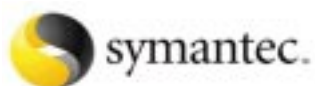


Information  
Security Breaches  
Survey **2002**

T E C H N I C A L   R E P O R T

In association with:





The blood vessel patterns of the retina and the pattern of flecks on the iris both offer unique methods of identification. These methods are presently used for high security access control at military and bank facilities. Retinal recognition is said to provide the most stable means of biometric identification over time.

# Information Security Breaches Survey 2002

Information is the lifeblood of today's business, underpinning day-to-day operations and facilitating effective decision-making. Increasingly, access to the right information by the right people is vital to gaining competitive advantage or simply remaining in business. To provide this access, businesses need to understand the associated risks and put in place appropriate counter-measures.

This survey is intended to help UK businesses understand the risks they face in the information security arena. The Information Security Breaches Survey 2002 (ISBS 2002) is the sixth survey that the Department of Trade and Industry has sponsored since 1991. ISBS 2002 has been managed by PricewaterhouseCoopers, in association with RSA Security, Symantec, Genuity and Countrywide Porter Novelli. The telephone interviews were carried out by PwC Consulting's International Survey Unit.

The key message from the survey is that information security has increased in priority over the last two years and many businesses have made significant improvements in their security controls. However, the threats have increased substantially, and roughly half of all UK businesses have had at least one malicious security incident in the last year. Investment in information security is still low, and, looking forward, there is an urgent need for action now.

Chris Potter,  
Partner, Information Security Solutions  
PricewaterhouseCoopers

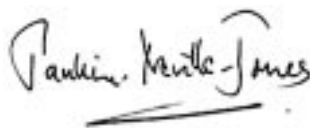
Geoff Smith,  
Head of Information Security Policy Group  
Department of Trade and Industry

## Foreword

Good corporate governance demands that business leaders have a duty to consumers, shareholders, employees and society as a whole to make effective information security and safety a high priority. Put simply, companies who build trust will win; those that do not will fail.

This survey demonstrates that the senior management of UK companies increasingly recognise the strategic importance of managing information risks. However, too often, board-level recognition of the risks has not been translated into adoption of best security management practice.

A safe and secure Information Society cannot be built by business, or by government alone. But it can be built in partnership. Prime Minister Tony Blair's stated aim is to make the UK the best place in the world to conduct e-business. Government, businesses and citizens can achieve this objective by working together to develop awareness and to adopt best practices.



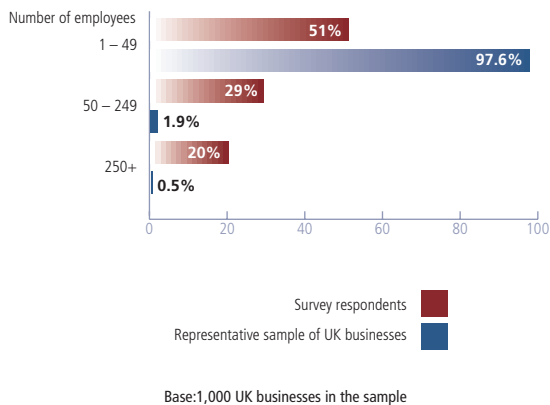
Dame Pauline Neville-Jones,  
Chair of the Information Assurance Advisory Council (IAAC).

The IAAC ([www.iaac.org](http://www.iaac.org)) is a private sector led and government supported forum that brings together corporate leaders, public policy makers, law enforcement and the research community to address the challenges of information infrastructure protection.

# Methodology

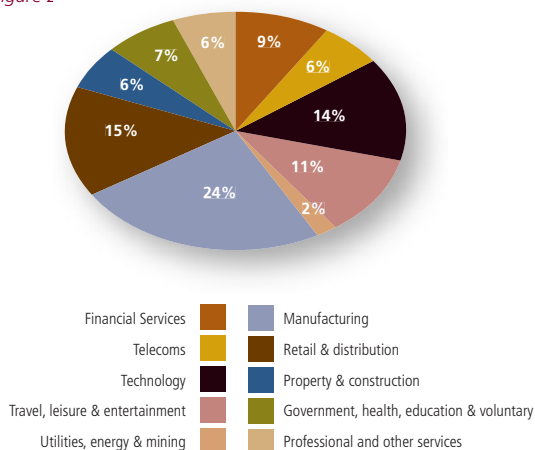
## How many staff did each respondent employ in the UK?

Figure 1



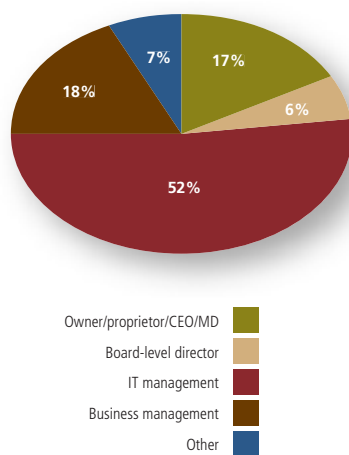
## In what sectors were the respondents' main business activity?

Figure 2



## What was the respondent's role within their organisation?

Figure 3



The core element of the research for ISBS 2002 was a quantitative survey, conducted using a structured questionnaire across a range of organisations in the UK. A total of 1,000 telephone interviews were conducted with individuals identified as being responsible for information security within their organisation. Each interview lasted on average 30 minutes and was computer assisted. Interviewing was conducted between 5 November 2001 and 16 January 2002.

During the research fieldwork phase, large companies were over-sampled to ensure adequate representation for specific analyses. However, in the final reporting, all results have been weighted to accurately reflect the distribution of businesses in the UK. Figure 1 (opposite) shows the sample of the companies which were contacted for this research and shows a representative distribution of businesses.

The proportion of businesses with fewer than 50 employees has a significant impact on the weighting. Consequently, the results from large businesses (defined for the purpose of this survey as having 250 or more employees) can get lost in the overall average results. Accordingly, where the results for large businesses are significantly different from the average, we have identified them separately throughout this report.

52% of those who participated in the interview were within IT management, and this proportion was greater (86%) in large businesses. As businesses decreased in size, there was a higher likelihood that the respondent was the highest executive in their organisation (i.e. owner, CEO or MD) or within business (rather than IT) management.

To supplement the telephone surveys, we also carried out face-to-face in-depth interviews with IT security officers, some of whom had participated in the telephone survey and some who had not. These interviews were used to confirm the validity of the telephone findings and to obtain additional qualitative information for inclusion in this report.

In addition, we made use of an on-line web-site poll to allow organisations not selected for either telephone or face-to-face interviews to contribute to the survey. The results of the web-site poll are not included in the main quoted statistics, but 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, and so should be treated with some caution.

Whereas past surveys have included accidental incidents (such as power outages and operator error), this year's survey focused purely on malicious security incidents.

# Headline News

- The business environment has changed rapidly over the last two years. 70% of UK businesses now have a web-site, and the number of transactional web-sites has nearly doubled. 77% allow staff to send or receive e-mail across the Internet (up from 65% in 2000), and 69% provide staff with web access.
- The risk of IT security breaches has increased significantly. 76% of businesses believe they have sensitive or critical information (up from 69% in 2000).
- As a result, 73% of businesses (up from 53% in 2000) believe information security is a high priority for senior management.
- 44% of UK businesses have suffered at least one malicious security breach in the past year, a continuation of the upward trend noted in the 2000 survey.
- The average cost of a serious security incident was £30,000. Several businesses surveyed had security incidents that cost them over £500,000.
- While most businesses restored normal operations within a day of their worst security breach, 20% of large organisations that had an incident took more than a week to get business operations back to normal.
- Virus infection was the single largest cause of serious security breaches (accounting for 33% of the most serious breaches). 42% of UK businesses that use Internet e-mail have suffered from virus infection as a result.
- 83% of businesses use anti-virus software (up from 75% in 2000). 94% of those that use Internet e-mail scan file attachments on incoming e-mails for viruses, and 85% of those that provide web access scan file downloads for viruses.
- While the number of UK businesses with a documented security policy has doubled since 2000, it is still only 27%.
- While BS 7799 has become the international standard for security, only 15% of people responsible for IT security in the UK are aware of its contents. Only 49% of businesses have documented procedures to ensure compliance with the Data Protection Act.
- Only 33% of UK web-sites have software in place to detect intrusion. Only 51% of transactional web-sites encrypt transactions passing over the Internet.
- Despite this, 68% of people responsible for IT security are confident that they caught all significant security incidents that occurred in the past year, indicating a potential knowledge gap.
- Business people find it difficult to apply normal commercial disciplines to IT security. Only 30% of UK businesses ever evaluate the return on investment (ROI) on their information security expenditure.
- As a result, only 27% spend more than 1% of their IT budget on information security.
- The future competitiveness of UK businesses depends on driving costs down by opening up systems to remote access by staff, customers and business partners. Already 71% of large businesses allow staff to access their systems remotely (e.g. from home), and the trend is for business partners to be given access next.
- Yet only 19% of businesses that currently provide remote access have implemented two-factor authentication, and only 69% of transactional web sites require customers to authenticate themselves in any way. If more attention is not paid to this area, the potential for fraud and reputational damage is enormous.

These factors together make a compelling case for action now. The solution is not simply more expenditure. Instead, it revolves around using the right expertise to make sound commercial decisions about which investments in security to make, and which risks to accept or insure.

**Information security has never been a higher priority at the board level**

**Security incidents cost UK business billions of pounds in 2001**

**Viruses caused the most damage, and the vast majority of UK businesses have anti-virus software in place to combat this threat**

**In other areas, there is a growing disconnect between the priority placed on IT security by Boards of Directors and the actual security controls in place**

**The root cause is that security is treated as an overhead rather than an investment**

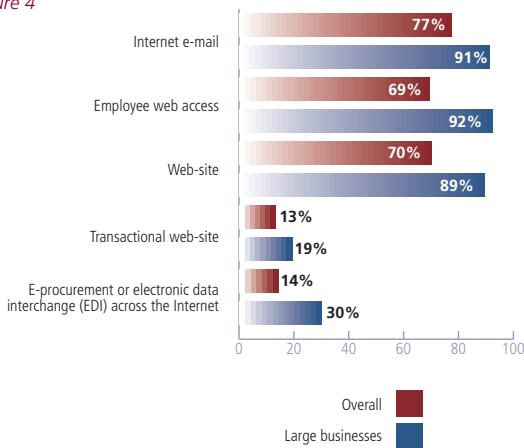
**Security is a critical enabler to business going forward**

**UK businesses need to take action now**

# The Changing Business Environment

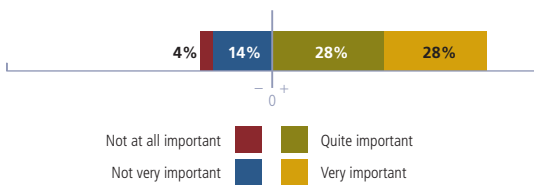
## What proportion of UK businesses are currently carrying out e-business activity?

Figure 4



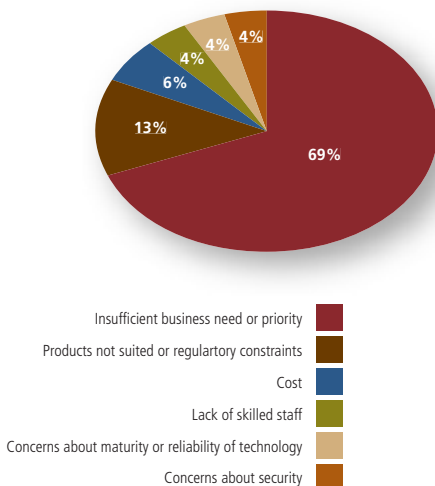
## How important to a UK business is its web-site?

Figure 5



## Why are UK web-sites not accepting transactions?

Figure 6



## E-Business Adoption

Our survey indicates that UK businesses are widely embracing the Internet, although the rate of new e-business adoption has now slowed.

77% of UK businesses (91% of large businesses) allow their staff to send or receive e-mail across the Internet, and 69% of UK businesses (92% of large businesses) provide their employees with access to browse the web. 70% of UK businesses (89% of large businesses) now have their own web-site, and more than half (56%) said that these web-sites were important to their business.

The number of UK businesses who are selling their products or services over the Internet has roughly doubled over the last two years. In 2000, less than 10% of web-sites were transactional. Today, roughly 18% of web-sites are now transactional and another 10% are planning to start trading on-line in the future.

While this is a significant movement forwards, it is slower than predicted at the height of the dot-com boom. At the time of the 2000 survey, 33% of organisations were using or were intending to use the Internet for buying and/or selling. Not all of those planning to do so in 2000 have yet implemented those plans.

The reality is that the majority of UK businesses of all sizes are, at this stage, content to operate without being able to sell their products or services on-line. Most of these businesses (69%) cited insufficient business need or priority as the main reason for not accepting transactions through their web-site(s). A further 13% felt that either their products were not suited to sale through a web-site or regulatory constraints prevented such sales.

Relatively few UK businesses have a clear focus and direction when it comes to e-business. Only 15% of UK businesses (35% of large businesses) have a formal documented e-business strategy in place. This itself may be the main obstacle to further e-business adoption. It is difficult to establish a clear business case without thinking through the strategic implications.

There is a clear consensus that e-commerce systems pose more security threats than traditional systems. 61% of UK businesses believe that e-commerce systems are more of a target for fraud than non e-commerce systems, compared with only 7% that think e-commerce systems are less of a target. Most UK businesses, therefore, believe the growth of e-business activity over the last two years has resulted in increased security threats.

Other recent surveys (such as the quarterly CBI financial services survey) have highlighted such security concerns as being a significant inhibitor to the growth of e-business.

