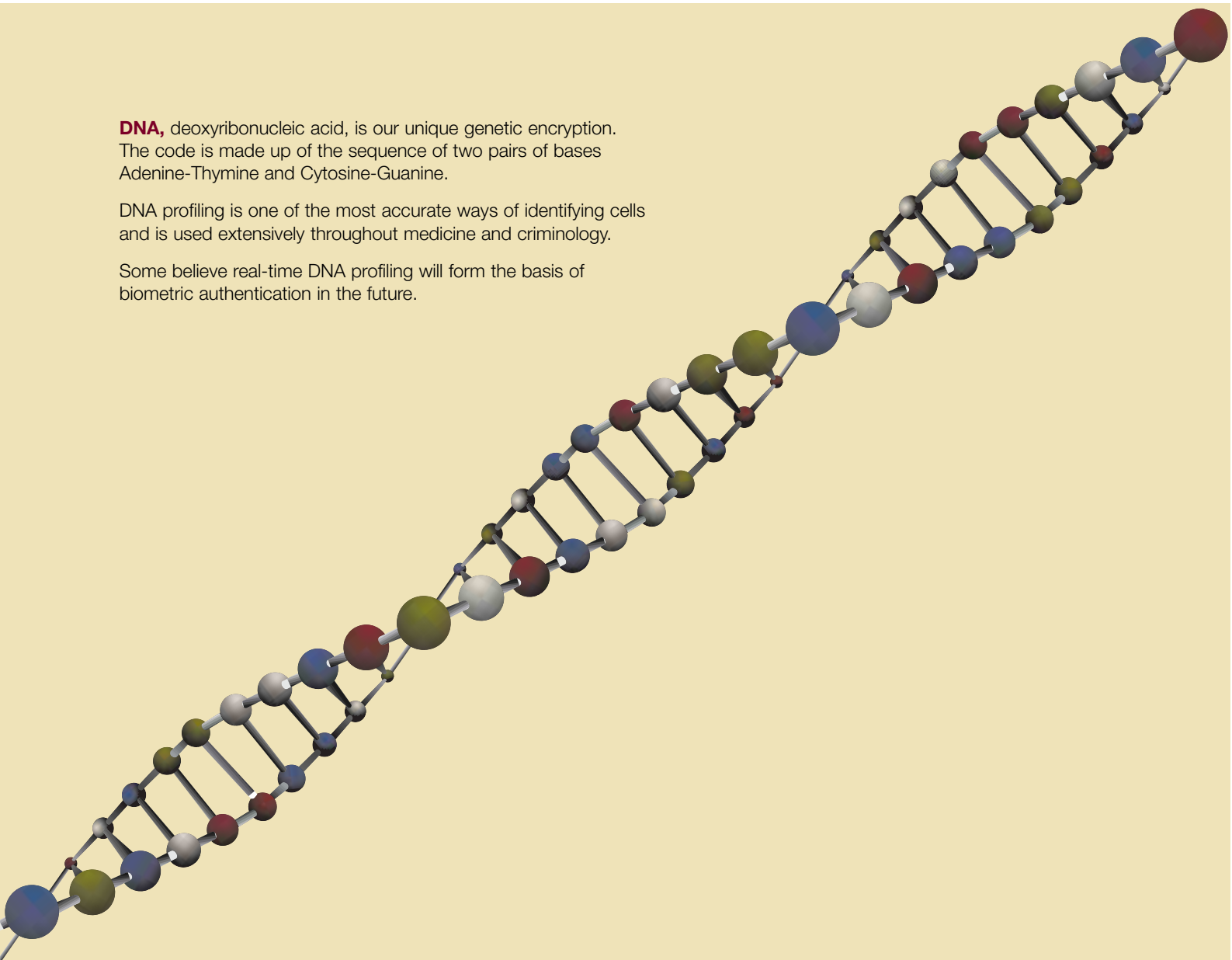
in association with:



DNA, deoxyribonucleic acid, is our unique genetic encryption. The code is made up of the sequence of two pairs of bases Adenine-Thymine and Cytosine-Guanine.

DNA profiling is one of the most accurate ways of identifying cells and is used extensively throughout medicine and criminology.

Some believe real-time DNA profiling will form the basis of biometric authentication in the future.



DTI recommends

- Draw on the **right expertise** 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.
- Invest appropriately in **security controls** (to mitigate the risks), or in **insurance** (to transfer them).
- **Check** your key **security defences** (such as operating system patches, disaster recovery plans, etc.) are **robust** and **up to date**.
- **Respond to security incidents** efficiently and effectively, to minimise business disruption.

Preface

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 2004 (ISBS 2004) is the seventh such survey, and has been managed by PricewaterhouseCoopers.

The survey results show that the UK is now firmly in the Information Age, with companies of all sizes embracing the use of the Internet. This is changing the way that business operates, improving efficiency and customer service. However, a side effect of this increased connectivity is greater exposure to information security issues. Indeed, this survey shows that security problems have now become a fact of business life, and not something that happens to someone else. As organisations struggle to contain these threats, the number of security incidents continues to rise.

It is encouraging, however, to note that information security remains a high priority at board level. More companies than ever have a security policy in place, and those that have adopted BS7799 have found it has yielded real benefits. It is also pleasing that many companies have drawn upon the guidance the Government, in particular my own Department, has issued to help them address their information security concerns. Our work in this area will continue and form a key part of the Government's agenda for promoting e-business in the UK.

The battle to contain the information security menace will be a long one, and it is far from won. However, it is not a battle UK businesses can afford to lose.



*Stephen Timms MP
Minister of State for Energy,
e-Commerce and Postal Services*

Introduction

ISBS 2004 continues to highlight the vulnerability of UK plc to information security threats. Awareness has never been higher, but many businesses are finding their precautions are inadequate. Almost every business has anti-virus software, yet half had virus infections last year. Everyone makes backups, but only one in ten test that their recovery processes would work in a disaster. Up to date skills and knowledge are often lacking, and new threats are emerging all the time.

Unsurprisingly, most respondents were pessimistic about the future for information security incidents. While there is no magic wand solution, passive resignation is not the answer. There are simple steps that businesses of all sizes can take to reduce the likelihood and impact of future incidents. Above all, this survey shows that too many organisations have waited until an incident hits them before putting counter-measures in place. Don't wait until the horse has bolted before closing the stable door.

To help you take action, we have sought to highlight good security practices throughout this report. Every business is different, so you need to interpret the recommendations in the context of your business. Effective risk assessment tailored to your organisation's circumstances is the cornerstone of good information security practice.

Large companies continue to suffer the greatest number of security incidents. Establishing an integrated information assurance approach, as part of the overall corporate governance structure, is vital to ensure all stakeholders' needs are addressed. Educating staff is as important as deploying the right technology.

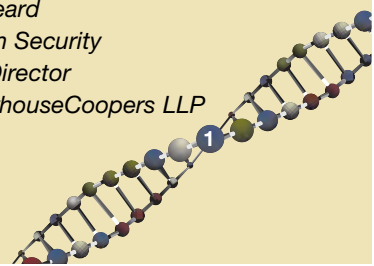
We thank all the sponsors and independent reviewers that worked on this survey with us. Their contribution kept the survey focused on the topics of most concern to UK businesses today. Their variety of perspectives helped ensure the analysis in this report is, as far as possible, balanced, objective and relevant.



*Chris Potter
Information Security
Assurance Partner
PricewaterhouseCoopers LLP*



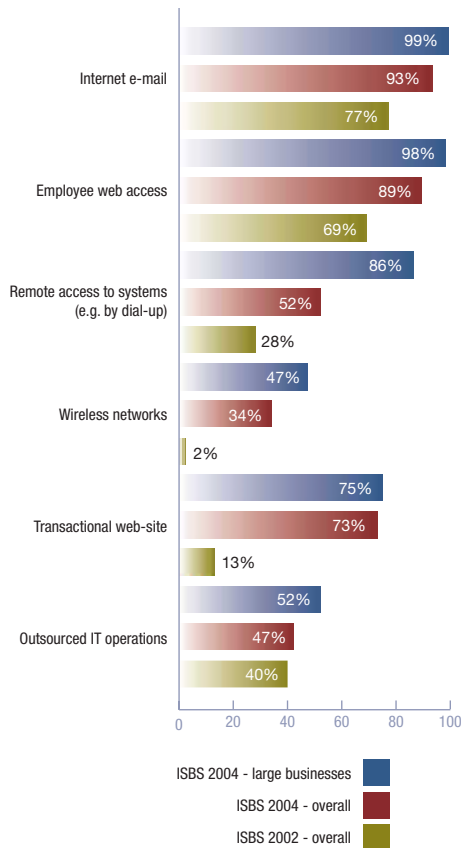
*Andrew Beard
Information Security
Advisory Director
PricewaterhouseCoopers LLP*



Headline News

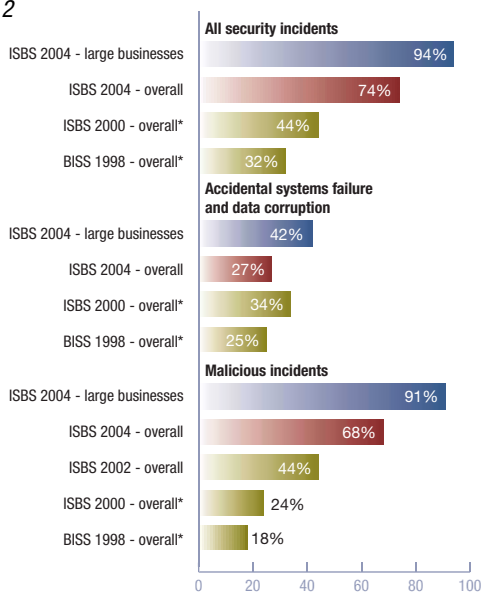
How has the business environment changed over the last two years?

Figure 1



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

Figure 2



*The 1998 and 2000 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.

The business environment continues to change with increased use of the Internet

- Roughly nine-tenths of UK businesses now send e-mail across the Internet, browse the web and have a web-site.
- Most web-sites now allow customers to initiate transactions online.
- There has been a massive increase in the number of organisations using wireless networks.
- The number allowing staff remote access to their systems via dial-up or the Internet has doubled.
- Dependence on electronic information and the systems that process it continues to increase. 87% of UK businesses are now highly dependent compared with 76% two years ago.

Greater connectivity has increased the exposure of UK businesses to security threats

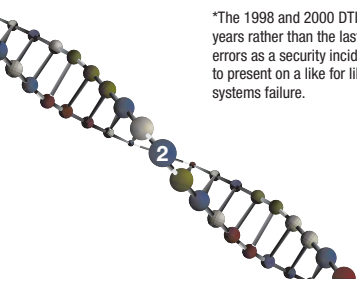
- These threats continue to evolve, with new viruses and vulnerabilities being identified every week.
- The average UK business now receives roughly twenty viruses a year, and has its web-site scanned or probed many times.
- Large businesses are attacked more, receiving on average a virus a week.
- As a result, information security continues to be a high priority for senior management. Three-quarters of organisations stated this was a high or very high priority for their top management or board of directors.

As a consequence, the number of UK businesses that suffered a security breach continues to rise

- Two-thirds of UK businesses had a premeditated or malicious incident compared with just under a half two years ago.
- In addition, a quarter had a significant incident involving accidental systems failure or data corruption.
- The average UK business now has roughly one security breach a month. Large businesses have roughly one a week.
- Virus infection and inappropriate usage of systems by staff were the cause of most of the incidents. Viruses also caused the greatest number of serious incidents.
- Unsolicited e-mail ('spam') is growing rapidly and has now become a significant issue for a third of UK businesses.

The cost to UK business is significant

- The average cost of an organisation's most serious security incident was roughly £10,000. In large companies, this was more like £120,000.
- The impact on availability was by far the biggest contributor to this cost, with some organisations suffering a very major disruption to their business operations for more than a month.
- Respondents were significantly more pessimistic about the future outlook for information security breaches than they were two years ago.



Some progress has been made in putting security controls in place

- The number of UK businesses with a security policy continues to rise. A third of all companies, and two-thirds of large businesses, now have one.
- Virtually every business has implemented anti-virus software, and most now update this software immediately a new virus signature is identified.
- Most businesses that outsource their IT operations have service level agreements that clearly set out their information security requirements.

However, there is still considerable room for improvement

- Increasingly, viruses are bypassing traditional anti-virus software and targeting vulnerabilities in computer operating systems. Processes for keeping these up to date with the latest security patches are generally weak.
- Businesses tend to rely solely on their firewall to defend their Internet gateway and web-site against attack.
- User ID and password are still the dominant mechanism for authenticating users' identities. However, a third of large businesses have moved to some degree of two-factor authentication, and have seen a reduced level of unauthorised access breaches as a result.
- New adopters of remote access, Internet e-mail and web access tend to have done so without implementing any controls.
- Only a half of all wireless networks have security controls in place.
- Fewer than one in ten businesses (and only a quarter of large ones) have tested their disaster recovery plans to see if they would work in practice.

One root cause is that many companies lack the expertise to address this complex, changing area

- Three-quarters of businesses are confident that their technical security processes are sufficiently good to prevent or detect all significant security breaches. Given the weaknesses in these controls, it appears that some do not fully appreciate the risks they are running.
- Only one in ten companies (and only a quarter of large ones) have staff with formal information security qualifications.
- Neither overall awareness of BS 7799, nor the number of UK businesses that have implemented it, has increased over the last two years. However, those organisations that have implemented BS 7799 have found that it has yielded real business benefits.

Another cause is that spend on information security, while increasing, is still relatively low and is seen as a cost rather than an investment

- Companies now spend on average 3% of their IT budget on security compared with 2% two years ago. Large businesses spend roughly 4%.
- Overall levels of investment in security are still considerably below the 5%-10% benchmark level.
- Under half of all businesses evaluate return on investment on security spend.

Headline News

How much did each organisation's worst security incident cost on average?

Figure 3

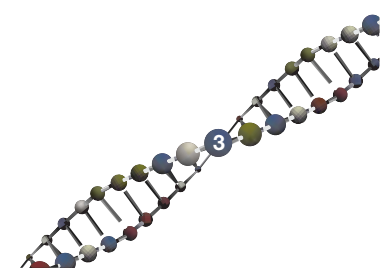
	Overall	Large businesses
Disruption to business	£5,000 - £10,000 <i>over 1-2 days</i>	£50,000 - £150,000 <i>over 1-3 days</i>
Time spent responding to incident	£500 - £1,000 <i>2-4 man-days</i>	£3,000 - £6,000 <i>10-20 man-days</i>
Direct cash spent responding to incident	£1,000 - £2,000	£5,000 - £10,000
Direct financial loss (e.g. loss of assets, fines etc.)	£200 - £500	£2,000 - £4,000
Damage to reputation	£100 - £300	£5,000 - £20,000
Total cost of worst incident on average	£7,000 - £14,000	£65,000 - £190,000

Ranges are quoted because of the inherent uncertainty involved in extrapolation.

How much progress has been made against the top ten actions identified two years ago?

Figure 4

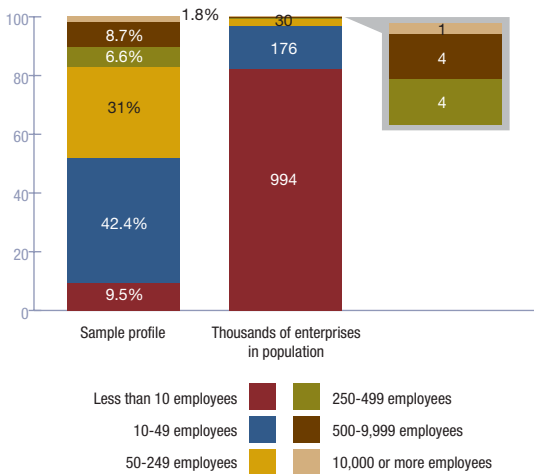
	Status	Trend since 2002
Staff education		↔
Security policy		↑
Security skills		↔
Investment in security		↑
Managing systems change securely		↑
Up-to-date technical security defences		↓
Legal compliance		↔
Contingency plans		↓
Insurance cover		↔
Security audits		↔



Methodology

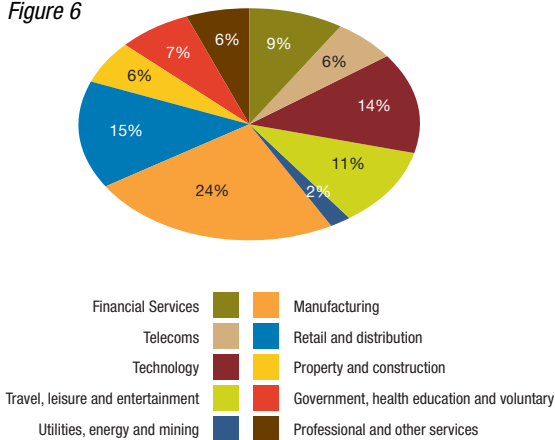
How many staff did each respondent employ in the UK?

Figure 5



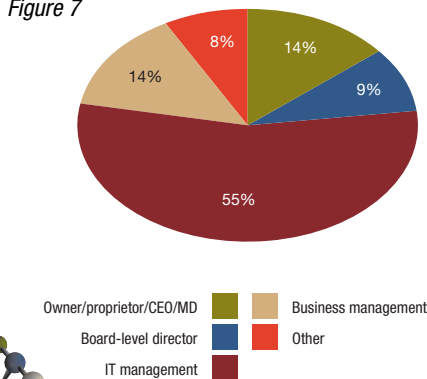
In what sector was each respondent's main business activity?

Figure 6



What was the respondent's role within their organisation?

Figure 7



The core element of the research for ISBS 2004 was a quantitative survey, conducted using a structured questionnaire. We selected the sample randomly from a register of UK businesses. In each case, we contacted the person identified as responsible for information security. In larger companies, they tended to be IT managers; in smaller ones, more were business managers. In total, we completed 1,001 computer-assisted telephone interviews, each lasting on average 30 minutes. The interviews took place between 2 October 2003 and 30 January 2004.

Businesses of different sizes tend to exhibit different security profiles. A representative sample of UK businesses would be predominately 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 93% +/- 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 +/- 8%.

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

As with any survey of this length and confidentiality, the response rate was relatively low. Compared with two years ago, fewer organisations contacted chose to participate. While this was partly due to survey fatigue, some of the reluctance (encouragingly) came from increased awareness of the risks associated with divulging confidential information over the telephone. When the survey response rate is low, there is a risk that the sample becomes biased. We have minimised this by ensuring our sample included an appropriate representation of size, industry sector and region, and by weighting the results accordingly.

Organisations without computers tended not to participate in the survey. Our estimates of overall figures should, therefore, best be interpreted as 'of UK businesses that use computers'.

To supplement the telephone surveys, we also carried out face-to-face in-depth interviews with information security officers. Some, but not all, of these had participated in the telephone survey. We used these interviews to confirm the validity of the telephone findings and to obtain additional qualitative information.

In addition, we used an online web-site poll to allow organisations not selected for either telephone or face-to-face interviews to contribute to the survey. We have not included the results of the web-site poll in the main quoted statistics. Instead, in places we have referred to the results of the web-site poll in our commentary. As with all web-site polls, the results are not necessarily indicative or representative, so treat them with some caution. Half of the online poll respondents were from large companies and only a third from small businesses. The self-select nature of the poll meant that respondents tended to be more aware of security issues than average. These biases should be taken into account when interpreting the results of this poll.