However, this survey shows that only 4% of web-sites are not accepting transactions as a direct result of concerns about security issues. UK businesses are confident about being able to address these security issues, with 76% of businesses with a web-site confident that they have sufficient controls in place to prevent or detect all web-site security incidents, compared with only 8% that are not confident.

The issue with security concerns appears to relate more to consumer confidence. Customers' concerns about security appear to be inhibiting the volume of on-line transactions, and hence indirectly reducing the business case for UK companies to sell their products and services on-line. A continued focus on earning consumers' trust and convincing them that it is easy and secure to transact on-line is necessary if the UK is to fully embrace the new economy. Each reported security incident undermines this effort, so it is critical that UK businesses put in place appropriate security over their web-site(s).

One bank interviewed commented that any Internet security incident in their industry has a general reputational impact on the whole sector and puts off tentative users of Internet services.

For most UK businesses that take transactions through their web-site(s), this still represents a secondary channel, with 70% reporting that less than 10% of their income comes through their web-site(s). However, there is an increasing number of UK businesses for which the Internet is their primary channel, with 8% of those that accept transactions on-line achieving more than 50% of their income through their web-site(s).

Interestingly, while many large multi-national organisations have recently praised the merits of business-to-business transactions, there remains heavy scepticism amongst UK businesses about whether e-procurement saves organisations money. Only 19% of UK businesses agreed that they could save money by using e-procurement while 26% disagreed. The 2002 survey also revealed that only 14% of UK businesses (30% of large businesses) have so far implemented e-procurement or electronic data interchange (EDI) across the Internet.

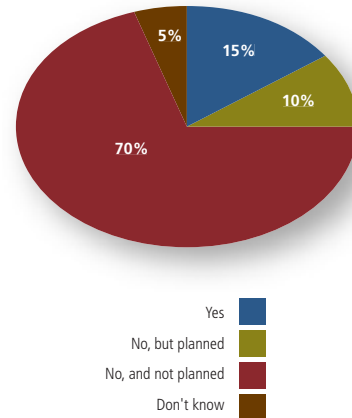
However, 41% of the businesses using e-procurement/EDI consider it important to their business. This is reinforced by the fact that 32% of those businesses use it to conduct more than 10% of their total purchasing on-line, with 8% conducting more than 50% of their total purchasing on-line.

Once again, security is not cited as the main obstacle to adoption of e-procurement. 20% of UK businesses believe that implementing security over e-procurement is straightforward versus 17% who believe it is not. Most, however, seem to have little experience or no strong views.

## The Changing Business Environment

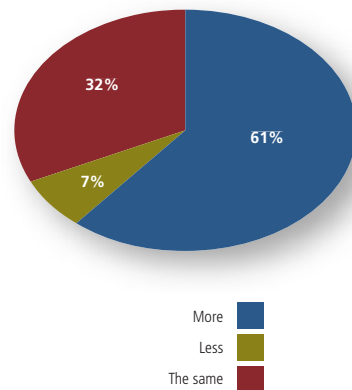
### Do UK businesses have a formal documented e-business strategy?

Figure 7



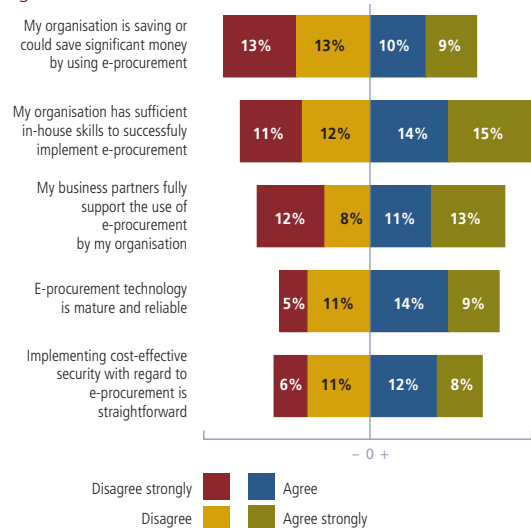
### Are e-commerce systems more or less of a target for fraud than non e-commerce systems?

Figure 8



### What do UK businesses think about e-procurement?

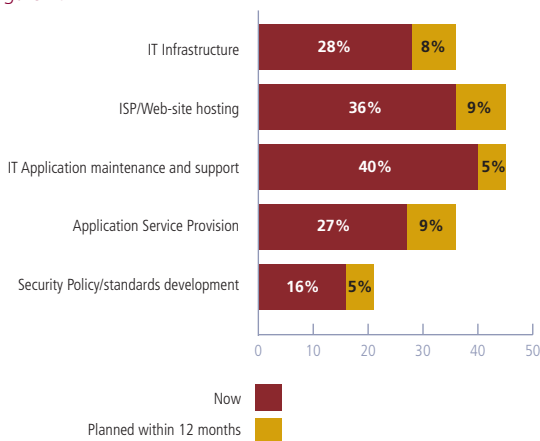
Figure 9



# The Changing Business Environment

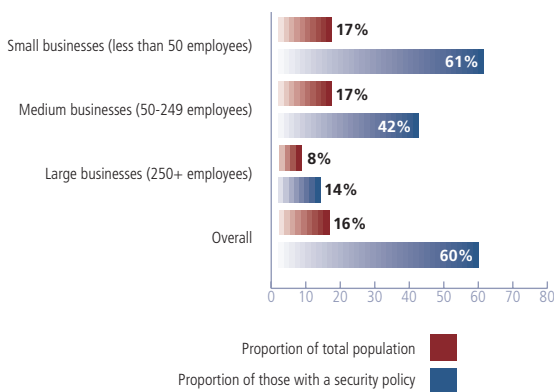
## Which of the following significant systems or security processes are outsourced?

Figure 10



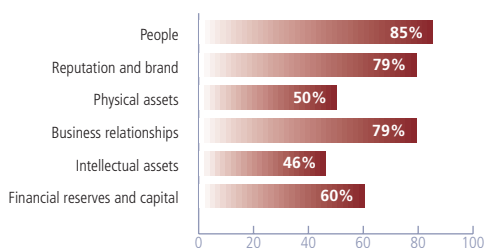
## Which UK businesses are outsourcing security policies and standards development?

Figure 11



## Which assets are very important to UK businesses?

Figure 12



## Outsourcing

Another significant change in the business environment has been the continued move towards outsourcing. Outsourcing is used as an effective means to remove operations and support for elements of their business that are not related to core business. In particular, IT systems and business processes are increasingly being outsourced and many organisations have further outsourcing planned.

The systems or processes most commonly outsourced by UK businesses are IT application maintenance, with 40% having outsourced this function. Web-site hosting is also common, with 36% outsourcing this; given 30% of UK businesses do not have a web-site, this represents over half of those that do. Web-site hosting is more common for large businesses, where 59% (i.e. two-thirds of those with web-sites) outsource.

Security policy and standards development is the area least likely to be outsourced, with 16% currently outsourcing. This, however, needs to be put in context. The number of UK businesses who are outsourcing the development of their security policy and standards in 2002 is greater than the total number who had any kind of security policy in 2000. Put another way, approximately 60% of UK businesses with a security policy in 2002 outsourced its development. Such activity is also growing; a further 5% are planning to outsource their security policy and standards development in the next year.

The driver for outsourcing security is the shortage of in-house expertise in this area. Outsourcing of security policy and standards is most popular among smaller organisations, at 17% of those surveyed. By comparison only 8% of larger organisation have outsourced this area. Smaller businesses tend to lack a dedicated or large security department and so are more likely to seek external assistance, while larger businesses have tended in the past to treat this as a core business activity.

Outsourcing security activities represents both an opportunity and a risk. A good outsource provider will be able to improve the quality of security in a highly cost-effective way, because it is their core business activity to do so. On the other hand, outsourcing to a poor provider may increase the security risks.

The marketing department of one business interviewed developed a web-site, which worked well. Then, without consultation, they outsourced the hosting and development to two different third parties, neither of which saw security as their responsibility. The site quickly ended up with no security!

Outsourcing does not remove an organisation's responsibility for the ownership and protection of its information and assets. A business remains ultimately responsible for its security, even if security-related tasks are carried out by an outsourced supplier. Where businesses outsource, they need to have monitoring processes to ensure their outsource providers meet their security requirements.

One building society commented that all their contracts for outsourced functions include the right for the society to carry out penetration testing of the outsource providers' systems.



## Attitudes to Information Security

Information security needs to be put in the context of what is important to the business as a whole. Unsurprisingly, the survey found that people, reputation and brand, and business relationships, are rated as very important by over three-quarters of UK businesses. People have traditionally associated information security with technology and administrative processes. Effective information security is just as much about educating and managing staff, managing incidents to avoid reputational damage, and providing business partners with assurance about security.

The trend continues towards a knowledge-based economy with a high dependence on IT. An increasing proportion of UK businesses (76% compared with 69% in 2000) believe that their business is highly dependent on sensitive or critical information. The 24% who do not believe they have any sensitive or critical information is surprisingly high; it suggests that these businesses are perhaps not fully aware of their dependency. Among large businesses, the importance of data is more marked. Only 9% (similar to the 2000 survey result) believe they have no sensitive or critical information. Given this degree of dependence on information, organisations need to have a clear strategy for managing and securing their data.

This survey confirms the view that information security has increased in profile at board level. 73% of UK businesses now rate security as a high or very high priority to their top management or director group, as opposed to 53% back in 2000. However, as we will see later, this has not yet fully translated into action.

One large retailer commented that, in the past, IT security had never made it into their top 20 risks in their corporate-wide risk assessment; in the last year, however, IT security has moved up to number 8. A shipping firm explained that IT security is given the same high level of priority by their board as health and safety. And, a media company stated that IT security expenditure had survived budget cuts in other areas, which was a sign of strong management commitment.

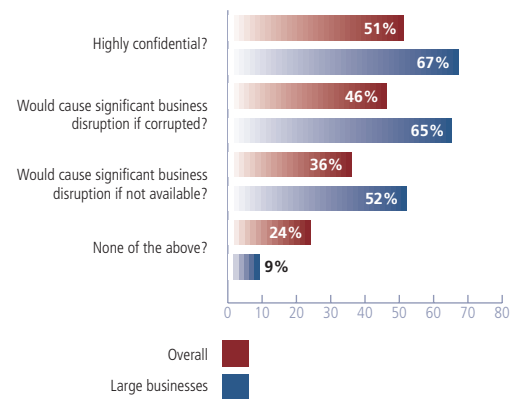
People responsible for security within UK businesses are upbeat about security in their own organisation. 68% of organisations are confident that they have caught all significant security breaches that occurred in the last year, compared to only 10% that said they were not confident. A similar pattern (though less extreme) was apparent in the responses to the ISBS web-poll.

It is arguable that, given the weakness of security controls and the number of security incidents occurring in many organisations, this confidence is misplaced. Other recent security surveys (such as the CBI Cybercrime Survey 2001) have reported similar complacency, where people consider security vulnerability to be high in business generally and in their own sector, but not within their own organisation.

# The Changing Business Environment

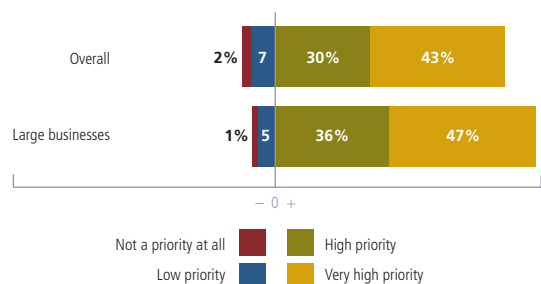
## What proportion of UK businesses have information that is:

Figure 13



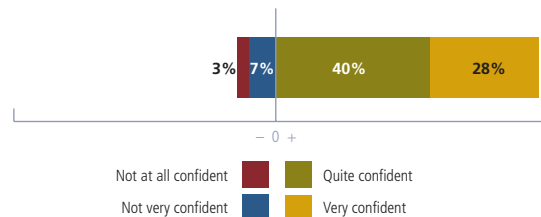
## How high a priority is information security to UK businesses' top management or director groups?

Figure 14



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

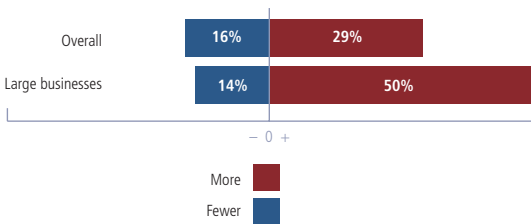
Figure 15



# The Changing Business Environment

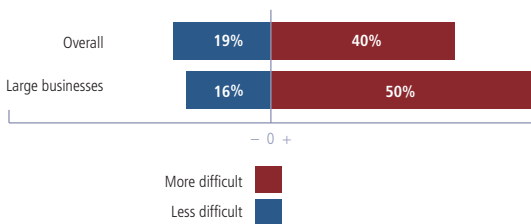
## Will there be more or less security incidents next year than last?

Figure 16



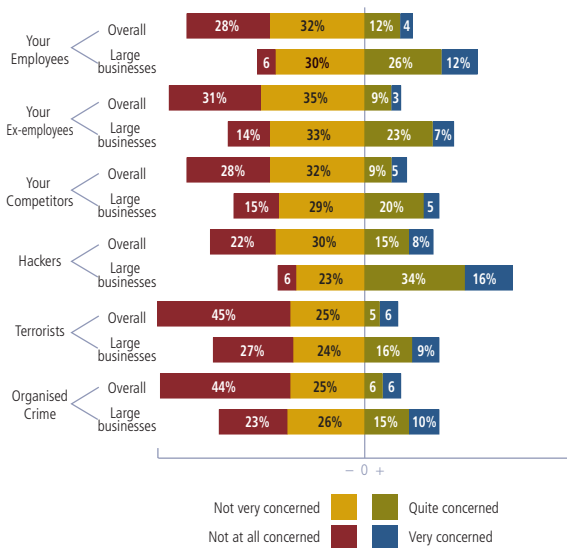
## Will it be more difficult or less difficult to catch security breaches in the future?

Figure 17



## Which of the following security threats are UK businesses concerned about over the next year?

Figure 18



## Future Outlook

UK businesses have a somewhat pessimistic outlook for the future of IT security.

While two-thirds of UK businesses currently feel confident that their systems are able to catch all significant security breaches, 29% of UK businesses believe that the number of security incidents will get worse in the future, and only 16% believe it will get better. This is more marked in large businesses, where 50% anticipate an increase in the number of security incidents compared with 14% who anticipate a decrease.

Several of the businesses interviewed cited keeping up to date with potential security vulnerabilities as their biggest problem.

A further gloomy picture is painted by the fact that 40% of UK businesses believe it will become more difficult in the future to prevent or detect security incidents, with only 19% believing it will get easier. Again the picture is more pronounced among large businesses, where 50% are pessimistic and only 16% optimistic.

This is similar to the pattern expressed in other recent security surveys. In the CBI Cybercrime Survey 2001 (in which over half the respondents were from large businesses), 73% of respondents felt that vulnerability to cybercrime would increase in business generally.

Despite this pessimistic outlook, very few UK businesses are concerned about the possible security threats to their organisation over the next year. Those that are concerned tend to be large businesses.

This relative complacency about the impact of future threats on people's own business is reflected in other recent security surveys. For example, the CBI Cybercrime Survey 2001 found that, while 73% of respondents felt that vulnerability to cybercrime would increase in business generally, only 42% felt it would increase in their own business. It seems human nature to think that it couldn't happen to me!

UK businesses are most concerned about the threat posed by hackers (23% concerned). The vast majority of organisations, at 69%, do not believe that security breaches as a result of organised crime or terrorist activities warrant much concern. However, in light of the terrorist activities of 11 September 2001, UK businesses are likely to be increasingly more vigilant.

One reinsurance company commented that if someone hacked into their data, they would be bored rigid within 5 minutes!

## Number of Security Breaches

ISBS 2002 has focused on security breaches arising from premeditated or malicious intent - viruses, unauthorised access, fraud, theft, etc.

Security breaches in these areas continue to increase. 44% of UK businesses suffered a security breach in the last year (with 78% of large businesses suffering a breach).

In terms of the severity, 79% of the UK businesses that had security incidents in the last year had at least one that they rated serious, and 20% stated that they had extremely serious incidents. The larger the business the less likely that a single security incident was considered serious. Only 56% of large businesses that had security incidents in the last year had at least one that they rated serious.

This is similar to the pattern observed in other recent security surveys, both in the UK and abroad. In the CBI Cybercrime Survey 2001 (in which over half the respondents were from large businesses), 66% of respondents had a serious security incident in the last year. In the 2001 CSI/FBI Computer Crime and Security Survey (which focuses on large US businesses), 91% of respondents detected computer security breaches in the previous year, and 64% acknowledged financial losses as a result of those breaches. Information security is just as subject to the effects of globalisation as any other area of modern business.

Compared with the 2000 survey, the number of security breaches has increased significantly. In the 2000 survey, 24% of UK businesses had suffered a security breach as a result of premeditated or malicious intent. By 2002, this figure has risen to 44%. This represents an even faster rate of growth than in the previous two years, when the total number of security incidents (including incidents such as operator user errors and power supply issues that are excluded from ISBS 2002) rose from 44% in 1998 to 60% in 2000.

## Internal or External?

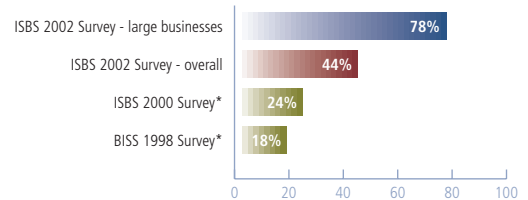
It used to be the axiom that 90% of security incidents were caused by insiders and only 10% by outsiders. ISBS 2002 confirms that the changing business environment has altered the balance of risk. Only 34% of UK businesses reported that their worst security incident was caused by an insider, whereas 66% were caused by external sources.

This is again consistent with trends in other surveys, both in the UK and abroad. In the CBI Cybercrime Survey 2001, only 25% of organisations identified employees or former employees as the main cybercrime perpetrators, compared with 75% who cited hackers, organised crime and other outsiders. In the 2001 CSI/FBI Computer Crime and Security Survey, 70% cited their Internet connection as a frequent point of attack compared with just 31% who cited their internal systems as a frequent point of attack. ➤

# Incidence of Breaches

## What proportion of UK businesses have suffered security incidents (arising from premeditated or malicious intent) in the last year?

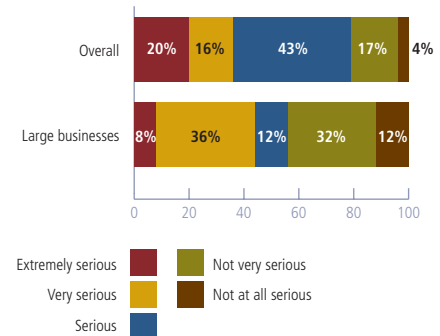
Figure 19



\*In 1998 and 2000, businesses were asked whether they had an incident in the preceding two years rather than the last year.

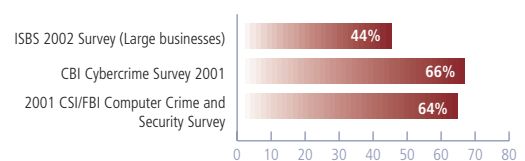
## How serious was the worst security incident suffered?

Figure 20



## What proportion of businesses have suffered a serious security incident in the last year?

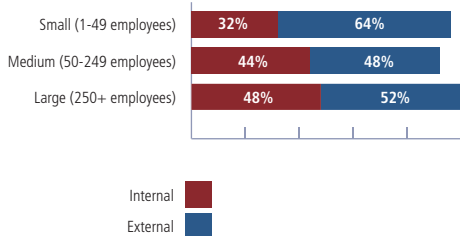
Figure 21



# Incidence of Breaches

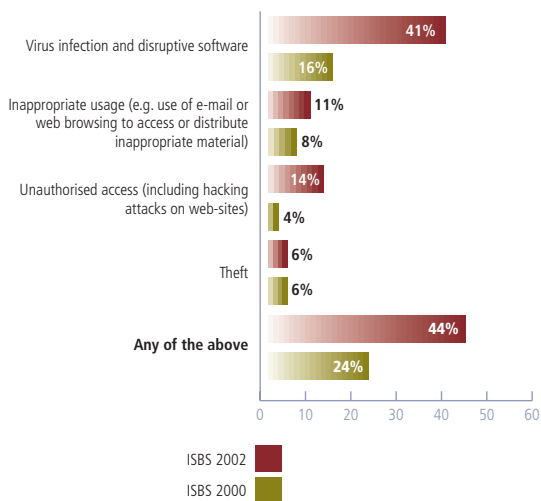
## Was the cause of the worst security incident internal or external?

Figure 22



## What proportion of UK businesses suffered security incidents in the last 12 months?

Figure 23



➤ Unsurprisingly, the larger the business, the more likely it is to have serious incidents caused by an internal source. 48% of large businesses stated their worst security incident was caused by internal activity, compared with 32% overall.

So, does this mean the threat from insiders has diminished? In the words of the 2001 CSI/FBI Computer Crime and Security Survey, "it would be premature and dangerous to assume so". Certainly, ISBS 2002 shows that the number of employee-related security incidents is growing rather than diminishing; however, given the huge increase in external threat, the internal threat is reducing as a proportion of the total.

One consumer products manufacturer had two instances of previous administrators leaving a Trojan or back-door behind. And, a financial services provider cited a major internal computer-based fraud, carried out by an employee who had been with the firm for many years and had accumulated excessive system access privileges during that time.

## Type of Security Incidents

Virus infection accounts for by far the largest number of security incidents. In ISBS 2000, 16% of UK businesses had suffered a virus infection or denial of service attack in the previous 2 years. This has nearly tripled by 2002 with 41% of UK businesses having suffered from a virus infection or denial of service attack in the last year. Recent high profile international virus attacks (such as the Nimda and Code Red blended threats - viruses that possess characteristics of worms, viruses and Trojans and blend these with hacking techniques) forced many UK businesses to shut down external connections to the internet, and the cost in terms of lost business, staff time and downtime ran to millions of pounds.

Another area of growth is the rise in web-site hacking attacks. Any computer connected to the Internet is typically scanned several times each day, as hackers attempt to find systems they can compromise. Some of these scans are looking for holes in perimeter defences and others may be part of sophisticated hacking attempts. The rise in unauthorised access from 4% of UK businesses in 2000 to 14% in 2002 is almost entirely due to web-site hacking attacks.

These figures are consistent with the upward trend shown in other recent UK surveys. In the CBI Cybercrime Survey 2001, 44% of respondents had suffered a virus infection and 16% had suffered a hacking attack. They are also similar to the US experience as reflected in the 2001 CSI/FBI Computer Crime and Security Survey, where 41% of respondents had suffered a virus infection or denial of service incident.

The growth of external threat was also apparent when looking at the worst security incident that UK businesses suffered in the last year. 33% of UK businesses stated their worst incident was due to virus infection and a further 11% stated it was due to a hacking attack on their web-site.

The 6% theft figure represents computer crime rather than physical theft of computer systems (which is not included in the ISBS 2002 figures for security incidents). Many of the organisations we

interviewed, however, also cited laptop thefts as a significant and growing concern.

One large company had many thefts of laptops and servers that were eventually traced back to their security guards; since then, they switched to a digital CCTV system that is centrally monitored, and the theft rate has reduced significantly. Another company uses encryption to protect the data on laptops; when a laptop was stolen, their security team was less than pleased to discover the encryption password had been stuck to the laptop's lid on a post-it note.

### Cost of Security Breaches

As part of the survey, UK businesses were asked the approximate cost of their worst security incident, including costs from lost business, staff time costs, costs to recover the situation, downtime and any other costs arising as a result of the breach.

Most security incidents resulted in only minor costs, with two-thirds of the most serious incidents costing less than £10,000 to resolve.

However, some UK businesses surveyed (approximately 4%) had suffered costs of more than £500,000 following a single security incident. This pattern was repeated in our web-poll, where 7% of respondents had incidents that cost them more than £500,000. The size of these incidents is significantly greater than the worst incidents identified in the 2000 survey, where the worst incidents cost in the range of £20,000 to £100,000.

Taking into account all sizes of incident, the average (mean) cost of a serious security incident was approximately £30,000.

While it may be unwise to extrapolate these figures over the whole UK population of 1.35 million businesses (with one or more employees), it is reasonable to project that security incidents cost UK business several billion pounds during 2001.

One manufacturer estimated the direct costs associated with a recent virus infection to be £80,000; this did not include some costs that were difficult to estimate, for example, the cost of losing their e-mail gateway and the resulting fall in productivity. An investment bank commented that the biggest costs of their security breaches were non-financial, e.g. lost data, wasted staff time, opportunity cost, remedial action and downtime; after some major virus outbreaks, they had to give their IT staff time off work to recover from the stress.

### Incident Response and Crisis Management

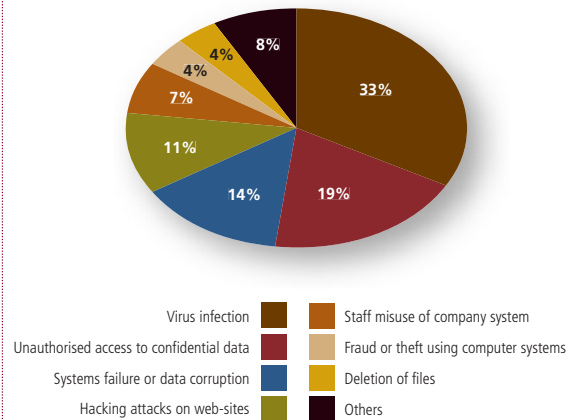
When a security incident arises, the ability to respond quickly and effectively is paramount. A comprehensive and well-planned incident response policy is critical to minimise the impact of security failures.

However, in 2000, this was identified as a major area of weakness. Only 11% of UK businesses had procedures for logging and responding to IT security incidents. Since then, there has been significant progress in this area, but good practice is by no means universal. 75% of large businesses (but only 41% of small businesses) now have procedures for logging and responding to security incidents. 73% of large businesses (but only 47% of small ones) have contingency plans in place for dealing with possible security breaches.

## Incidence of Breaches

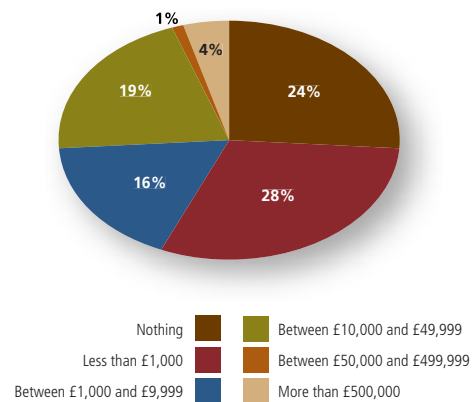
### What were the worst security incidents suffered by UK businesses in the last 12 months?