The Changing Business Environment

In the 2002 survey, the after-effects of the dot.com boom were still very evident. There was a large increase in the number of UK businesses using the Internet. The intervening two years have seen this trend continue. In particular, small and medium-sized businesses have increasingly seen the benefits the Internet can bring. Web and Internet e-mail access is now commonplace among all sizes of business. Technology and telecommunications companies lead here, while retailers lag. Overall, nine out of ten UK companies provide staff with Internet access. Sadly, a side effect of this is greater exposure to viruses, inappropriate usage and spam.

More UK businesses than ever have a web-site. Retail, travel and services businesses tend to lead here, while energy, health and education lag. The number of businesses accepting transactions through their web-sites has risen significantly. Small and medium-sized businesses tend to use a simple externally hosted online store, or just allow customers to e-mail orders in. Web-sites of larger businesses tend to be a fully integrated channel into core business systems. As the volume of transactions through web-sites increases, the potential impact of security incidents, such as hacking attempts or denial of service attacks, is rising.

Two years ago, we commented on the trend towards businesses enabling staff to connect to their systems while out of the office. Over the last couple of years, adoption of remote access has nearly doubled. Roughly half of all UK businesses now allow this. Large businesses continue to be the trendsetters in this area. Technology, telecommunications and energy companies are early adopters. Agriculture and property companies use this least. While remote access enables greater flexibility, it can become a gap in the security perimeter.

In 2002, wireless networking was in its infancy. Unsurprisingly, since then, wireless networks have proliferated. Overall usage has risen from 2% to 34%. Nearly one in two large businesses now has a wireless network. Technology and telecommunications companies tend to be early adopters. However, wireless remains a relatively immature technology. There remain many usability, security and cost issues. New high-speed wireless services have recently been launched, however these tend to rely on subscription and per-minute charges. This can make them difficult to control as a business tool.

One medium-sized services company had an issue with IT staff 'playing' with the latest technologies when there was not a proven business case for doing so. The IT Director's solution was to give each IT staff member a small budget for the latest gadgets and some time for research. This has helped staff motivation and saved a lot of money in failed initiatives.

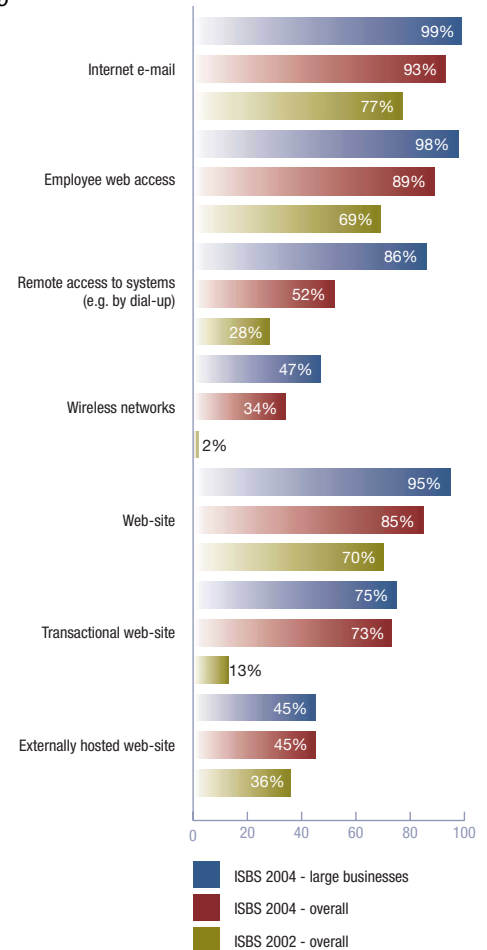
Outsourcing of at least one aspect of a company's IT operations continues to increase. Roughly half of all UK businesses have now outsourced their application development and support, systems administration, web-site hosting or helpdesk operations. As a result, many businesses now depend on their outsource provider for important aspects of information security. Many large organisations are also moving operations to lower cost countries (such as India or China). This "off-shoring" can make security vetting and awareness training more difficult.

Overall, the business environment continues to become more inter-connected. Traditional boundaries between organisations are eroding. The pace of change continues to increase. Keeping on top of these changes is time-consuming for any business, let alone making sure changes are made in a safe and secure manner.

Security Strategy

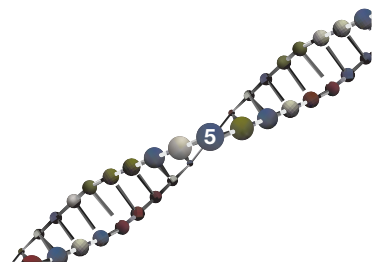
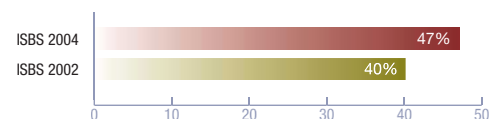
How has the business environment changed over the last two years?

Figure 8



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

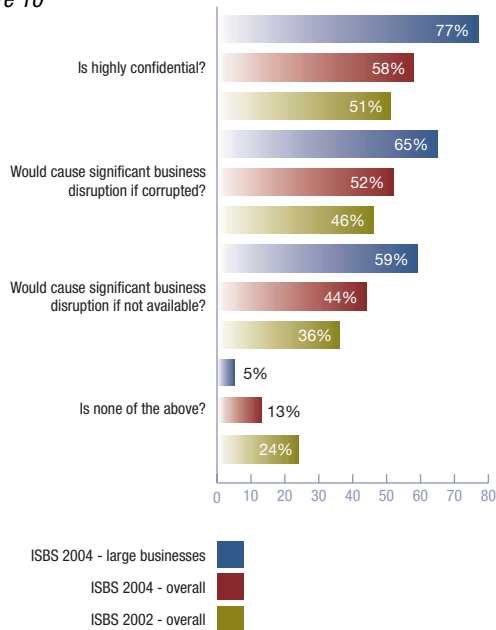
Figure 9



Security Strategy

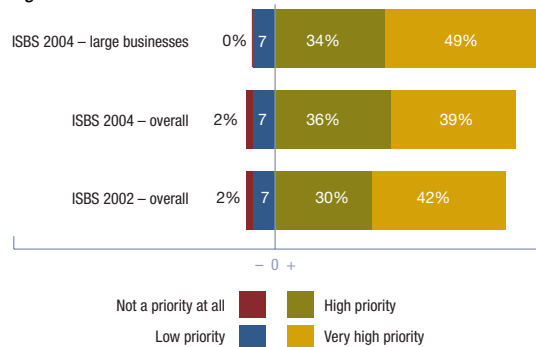
How many UK businesses have information that:

Figure 10



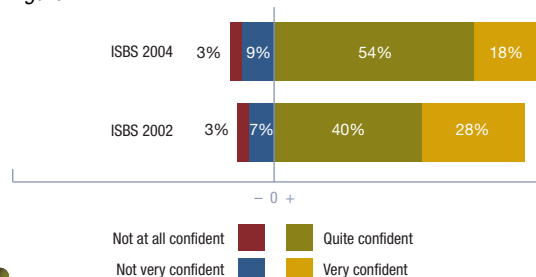
How high a priority is information security to UK businesses' top management or director groups?

Figure 11



How confident are staff responsible for information security that they have caught all significant security breaches that occurred in their organisations in the last year?

Figure 12



Attitudes towards Information Security

Information is widely regarded as the lifeblood of modern business. This survey shows that UK companies are increasingly reliant on the confidentiality, availability and integrity of their data. The number for whom computer usage is peripheral has halved since 2002.

More UK businesses hold sensitive data than two years ago. Over half store highly confidential records on computers. Large businesses are more likely to do so. As you might expect, the government, health and financial services sectors had the most sensitive data. In contrast, less than half manufacturing and agricultural businesses were concerned about confidentiality. Given that most businesses hold personal data about staff for payroll, these figures may be understated.

Over half of all companies would have significant business disruption if their information were corrupted. Again, large companies are more likely to be affected. Dependency is greatest in the telecommunications, technology and manufacturing sectors. Agricultural, property and construction businesses showed least concern.

Roughly half of all organisations now depend on systems to carry out normal operations. Availability is more important than ever, and is a fairly consistent issue for all sectors. Large companies again are most dependent on their systems.

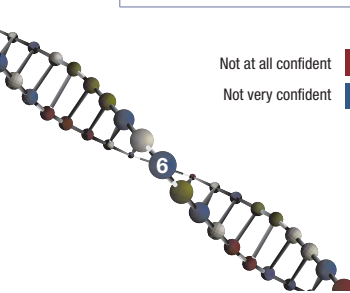
In the immediate aftermath of 9/11, the 2002 survey showed a big rise in the attention senior management gave to information security. Two years on, security is still firmly on the board agenda. Three-quarters of companies rate security as a high or very high priority. The priority is highest in large businesses, with five in six considering it important. Every financial services respondent felt security was highly important. Agriculture and retail were least concerned, but even there roughly 60% saw this as a high priority.

The security manager of a telecom provider delivers monthly reports to his board on information security issues. He recently started including the number of virus incidents, external scans and Internet probes. At first, the directors were reluctant to believe the statistics. In the next budgeting cycle, however, they significantly increased the budget for security monitoring tools.

One of the key concerns raised in the 2002 survey was overconfidence among those responsible for information security. Two years on, confidence levels remain high. Roughly three-quarters of businesses believe their security controls prevented or detected all significant security breaches. However, the number of businesses that are very confident about this has fallen by 10%. This is not surprising, given the changing business environment and the rise in the number of incidents.

Confidence is highest in financial services. This reflects the high priority given to security at board level. Confidence is lowest in professional services and energy companies. Both of these sectors have many staff off-site accessing confidential information. Confidence is also low in agricultural businesses, where information security is a low priority.

Online poll respondents tended to come from particularly security aware organisations. 76% had highly confidential information and 78% were concerned about possible data corruption. Only 5% felt that security was a relatively low priority to their senior management. Interestingly, they were less confident about their security controls than telephone respondents. Despite generally having better security controls, twice as many were not confident in their ability to detect all breaches. It seems the more aware you are, the less confident you become.



Future Outlook

In 2002, UK businesses had a somewhat pessimistic outlook for the future of information security. Two years on, they are markedly more concerned.

Despite their high confidence in their current controls, over half of all businesses believe that there will be more security incidents in the future, compared with only 15% who believe there will be fewer. Large businesses are particularly concerned, as are financial services companies. Professional services and agriculture are least concerned, but even here twice as many are pessimistic as are optimistic.

This situation is compounded by concerns over the nature of future breaches. More than twice as many believe it will become more difficult to detect security breaches, as think it will be easier. This is slightly more pessimistic than two years ago. There is broad consensus about this across industry sectors, except for telecom providers who are slightly more optimistic.

Overall, UK businesses expect the recent growth in the number of security breaches to continue. If anything, they expect the rate of increase to accelerate.

Given this strongly negative outlook, we asked what would help businesses manage their information security risks. Nearly half believe that provision of more information security advice by third parties (such as the Government) would be helpful. Interestingly, large companies, which tend to be more advanced in their security controls, felt the greatest need for such guidance. The agriculture sector, where security is seen as low priority, saw the least benefit.

Nearly as many felt that more education for the general public about information security risks would be helpful. This is striking given the relatively low priority businesses give to educating their own staff, as we will see later.

A retail bank identified user education as the biggest threat to their Internet banking operation. They have recently suffered 'phishing' attacks, where fraudsters send out e-mails asking users to enter their passwords into fake web-sites. If public behaviour cannot be changed while retaining their confidence, the future of Internet banking in the mass market may be doomed.

A third believe that wider promotion of information security management standards such as British Standard BS 7799 would be helpful. Telecom providers and companies working for the government were most keen on this. Financial services, health and education saw the least need. Many of the businesses we spoke with in our face-to-face interviews would greatly value additional information, provided it is carefully screened and tailored to their needs.

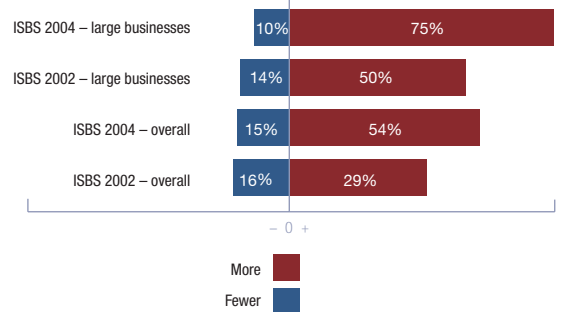
A similar proportion would like more industry initiatives to address security risks. This was strongest in the retail and publishing sectors. Large companies were particularly keen on their industry working together.

Very few organisations felt that there was enough being done to support them at present. Given their perception of future risk, most businesses want more help.

Security Strategy

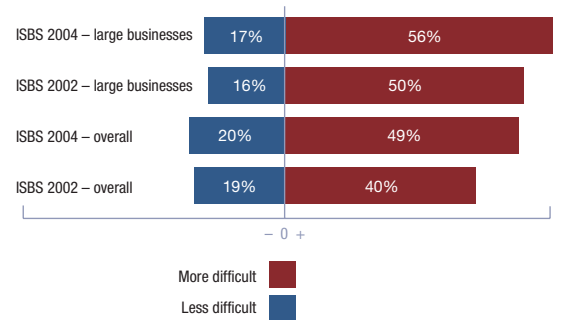
How many security incidents do UK businesses expect next year compared with last?

Figure 13



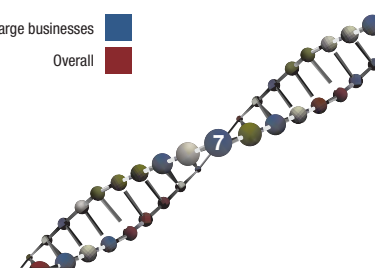
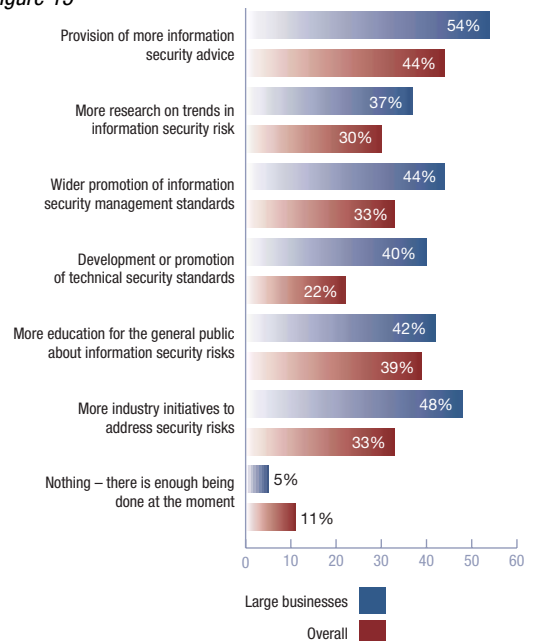
Do UK businesses expect it to be more or less difficult to detect security breaches in the future?

Figure 14



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

Figure 15



Security Strategy

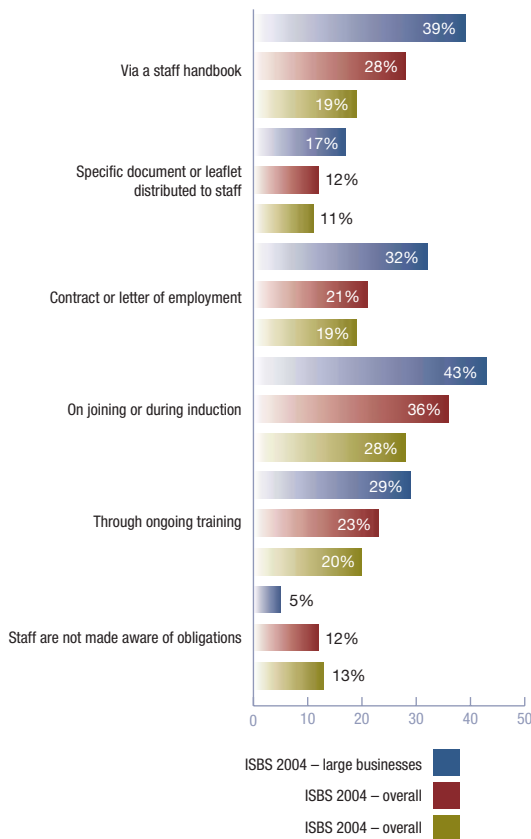
How many UK businesses have a formally defined and documented information security policy?

Figure 16



How are staff made aware of their obligations regarding information security issues, if at all?

Figure 17



Security Awareness

Human error rather than flawed technology is the root cause of most security breaches. So, the challenge for many organisations is to create a security-aware culture. Making staff aware of the risks and their responsibilities helps them act in a sensible and secure manner. This is not a new message. Yet, progress appears slow. Many businesses seem reluctant or unable to invest in staff awareness.

Overall a third of UK businesses now have an information security policy in place. This is a slight increase on 2002's 27%, and is the highest ever result. However, it still seems inconsistent with the perceived high priority of information security in three-quarters of businesses.

Financial services had by far the best result. Here, three-quarters have a security policy. The influence of regulators helps here. Online poll respondents were also particularly good, with 71% having a security policy. In contrast, only one in five retail or agricultural businesses had a security policy.

Without a clear and communicated policy, it can be difficult to take action against staff who misuse systems. All too often, a security policy is developed after the bitter experience of an incident.

A small reinsurer had difficulties when an employee was dismissed for visiting mildly pornographic web-sites at work. At an employment tribunal, he claimed that this was not breaking the law. Since the company did not have a clear policy on such matters, he argued that his dismissal was unfair. The company decided to agree a settlement rather than pursue the matter.

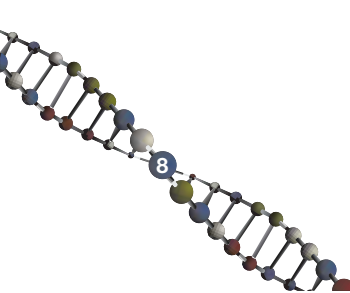
Having a security policy is not, in itself, enough. The policy needs to be up to date. As businesses change, the security risks they run change too. The organisation structure itself is rarely static, and new systems and technology also have a security impact. All too often, an organisation's security policy is out of step with the current business priorities.

Communication is also vital. The best policy in the world is useless if no-one knows about it. New employees should be briefed on the policy when they join. Existing employees should be informed about changes in policy in an efficient manner.

More UK businesses incorporate security policy in their staff handbook than two years ago. Communication to new employees on joining or during induction has also risen. Other possible mechanisms such as leaflets and on-going training have not increased in usage, however.

One in eight businesses is still failing to make staff aware of their obligations. This has not really changed since 2002. The changes result from those businesses that do communicate increasingly using multiple means to drive the messages home.

Background checks on potential staff during the recruitment process are important to keeping a strong culture. The number of UK businesses doing this has remained fairly constant. 43% of companies always follow up references, perform credit checks or take other action of this nature. 14% usually carry out checks, and 9% sometimes do so. This compares with 59% overall who carried out background checks in 2002. Sadly, a third of businesses are still taking a gamble with their security by recruiting staff without fully checking their identities and backgrounds. One might expect large companies would be better at this, but they show very similar results. Health, education, financial services and telecom providers were best at this. Manufacturing was the worst sector.