Figure 24



### What was the cost of the worst security incident in the last 12 months?

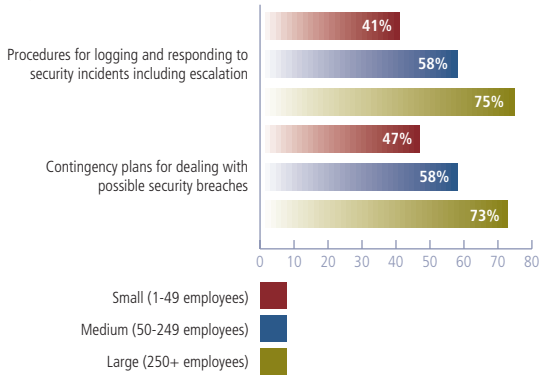
Figure 25



# Incidence of Breaches

## What proportion of UK businesses have incident response procedures in place?

Figure 26



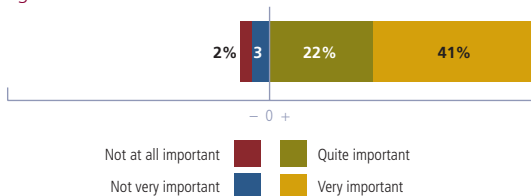
## Which of the following objectives are very important to UK businesses in the event of a security incident?

Figure 27



## How important would reporting incidents to the police or to regulators be if a security breach arose?

Figure 28



➤ The driver for the development of contingency plans appears to have been the large number of security incidents. Organisations that have suffered security incidents tend to put contingency plans in place for the future. 83% of UK businesses that suffered a serious security incident had contingency plans in place, and 47% said they were very effective.

It is important that contingency plans make allowance for false alarms. One bank cited an incident where someone phoned the security team and claimed a member of staff was copying personal information and using it outside work; the allegation was untrue, but caused a great deal of wasted time.

One area where incident response procedures are weak is that only 10% have documented computer forensic guidelines. Forensic guidelines set out how to maintain evidence during an investigation from a legal perspective, and therefore increase the ability of a company to investigate incidents, fix problems and recover any lost assets. Few UK businesses appear to understand the importance of such guidelines - 72% of UK businesses (56% of large ones) do not have and do not plan to develop forensic guidelines.

One large company interviewed experienced problems due to lack of such guidelines. During a forensic investigation of downloaded pornography, the system administrator copied all the offensive material to present to the investigating officers, without realising that he himself was committing a crime by making copies. Another organisation's security team commented that they find interpreting the potentially conflicting legislation relating to IT security incidents to be a headache.

Earlier in this report, we saw that UK businesses rated their people, reputation and brand, and business relationships, as their most valuable assets, more important than their physical assets and intellectual property. This is entirely consistent with their priorities during security incident response, which are to resume normal business operations, prevent similar incidents occurring in the future and prevent damage to their reputation. Interestingly, preventing loss of staff morale is more important than recovering any stolen assets.

Reporting security incidents to the police or regulators tends to be the least important concern to UK businesses. 63% of UK businesses still believe this is important compared to only 5% that believe this is not important. However, it tends to lose out in practice, because often businesses fear that reporting incidents could attract unwanted attention from regulators or result in bad press.

This is consistent with other security surveys, both in the UK and abroad. For example, the 2001 CSI/FBI Computer Crime and Security

Survey showed that only 36% of US businesses reported security incidents to law enforcement agents, but that this had risen from only 15% in 1996.

Only 16% of organisations that had an incident took legal action. Most of the time, either no laws were broken (20%) or it wasn't considered serious enough (52%). 8% did not know who to prosecute and 4% did not want bad publicity. Given the poor quality of most organisations' forensic investigation procedures, it is likely that the ability of most UK businesses to successfully pursue legal action would, in any case, have proved limited.

A telecommunications company commented that legislation is not keeping up with technology and that this makes prosecution difficult.

Most UK businesses (53%) that suffered security incidents were able to restore normal business operations within a day. However, 20% of large organisations that had an incident took more than a week to get business operations back to normal. Many of these incidents were virus related, where viruses such as Sircam have proved extremely difficult to eliminate from an organisation.

It took one investment bank two weeks to track down the physical location of a rogue modem on one of their trading floors.

Most security incidents could have been prevented by better systems configuration (43%) or mitigated by better backup and contingency plans (32%). After serious security incidents, most businesses (84%) took actions, changing system configuration to prevent future problems (47%), updating detection software (28%) and amending backup and contingency plans (16%).

A retail bank explained that they routinely conduct post-incident reviews to record the lessons learnt from serious security incidents.

## Insurance

As the trend for organisations to participate in the global electronic economy increases, organisations are increasingly reporting a rise in more complex threats to their businesses from both internal and external sources, and the associated cost of incidents.

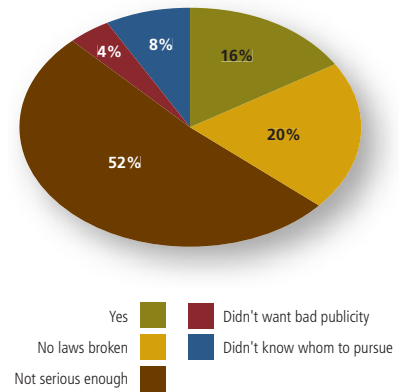
In this context, UK businesses need to decide how they are managing these risks. As with any other area of risk management, businesses can choose to accept the risks, mitigate them or transfer them using insurance cover.

For organisations that are highly dependent on their computer systems and the data contained within them, the risk management strategy for tackling these threats needs to be both proactive and reactive. ➤

# Incidence of Breaches

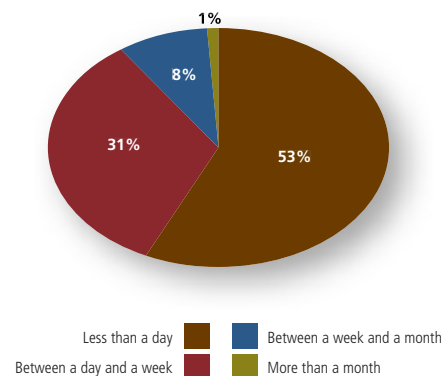
## Was legal action pursued?

Figure 29



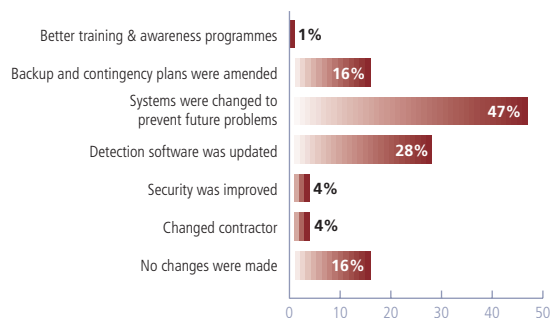
## How long did it take to restore business operations back to normal after a security incident?

Figure 30



## After the security breach, what changes were made to prevent future incidents?

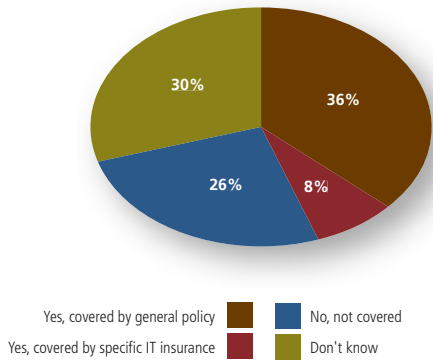
Figure 31



# Incidence of Breaches

## What proportion of UK businesses believe their insurance policies cover them for damage arising from security breaches?

Figure 32



► Insurance can be a useful tool for covering against the residual risk left after security controls have been implemented. It can also be a proactive control to transfer risk when the cost of mitigation would be too great.

Unfortunately, for many UK businesses, risk transfer is no longer an option. Increasingly, insurance companies are tightening their general policies to exclude the rising costs of insurance payouts in the light of high profile IT-related incidents.

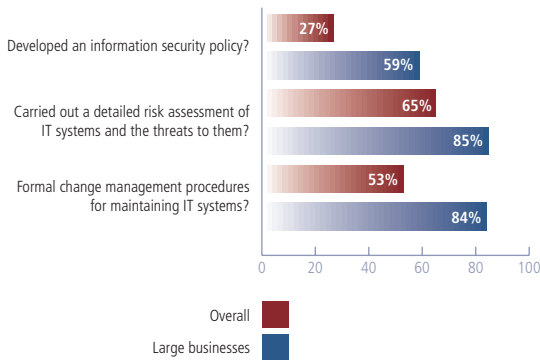
As a result, most UK businesses (56%) either are not covered by any insurance policy for damage arising from IT security breaches or do not know whether they are covered. This pattern is similar for all sizes of UK business.

To fill this gap, insurance companies are increasingly developing specific IT security insurance policies. Although in this survey only 8% of companies currently have specific IT insurance coverage, the adoption of such policies is rapidly growing.

UK businesses should check the status of their insurance cover for IT security breaches, to ensure their cover is in line with their overall risk management strategy.

## What proportion of UK businesses have:

Figure 33





## Basic Security Disciplines

A security policy represents the most basic discipline in information security. For information security to be effective, management need to set out their policies in respect of information security and communicate them across the organisation. With the increased board level sponsorship of information security, it is surprising to find that only 27% of UK businesses (59% of large businesses) have a documented security policy. This, however, is significant progress since 2000, when only 14% had a security policy.

It is essential that the security policy is reviewed periodically and revised to take account of changing circumstances across the business. There has been some progress here. 76% of businesses with a security policy review and update their security policy at least annually (compared to 68% in 2000), and 31% do this at least every six months (compared to 28% in 2000).

*This is not always the case. One consumer products manufacturer admitted that its security policy was out of date by at least 4 years.*

More encouraging is the progress in the number of UK businesses that have carried out a detailed risk assessment of their IT systems and the threats to them. In 2000, only 37% of UK businesses had done this. In 2002, this figure has increased to 66%, a marked improvement. This suggests that the increase in number of security incidents over the last two years has encouraged more organisations to understand the risks they run and manage the potential business impact. As in 2000, large businesses are more likely to carry out risk assessments than smaller enterprises.

Over the last two years, a number of security incidents were caused by software errors being introduced either on the launch of a new system or during regular systems maintenance.

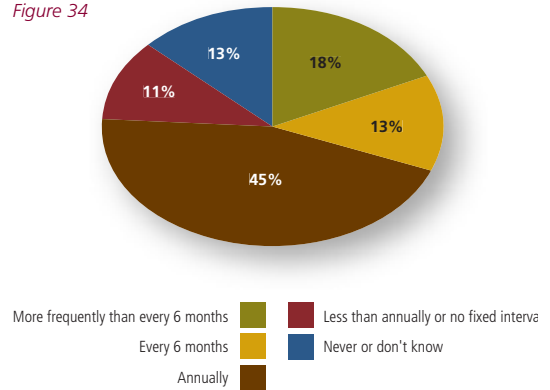
To minimise the risk of security weaknesses being introduced during routine systems maintenance, all organisations should have clear processes for managing, testing and promoting changes into the live environment. However, not all UK businesses appear to have this basic discipline in place. Only 53% (85% for large businesses) have formal change control procedures for maintaining their IT systems.

In addition, it is critical that security requirements are adequately addressed in the design of new IT systems. If security is, instead, a later bolt-on, it will be neither fully effective nor cost-effective. Yet, only 14% of UK businesses (32% of large businesses) always document how security requirements are being addressed in the design of IT projects and 25% (8% of large businesses) never do.

# Information Security Management

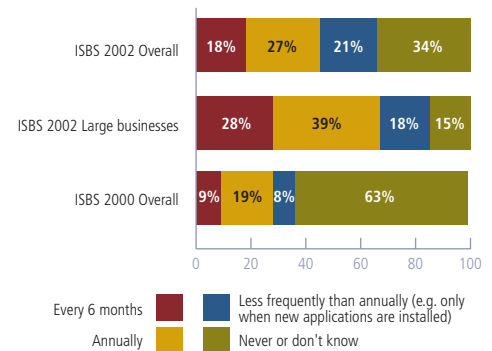
## How often do UK businesses with an information security policy review and update it?

Figure 34



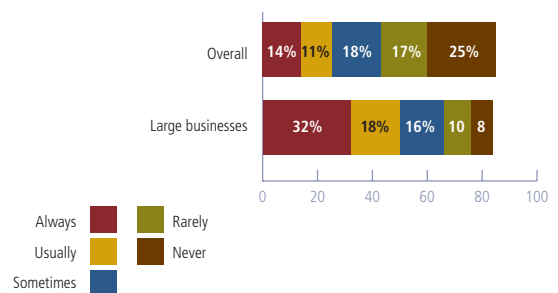
## How often, if at all, do UK businesses carry out a detailed risk assessment of their IT systems and the threats to them?

Figure 35



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

Figure 36

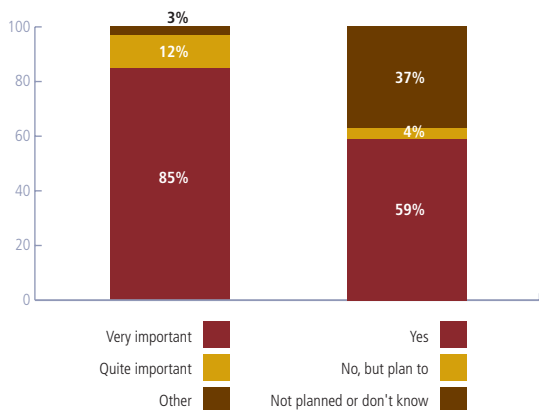


# Information Security Management

**How important do UK businesses feel their people are to their business?**

**Do UK businesses carry out background checks on staff and potential staff?**

Figure 37



**Why did UK businesses with a security policy develop that policy?**

Figure 38



## Employees, the Weakest Link?

People are often the weakest link for security, yet many organisations are failing to address this.

The vast majority of UK businesses (85%) rated their people as very important to their business, and less than 1% felt their people were not very important to their business.

Security risks from staff are becoming greater as a result of higher levels of staff turnover and changing staff roles. As a result, 16% of UK businesses (37% of large businesses) are concerned about the security threat to their organisation over the next year from their own staff.