Security Strategy

A similar patchy pattern applies to compliance with the Data Protection Act. Six years since the Act was passed, there is still a long way to go. In fact, there has been a slight drop in the number of companies overall that said they have procedures in place here. 44% overall have documented procedures in place, with a further 15% planning to introduce them.

A third of companies have no plans to introduce such procedures. This is consistent with 2002, but still worrying. Almost every business holds sensitive information about its staff for payroll purposes, and so has a data protection obligation. Some UK businesses remain either unaware of their data protection responsibilities or see compliance with them as a low business priority.

Large businesses are much more likely to have procedures to comply with the Data Protection Act than small ones. Slightly more large companies do so than two years ago. Financial services companies are most likely to have procedures. Retailers and manufacturers are least likely.

Interestingly, a higher proportion of UK businesses have documented procedures to ensure compliance with the Data Protection Act than have a security policy. Principle 7 of the UK Data Protection Act requires businesses to keep personal data secure. It is difficult to see how data can be kept truly secure and under control without a security policy in place.

A financial services provider commented about the volume of different legislation and regulation. They find some of it appears to have contradictory requirements. Processing data across country borders is particularly complicated.

A security-aware culture is all about staff acting in accordance with the organisation's security policy. It is important, therefore, to have processes to monitor this compliance. Interestingly, more companies do this than have a formal security policy to check against. The vast majority of large companies monitor compliance. Twice as many small businesses carry out checks as have a security policy.

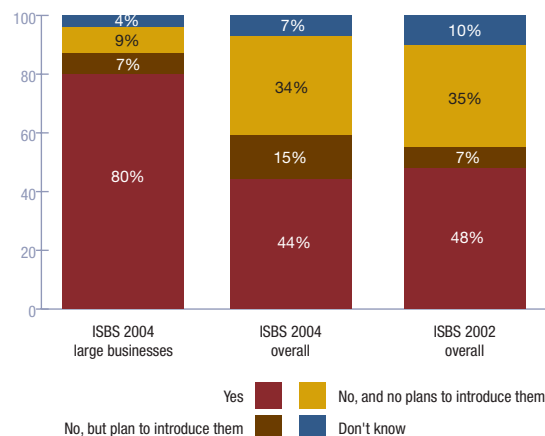
The most favoured technique for checking compliance was to monitor activity and log unusual events. This was particularly so in financial services, where more than half do this. Only 8% of agricultural businesses do this, though. A third of businesses carry out periodic audits of their security processes. This was most common in energy companies. Telecom providers were least likely to do this.

Use of automated tools to check for vulnerabilities is on the increase. A third of large businesses scan their internal network. A further third carry out penetration testing, war-dialling (i.e. checking for unauthorised modems) and social engineering tests. These blind tests provide a fresh perspective and a reality check on true levels of security. Overall, penetration testing has declined slightly since 2002, as some businesses have moved to use of automated scanning tools instead. Financial services providers, retailers and companies working for the government are most likely to use automated tools. Interestingly, technology companies are among the least likely to do so.

One business commissioned an outside company to carry out social engineering tests. It was incredible how much information they were able to access. They were also able to gain access to what the business thought were its most secure buildings. Their favourite trick to get past security guards was to pretend to be delivering a birthday cake from a staff member's wife or partner. The results really focused the minds of senior management on improving security.

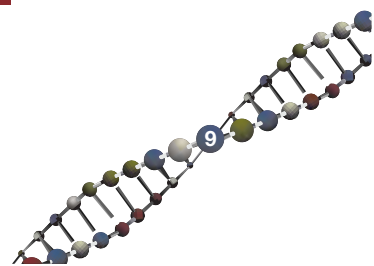
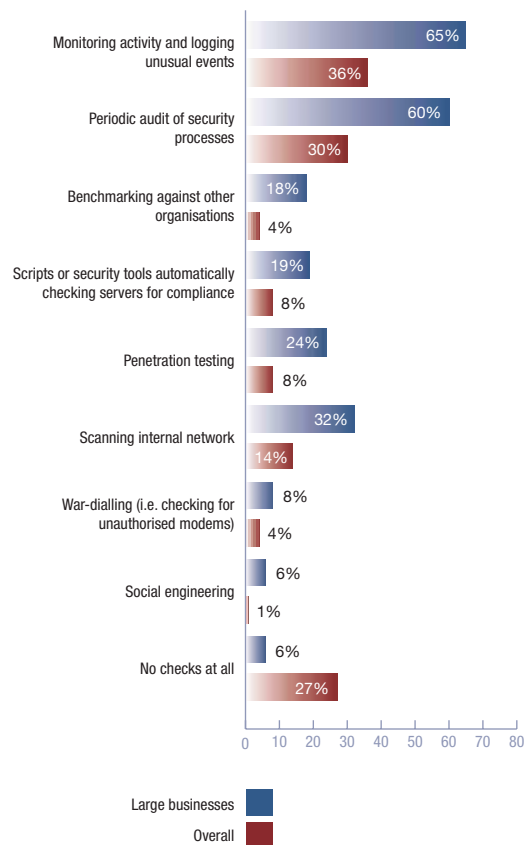
Do UK businesses have documented procedures to ensure compliance with the Data Protection Act 1998?

Figure 18



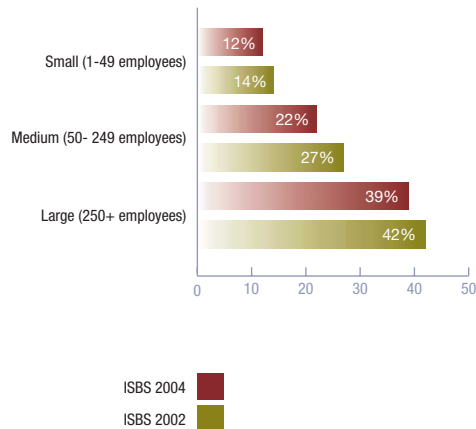
How do UK businesses check compliance with their security policy?

Figure 19



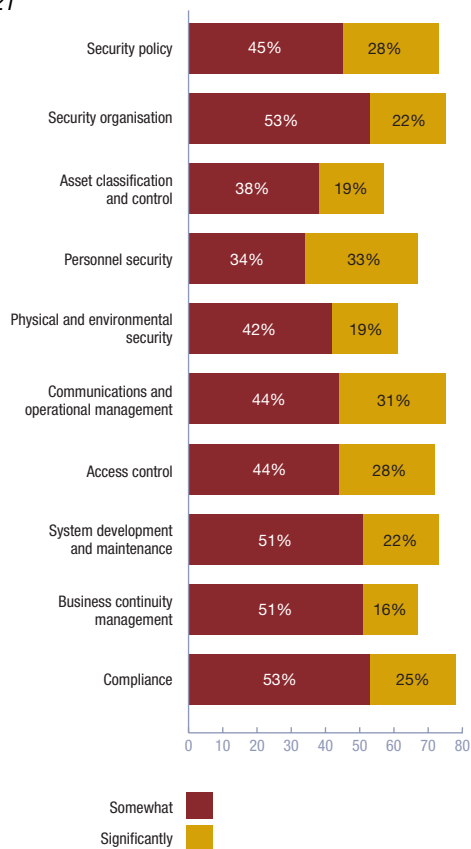
What proportion of UK businesses are aware of the contents of BS 7799, the British Standard for Information Security Management?

Figure 20



How has moving to compliance with BS 7799 changed attitude and behaviours?

Figure 21



BS 7799 Adoption

The British Standard for Information Security Management, BS 7799, has been out for many years. It is widely acknowledged as an important framework for security. In December 2000, Part 1 of the standard was adopted as an international standard, ISO/IEC 17799. As a result, overseas companies are increasingly using it to structure their security processes. Part 2 of BS 7799 defines a management framework for identifying security requirements and applying best practice controls defined in ISO/IEC 17799. It defines a step-by-step process that can be used to design, implement and maintain an effective information security management system.

BS 7799 helps organisations assess both their own information security procedures and those of their business partners. It is not prescriptive in nature. Instead, it sets out good practice principles and guidelines.

The 2002 survey found levels of awareness of BS 7799 were disappointingly low. Two years on, this picture has not changed. Only 12% of people responsible for information security said that they are aware of its contents. In large companies, this rises to 39%. Even this level is very low.

Awareness is greatest in telecom providers and companies working for the government. In contrast, only 4% of property and construction companies were aware of BS 7799's contents. The online poll respondents were at the other end of the spectrum, with 73% aware.

Why is BS 7799 not more widely recognised and used by UK businesses? The most commonly cited reason is the cost of obtaining a copy of BS 7799. While this is relatively small, it does appear to be a real inhibitor. In today's world, busy professionals expect to be able to pull up information instantly using an Internet search engine. Many businesses would prefer to have the standard available free of charge in electronic form.

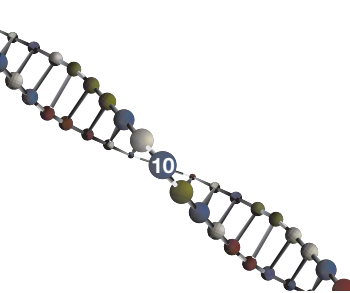
Secondly, many small businesses perceive BS7799 to be based around a large company model. They think it would take a lot of expertise, time and expense to implement.

Those organisations that are aware of BS 7799 are increasingly adopting it. Over half of them are now partly or completely compliant, up from 38% in 2002. This is a fairly consistent pattern across industry sectors. Effectiveness and efficiency are driving the adoption of BS 7799, rather than the desire for a kite mark. The number of organisations whose compliance is reviewed or accredited by an independent third party has remained fairly static.

One bank applied the 80:20 principle to BS 7799 adoption and achieved some quick wins. Its status as a British Standard made it easy to convince senior management. Real benefits were achieved. There has been very little rework needed since introduction. The bank would ideally like to become accredited in future, but this is not a priority today.

For the first time, this year's survey asked BS 7799 compliant businesses whether this has changed their organisation's attitudes and behaviours. Most businesses changed practices in several areas, as they recognised gaps in their existing processes.

There was strong agreement that implementing BS 7799 Part 2 had generated business benefits. 87% felt it had improved their business continuity. 85% believed it had minimised the damage to their company from security incidents. 53% commented that it had maximised their return on investment and business opportunities. These results are encouraging. They reinforce the view that organisations willing to invest time and effort in their security management reap real rewards.



Security Skills and Expertise

The 2002 survey uncovered a clear knowledge gap among those people responsible for information security. Two years on, this gap appears as wide as ever. This is not surprising given the pace of change in both technology and security threats. There still seems to be a shortage of IT staff with security expertise.

Three-quarters of businesses are confident that their technical security processes would catch all significant security breaches. Yet, some of their security controls appear to have significant weaknesses, and some have also had many security breaches. These respondents did not seem to fully appreciate the risks they face. Their misplaced confidence could result from lack of appropriate skills or expertise.

People gain skills in information security in many ways. It can be difficult to measure expertise in a fast-moving field like this. Awareness of relevant standards is one measure. As already reported, only 12% of businesses are aware of BS 7799 - a very poor result.

Formal qualifications are another useful indication of knowledge. Over the last few years, a number of specific qualifications in information security have been developed. These include specialist MSc degrees and several professional qualifications, such as CISSP, CISM and CISCO.

It is early days for these qualifications, however adoption seems to be growing. Overall, 11% of UK businesses have someone with a specialist information security qualification. In smaller companies, specialist security qualifications help generalist IT staff to understand the risks. Large companies are more likely to have dedicated security staff, where the payback from qualifications is greater. As a result, security qualified staff are twice as common in large businesses. It varies a lot by sector, from over a third of telecom providers to only one in twenty property and construction companies. Security qualifications were relatively common in online poll respondents; nearly half came from organisations with qualified staff.

A small software company finds it difficult to find staff with the right skills for its security roles. Some applicants have good technical skills but little business knowledge. Others have good business awareness but lack technical ability. The right combination of these skills is in short supply and difficult to evaluate at interview. More widespread adoption of qualifications may help.

In large businesses, the person responsible for information security was most likely to have an IT qualification. In small businesses, they were equally likely to have a business qualification, such as an MBA or accounting qualification. This is consistent with the profile of the respondents. In large businesses, they were mostly in IT management. In small businesses, they tended to describe themselves as business management.

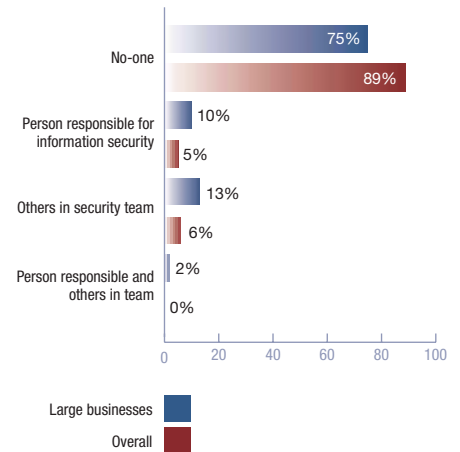
Only 42% of UK businesses have somebody with IT qualifications in their security team. This highlights the challenge small enterprises face. An effective security response often requires a good understanding of the technologies used. In small businesses, this may not be there. Security vendors targeting this sector need to make their products simple and effective.

A major retailer has a large team of IT staff and access to all the latest tools and information sources. Even so, their IT manager said he struggles to keep up to date with changes in technology and security. He feared that, if he worked for a small company, the ever-changing threats would swamp him.

Security Strategy

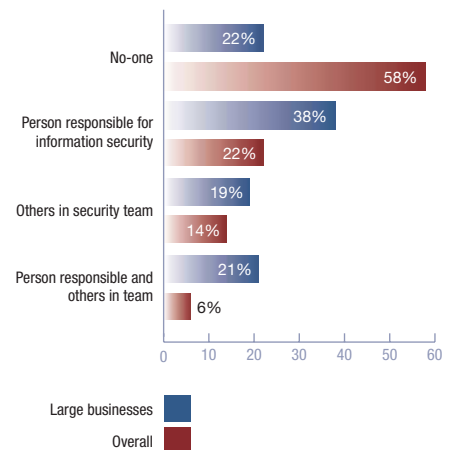
Does the team responsible for information security have any formal security qualifications?

Figure 22



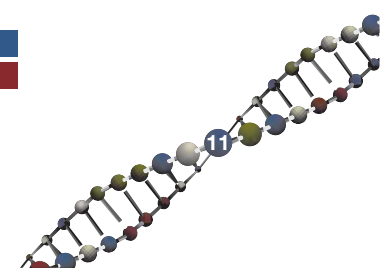
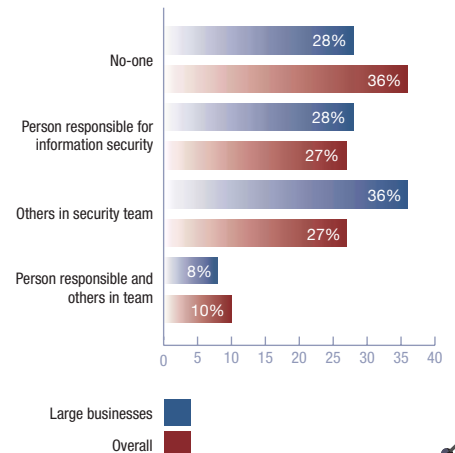
Does the team responsible for information security have any formal IT qualifications?

Figure 23



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

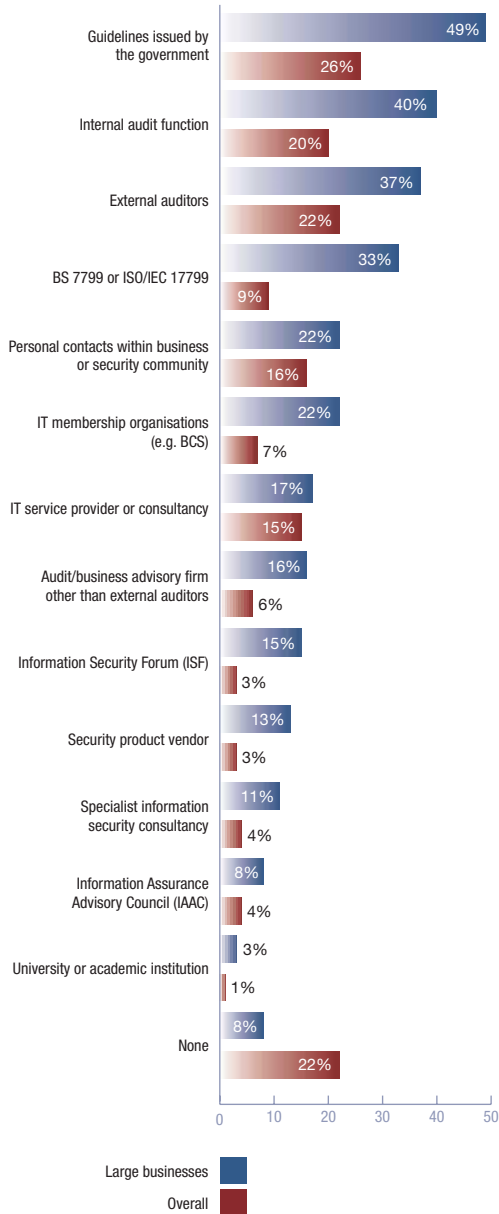
Figure 24



Security Strategy

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

Figure 25



Many businesses are too small to be able to justify in-house security specialists. Three-quarters of UK businesses obtain external advice on security matters. Interestingly, large businesses, where there tends to be more in-house security expertise, tend to consult externally more. A similar pattern occurs by industry. Mature sectors, such as energy, telecommunications and financial services, consult most. Agriculture and property companies consult least. It seems that the more you know about security, the more you realise you do not know. But, more importantly, one of the first things you learn is where to get the information you lack.

Over the last two years, the government has issued a number of useful guidelines on information security. Examples include the DTI's web guidance (including its Information Security Health Check) and National Hi-Tech Crime Unit (NHTCU) research. These appear to have achieved widespread penetration into the business community. They represent the single largest external source that businesses consult. A quarter of companies overall, and half of all large ones, have done so in the last year.

Internal and external auditors were another commonly used resource. One in five businesses said that their auditors had provided some form of guidance or expertise on information security matters. Many smaller companies do not require statutory audits of their financial statements, so this is a high proportion. Large companies were twice as likely to consult with their auditors as small businesses. Many businesses find it helpful to discuss these matters with business advisors they trust. Since they know their auditors, they are often the first point of call. Auditor independence does not appear to be a major concern in the area of security advice. Three times as many businesses discuss security issues with their external auditors as consult with another audit or business advisory firm.

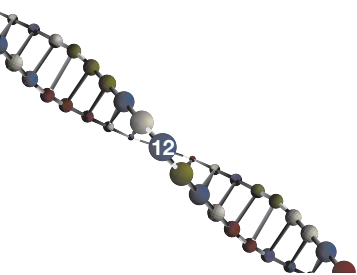
Three-quarters of the businesses that are aware of BS 7799 refer to the standard to help them manage their security risks. So, while awareness is low, usage among the aware is high. Usage is wider than just the businesses that describe themselves as partly or fully compliant.

Contacts within the business and security community were also widely consulted. One in six businesses did this. People often like to talk with someone they trust who is in the same position as them. Security is not normally seen as an area of competitive advantage, but more a shared problem. While many businesses are shy to comment publicly on security matters, private discussions are common. Many security officers draw heavily on the information security community. Similarly, some also consult with others in the British Computer Society or other IT membership bodies.

IT suppliers and security vendors provide much valuable guidance and expertise. However, only 15% of businesses rely on it. This may reflect concerns about the independence of such information. In particular, people worry that it is biased towards particular products or services.

One IT security coordinator interviewed often searches on the Internet for information about a security threat. He tends to be swamped with information that is excessively technical. He is never certain how much of it to believe. He would ideally like a single trustworthy and consolidated source of information in every-day language.

It is worth mentioning a few of the sources of information that appear under-used. For large companies, the Information Security Forum (ISF) provides very valuable benchmark information to its members. Similarly, the Information Assurance Advisory Council (IAAC) focuses on corporate governance aspects. A number of academic bodies, such as Royal Holloway, have established strong security credentials.



Investment in Security

Two years ago, we highlighted under-investment as a root cause for the rise in security incidents. Encouragingly, UK businesses are investing more in information security than at any time in the past. The vast majority had either increased their security spend in the last year or kept it at the same levels.

Only one in twenty businesses reported a decrease in their spend. The economic climate over the past few years has generally dampened IT expenditure. The high priority at the board level appears to have protected security expenditure against cuts.

Companies now spend on average 3% of their IT budget on security. This compares with 2% two years ago. Large businesses spend a greater proportion of their IT budget, about 4%, on information security.

A reasonable yardstick for security expenditure, based on experience in other countries, is 3-5% of the IT budget on average. In high risk sectors such as financial services, an average of 10% might be expected.

Overall, levels of investment in security are getting closer to these levels. However, there is still some way to go. The averages mask a mixed position. Roughly a quarter of companies are investing in security at, or above, benchmark levels. In large companies, this rises to roughly half. The majority of businesses, however, are still spending less than 1% of their IT budget on security.

This shortfall goes some way to explaining why security remains such a difficult area for UK businesses. It causes considerable frustration for the company staff responsible for keeping the business secure.

Most businesses include their information security spend within their IT budgets. This is not always the case in large businesses, where the information security team may be separate from the IT function. This may explain the higher level of large businesses that could not immediately say how much of their IT budget was spent on security.

One might assume that the variations in expenditure reflect the different natures of the businesses. The results show that, to some extent this is true. Sectors with high dependence on technology or significant confidential material tended to spend more. Sectors with less exposure tended to spend less. All industries reported a significant average increase in their security expenditure. Even in the sectors where growth in security spend is slow, less than 10% of businesses reported it was decreasing.

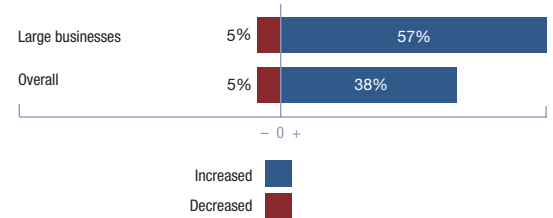
However, the industry variation is only part of the story. The reality is that, within every sector, there was an enormous range of expenditure. No sector was immune from under-investors. In every sector, at least a third of companies spend less than 1% of their IT budget on security.

Online poll respondents tended to come from organisations that invest more in security. Only one in six of them spent less than 1% of their IT budget on security. An equal number spent more than 10%.

Security Strategy

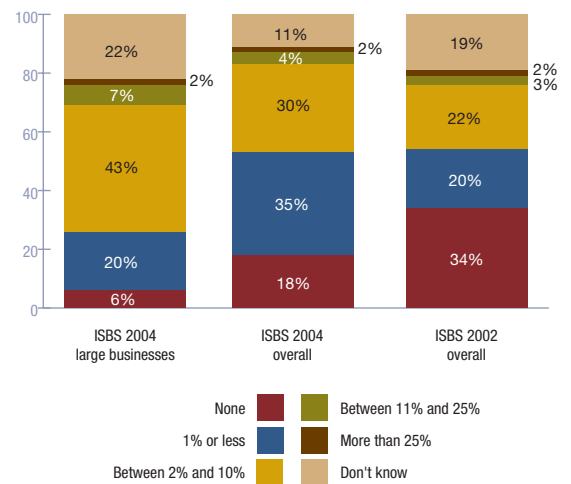
Has information security expenditure increased or decreased over the last year?

Figure 26



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

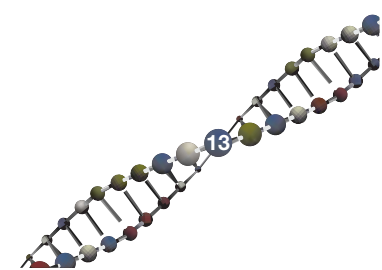
Figure 27



Which sectors spend most on security?

Figure 28

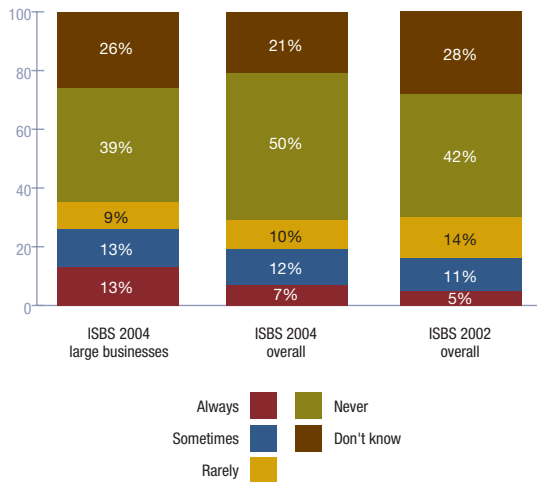
Rate of increase (net number of companies reporting increase)	Current security spend (% of IT budget)		
	Low (less than 3%)	Average (between 3% & 4%)	High (more than 4%)
High (more than +40%)	Environmental, Government	Publication, Agriculture, Services	Telecoms, Technology
Average (between +30% and +40%)	Retail, Property and construction	Utilities energy and mining	Financial services
Low (less than +30%)	Travel, leisure and entertainment	Manufacturing	Health and education



Security Strategy

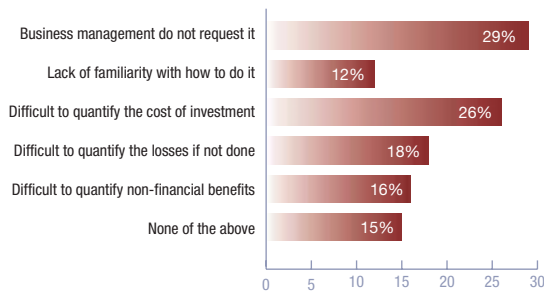
How often do UK businesses estimate the Return on Investment (ROI) on security expenditure?

Figure 29



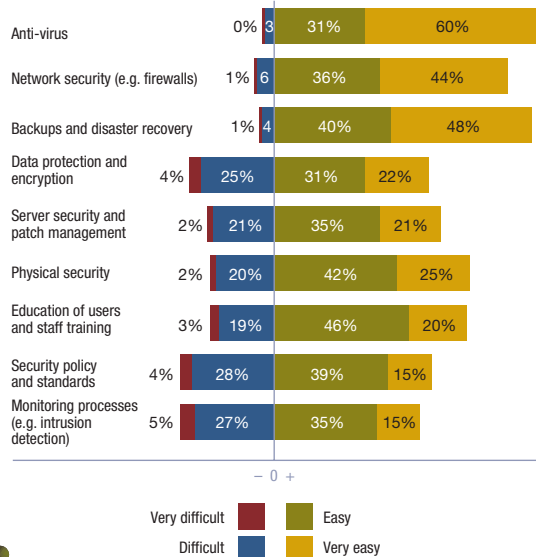
What are the main barriers to estimating return on investment on security expenditure?

Figure 30



How easy is it to build a business case for security expenditure?

Figure 31



One factor behind the under-investment is that security is often seen as an overhead rather than an investment. Less than half of all businesses ever evaluate their return on investment (ROI) on security spend. This has not significantly changed since two years ago. Also, this is one of the few areas where large companies are not significantly better at this than small ones.

It is not always the case that lack of return on investment calculations equates to lack of investment. However, without this information, it can be difficult to prioritise security spend against other projects. Senior management can also regard security as forced expenditure rather than something that can bring positive business benefits.

Surprisingly, the main reason why businesses do not estimate return on investment is that no-one asks for it. This was the case in almost a third of businesses. In a further one in eight companies, the person responsible for information security does not know how to do the calculation. Many of these people come from a technical rather than a commercial background, so have never learned the technique.

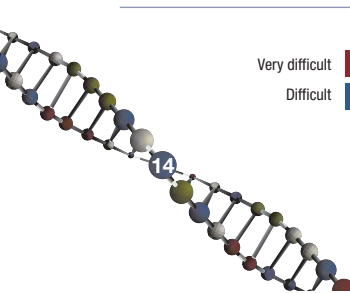
A quarter found it difficult to quantify the expenditure required. This was an unexpected result. The direct costs tend to be the easy part. The genuine difficulties lie in quantifying intangible benefits from investment or estimating the losses from not investing. In regulated or sensitive sectors such as financial services or telecommunications, potential reputational damage is very hard to quantify. One might assume that these sectors would, on average, carry out return on investment calculations less than other sectors. In practice, this is not the case.

One large bank does not use return on investment calculations for its security expenditure. The bank's reputation is paramount. Security breaches can undermine this, and so cause disproportionate damage. Security controls are considered essential, and cost is a secondary issue. As a result, the business case tends to focus on the likelihood of incidents if the expenditure is not made.

Guidance is increasingly available on how best to carry out these calculations. Security vendors are becoming smarter in providing the means to evaluate the return on their particular products. Of course, businesses need to check that any information they rely on is unbiased and fair.

Despite the lack of return on investment calculations, most businesses consider it is easy to build a business case for security expenditure. Particularly easy areas were anti-virus and backups, where senior management appear to be convinced of the need. The case was harder for areas such as data protection, encryption, server security, security policies and standards. Here, senior management appear less convinced of the benefits. But, even here, most found it easy to make a case.

Given the relative ease of justifying expenditure, the question remains: Why are so many UK businesses under-investing in security?



Incidence of Security Breaches

ISBS 2004 highlights the continuing rise in the number of UK businesses suffering a security breach. Three-quarters of companies and almost every large one had at least one security incident in the last year. Overall, a third of UK businesses and two-thirds of large ones had a serious security breach.

Malicious incidents are driving this increase. These include viruses, unauthorised access, misuse of systems, fraud and theft. Two-thirds of UK businesses had a malicious security incident in the last year. This is an increase from just under half two years ago. This continues the high rates of growth observed between the 2000 and 2002 surveys.

In addition to malicious breaches, over a quarter of businesses suffered a significant incident arising from accidental systems failure or data corruption. The 2002 survey focused solely on malicious incidents, so the last comparative data is from the 2000 survey. Current levels of accidental incidents are similar to those seen four years ago. The big difference is that in 2000 the accidental outweighed the malicious. Now, the reverse is true.

The breaches suffered are not isolated incidents. Each business had on average ten in the last year, roughly one a month. Excluding businesses that had no incidents the average number rises to fifteen.

Large businesses had roughly three times as many security breaches, suffering on average a breach a week. One reason is that large companies have more systems that might fail and more staff who might misuse systems. Another reason is that they tend to be targeted more by outsiders.

This bombardment of large businesses is illustrated by attempts to probe their Internet gateways. Large companies were probed on average once every couple of weeks, three times as often as the average small company.

The survey results suggest that large businesses are more successful at repelling attacks. Less than one probe in a hundred on large organisations resulted in successful penetration of their systems. For small companies, one probe in fifty successfully breached their defences.

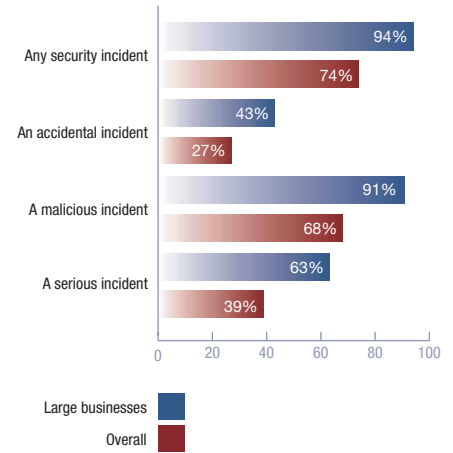
Financial services providers, technology companies and businesses working for the government had the highest incidence of security breaches. Agriculture, leisure, health and education experienced the fewest incidents. This correlates with the priority that organisations place on information security. In other words, businesses often wait until they have breaches before they take security seriously.

Online poll respondents had similar incidence of breaches as large companies in our telephone survey. 92% had an incident during the last year.

Security Breaches

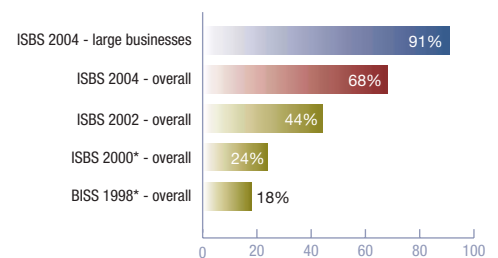
What proportion of UK businesses had a security incident last year?

Figure 32



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

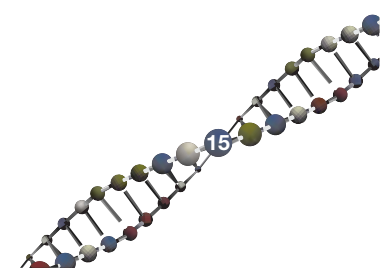
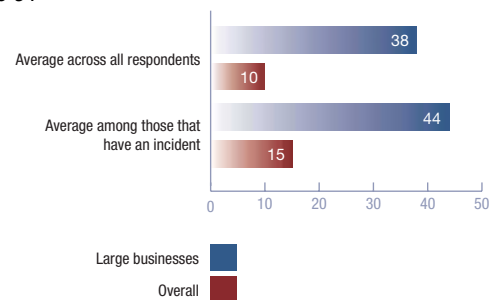
Figure 33



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

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

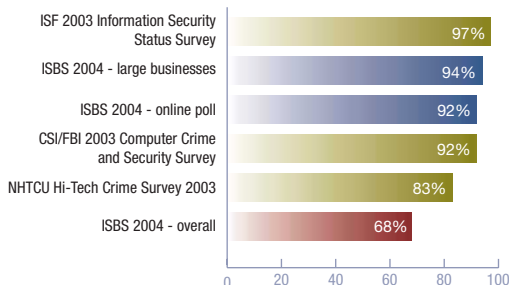
Figure 34



Security Breaches

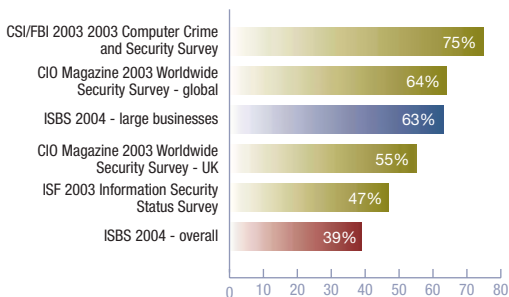
How do the levels of security incidents in ISBS 2004 compare with other similar surveys?

Figure 35



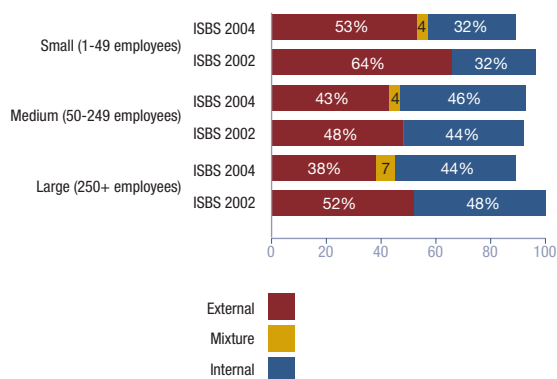
How do the levels of serious security breaches in ISBS 2004 compare with other similar surveys?

Figure 36



Was the cause of the worst incident internal or external?

Figure 37



Comparison with Other Security Surveys

ISBS 2004 is the largest survey of information security in the UK. It is likely, therefore, to yield the most accurate picture of the state of security in the UK. However, comparison with other similar surveys is a helpful check on the results. When comparing results, it is important to understand the differences between survey approaches.

Most other surveys have smaller sample sizes and therefore a greater margin of error. They also tend to be biased towards larger and more security-aware organisations. Finally, their definition of a security incident can vary from that used in ISBS 2004. Taking these factors into account, the results from ISBS 2004 are consistent with patterns observed in other recent security surveys.

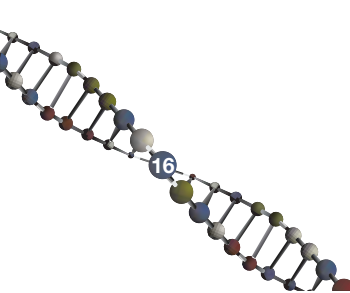
In the UK, NOP carried out a survey for the National Hi-Tech Crime Unit covering the same period. 201 companies responded. Half of these had more than 1,000 employees. 83% of respondents experienced hi-tech crime. This is close to the average of ISBS 2004 overall and large company results for malicious incidents, as one might expect given the nature of the NHTCU sample.

The Information Security Forum (ISF) is a body that gathers information about good security practice from its members. These are predominately very large businesses. Its 2003 Information Security Status Survey covered 189 respondents. 97% of these suffered at least one type of incident. This is very close to the ISBS 2004 result for large companies (94%). The ISF survey also showed that 47% had suffered at least one major incident. The definition of major is subjective, so direct comparison is hard. However, this appears broadly consistent with ISBS 2004 results, which show 37% of large businesses had a very serious incident and 63% had a serious one.

Comparing the UK experience with that of the rest of the world also has value. This shows that the Internet has globalised security trends.

One of the largest global security surveys is that done by CIO Magazine in conjunction with PricewaterhouseCoopers. This self-select survey took place from April to July 2003. Over seven thousand organisations from sixty countries took part. Five hundred of these were from the UK. Roughly half of the respondents had more than 1,000 employees. The survey asked respondents whether they had suffered a breach of security with a 'negative impact', broadly equivalent to ISBS 2004's serious incidents. 64% globally and 55% in the UK reported at least one such breach. UK respondents had roughly fifteen such incidents in the last year.

The CSI/FBI survey is the longest-running survey of information security in the US. It is a self-select survey. Respondents are typically security officers from large US companies. Of the 530 respondents to the 2003 survey, two-thirds had more than 500 employees. 92% had a security breach, very similar to the ISBS 2004 profile for large companies. The three most common breaches were virus infections, staff misuse of the Internet and physical theft of computer equipment. This is also consistent with the pattern shown for large UK companies in ISBS 2004. Finally, 75% acknowledged financial losses as a result of their breaches.



Internal or External

Conventional wisdom has, for years, considered that 'insiders' caused the majority of security incidents. ISBS 2002 identified a significant change from this position. It showed that roughly two-thirds of incidents in small companies were external. In large companies, roughly half were internal and half external.