With the human factor in information security so important, it is worrying that only 59% of UK businesses carry out background checks on staff and potential staff. Even more of a concern is that large businesses, that are most at risk, are no better at carrying out background checks than smaller enterprises.

One large bank commented that its business units tend to use large numbers of contractors for IT projects with minimal staff vetting, yet these contractors have access to highly sensitive systems.

It appears that many UK businesses are spending considerable time, effort and money on implementing sophisticated technology, without developing a security awareness culture within their organisation to support it.

As we saw earlier, only 27% of UK businesses have a security policy. More of a concern is that only 7% of those with a security policy said they developed it to educate employees about security issues and their responsibilities (e.g. to prevent fraud). Most businesses with a security policy developed it either out of a notion that it was good business practice to have one, or for legal or regulatory reasons.

The suspicion is that UK businesses are not educating their employees about security issues and staff obligations. Only 28% (33% for large businesses) make staff aware of their obligations regarding information security issues on joining or during induction, and 13% (but thankfully only 4% of large businesses) have no mechanism for making staff aware of their obligations at all. The picture is better for businesses that have a security policy, but still leaves a great deal to be desired.

Several organisations commented that people within the business do not take security seriously. One insurance company stated that their people tend to think data protection is the Data Protection Officer's responsibility, security is done by someone in IT and disaster recovery is down to Facilities to sort out.

However it is not always this way. One business now runs a quarterly security awareness competition on their Intranet. Last month, over 40% of staff entered the competition. This means that 40% of their staff had taken time to think

about security issues and their security policy, and read up on more difficult areas. Considering the £50 prize money awarded, that business felt this represented excellent value for money.

The sad reality is that staff's non-compliance with security obligations usually only comes to light in the event of a security incident and the subsequent investigation. Furthermore the number of such incidents is increasing. For example, 19% of UK businesses (49% of large businesses) have experienced security incidents in the last year related to employee web access, and 37% (55% for large businesses) have had security incidents in the last year related to Internet e-mail. These incidents include both inadvertent damage (e.g. virus infection) and the deliberate abuse of facilities provided to employees (e.g. access to, or distribution of, inappropriate content).

One business estimated that they had about 100 disciplinary cases a year for staff misusing company IT systems, mostly in respect of inappropriate e-mails or Internet surfing. Another commented that, at one point, their security team had 65 investigations into employees happening at the same time, roughly 25% of which resulted in formal disciplinary proceedings.

Interestingly, while most employee-related incidents are relatively minor, 4% of large businesses attributed their worst security incident in the last year to poor staff vetting, and 16% to poor staff training on security issues.

Yet, after serious security incidents, less than 1% of UK businesses affected (down significantly from the 12% observed in 2000) put in place better training and awareness programmes for their staff.

## Human Rights Exposure

While employers have a legitimate right to protect their systems against abuse by employees, employees have rights under Human Rights and Data Protection legislation to have their privacy respected.

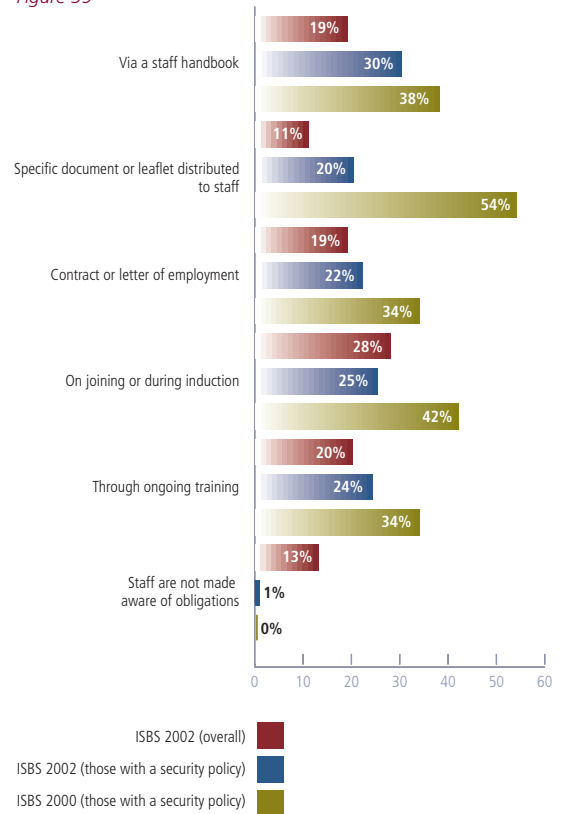
Unfortunately, only 24% of UK businesses (39% of large businesses) have put in place procedures to ensure compliance with the Human Rights Act and 56% (36% of large businesses) have no documented procedures and no plans for their introduction.

An example of an issue related to the Human Rights Act is the need for employers to identify when they can or cannot read an employee's e-mail and if necessary get permission from their employees to do so. 35% of UK businesses (62% of large businesses) ask employees to consent to the employer's right to read their e-mail (for example, in the event of an investigation). However, 51% (22% for large businesses) have no plans to introduce this consent. Many organisations consider their e-mail system as a business tool and therefore automatically assume their right to monitor it; this assumption could be dangerous given developments in Human Rights and Data Protection legislation.

# Information Security Management

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

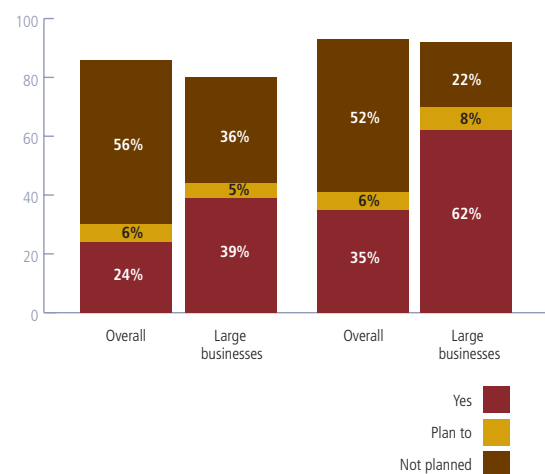
Figure 39



## Procedures for compliance with Human Rights legislation

## Employee consent to employer's right to read their e-mail in an investigation

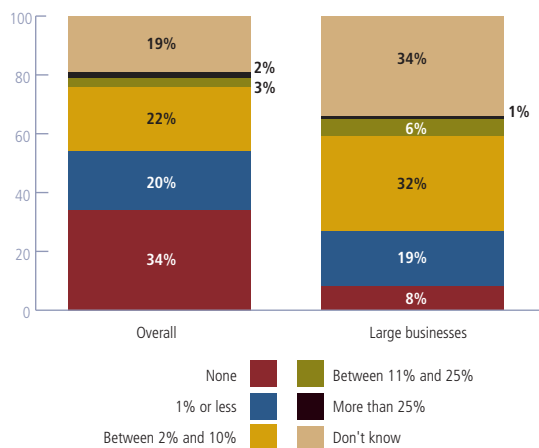
Figure 40



# Information Security Management

## What percentage of IT budget for the last year was spent on information security, if any?

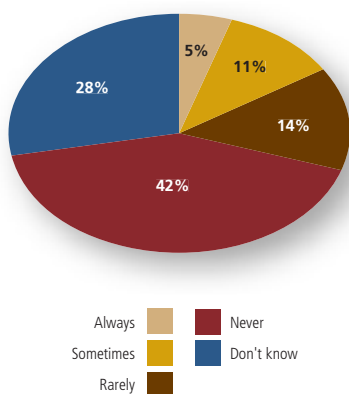
Figure 41



The 2000 survey reported that only 1% of organisations had a specific budget dedicated to information security.

## How often do UK businesses estimate the return on investment (ROI) on IT security expenditure?

Figure 42



## Investing in Security

In the 2000 survey, only 1% of UK businesses reported that they had a specific budget dedicated to information security. There has been progress since then, in that 81% of survey respondents in 2002 were able to estimate what percentage of their organisation's IT budget was devoted to information security. This was understandably harder for large businesses (where IT budgets are more complex), but even then 66% were able to provide an estimate.

The appropriate level of information security expenditure clearly depends on an organisation's business circumstances. However, a reasonable benchmark, based on global experience, is that an average of 3% to 5% of an organisation's total IT budget should be spent on IT security, rising to an average of 10% in high risk sectors, such as financial services.

Worryingly, UK businesses are not spending anywhere near that benchmark on their information security. Only 27% (39% for large businesses) spend more than 1% of their IT budget on information security. Only 5% (7% for large businesses) spend more than 10% of their IT budget on information security.

Some organisations feel that, as many security features are built into systems and processes, only specific IT security initiatives (e.g. security monitoring systems, intruder detection systems, time spent on investigations, etc.) are budgeted for separately.

More significantly, spend on information security is still seen as an overhead by the majority of UK businesses, rather than as an investment. Only 30% have ever evaluated return on investment (ROI) for IT security expenditure, and large businesses do not seem any better at this than smaller enterprises.

There are genuine difficulties associated with ROI calculations for IT security. Many of the benefits are intangible or difficult to measure, such as the reduction in wasted staff time or the prevention of reputational damage. It is also the case that most IT security professionals have a technical rather than commercial background, and so may lack skills in the development of commercial business cases.

However, guidance is increasingly available on how best to carry out these calculations. This survey has shown that the costs of inadequate security are rising fast, and that security is a critical enabler to effective business use of the Internet.

While the hearts of senior management now seem to embrace information security as a high priority to their business, until the case for IT security expenditure is expressed in terms that make sense to their heads, the pattern of under-investment is likely to continue. ROI is critical to breaking this cycle.

One security function commented that sometimes they almost wanted a serious security incident in their organisation so that the company would realise the importance of security and see the need to invest some money.

## BS 7799 Adoption

The British Standard for Information Security Management, BS 7799, has been widely acknowledged as an important framework for information security management. BS 7799 provides a benchmark against which organisations can assess their own IT security position, and that of their business partners.

In December 2000, BS 7799 received wider recognition through being adopted as an international standard, ISO 17799. Increasingly overseas companies are using the standard as a flagship for their information security management.

In the 2000 survey, only 25% of UK businesses were aware of the standard, and only 6% were able to quote its number. Given the amount of publicity about BS 7799 in the last two years, it might have been expected that awareness would now be significantly greater.

Rather than ask whether respondents knew of the existence of the standard, this year's survey focused on whether they were aware of its content. Since the respondents are the people responsible for IT security in their respective businesses, this provides a reasonable measure of how far BS 7799's concepts have permeated out into the UK IT security community.

In the event, only 15% of the people interviewed said that they were aware of the content of BS 7799. In large organisations, this number only rose to 42% which is still disappointingly low. Interestingly, in the separate ISBS web-site poll (not included in the above statistics), 69% of respondents were aware of the contents of BS 7799, an indication that the on-line poll attracted a different type of response to the statistically sampled telephone survey.

The low penetration of BS 7799 into UK businesses appears due to two main reasons. Firstly, while the cost of obtaining a copy of BS 7799 is relatively small, it appears to inhibit widespread awareness of the standard's contents, and many businesses would prefer to have the standard available free of charge in electronic form. Secondly, the perception of many is that BS 7799 is based around a large enterprise model and would require quite a lot of expertise and expense to implement.

While awareness is still patchy, significant numbers of UK businesses are now compliant with BS 7799. 38% of those aware of the standard have already adopted it in their organisation and 18% are planning to in the near future. This means that approximately 80,000 UK businesses are now compliant with BS 7799, and a further 40,000 are planning to be in the next year.

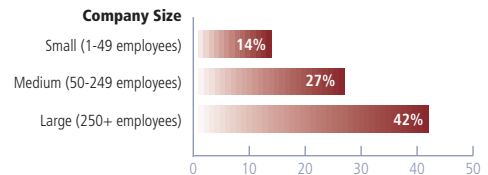
What is more, 48% of those that are compliant have obtained some form of accreditation of their compliance against the standard by a third party - this equates to roughly 40,000 UK businesses. Very few of these were formally certified on the BS 7799 Certificate Register; most have simply had some form of security audit.

One financial services provider certificated to BS 7799 commented that this had brought significant benefits. As well as an obvious marketing benefit, it has provided a useful forum to bring user security education and awareness up to a meaningful benchmark. They also use the BS 7799 compliance audits to flush out security good practice points and to provide a useful framework for ensuring security issues are resolved in a timely manner.

# Information Security Management

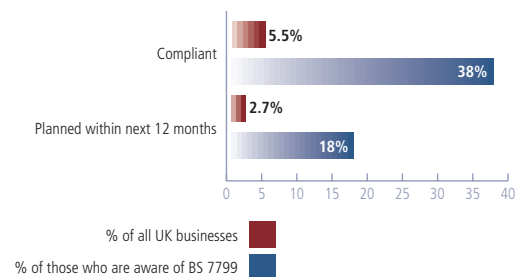
## What proportion of UK businesses are aware of the contents of BS 7799, the British Standard for Information Security Management?

Figure 43



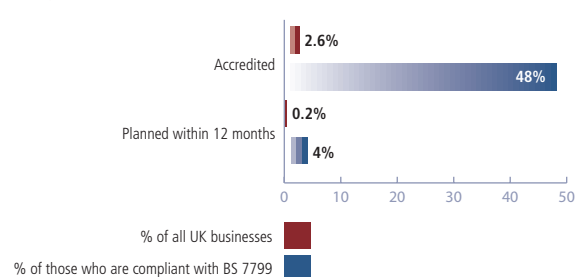
## What proportion of UK businesses are compliant with BS 7799?