ISBS 2004 shows a broadly consistent picture to that seen two years ago. Overall, approximately a third of UK businesses said that the source of their worst security incident was internal.

In the 2004 survey, respondents could, for the first time, identify an incident as having been caused by a combination of internal and external agents. 4% reported that their worst incident was a mixture of both. Large businesses were most affected by incidents of this kind. Examples given included viruses spread by staff action, systems failures partially caused by external events (such as power failure), and collusion between staff and outsiders. The 4% figure is probably understated. For virus infections (strictly an external threat), a quarter of respondents said the cause was internal only. Adjusting for these would increase the estimate of events involving a mixture of internal and external causes to 23%.

The figures are broadly consistent with the CIO Magazine Worldwide Information Security Survey. This reported that about two-thirds of respondents thought the most likely source of an incident was external, and a third considered it to be internal. The differences between the surveys are relatively small. The most important message is that internal and external threats can, and do, cause significant disruption. Accordingly, UK businesses need to deploy protective measures that recognise both sources of threats.

Type of Security Incidents

All types of malicious security incident show an increase since 2002. In contrast, levels of systems failure and data corruption show a slight reduction compared with levels reported in 2000. As a result, businesses are now twice as likely to have a malicious breach as an accidental one.

In all cases, large businesses are more likely to have suffered an incident than small ones.

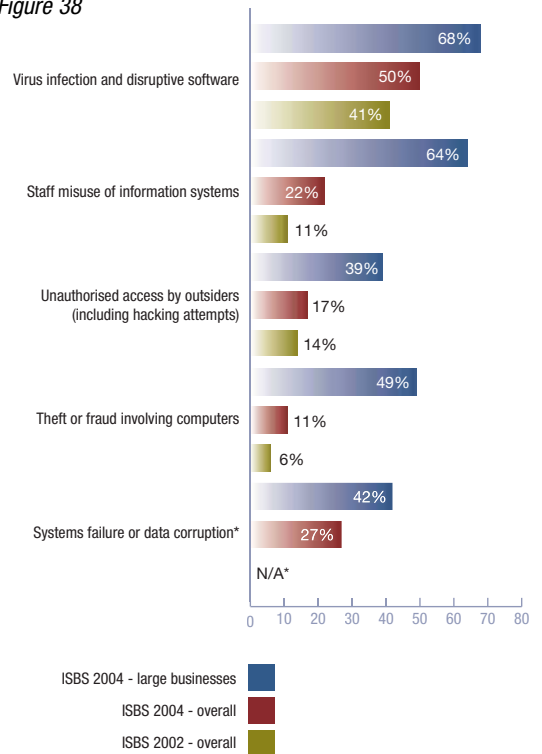
Virus infections continue to account for by far the largest number of security breaches. Two-thirds of organisations that had any security incident said that a virus infection was their worst one. This was a consistent pattern across all sizes of UK business. Two years ago, while viruses were the single largest cause of worst incidents, they only accounted for a third of them.

In addition to these incidents, many organisations reported unsolicited e-mail ('spam') as an increasingly significant issue for their business. While not a security breach per se, spam is clearly disruptive, and many IT and security staff are grappling with how best to address it. For further information, see the separate fact sheet on *Spam*.

Security Breaches

What type of breaches did UK businesses suffer?

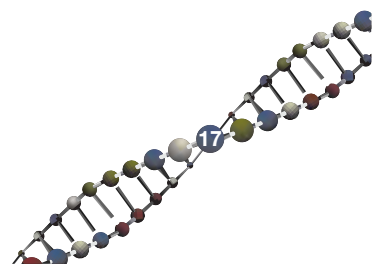
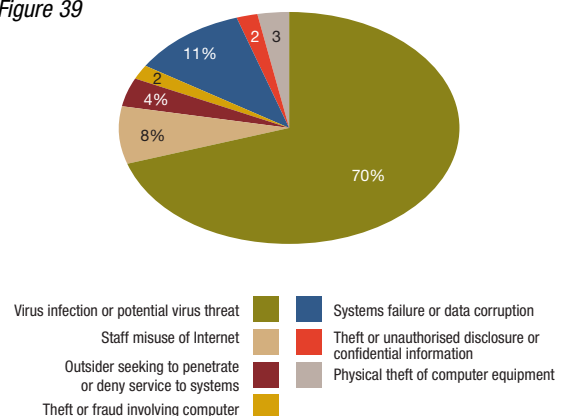
Figure 38



* ISBS 2002 focused on malicious breaches and so did not cover accidental incidents. The comparative figure from ISBS 2000 is 34%

What was the worst security incident faced by UK businesses?

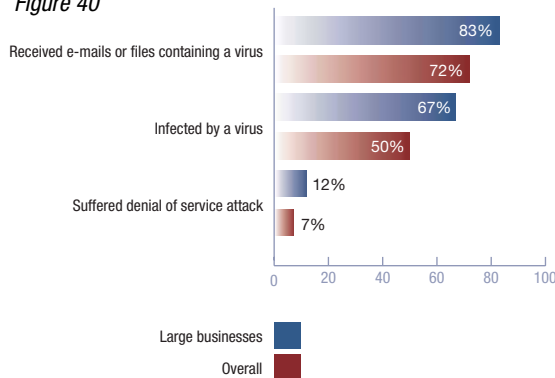
Figure 39



Security Breaches

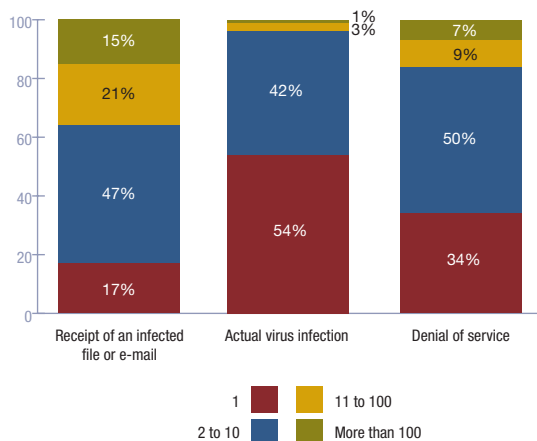
How many UK businesses have suffered from virus or denial of service attacks?

Figure 40



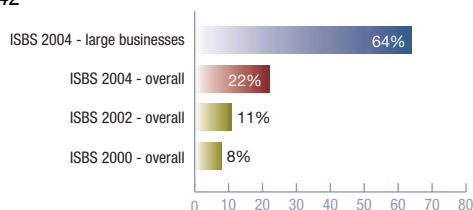
How many attacks did affected UK businesses suffer?

Figure 41



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

Figure 42



Virus Infection and Disruptive Software

Viruses and malicious code were by far the most common security incident reported. They also accounted for two-thirds of the most serious incidents.

Nearly three quarters of UK businesses reported that they had received an email or file that contained a virus or Trojan. Large companies were more likely to receive a virus than small ones. It is possible that the figures are understated since 7% of businesses did not have anti-virus software in place, and therefore might be unaware if they received a virus.

The industry analysis seems to support this conclusion. The proportion of companies reporting having received viruses was highest in financial services, which also had the highest adoption of anti-virus software. Every financial services company in the survey had anti-virus software in place and 97% reported receipt of an infected e-mail or file. At the other end of the scale, only 60% of agricultural firms reported receiving an infected e-mail or file, but only 78% had anti-virus software in place.

Receipt of viruses, worms and Trojans was rarely an isolated incident. One in six businesses that received any infected e-mails or files reported having more than 100 in the last year. In large businesses, this was one in three. As a conservative estimate, each UK company received on average two viruses a month. The average large business received one virus a week. Other surveys have reported even larger numbers. The NHTCU 2003 Hi-Tech Crime Survey indicated respondents were attacked by viruses an average of 254 times a year.

Not every company receiving a virus or worm was infected. In addition, the average number of outbreaks was significantly lower than the number of viruses received. Only 5% of UK businesses reported more than ten virus outbreaks in the last year. The difference provides an indication of the extent to which anti-virus protection is effective.

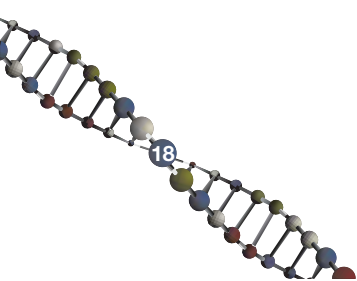
However, the number of infections is still significant. As a conservative estimate, each UK company had two virus outbreaks in the last year. The average large business had a virus outbreak every month. 7% of large companies had over 100 separate virus outbreaks in 2003.

Three worms (Blaster, Sobig and Bugbear) accounted for over three-quarters of the worst virus outbreaks. These highlight the evolving nature of the virus threat. They are all blended threats, capable of bypassing traditional anti-virus software and attacking network security instead. Blaster was particularly rampant amongst larger businesses, accounting for 56% of the worst incidents. Failure to keep servers and PCs up to date with the latest security updates was often the cause.

One organisation summed up the situation by saying it had been 'bitten' due to poor patch management.

Denial of service attacks, while still relatively rare, are a growing problem. In 2002, one in twenty businesses reported an attack. In 2004, the figure was nearer one in fifteen. Denial of service attacks were rarely isolated incidents. Most businesses affected were targeted many times.

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



Staff Misuse of Information Systems

Misuse of information systems has grown significantly over the last two years. Nearly a quarter of all businesses reported incidents of their staff misusing systems. This is twice as many as in 2002. The rise has been driven by the increased adoption of the Internet. Abuse of e-mail and web browsing make up the majority of misuse incidents.

Large companies were three times as likely to have had incidents involving staff misuse as small ones. The more staff you have the greater the chance of misuse. Large organisations are also more likely to have implemented monitoring tools, so tend to be better at detecting incidents.

Businesses that experienced Internet abuse tended to have many such incidents during the year, on average one a week. Interestingly, those small companies affected had roughly as many breaches as large ones, despite having fewer employees.

One in twelve companies said their worst security incident of the year involved staff misuse of the Internet. Roughly one in five of these had a very serious impact. Excessive personal e-mail was the cause of a third of these incidents. Access to inappropriate web-sites was the next most significant, accounting for a quarter. One in five of the worst incidents related to excessive web surfing. The remainder were mostly staff sending inappropriate e-mail or accessing another person's e-mail account.

Online poll respondents reported significantly higher incidences of system misuse than those responding to the telephone survey. Over half reported abuse of web browsing, similar to the level for large companies in the telephone survey. For e-mail abuse, 45% of online poll respondents reported incidents, an even higher level than for large companies in the telephone survey.

One company reported that some of its staff had used the firm's computer systems to run a private business on the side. The firm's Internet access made this possible.

Financial services companies were most likely to have experienced Internet misuse. 39% had abuse of web browsing and 26% had inappropriate use of e-mail. Most banks and insurance companies have many desk-based staff with access to the web and e-mail. The sector prides itself on its codes of ethics and tends to have high levels of monitoring for inappropriate behaviour by staff. At the other end of the scale, virtually no agricultural companies reported incidents. Here, staff tend not to be desk-based and so have less opportunity to access the web and e-mail.

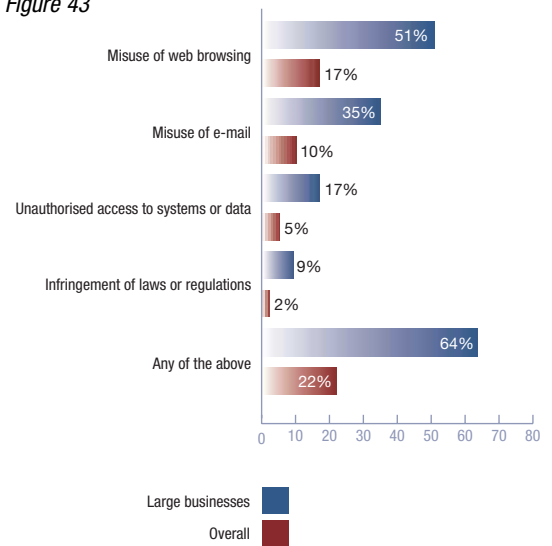
The greatest difference between the online poll and the telephone survey was in the area of unauthorised access to systems. Nearly a third of online poll respondents reported an incident in this category; in contrast, only 5% of companies overall and 17% of large ones reported such incidents in the telephone survey. Online poll respondents tend to have better controls in place. This suggests that some less controlled organisations may not be detecting breaches of this kind.

One in twenty small businesses, and nearly one in five large companies, had incidents relating to staff gaining unauthorised access to systems or data. Typically, this was due to staff guessing or obtaining another person's password. Actions of this type are harder to rationalise than, say, personal use of the Internet. As a result, the number of incidents any business suffers tends to be lower than other types of staff misuse. Still, over half had more than one such incident during the year.

Security Breaches

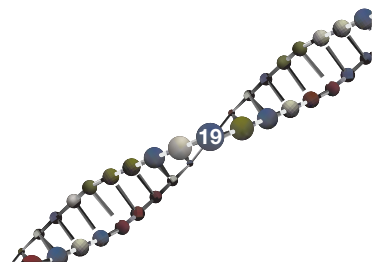
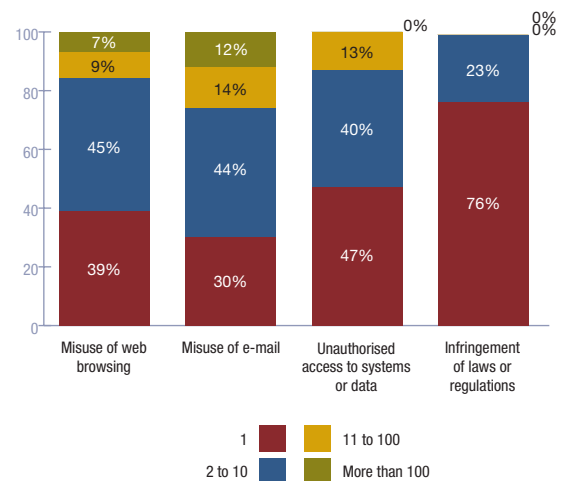
What type of staff misuse did UK businesses suffer?

Figure 43



How many misuse incidents did affected UK businesses suffer?

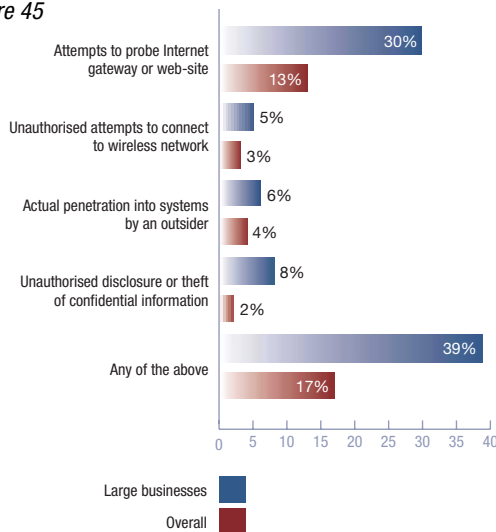
Figure 44



Security Breaches

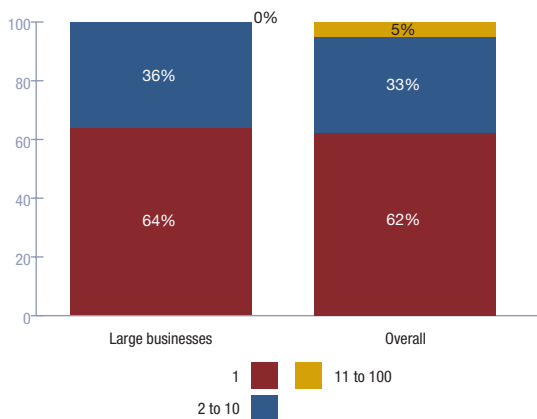
What type of unauthorised access attempts by outsiders did UK businesses suffer?

Figure 45



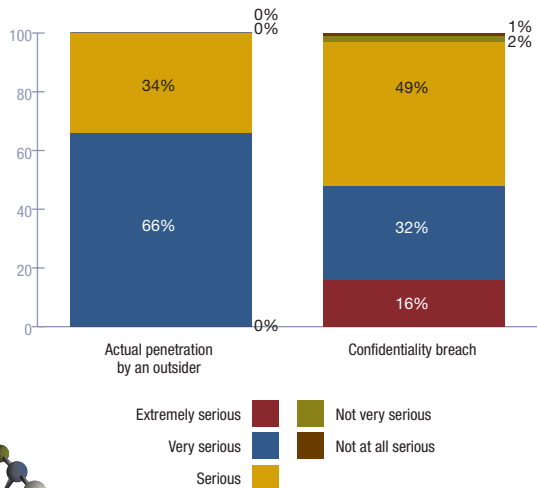
How many penetrations into their systems by an outsider did affected UK businesses suffer?

Figure 46



How serious were incidents involving unauthorised access?

Figure 47



When laws or regulations were infringed, these tended to be the Data Protection Act or the Computer Misuse Act. Large companies reported four times as many breaches. They are more likely to have procedures in place for compliance with legislation, and so are more likely to understand what constitutes a breach. For some medium-sized companies, infringement of these laws resulted in their worst security incident of the year.

For further information, see the separate fact sheets on *Staff misuse of the Internet* and *Identity management*.

Unauthorised Access by Outsiders

As more businesses connect to the Internet, they present a potential opening for outsiders, such as hackers, to break into their networks. One of the striking results of this survey is the increase in attempts to probe Internet gateways. Scanning activity across the Internet is on the increase. Two years ago, only one in twelve UK businesses reported probing attempts. Now, the figure has risen to one in eight, and to one in three large companies. It is likely, if anything, that these figures are understated. Many organisations have weak firewalls and lack intrusion detection - this may make them unable to spot such probes.

There were considerable differences in the levels of scanning activity detected. A fifth of those reporting scanning identified just one instance. Conversely, over a quarter identified more than a hundred separate probes during the year. A conservative estimate, based on these results, is that the average UK business has its Internet gateway probed once a week.

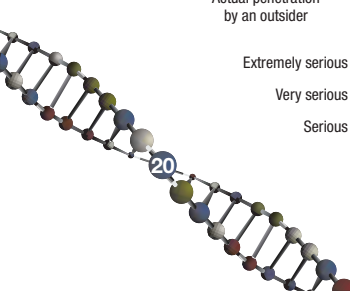
Medium-sized companies reported the greatest number of probes. This is consistent with the pattern two years ago. They are interesting enough for a hacker to target, but often lack the security controls of a large business, so are easier targets.

One medium-sized organisation explained they were scanned on almost a daily basis. Although few of the attempts led to penetration, the sheer volume of scanning activity made it difficult to be sure.

Wireless networks, and in particular, their perceived security weaknesses, have received significant press coverage in the last year. A third of all UK businesses are now using wireless networks. The technology and telecommunications sectors are the highest adopters of wireless networks, with usage in 60% of companies. There has been a big rise in the number of security incidents as a result. While only 3% of UK businesses reported attempts to hack into their wireless networks, this is higher than the percentage of companies that had a wireless network two years ago. There have been unauthorised attempts to connect to one in ten wireless networks. 15% of these reported more than a hundred attempts to break in. Not surprisingly given their higher adoption rate, twice as many telecoms providers had unauthorised access attempts as normal.

Thankfully, very few of these probes have resulted in actual penetration. Only 4% of companies reported being penetrated in the last year. Some with weak controls may not realise that penetration has taken place, so the true figure may be higher. In any event, this is a massive rise since 2002, when only 1% reported being hacked.