Figure 44



## What proportion of UK businesses have had their compliance with BS 7799 accredited by a third party?

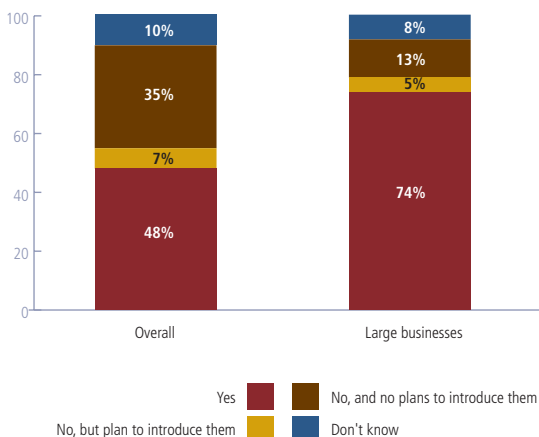
Figure 45



# Information Security Management

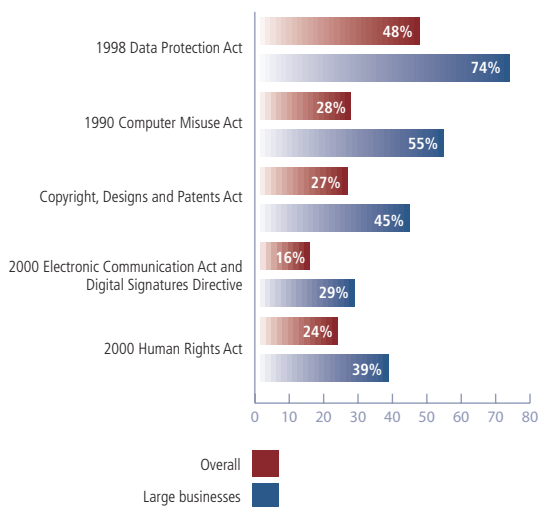
## Do UK businesses have documented procedures to ensure compliance with the Data Protection Act 1998?

Figure 46



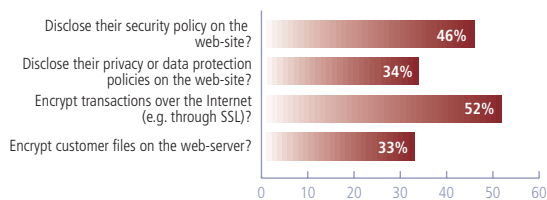
## For which laws do UK businesses have documented procedures?

Figure 47



## What proportion of the UK's transactional web-sites:

Figure 48



## Data Protection

Data Protection legislation continues to develop across the globe as a result of constant press attention to privacy issues. Businesses need to respond by ensuring they are aware of the risks to which they are exposed and how those risks are mitigated.

The principles of the UK Data Protection Act require that personal data should be processed fairly and lawfully. It is the organisation's responsibility to ensure that personal data is accurate.

Worryingly, only 48% of UK businesses (but 74% of large businesses) reported having documented procedures to ensure compliance with the UK Data Protection Act 1998. This indicates that a significant number of UK businesses either are unaware of their data protection duties or see compliance as a low business priority.

If the Act is contravened, the data controller can be ordered to pay compensation to an individual if the controller has caused him or her to suffer any damage. In addition to this, there is significant reputational risk associated with non-compliance. However, the Data Protection Commissioner has so far publicly admonished only relatively few UK businesses, so the evidence is that most UK businesses do not yet perceive this as a real threat to them.

There have been several high profile news reports of customers inadvertently accessing other customers' information on-line or hackers breaking into web-sites and stealing customer information. These are reinforced by this survey, which shows 2% of transactional web-sites acknowledge they have suffered theft of customer data (e.g. credit card details).

A significant number of transactional web-sites do not appear to be providing the information a consumer would need to give informed consent to provide his or her personal data to the web-site. Only 34% of transactional web-sites (39% for large organisations) disclose their privacy or data protection policy on the web-site. Closely related, only 46% of transactional web-sites (whether large or small) disclose their security policy on the web-site. Anecdotal evidence also suggests that many web-sites lack the necessary controls to prevent marketing approaches to any customers who have asked (either directly or via preference services) to be excluded from such marketing.

Finally, many multi-national organisations are processing personal data and are routinely transferring it to countries or territories that are outside the European Economic Area. Many of these have encountered significant practical difficulties with meeting the requirements of the Data Protection Act.

## Use of Experts

ISBS 2002 has uncovered a clear knowledge gap among many people responsible for IT security in UK businesses. This is not surprising given the changing environment and the general shortage of security professionals.

In many cases, this security knowledge gap can be addressed by the use of external security consultants to supplement in-house capabilities. Surprisingly, only 12% of UK businesses (32% of large businesses) have used external security consultants for advice and guidance in the last year (similar to the levels of third party testing seen in the 2000 survey). It seems likely that this proportion will increase rather than decrease in the coming years, with external experts playing a useful role helping businesses with risk assessment, security design, and security product selection and implementation.

The single biggest use of external security consultants (and one which is rapidly growing) was in the provision of penetration testing. Penetration testing (also known as vulnerability assessment) involves attempting to breach security controls using the same tools and techniques that hackers use. It is often very effective for detecting security vulnerabilities, for example in web-sites or Internet gateways. 21% of UK businesses with web-sites (rising to 46% of large transactional web-sites) have commissioned penetration testing. A further 7% of UK businesses plan to do so in the near future.

Another significant role for the external security consultant is in the provision of assurance about an organisation's compliance with standards. External consultants have been busy reviewing BS 7799 compliance, with almost half of BS 7799-compliant organisations having their compliance independently assessed by a third party.

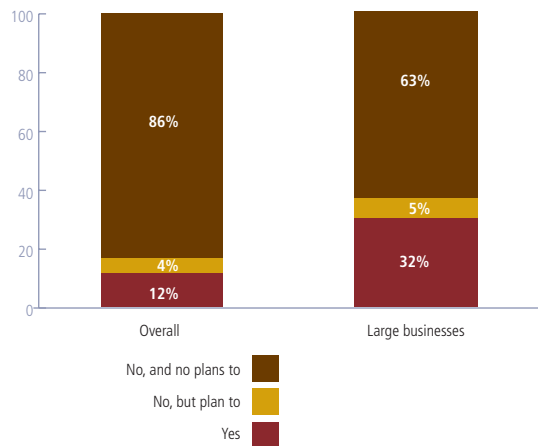
In addition, web-seals and other forms of third party accreditations are increasingly being displayed on organisations' web-sites to improve customer confidence in the web-site's security. 14% of transactional web-sites (23% for large businesses) have some form of third party accreditation (e.g. web-seal) on them, and a further 6% are planning to obtain such accreditation. External security consultants are often used to help web-sites achieve the necessary standard to receive the web-seal.

When selecting external security consultants, integrity and trustworthiness were by far the most important attributes, with 78% of UK businesses citing them as very important. A similar tendency has been noted in other recent surveys; for example, the CSI/FBI 2001 Computer Crime and Security Survey showed that only 16% of respondents would consider hiring reformed hackers as consultants.

# Information Security Management

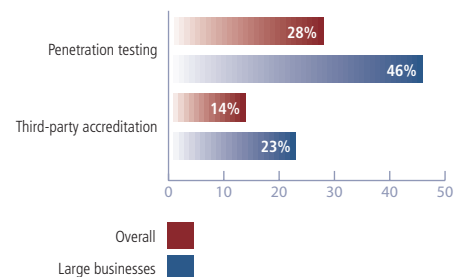
## Have UK businesses used external security consultants in the last year?

Figure 49



## Have transactional web-sites used external security consultants in the last year?

Figure 50



## Which of the following attributes are very important when selecting security consultants?

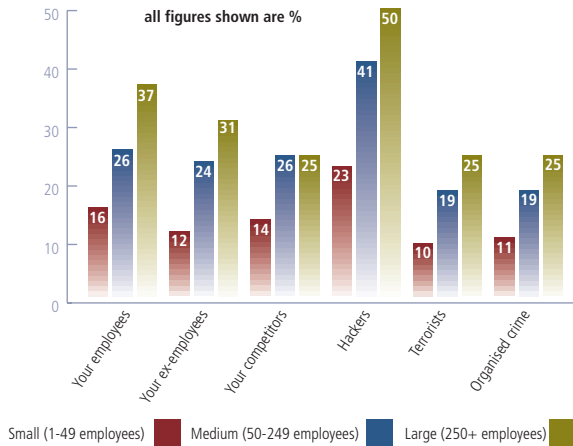
Figure 51



# Information Security Management

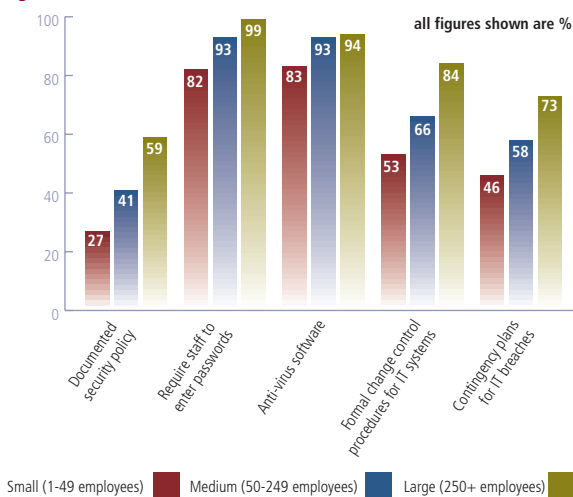
## How concerned are UK businesses about the threat from:

Figure 52



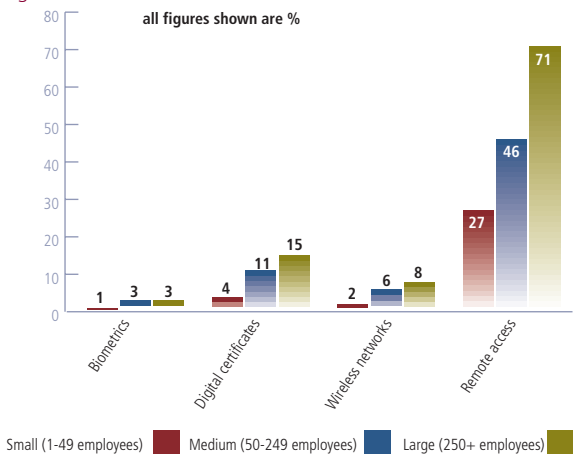
## Which of the following security procedures do UK businesses currently have in place?

Figure 53



## Which of the following technologies are used in UK businesses?

Figure 54



► While the price of security consultants was still an important consideration, it appears that most UK businesses place a higher priority on other attributes, and so are correctly focused on a 'value for money' rather than 'lowest bidder' solution to their security needs.

## Variations by Size

The ISBS 2000 survey demonstrated how the perceived value of information security differed between large businesses and smaller enterprises. A similar pattern has emerged in 2002.

Large businesses are still more concerned about all types of security threat than smaller enterprises. More large businesses think the number of security incidents will increase in the next year (50% versus 29% for small businesses) and less think the number of incidents will decrease (14% versus 16% for small businesses).

Large organisations are also more pessimistic (some might say realistic) about the difficulty of catching future security breaches, with 50% (versus 40% for small businesses) believing it will get more difficult to catch incidents and only 16% (versus 19% for small businesses) who think it will get easier.

As a consequence, large businesses tend to be better at putting in place security controls than smaller enterprises. Large businesses are twice as likely as small ones to have a security policy. It is virtually unheard of for a large business not to require staff to authenticate themselves (e.g. through passwords) to access systems, whereas nearly one in five small businesses do not require this. Large businesses are nearly twice as likely to have procedures for responding to incidents and contingency plans as small businesses.

Large businesses invest more in security technology. 39% of large businesses spend more than 1% of their IT budget on information security, compared to only 27% of small businesses that do so. Large organisations are 3-4 times more likely to be early adopters of technology than small organisations, as can be seen by the latest adoption rates for emerging technologies in this survey.

While large businesses are spending the most and generally doing best at security, and small businesses are least likely to be targeted by a security attack, medium-sized businesses fall unhappily in-between. Not as well-controlled as the large businesses, but an attractive enough target to the hacker, medium-sized businesses have suffered the greatest incidence of web-site security incidents (19% compared with only 13% in large businesses).

Many small businesses seem to be relying on it never happening to them. Given the increasing sophistication and usage of automated tools that roam the Internet for interesting gateways or web-sites, this may prove a dangerous assumption.



## Web-site Security

The use of web-sites is now widespread. 70% of UK businesses (89% of large businesses) now have their own web-site, and more than half (56%) said that these web-sites were important to their business.

Despite the horror stories in the press about web-sites being attacked by hackers, 76% of UK businesses with a web-site are confident that they have in place sufficient controls to prevent or detect all security incidents associated with their web-site(s). Furthermore, only 23% of organisations (50% of large ones) are concerned about the security threat to their organisation over the next year from hackers.

However, this high level of confidence may be misplaced. Many UK businesses are lacking the most basic security controls over their web-sites.

Every UK business with a web-site should ensure that it has a firewall in place between the Internet and its web-server. A firewall is a device that acts as a filter, allowing only permitted network traffic to pass through the Internet gateway. Without a firewall to protect it, a web-site is exposed to a variety of possible attacks from the Internet. Yet, only 66% of UK web-sites (88% for large businesses) have a firewall in place. This is progress since the 2000 survey, when only 41% of UK web-sites had web-site protection, but compares poorly with the 95% of US large businesses who have firewalls in place (according to the CSI/FBI 2001 Computer Crime and Security Survey).

A firewall is only effective if it is adequately hardened and kept up to date with the latest security patches. Often, the only way to be sure a firewall is effective is to scan it using the same tools and techniques the hackers use (penetration testing). Only 21% of UK web-sites (45% for large businesses) have so far commissioned penetration testing, but this is rising rapidly.

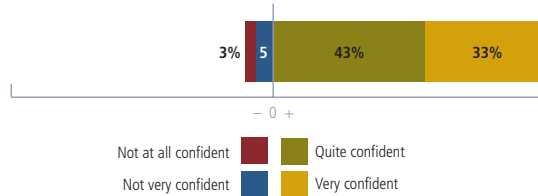
An integral part of defending against hacking activity is to be able to see and understand the network traffic through the firewall. At a minimum, web-site logs should be retained, and 64% of UK web-sites (74% for large businesses) are doing this. A more recent trend is the increasing use of intrusion detection software, and 33% of UK web-sites (46% for large businesses) now have intrusion detection in place. This compares with 61% of US large businesses (according to the CSI/FBI 2001 Computer Crime and Security Survey).

UK web-sites also appear exposed to downtime. Only 40% of businesses with web-sites (47% for large businesses) have any form of redundancy or fall-back site for their web-site.

## Security Practices in Place - Technology

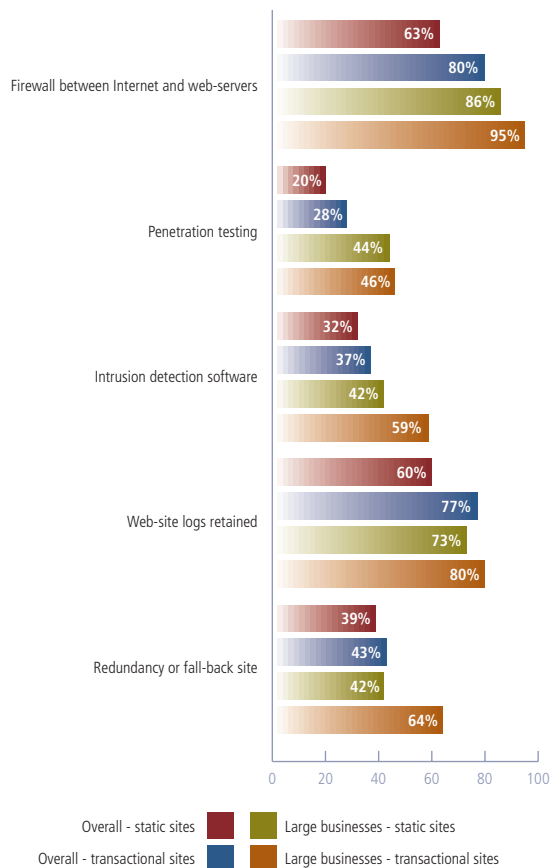
**How confident are UK businesses that sufficient controls are in place to prevent or detect all security incidents associated with their web-site(s)?**

Figure 55



**What security controls are currently in place over UK web-sites?**

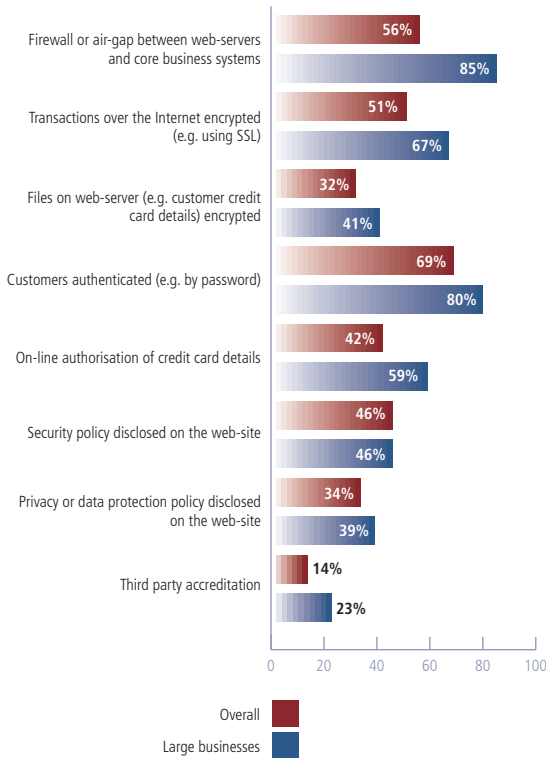
Figure 56



# Security Practices in Place - Technology

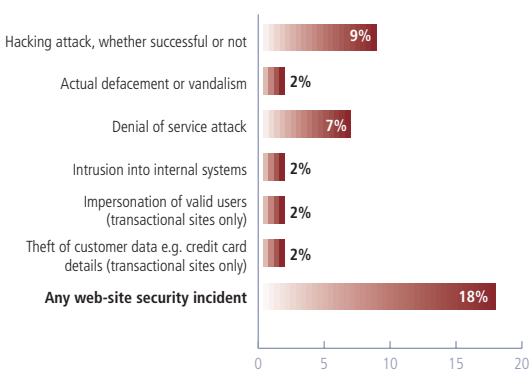
## What security controls are currently in place over transactional web-sites?

Figure 57



## What kind of security incidents have UK web-sites suffered?

Figure 58



## Transactional Web-sites

Selling products across the Internet is becoming a common way of doing business, with roughly 18% of web-sites now accepting transactions.

Transactional web-sites have the added burden of needing to protect transaction information. Unless transactions are encrypted while travelling over the Internet (e.g. through use of SSL), they can potentially be intercepted in transit. Yet, surprisingly only 51% of transactional web-sites (67% for large businesses) encrypt transactions over the Internet and only 32% of transactional web-sites (41% for large businesses) encrypt files (e.g. credit card details) held on their web-servers.

In addition, transactional web-sites need to check the identity of customers seeking to transact on the web-site. Again, only 69% of transactional web-sites (80% for large businesses) require customers to authenticate themselves (e.g. by passwords), and only 42% of transactional web-sites (59% for large businesses) check credit card authorisation on-line. Some web-sites are likely to be significantly exposed to credit card fraud as a result.

## Hacking Activity

Hacking activity captures a lot of press activity. ISBS 2002 shows, however, that, while hacking activity in the UK has tripled since 2000, the number of actual hacking incidents is still relatively low. 82% of UK businesses with a web-site were not aware of any attacks on their web-site(s).

However, hacking activity has seriously disrupted some UK web-sites. Roughly 2% (17,000 sites) have suffered actual defacement or vandalism (either directly or as a result of events like the Netnames incident), roughly 7% (66,000 sites) have been subject to a denial of service attack, and 2% have suffered actual intrusion through their web-site into their internal systems. Roughly 2% of transactional web-sites (3,000 sites) have had consumer data (e.g. credit card details) stolen from them.

Interestingly, the incidence rate for hacking activity in the UK appears to be much lower than in the US. According to the CSI/FBI 2001 Computer Crime and Security Survey, 40% of respondents (mostly large US corporations) detected system penetration through their Internet gateway and 36% detected denial of service attacks on their web-site(s). There are two main reasons for this. Firstly, US dot-com sites tend to be higher on hackers' target lists than UK sites. But, secondly, US businesses are much more advanced in their use of intrusion detection systems. Put another way, many UK businesses have no idea that they are under attack or whether they have been penetrated.

One financial services provider commented that their web-site is frequently port-scanned and attacked; the first attack took place within 10 minutes of their web-site going live. An oil company observed that their intrusion detection systems normally log an average of 3,000 pings or scans per hour, peaking at 70,000 per hour when Nimda was at large.

Sometimes incidents are outside an organisation's direct control. A bank had recently launched its on-line banking service, when its call centre received several

complaints saying that customers could see pornography on the bank's site. When finally tracked down, this was identified as a cache overflow problem at the customers' ISP, which had performed unpredictably under load and displayed other sites' pages!

One might expect that large businesses would have the greatest number of web-site security incidents, given they are most likely to be targeted by hackers. In fact, this is not the case. As an organisation's size increases, the threat of attack increases but usually the vulnerability reduces (due to better controls being in place). As a result, medium-sized businesses have suffered the greatest incidence of hacking attacks (19% compared with only 13% in large businesses).

While one business lowered its e-mail gateway security to carry out routine maintenance, a hacker was able to gain access and launch an advertising campaign from their gateway. Over the next few days, the business received 22,000 responses to the e-mail!

Unfortunately, it is likely that the upwards trend in hacking attacks will continue. Attack techniques are getting ever more sophisticated and easier to employ. UK businesses need to ensure they have well-configured firewalls and intrusion detection systems in place to protect their web-sites against the hacker threat.

For organisations lacking in-house expertise, not least the medium-sized businesses that seem to be most exposed, outsourcing may prove the best option. Some (but not all) web-site hosting providers offer managed firewall and intrusion detection services as part of that hosting service. Even if web-servers are hosted internally, a number of managed security service providers can remotely manage firewall configuration and intrusion detection on a continuous (round the clock) basis.

### Internet E-mail and Web Browsing

Internet e-mail and web browsing are ubiquitous. At the time of ISBS 2000, 70% of organisations already had access to the Internet. ISBS 2002 shows that 77% of UK businesses (91% of large ones) now allow their staff to send or receive e-mail across the Internet and 69% (92% for large businesses) give web access to their employees. In addition, 82% of these organisations believe Internet e-mail is important to their business (57% believe it is very important), and 62% of these organisations also believe employee web access is important to doing business.

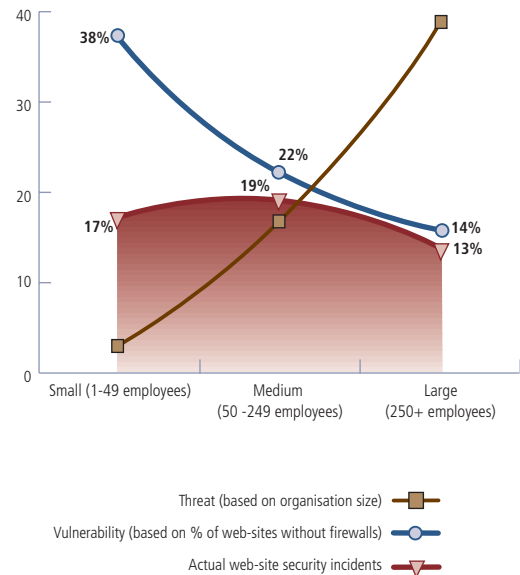
Unfortunately, as mentioned previously in ISBS 2000, the Internet has rapidly become the most significant means through which viruses (and other malicious code) are spread. According to the CSI/FBI 2001 Computer Crime and Security Survey, 94% of respondents (mostly large US corporations) detected viruses in their incoming e-mails or web downloads. Employees have also abused the privileges given to them by accessing or distributing inappropriate material over the Internet.

Despite these threats, over three-quarters of businesses that provide employees with Internet e-mail or web access are confident that sufficient controls are in place to prevent or detect all security incidents associated with it.

## Security Practices in Place - Technology

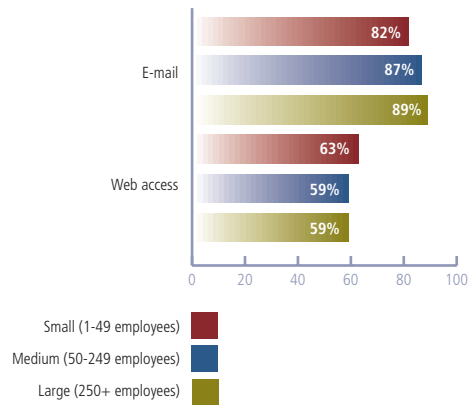
### Which web-sites are most at risk?

Figure 59



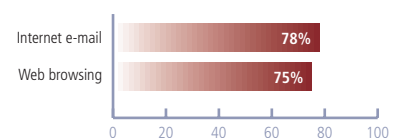
### Is Internet e-mail and employee web access important to UK businesses?

Figure 60



### How confident are UK businesses, that provide Internet e-mail or web browsing, that sufficient controls are in place to prevent or detect all security incidents associated with them?

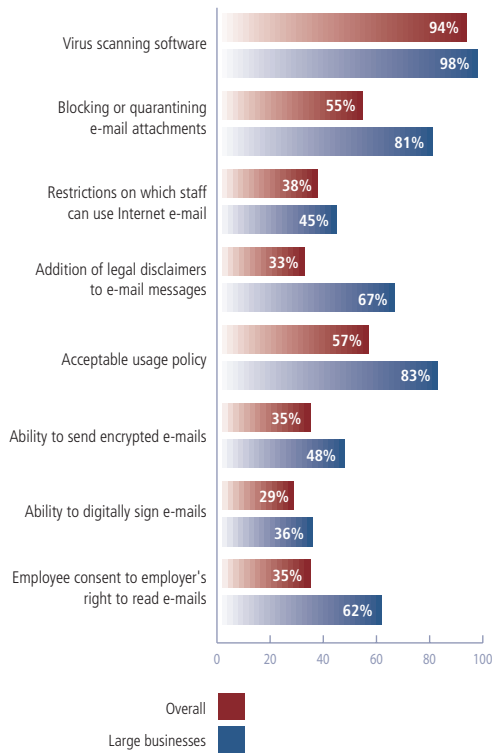
Figure 61



# Security Practices in Place - Technology

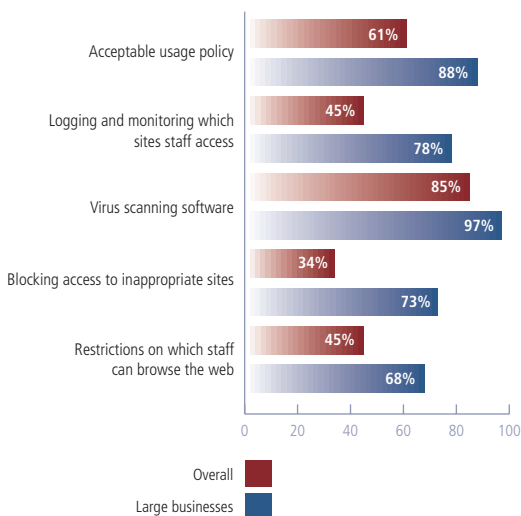
## What security controls do UK businesses have in place over Internet e-mail?