Nearly two-thirds of those reporting penetration had a single incident. Only one in twenty reported more than ten incidents. Unlike many other types of security breach examined in this survey there was very little difference in responses based on the size of business.



Security Breaches

Some sectors seem more attractive to would-be hackers than others. Financial services and telecoms providers were twice as likely to be probed as retailers. Financial services companies in particular appear to have recognised this. Despite the higher frequency of probes, they have a lower incidence of actual penetration. In contrast, technology companies reported three times the average number of actual penetrations by an outsider into their systems.

Most companies that were penetrated rated this as their worst security incident of the year (outweighing virus infections, etc.).

Unauthorised disclosure or theft of confidential information is relatively rare. Only 2% of companies had this type of breach. Furthermore, in the vast majority of cases, these were isolated incidents. However, when these breaches did occur they were almost always serious. Half were rated very or extremely serious. Over half of the organisations that had such a breach rated it as their worst security incident of the year (eclipsing others such as virus infections, etc.).

Large businesses were four times as likely to have a confidentiality breach as small ones. They were also over ten times as likely to have multiple breaches during the year. On average, technology companies were three times as likely to have an incident. In contrast, agricultural businesses reported no such breaches. This reflects the amount of highly confidential information these companies hold and the value of that data.

Online poll respondents recorded more unauthorised access incidents than those responding to the telephone survey. 56% of online poll respondents reported attempts to scan or probe their Internet gateway. This is significantly greater than even the large companies in the telephone survey. Interestingly, there is a direct correlation with the numbers reporting actual penetration of their systems. One in ten of the online poll respondents reported a breach of this nature; the percentage in the telephone survey were 6% for large and 4% overall for business. Unauthorised disclosure or theft of information was broadly consistent with large companies.

For further information, see the separate fact sheets on *Intrusion prevention*, *Identity management* and *Remote access*.

Theft and Fraud Involving Computers

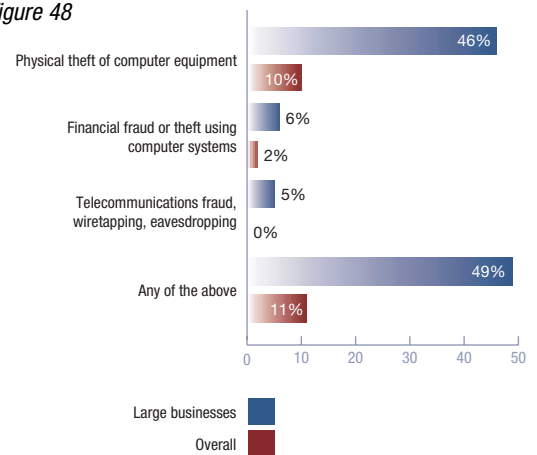
Physical theft of computer equipment was the most commonly reported incident in this category. One in ten businesses had computers stolen in the last year. Large businesses were over four times as likely to have been affected as small ones. This suggests thieves will go where they anticipate the richest pickings. Similarly, technology companies (who tend to have more modern and expensive equipment) reported twice as many thefts as the average.

Thieves targeted one large professional services company. Over a weekend, they entered the building and systematically stripped it of computer equipment. The thieves focused on laptops, leaving other valuable electronic equipment untouched. Their portability and the ease with which they can be resold made laptops an attractive target.

Physical thefts were, by and large, isolated instances. Over two-thirds of businesses affected had just a single instance. No-one reported more than ten thefts. Their severity varied, with only 3% of businesses overall considering a physical theft their worst incident. Technology and energy companies had most of the worst such breaches.

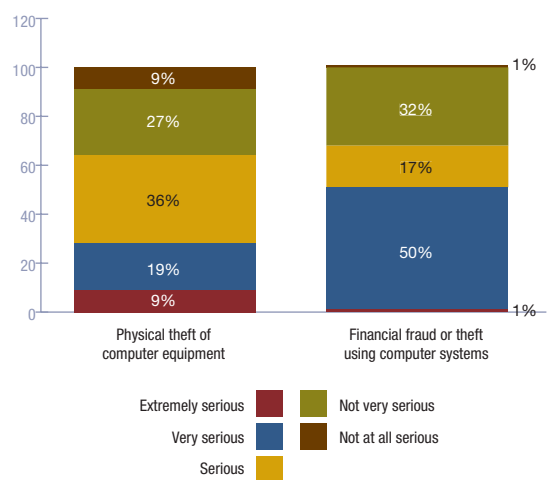
What type of theft and fraud did UK businesses suffer?

Figure 48



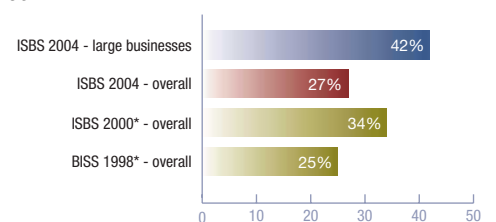
How serious were incidents involving theft or fraud?

Figure 49

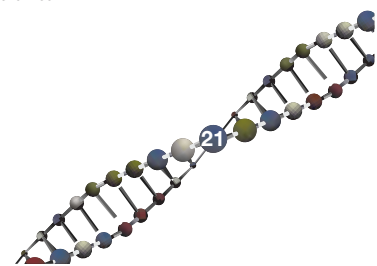


What proportion of UK businesses had a systems failure or data corruption incident in the last year?

Figure 50



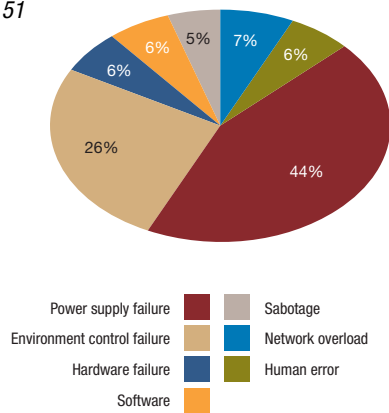
*The 1998 and 2000 DTI survey figures were based on the preceding two years rather than the last year. ISBS 2002 did not cover accidental systems failure, so there are no comparative figures for 2002.



Security Breaches

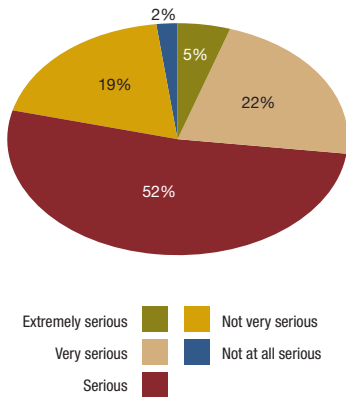
What caused system failures or data corruptions?

Figure 51



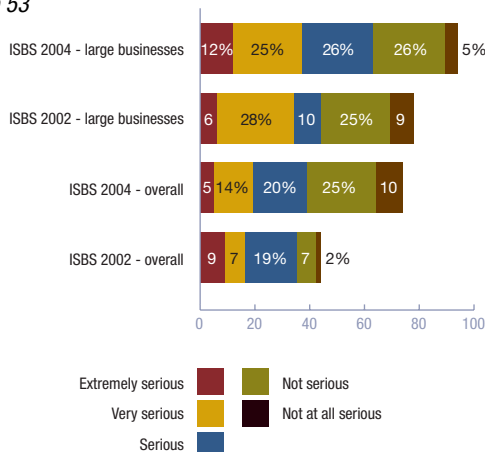
How serious were incidents involving systems failure or data corruption?

Figure 52



What proportion of UK businesses had a serious incident?

Figure 53



Financial fraud or theft using computer systems remains relatively rare. Only 2% of companies had a computer fraud in the last year. In three-quarters of cases, the fraud was an isolated incident. However, two-thirds of those that had a fraud rated it as their worst incident of the year, outweighing virus infections, etc. Most of these frauds were very serious to the business concerned.

Large companies were three times as likely to have a computer fraud as small ones. They were also more likely to have multiple frauds. Telecoms providers had the greatest number, with some reporting more than ten instances during the year. A third of manufacturers that experienced a computer fraud had multiple instances.

Instances of telecommunications fraud, wiretapping and eavesdropping were low, and tended to have relatively minor impact. Overall, the financial services sector reported the greatest incidence of such problems. Large companies in other sectors also suffered breaches of this kind.

For further information, see the separate fact sheets on *Backups and recovery* and *Identity management*.

Systems Failure and Data Corruption

A quarter of UK businesses had suffered a significant systems failure or data corruption. In common with most types of breaches, large companies were more affected than small and medium size businesses. Large organisations generally have higher availability requirements and more systems to go wrong. They also tend to rely more on heavily customised or bespoke systems, rather than off-the-shelf packages. So, while they tend to have more rigorous change control and backup processes, they still end up having more incidents.

The sectors most likely to have problems were financial services and technology. These were twice as likely to have an incident as retail and publishing companies, who had the fewest problems. Again, the number and complexity of systems appear to be the drivers.

Those suffering problems did not have many such incidents during the year. On average, they had roughly one a quarter. Large businesses tended to have slightly more. Only 6% had more than ten incidents.

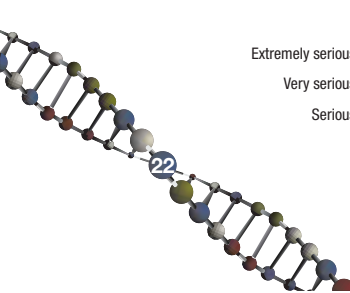
Quite often, systems failure or data corruption was the worst incident of the year. 11% of organisations that had any security incident rated a systems failure as their worst of the year. This proportion showed little variation between large, medium and small businesses.

However, there was a marked difference across industries. Systems failure was most likely to have been the worst incident of the year in government, manufacturing, technology and retail sectors. It was least likely to have been the worst in the financial sector and in other services.

Over half (53%) of online poll respondents reported systems failure or data corruption incidents. This was significantly higher than the telephone survey results.

The two most significant sources of systems failure were hardware failure and software bugs. Power supply issues were also a significant cause of problems in large companies.

For further information, see the separate fact sheet on *Backups and recovery*.



Impact of Breaches

For risk assessment to be effective, businesses need to understand not only the trend in number of incidents but also their impact.

Half of all organisations that had a security incident considered their worst one to be serious. A quarter had a very serious breach. There has been a slight decline in the average seriousness of incidents compared with two years ago. However, this is slightly deceptive. The number of breaches has risen so fast that, overall, more companies had serious incidents than two years ago. This is particularly true for large businesses, where two-thirds had a serious breach.

Many security surveys use the cost of an incident as a measure of its overall impact. They normally ask respondents to estimate its total cost, but this is a very difficult question to answer. Breaches can have many different impacts. Direct cash expenditure is only one of these. Other costs, such as time spent investigating and responding, need to be included. Some, such as the cost of business disruption or damage to reputation, are hard to quantify. Breaking down the cost of breaches into its component parts sheds light on this.

Business Disruption

The biggest impact from the worst security incidents was business disruption. Half of them resulted in significant interruption to normal service. A quarter resulted in more than a day's disruption. In a small number of cases, it took more than a month to restore operations to normal. Systems failures, virus infections and confidentiality breaches caused the longest disruptions. In contrast, attacks on web-sites (such as denial of service) tended to be short-lived.

The longer the interruption, the more serious it tended to be. Confidentiality breaches were most likely to result in major disruptions to the business. These were typically as a result of senior management distraction rather than systems availability issues. Other incidents that were more likely to cause major disruption were systems failure, staff misuse and penetration of systems by outsiders.

Following infection by the Blaster worm, a publishing company suffered very major disruption to its business for more than a month.

The pattern of business disruption was very similar between all sizes of business. On average, small businesses suffered one to two days of disruption from the worst security incident. Large businesses suffered an average of one to three days disruption from theirs.

It is possible to make a crude estimate of the cost associated with the business disruption, using average turnover and assumptions about the impact of disruption. On this basis, the disruption from a small company's worst security incident cost it roughly £5,000 to £10,000 on average. The average large company lost £50,000-£150,000 in business disruption from its worst breach.

Incident Response Costs

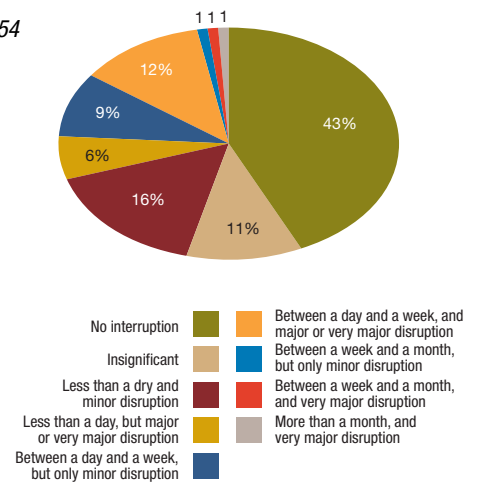
Most incidents were relatively easy to investigate and fix. Two-thirds of worst incidents required less than a man-day. A similar proportion needed no cash expenditure to recover the situation.

However, the other third of worst incidents involved significant costs. Some small companies had breaches that involved more than 50 man-days to address. Similarly, some small businesses spent more than £100,000 of cash expenditure addressing the issue. This must have placed a heavy burden on their business.

Security Breaches

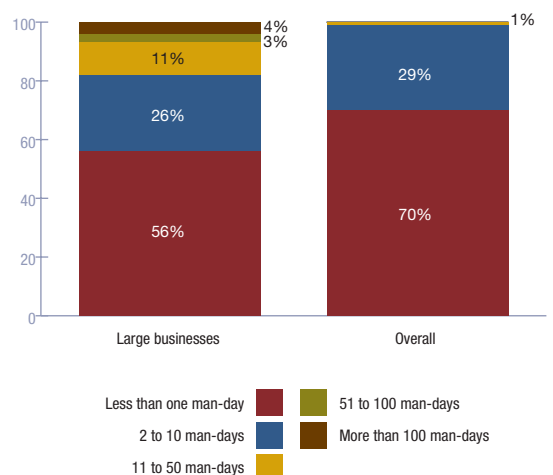
How much disruption to the business did the worst security incident cause?

Figure 54



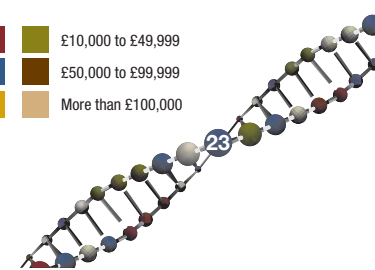
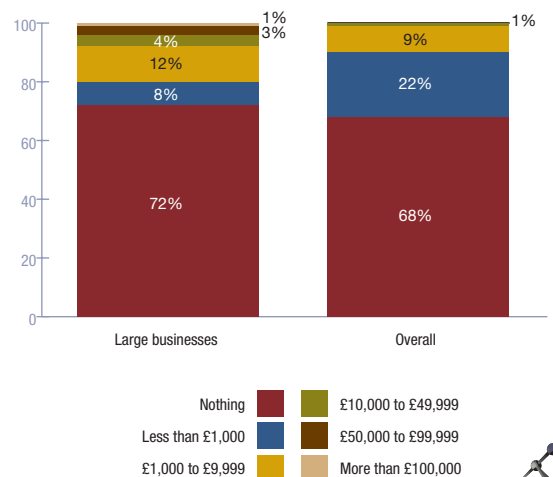
How much time was spent responding to the worst incident?

Figure 55



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

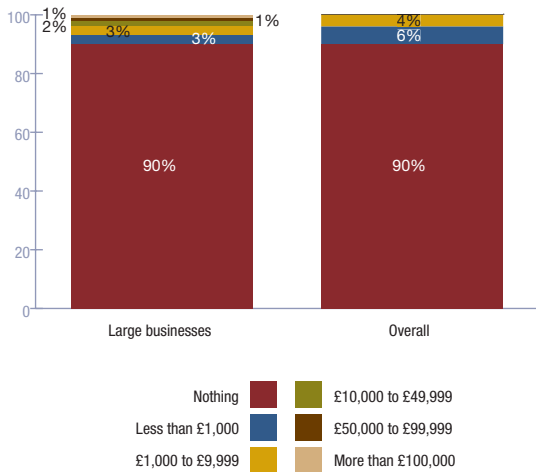
Figure 56



Security Breaches

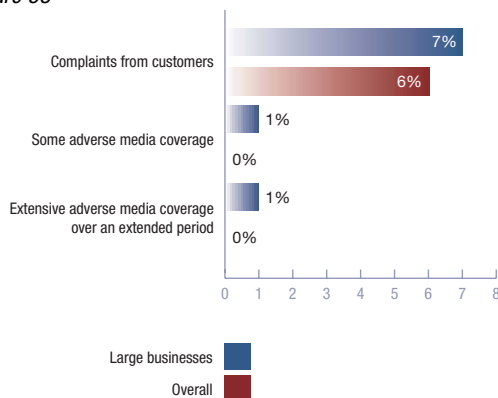
How much direct financial loss resulted from the worst incident?

Figure 57



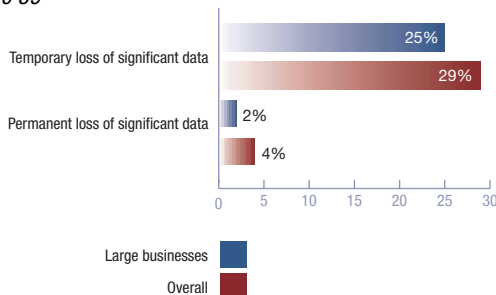
To what extent did the incident damage the reputation of the organisation?

Figure 58



Did the incident cause any significant loss of data, either temporarily or permanently?

Figure 59



As a result of this, the average UK business spent two to four man-days responding to their worst security incident of the year. This equates to roughly £500 to £1,000. Large companies tended to have to spend more time on incident response. The average large company spent 10 to 20 man-days on their worst breach. This equates to roughly £3,000 to £6,000.

Confidentiality breaches and legal infringements consumed the most time on investigation and response. Attacks on web-sites tended to require the least.

In addition to staff time, the average UK business spent £1,000 to £2,000 recovering from its worst security breach. The average large business spent £5,000 to £10,000.

Physical thefts of computer equipment tended to result in the highest cash expenditure. The average cash spent after a physical theft was three times that spent after other incidents. In contrast, virtually no attacks on web-sites or systems penetrations resulted in more than £1,000 of cash spent to recover the situation.

It is not clear whether businesses fully recognise all their incident response costs. It is possible these are under-estimates.

One security officer conceded that the greatest impact of his worst security breach was the time and money spent investigating and fixing it. However, he was unable to quantify either cash cost or the value of time.

Direct Financial Losses

Some security breaches caused direct financial loss, for example through fines or compensation payments. In the vast majority of cases, no such costs were incurred. However, some incidents did result in a significant cash loss. As you might expect, these included financial frauds and physical thefts. The highest direct cash losses were as a result of confidentiality breaches.

One medium-sized business reported direct financial losses of more than £250,000 as a result of theft of their confidential data.

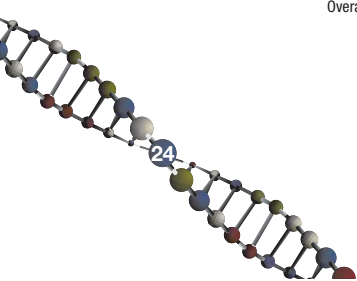
The relative rarity of direct financial losses means that the average company incurred only £200 to £500 of such costs. The average large company incurred £2,000 to £4,000.

Damage to Reputation

Having a security breach featured in the news headlines is probably the nightmare scenario for most security officers. Businesses whose brand is well known tend to fear damage to their reputation the most. Companies like to keep their security incidents secret from their customers and the media.

In this respect, UK businesses have been lucky so far with their security breaches. Only one in fifteen had resulted in customer complaints. Unauthorised disclosure of confidential personal information was most likely to cause these. One in six financial frauds also caused complaints. In many cases, however, it was availability issues due to accidental systems failure or virus outbreaks that upset customers.

Some large companies did report adverse media coverage as a result of their worst security breach. Virus infections and staff misuse of the Internet were the subjects that excited the press. The companies worst affected were in the manufacturing, health and education sectors.



Putting a cost on damage to reputation is very hard. There are plenty of examples of companies that have shrugged off adverse media coverage with minimal impact. There are others that have been literally destroyed by a single story. Because of the low number of incidents, our estimate of the average cost is also low, roughly £100 to £300. For large businesses, the average cost is greater, roughly £5,000 to £20,000.

Loss of Data

Nearly two-thirds of businesses recorded no significant loss of data as a result of their worst security incident. Most of the rest suffered temporary loss, and were able to restore from backups. However, roughly one in twenty lost significant information permanently as a result of their worst security incident.

Roughly half of all confidentiality breaches involved theft of data. Similarly, half of systems failures resulted in data corruption. A third of physical thefts involved computers that held significant data. Systems failures were most likely to cause permanent loss or corruption of significant data.

Total Cost of Incidents

Combining these different impacts, the average UK business suffered £7,000 to £14,000 of cost from its worst security incident. For large companies, the equivalent cost was more like £65,000 to £190,000.

The average cost has fallen slightly since 2002, when the estimate was £30,000. This is in line with the dip in the average seriousness of breaches. However, the rise in number of incidents means that the total cost to UK business is of the same order of magnitude as in the past. In other words, security breaches continue to cost several billions of pounds.

The majority of businesses are pessimistic about the outlook for the next year. It is likely in this context that the total cost to UK business will continue to rise. Companies need to redouble their efforts to reduce both the number of incidents suffered, and the impact those incidents have.

Incident Response and Contingency Planning

The 2004 survey has shown that UK organisations are increasingly likely to suffer a security incident. These incidents continue to have a significant impact on business. In this environment, companies should deploy effective defence against attacks, however these defences will never be infallible. It is, therefore, vital that UK businesses are well prepared to respond to incidents and have contingency plans in place. Such plans can significantly reduce recovery time and effort.

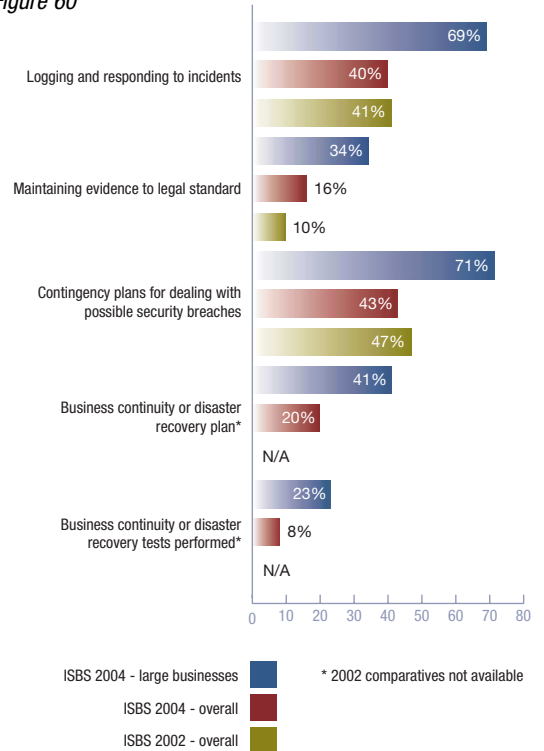
When a security incident arises, the ability to respond quickly and effectively is paramount. Procedures to log and respond to breaches are critical to this. Roughly the same number of UK businesses has these in place as two years ago. Two-thirds of large companies have a formal process for this, including escalation procedures.

In an increasingly litigious environment, businesses may need to take, or defend against, criminal or civil action. To do this, they need to maintain evidence in a form that would meet legal standards. Forensic procedures to do this are in place in one in six UK businesses. Large companies are significantly more likely to do this. These figures are still not high. However, they do mark an improvement since 2002, when just one in ten was able to maintain evidence to legal standards.

Security Breaches

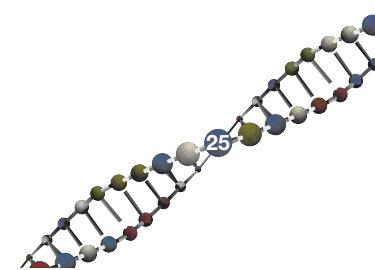
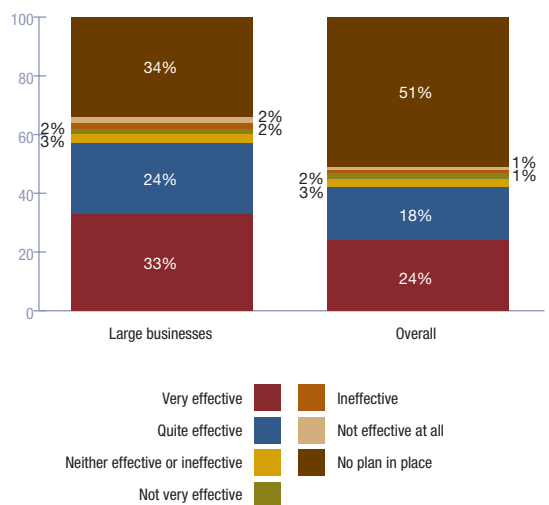
What procedures do UK businesses have in place to respond to security incidents?

Figure 60



How effective were contingency plans at dealing with the worst security incidents?

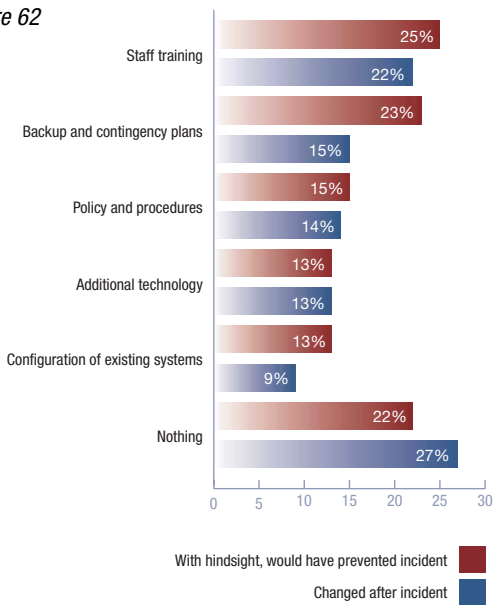
Figure 61



Security Breaches

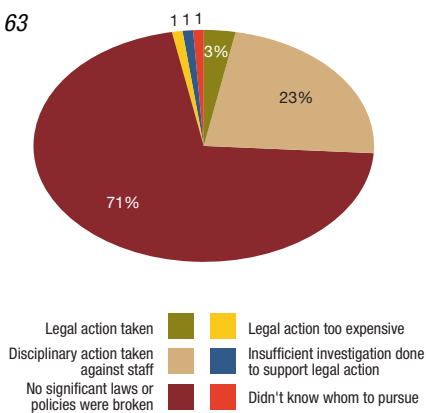
Did UK businesses address the weakness that caused their worst incident?

Figure 62



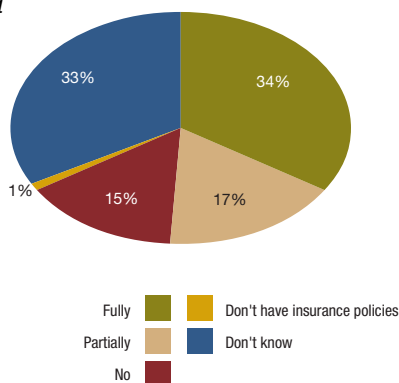
Was legal or disciplinary action taken after the worst incident?

Figure 63



Do UK businesses believe their current general insurance policies cover them against damage arising from security breaches or data loss?

Figure 64



Contingency planning provides some comfort in that, in the event of security breaches, the business impact will be minimised. Roughly half of UK businesses had contingency plans for dealing with security breaches. This is broadly consistent with two years ago. Large companies tend to be better prepared. One might expect that contingency planning would include effective disaster recovery planning and testing. However, this does not appear to be the case. Only one in five UK businesses has a disaster recovery plan and fewer than one in ten test their plans. Large companies are twice as likely to have plans and test them as small ones.

When their worst security incident struck, roughly half of the affected businesses had a relevant contingency plan in place. This was a significant drop from 2002, when 83% had such plans. The effectiveness of plans, when they were in place, was similar to two years ago.

Nearly a quarter of companies indicated that they believed better backup and contingency plans could have prevented their worst security incident. Two-thirds of these organisations improved their backup and contingency plans following the breach.

Overall, after an incident, businesses were good at changing their security controls so they would not suffer a similar breach in future. The issue is more that companies tend to wait until they have experienced an incident before they appreciate the risk.

Companies were generally good at taking disciplinary action against staff when policies were breached. However, very few took any form of legal action. For virus infections, there was a general perception that no-one had broken the law. There was little appetite to pursue the virus writers. When staff caused breaches, internal disciplinary measures were normally considered sufficient.

Insurance

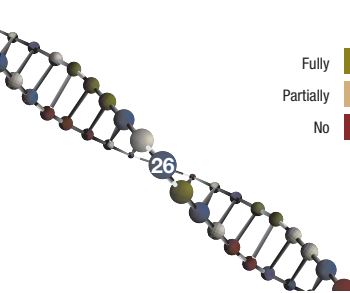
With any risk, one can accept it (do nothing), mitigate it (by putting countermeasures in place that prevent it arising) or transfer it (typically through insurance). Security is no different from any other risk in this respect.

Over the last few years, insurance companies have increasingly excluded risks associated with security incidents from general security policies. This has created uncertainty within many businesses as to whether they have insurance cover. In some cases, it has effectively moved organisations from risk transfer to implicit risk acceptance. To meet the gap, some insurance companies have introduced IT specific insurance. However, the take up of these specialist policies is still very low.

Given this, it is perhaps surprising to find that a third of UK businesses believe that their general insurance policies provide full cover for damage arising from security breaches or data loss. This is similar to the level reported two years ago. The third of UK businesses that do not know whether they are covered are probably more realistic. One in six know they have no cover at all, and a similar number believe they have partial cover.

When discussing insurance, one security officer commented that this was outside her remit. Her role covered information security rather than more general information risk. As a result, she was not consulted when insurance policies were renewed or negotiated.

The survey has shown how dependent UK businesses are on their computer systems, and how costly security breaches can be. In this environment, it is important that businesses make sure they are fully aware of the limitations of their existing insurance policies. Where necessary they should supplement them with additional policies that provide cover for the emerging security threats.



E-mail and Web Usage

Web and Internet e-mail usage is now commonplace among all sizes of business. Overall, nine out of ten UK companies provide staff with Internet access. Sadly, a side effect of this is greater exposure to viruses, inappropriate usage and spam.

Viruses and malicious code are by far the biggest concern. 93% of UK businesses, and 99% of large ones, have anti-virus software in place. Almost every business that connects to the Internet uses anti-virus software. The larger the business the more likely it is to adopt a multi-layer defence. Over half of large businesses scan incoming e-mail and web downloads at their Internet gateway, as well as having anti-virus software on the desktop.

Despite this, incidents of virus infection are on the increase. There are two main reasons.

Firstly, anti-virus software is only as good as its last update. While 59% of companies automatically update it whenever a new virus signature is identified, in some cases it is never updated.

Secondly, the nature of viruses is evolving. Increasingly, businesses are facing blended threats that possess the characteristics of viruses, worms and Trojans, and blend these with hacking techniques. Blended threats, like Blaster, can bypass anti-virus software and attack weaker areas of network security.

Staff misuse is also a significant concern, particularly in large companies. Virtually every organisation that has an overall security policy also has a specific acceptable usage policy for e-mail and web browsing. Companies that have restricted staff access and put policies in place tend to have significantly fewer e-mail abuse incidents.

The average levels of control over e-mail and web browsing are lower than two years ago. This is largely due to new adopters failing to implement controls, rather than abandonment of existing controls. One exception is quarantining e-mail attachments. Many businesses have given up doing this, after finding it too time-consuming.

Companies logging and monitoring web access reported a higher number of Internet abuse incidents. This implies that among those organisations without this control, similar incidents are going undetected.

Large businesses are more aware of the potential impact of inappropriate e-mail usage than small businesses. For example, large businesses are three times as likely to add legal disclaimers to their e-mails as small ones. They are also three times as likely to have sought consent from employees to their right as employers to read e-mails in an investigation situation.

Use of encryption and digital signatures for e-mail has still not taken off. Most UK companies send their e-mail across the Internet in clear text.

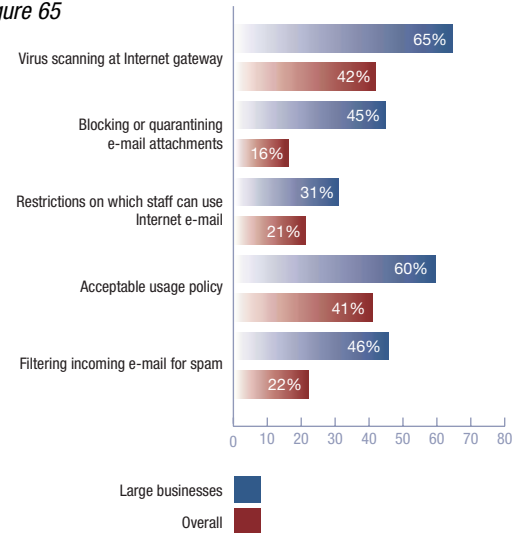
There is growing concern over the volume of unsolicited e-mail ('spam') that companies receive. Most businesses are seeing an increasing volume of spam. It makes up more than half of all incoming e-mail in 17% of UK businesses. One in ten now rate spam as a major business issue, causing significant time to be wasted. As a result, nearly one in four businesses (and nearly half of all large ones) filter incoming e-mail.

For further information on these areas, see the separate fact sheets on *Viruses and malicious code*, *Spam* and *Staff misuse of the Internet*.

Security Controls

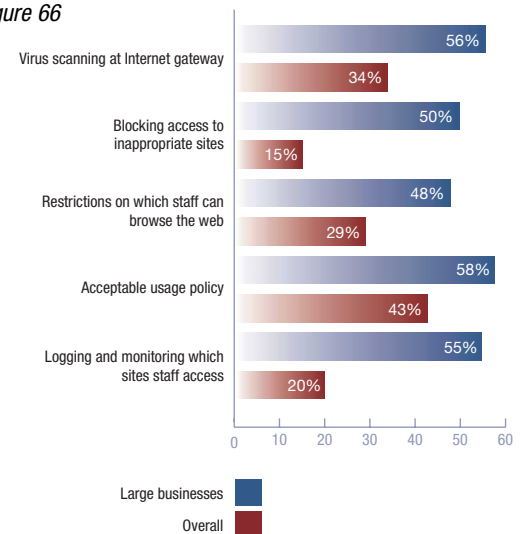
What security controls do UK businesses that send Internet e-mail have over its usage?

Figure 65



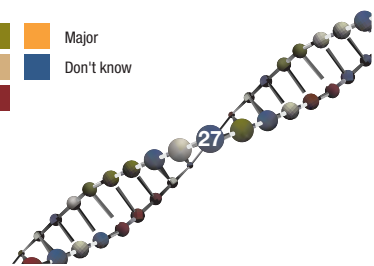
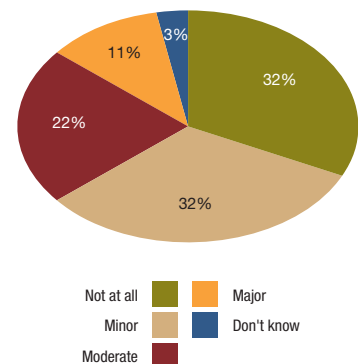
What security controls do UK businesses that allow web browsing have over its usage?

Figure 66



How important an issue is spam to UK businesses?

Figure 67



Security Controls

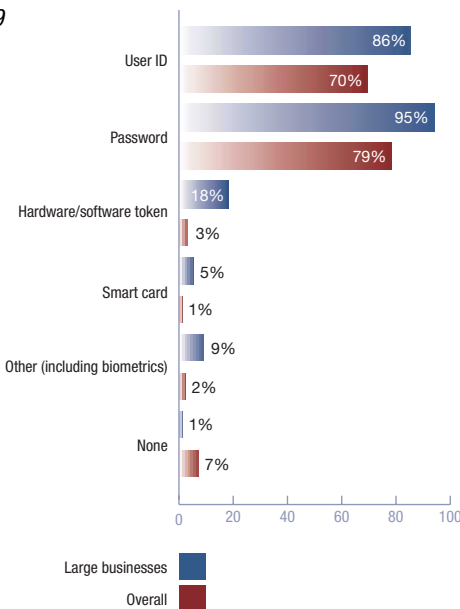
Identity management

Figure 68



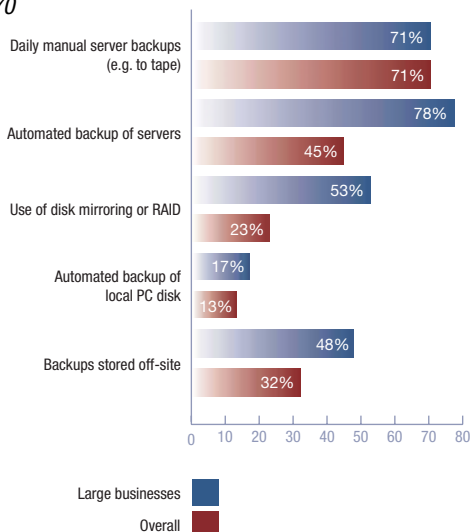
What techniques do systems use to authenticate users?

Figure 69



What backup and recovery controls do UK businesses have in place?

Figure 70



Enterprise Security

A key requirement of effective information security is controlling access to systems and information. Businesses need to make sure the right people have access to the right systems at the right time. It is equally important to block unauthorised people.

A key element of enterprise security is Identity Management. This involves robust controls to make sure that users:

- are who they say they are;
- can see only the information that is appropriate; and
- are set up on systems when they join, and are deleted from systems when they leave, efficiently and promptly.

The increasing complexity of IT systems makes it difficult to control user access. As more businesses open up their systems to customers, business partners and suppliers online, the challenge increases.

The average user often needs to access several different IT systems for their daily work. The bigger the company, the more systems each individual uses. As a result, companies are increasingly automating the process for granting, changing and removing access. 16% of all businesses and 31% of large ones now do this.

Single sign-on, where a user has a single user ID and password across all systems, has been a target for many organisations. Users find this less painful and are less likely to choose easy passwords or write them down.

Under single sign-on, a breach can enable unauthorised access to all the systems a person uses. Strong authentication (i.e. two-factor, with tokens, smart cards or biometrics) can mitigate this risk. Unfortunately, the survey results show this is quite rare.

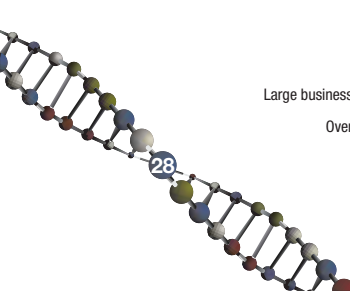
Tellingly, businesses with single sign-on alone, without strong authentication, had a higher than average incidence of unauthorised access. In contrast, the early adopters of strong authentication suffer many fewer incidents.

Enterprise security is as much about availability and integrity as it is about confidentiality. Accidental systems failure or data corruption is a significant threat, with many businesses suffering damage as a result. The good news is that 95% of companies have some form of backup processes in place. The bad news is that these vary significantly, and in many cases appear inadequate.

Only a third of businesses store their backups off-site. Backups also tend to rely heavily on tape storage, despite the well-known reliability issues of tapes. Many businesses do not realise the value of their data until it is too late.

Only 20% of companies (41% of large ones) have disaster recovery plans in place. Only 8% have actually tested that their disaster recovery plans would work in practice.

For further information on these areas, see the separate fact sheets on *Identity management* and *Backups and recovery*.



Network Security

For many businesses, the traditional boundary of their network has been their Internet gateway. Organisations have focused on defending their perimeter, and done less to secure computers within the network. 'Hard on the outside, soft on the inside' was a common mantra.

By their nature, web-sites sit on the network perimeter, and so tend to be relatively hardened. Businesses are deploying a range of intrusion prevention techniques to protect their web-sites. Firewalls predominate. Three-quarters of in-house web-sites have a firewall, but for over half of these this is their sole defence. The larger the business, the more likely it is to protect its web-site with intrusion detection software as well as a firewall.

Roughly half of all businesses with a web-site host it externally. They rely on the security provided by their service provider. Many do not know what defences their service provider has against attack.

Network boundaries are extending as businesses increasingly allow their staff to access systems remotely. Over half of UK businesses now do this.

One might expect the increased adoption of remote access to be accompanied by the deployment of additional security controls. The survey indicates this is not the case. A quarter of businesses that provide remote access have no additional controls. Only a quarter encrypt their transmissions using Virtual Private Network (VPN) technology.

Personal Digital Assistants (PDAs) are also being used to provide easy access to business information on the move. A third of businesses (and half of large ones) now use these devices. Increasingly, sensitive data is held on PDAs, however, less than half of businesses using them have any security controls over their usage.

Adoption of wireless networks has mushroomed over the last two years. In 2002, only 2% of UK businesses had a wireless network. Now a third do. However, only half of these have implemented any security controls over their wireless networks. Only one in five uses Wired Equivalent Privacy (WEP) or other additional encryption to protect their information from unauthorised disclosure. Large businesses tend to be more security conscious, but even here a third of wireless networks are unprotected.

These expansions of the network perimeter are putting the traditional perimeter defence model under strain. For example, blended threat viruses have increasingly attacked weaknesses in network security.

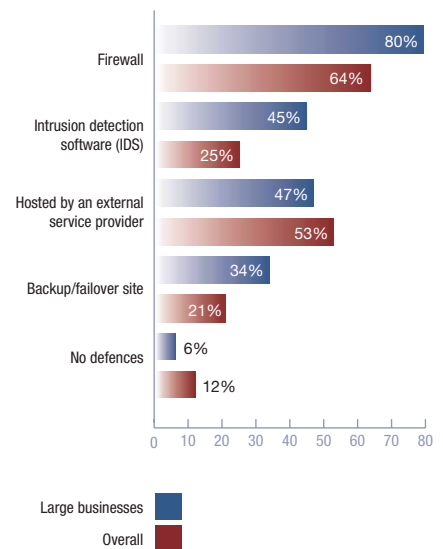
To protect their extended networks, businesses need to make sure they have the latest security updates and patches installed on all their computers. In large organisations, often the only way to ensure this is to have a security audit process that frequently checks all the servers for vulnerabilities. Increasingly, this is being automated.

For further information on these areas, see the separate fact sheets on *Intrusion prevention*, *Remote access* and *Viruses and malicious code*.

Security Controls

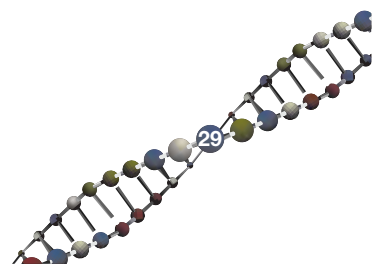
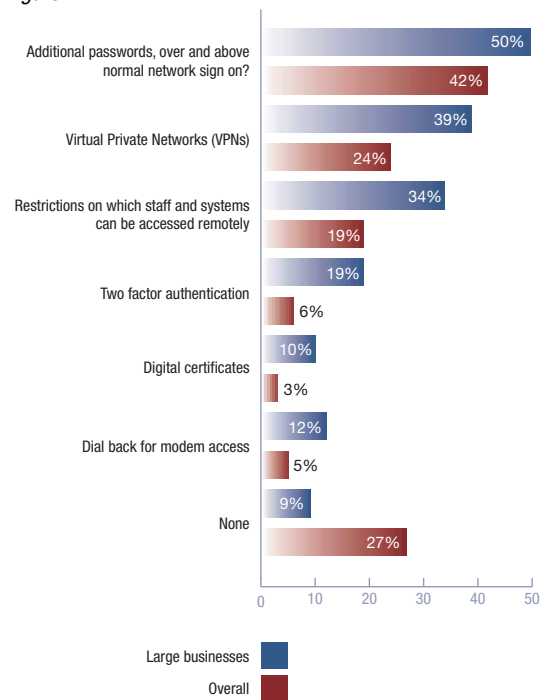
How do UK businesses with a web-site protect it?

Figure 71



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

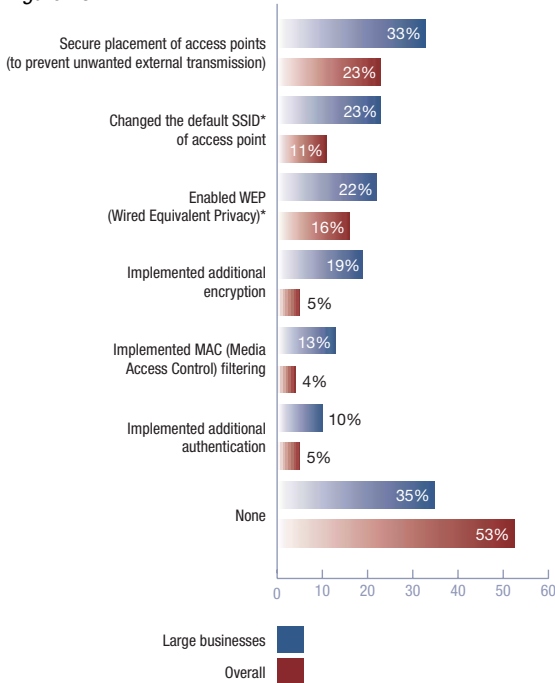
Figure 72



Security Controls

What security controls are in place over wireless networks?

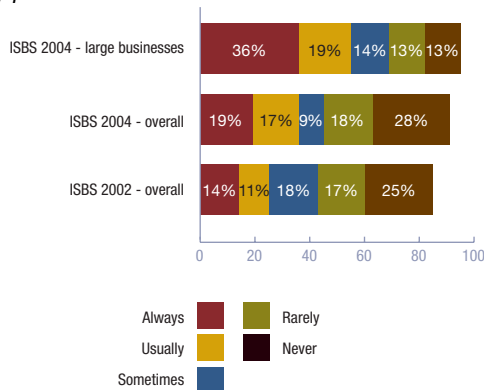
Figure 73



* The SSID is an identifier attached to packets sent over a wireless LAN and functions as a 'password' for joining a particular radio network. WEP encrypts signals to avoid disclosure to eavesdroppers.

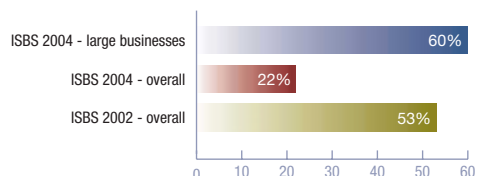
How often do IT projects formally document the security requirements and how they will be addressed in the systems design?

Figure 74



How many UK businesses have formal change control procedures for maintaining IT systems?

Figure 75



Managing Change

Not only are IT infrastructures increasingly complex, they are also subject to more rapid change than ever before. Change almost always introduces risk. Most system failures occur as a result of changes.

The introduction of a new system can introduce a security exposure. Appropriate role-based access should be built into the application to support any requirements to segregate duties. For example, a person who sets up suppliers should not normally be able to authorise invoices for payment. Otherwise, this may present a fraud risk. Any new system should also have a sufficient audit trail, so that transactions can be traced to the individual who initiated them.

Systems that process confidential information should have security controls to protect their data. For example, that data might be held in an encrypted form, and access to data analysis tools for ad-hoc reporting might be restricted.

With web applications, messages should be encrypted (e.g. through the use of SSL, Secure Sockets Layer). Checking the identity of the user and ensuring that sessions are not hijacked are also important.

Any project to develop or implement a new system should consider the security requirements. A formal specification is normally the best way to capture these and track them through the project.

However, there is patchy adoption of this good practice. Only about half of UK businesses do this, a picture that is largely unchanged since 2002. The good news, though, is the increased frequency with which security requirements are specified among those businesses that do this at all.

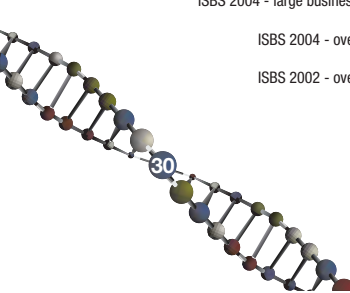
Large businesses tend to have more formal controls. Over half of them build formal security specifications into most of their IT projects. Financial services and telecom providers were the best sectors. This reflects their high dependence on systems and the priority they put on security. Retail and property companies were least likely to have formal security specifications.

Routine maintenance of systems is just as big a source of security problems as new systems implementations. To mitigate the risks, changes should be clearly specified and tested before being implemented.

In addition, it is important that there is a formal process for migrating changes from the development or test environments into live running. An important segregational control is to restrict developers' access to the live environment.

In practice, however, only one in five small businesses has formal change control processes. One reason for this is that many use only off-the-shelf packages, with minimal customisation. As a result, they do not have in-house developers, and make few changes. There are, however, some small businesses with in-house IT staff making ad-hoc changes to systems in an uncontrolled way.

The larger the business the more likely it is to have formal change control procedures. Nearly two-thirds of large organisations have these. Telecoms, technology and financial services companies are most likely to have formal processes. In contrast, only 4% of health and education providers have a formal process.



Outsourcing

More UK businesses than ever outsource part of their IT operations. Approximately half now do this. Areas that are outsourced include application development and support, systems administration, web-site hosting and help-desk operation.

The degree of outsourcing is similar for all sizes of business, however the reasons for doing this vary. In smaller businesses, the main driver tends to be more cost effective acquisition and maintenance of skills. In larger businesses, there is more focus on removing operations and support for areas that are not seen as core to the business. The growing complexity of IT infrastructures is increasing both the level of skills needed to service them, and the amount of management attention required. Outsourcing is often seen as a solution to this.

As a result, many businesses now depend on their outsource provider for important aspects of information security.

Two-thirds of businesses that outsource IT operations have a formal Service Level Agreement (SLA) in place. SLAs generally set out pre-defined targets to be achieved by the outsource provider. Failure to achieve these can lead to escalation of the issues, penalties or even termination of the agreement. Where outsourcing is done on an 'as-is' basis, agreements are often simple documents, defined by analysing current service levels. Where outsourcing is done to drive cost reduction or service benefits, agreements tend to be more complex, defined with input from IT specialists and lawyers. Formal SLAs were more common for large businesses that outsource, with 81% having them. This reflects the greater culture of internal control within large companies.

A very high proportion (90%) of SLAs in place contain information security requirements. This is a very encouraging result. In the early days of outsourcing, this was rarely the case. It appears significant progress has been made. The proportion for large companies is lower, at 71%. This probably reflects the greater complexity of the relevant outsourcing arrangements and their security needs.

An important question when outsourcing is which company's information security policy and standards should be used, yours or theirs? Two-thirds of outsourcing arrangements require the IT service provider to comply with the customer's security policy and standards. This shows good flexibility on the part of outsource providers. However, it does increase the onus on the customer to clearly define their security requirements.

A medium-sized financial services company recently performed due diligence work on a potential outsource provider. The IT manager was surprised, on visiting the provider's data centre, to observe how weak the security controls were. Given the high profile of some of their other clients, she was astonished this had not been taken up with them before. She insisted on tighter controls being built into the contract with them.

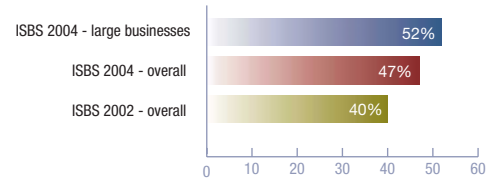
Interestingly, some organisations that expect their provider to adopt their policy and standards have not yet put a formal security policy in place. The businesses that do not require their outsource provider to follow their security policy tend to be the same ones that do not have any Service Level Agreement in place.

The trend towards moving operations to lower cost countries (such as India or China) is likely to increase the need for strong security controls within outsourced operations.

Security Controls

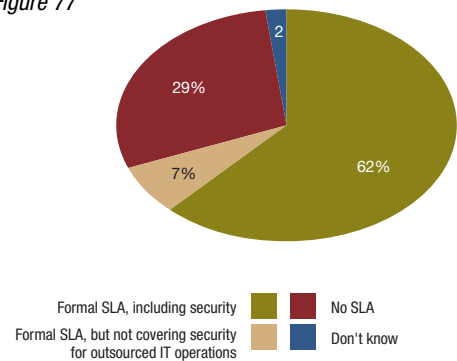
How many UK businesses have outsourced any of their IT operations?

Figure 76



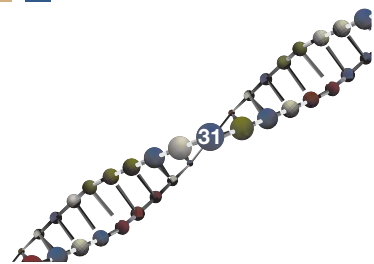
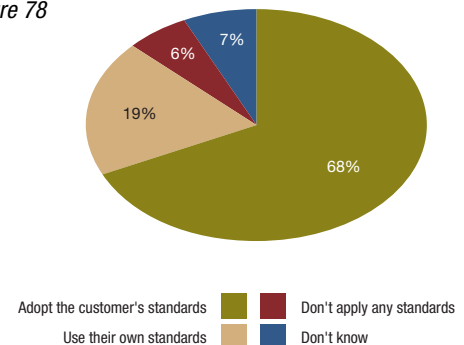
How many outsource arrangements have Service Level Agreements in place?

Figure 77



Which security policy and standards do outsource providers adopt?

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. Our information security business advice pages are at:

www.dti.gov.uk/bestpractice/infosec.



PricewaterhouseCoopers LLP (PwC) provides industry-focused assurance, tax and advisory services for public and private clients. More than 120,000 people in 139

countries connect their thinking, experience and solutions to build public trust and enhance value for clients and their stakeholders. PwC has one of the UK's largest security consultancies, with extensive experience of investigating security breaches and in-depth knowledge of the techniques available to protect against and limit the damage from such breaches. For more information, see www.pwc.com/security.



Computer Associates®

Computer Associates eTrust™ security management solutions enable organisations to consistently enforce their security policies, assess vulnerabilities, and monitor and evaluate information to properly protect their assets while enabling business growth. CA's eTrust solutions are open and integrated, and can work with all existing security technologies to help organizations reduce costs and improve operational efficiencies. CA's eTrust solutions are grouped into three solution areas - eTrust™ Identity

Management, eTrust™ Access Management and eTrust™ Threat Management - and are brought together with unified visualisation and management through eTrust™ Security Command Centre to help manage today's ever-evolving computing environment. These solutions are seamlessly integrated and can operate with an organisation's existing security infrastructure. For more information, see www.ca.com/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.

Over 1,200 enterprises and government agencies in more than 50 countries use Entrust's portfolio of security software solutions that integrate into the broad range of applications organisations use today to leverage the Internet and enterprise networks. For more information, see www.entrust.com.



Microsoft is committed to enabling every customer to work, communicate, and transact business more securely. We are working to simplify security and drive the intelligence of security protection deeper into our software and we measure our efforts using the SD³+C framework (Security by

Design, Default, Deployment, and Communications). With Windows Server 2003 and Windows XP at the foundation, Windows Server and Desktop Systems provide comprehensive IT infrastructure for operations (security, systems management, networked storage), applications (data management and analysis, e-business), and information work (messaging, communications and collaboration). Founded in 1975, Microsoft (Nasdaq "MSFT") is the worldwide leader in software, services and Internet technologies for personal and business computing. The company offers a wide range of products and services designed to empower people through great software - any time, any place and on any device. For more information, see www.microsoft.com/security.

Independent reviewers



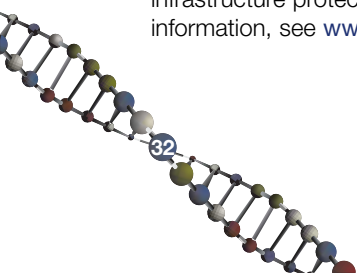
The Information Assurance Advisory Council is a unique partnership that brings together corporate leaders, public policy makers, law enforcement and the research community to address the challenges of information infrastructure protection. For more information, see www.iaac.org.uk.



The National Hi-Tech Crime Unit works with government and industry here and abroad to combat national and transnational serious and organised hi-tech crime both within, or which impacts upon, the UK. For more information, see www.nhtcu.org.



Royal Holloway is a multi-faculty College of the University of London. Its Information Security Group is recognised worldwide and in 1999 was awarded a Queen's Anniversary Prize. The College has earned a world-class reputation for high quality, original research across the sciences, performing arts and humanities. For more information, see www.isg.rhul.ac.uk.



Other DTI Information Security Breaches Survey 2004 reports

In addition to this technical report, eight other ISBS 2004 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 Department at www.dti.gov.uk/publications 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 04/618).

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



Backups and recovery
(URN 04/610) - 2 page fact sheet.
Produced in association with:



www.attix5.com



Intrusion prevention
(URN 04/614) - 2 page fact sheet.
Produced in association with:



start.mcafeesecurity.com



Viruses and malicious code
(URN 04/611) - 2 page fact sheet.
Produced in association with:



www.qualys.com



Remote access
(URN 04/615) - 2 page fact sheet.
Produced in association with:



www.safenet-inc.com



Identity management
(URN 04/612) - 2 page fact sheet.
Produced in association with:



www.entrust.com



Spam
(URN 04/616) - 2 page fact sheet.
Produced in association with:



www.ca.com



Staff misuse of the Internet
(URN 04/613) - 2 page fact sheet.
Produced in association with:



www.websense.com