Figure 62



## What security controls do UK businesses have in place over web browsing?

Figure 63



## Use of Anti-Virus Scanning Software

Almost all UK businesses have implemented anti-virus software to protect themselves against incoming viruses from the Internet. 83% of businesses (and 94% of large businesses) have anti-virus software in place on desktops and servers.

In addition, 94% of UK businesses that provide employees with Internet e-mail (98% of large ones) have software installed that scans file attachments for viruses. 85% of businesses that provide employee web access (97% of large ones) have software installed that scans file downloads for viruses.

This represents significant progress since 2000, when only 67% of UK businesses had anti-virus scanning software, and only 32% and 28% had e-mail scanning and web scanning software respectively. UK businesses are now almost up to the same level as their US counterparts, where according to the CSI/FBI 2001 Computer Crime and Security Survey, 98% of respondents (mostly large US corporations) had anti-virus software in place. It does, however, seem incredible, given the recent spate of serious virus outbreaks, that any business connected to the Internet would choose not to have anti-virus software in place.

## Other Controls over E-mail and Web Browsing

A significant and increasing number of UK businesses restrict which employees are allowed to use Internet e-mail or browse the web. 45% (68% for large businesses) restrict web browsing, compared to 30% in 2000. 38% (45% for large businesses) restrict Internet e-mail, compared to 17% in 2000.

Most UK businesses that provide employees with Internet e-mail or web browsing have an acceptable usage policy, that sets out what employees may and may not do with that access. 57% (83% for large businesses) have a policy for e-mail usage, and 61% (88% for large businesses) have one covering web access.

A growing number of UK businesses, particularly large ones, also block access to certain types of information. 55% (81% for large businesses) block and quarantine certain e-mail attachment types. 34% (73% for large businesses) block access to inappropriate web-sites. 45% (78% for large businesses) log and monitor which web-sites staff access. It tends to be businesses that have suffered employee abuse in the past that put these preventative controls in place.

Several businesses commented that they would like to implement site blocking at the proxy server, but could not because of internal debate as to which sites should be blocked. For example, an investment bank did some analysis and found certain staff were visiting gambling web-sites, however it turned out this was part of an important business project.

The use of cryptographic tools does not seem to be as common as one might hope. Only 35% of UK businesses that provide employees with Internet e-mail (48% of large businesses) have the ability to encrypt e-mails passing over the Internet, and only 29% (36% of large ones) can digitally sign Internet e-mail.

One insurance company explained that it has not implemented e-mail encryption because of the need to scan incoming messages for viruses and inappropriate content.

Finally, two-thirds of large businesses using Internet e-mail have a legal disclaimer added to all outgoing e-mails, but this is less common amongst smaller businesses.

### Virus Infection

This survey shows that 42% of UK businesses (52% of large ones) that provide Internet e-mail have suffered from virus infection as a result of e-mail attachments and 20% of UK businesses (36% of large ones) that provide employee web access have experienced virus infection arising from files downloaded from the web. Overall, about 41% of UK businesses suffered from virus infection or disruptive software, a massive increase from the 16% in ISBS 2000.

Interestingly, there is a strong correlation between small enterprises suffering virus infection from e-mail and those suffering it from web access, suggesting poor controls are to blame. In large businesses, however, there is less strong correlation, suggesting incidents are arising despite the level of control.

These figures are similar to the levels experienced in large US corporations, where, according to the CSI/FBI 2001 Computer Crime and Security Survey, 35% of respondents had quantifiable losses as a result of virus infection.

*One business interviewed picked up 55,000 viruses at the perimeter of their network in the last year, and had roughly 500 PCs infected by a virus per quarter.*

One might ask why the incidence of virus infection is so high given that almost every UK business has anti-virus software in place. Unfortunately, the war against viruses is a continual struggle; these days, new viruses come out with alarming frequency and are increasingly sophisticated. During 2001, Code Red, Nimda and Sircam have all taken virus evolution on a stage, in the same way that the Love Letter did in 2000 and Melissa before that in 1999. Organisations are now facing blended threats that possess characteristics of worms, viruses and Trojans, and blend these with hacking techniques to achieve several new methods of distribution. As the threat from virus writers and hackers converges, businesses need a combination of firewall, anti-virus and intrusion detection – anti-virus alone is no longer sufficient (as many businesses that suffered from Code Red will testify). While the vast majority of UK businesses have anti-virus software, less have good firewalls and intrusion detection in place.

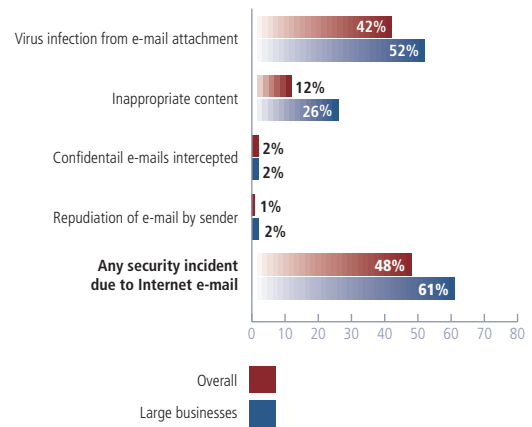
In addition, anti-virus software is only as good as its last update. New viruses are sweeping the world within hours of release. System administrators, therefore, have to continually monitor for new virus outbreaks, and are then faced with a race to get the latest anti-virus updates and security software patches installed on their systems before the wave of virus infections strikes. Increasingly, organisations are implementing a layered defence of anti-virus measures, with automatic frequent update of anti-virus software.

*One large insurance company commented that the complexity of their infrastructure made it a major undertaking to apply all new patches and upgrades to anti-virus software and get this rolled out across all systems and desktops.*

## Security Practices in Place - Technology

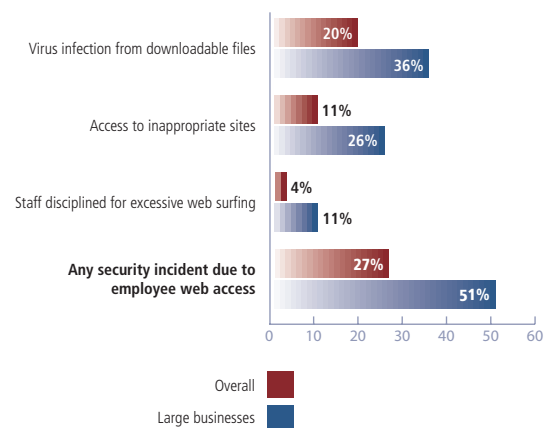
### What security incidents have UK businesses that provide Internet e-mail suffered?

Figure 64



### What security incidents have UK businesses that provide employee web-browsing suffered?

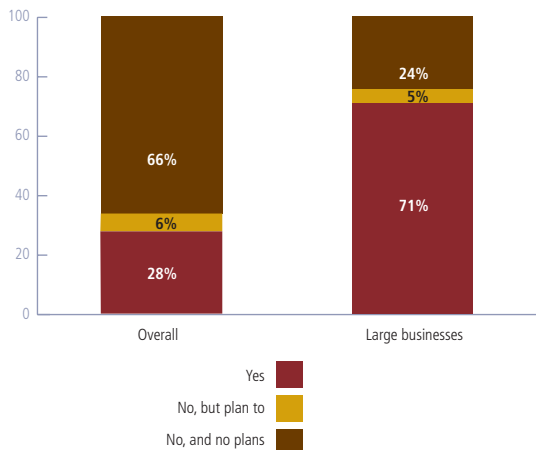
Figure 65



# Security Practices in Place - Technology

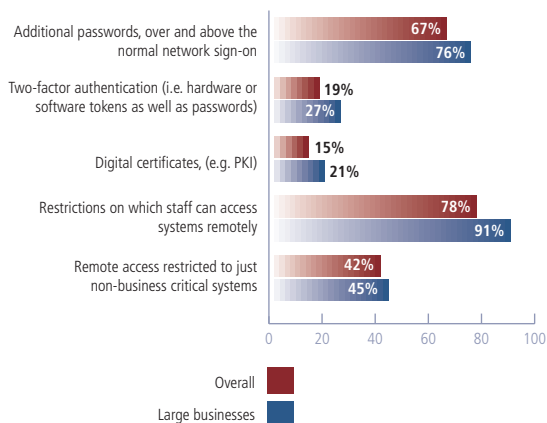
## Can employees access any computer systems from a remote location?

Figure 66



## What security controls are typically in place over remote access?

Figure 67



## Net Abuse

Abuse of Internet access has occurred in a significant number of UK businesses. 12% of UK businesses that provide Internet e-mail (26% of large ones) have experienced staff sending or receiving inappropriate content (e.g. pornography) by e-mail. Similarly, 11% of UK businesses that provide employee web access (26% of large ones) have experienced staff accessing inappropriate web-sites (e.g. pornography), and a further 4% (11% of large ones) have disciplined staff for excessive web surfing.

This is still a relatively low level compared to experience in large US corporations, where according to the CSI/FBI 2001 Computer Crime and Security Survey, 91% of respondents detected employee abuse of Internet access privileges. However, this may be a matter of degree, since only 18% of respondents had quantifiable losses as a result of this type of security incident.

One large financial services provider had grown through acquisition, with the result that there were many different Internet gateways. This hindered putting in place preventative controls over web browsing. As a result, they had to deploy a team of security specialists focused on investigating employee abuse.

## Remote Access

An increasing number of UK businesses are opening up their systems to remote access by staff; this happens in 28% of UK businesses (71% of large ones). This is a continuation of a trend noted in ISBS 2000, where 37% of UK businesses allowed some employees to work from home but relatively few allowed remote access into corporate systems. Remote access can be by dedicated dial-up or increasingly directly across the Internet.

69% of organisations providing remote access believe it is important to their business (42% believe it is very important), compared with 15% who believe it is relatively unimportant. The main drivers for employee remote access are increased productivity (ability to access corporate systems when on the move), staff satisfaction and loyalty (flexible working hours and working from home) and cost reduction (ability to hot desk or hotel office space).

85% of organisations providing remote access are confident that sufficient controls are in place to prevent or detect all security incidents associated with remote access, compared with only 7% who are not confident.

A process of authentication to verify users' identities is vital to controlling remote access. Two-thirds of businesses rely on additional passwords to protect their remote access, with only 19% using two-factor authentication (i.e. use of hardware or software tokens as well as passwords) or digital certificates (e.g. PKI) to prove identity. Worryingly, a third of businesses that are providing remote access do not require any additional authentication over and above the normal network sign-on.

It is also important to have a process for access control, to ensure that remote users can access only appropriate resources. 78% of UK businesses that provide employees with remote access (91% of large ones) restrict which staff can access systems remotely. A further 42% restrict remote access to just non-business critical systems.

Relatively few UK businesses (5%) have identified security incidents associated with remote access (e.g. outsiders attempting to break

into corporate systems through remote access). However, a very high number (20%) did not know whether they had any security incidents associated with remote access.

### The Identity Management Challenge

Increasingly, organisations are seeking to replace their existing remote access mechanisms with staff accessing systems across the Internet instead. Both internal and remote access to systems can then be managed through a web portal.

The main benefit of this approach is that it potentially provides a simple mechanism for staff to access all the enterprise resource planning (ERP) or legacy systems they use on a day-to-day basis. It can also reduce the number of passwords each user has to remember, and the associated cost of user administration. Use of the Internet is significantly cheaper than dedicated dial-up facilities for remote access. Furthermore, employee portals can be progressively opened up over time to business partners and customers, improving service to them and reducing administrative costs.

The key challenge with this approach is one of identity management - how to ensure that the right people have the right access to the right information at the right time. This is difficult to achieve, especially in a large organisation where staff come and go, and people's roles change. Adopting the right security techniques is a critical business enabler, since without the right security, the risks associated with opening up core business systems to access across the Internet are prohibitive.

To achieve the remote access, typically a virtual private network (VPN) uses the infrastructure of the Internet to securely transmit data between the user's computer and the corporate site. So far, 26% of UK businesses that provide employees with remote access (49% of large ones) have already moved onto VPN technology, with a further 10% of large businesses planning to do so.

As with other remote access, authentication is critical. Most implementations have involved a range of authentication techniques from username and passwords, to more powerful mechanisms like tokens and digital certificates.

Access control is normally provided by privilege management infrastructure (PMI) software. This controls which people can access which systems or resources across the Internet. Most implementations rely on a single directory of user details (either in a lightweight directory access protocol (LDAP) directory or in a database), against which user rights can be checked.

Finally, new techniques are emerging to reduce the cost of managing a large user community (sometimes up to several million users) across a distributed enterprise. User management typically involves automated workflow processes that streamline user administration.

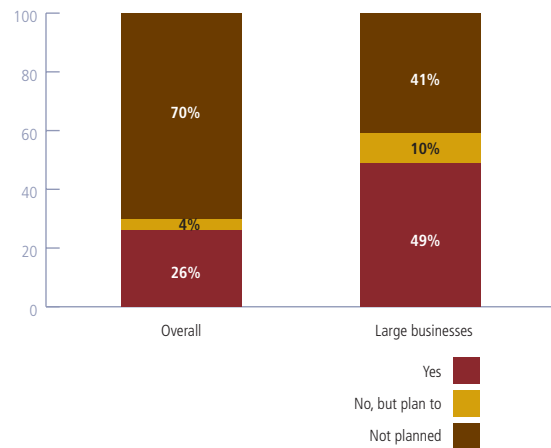
*One large insurance company highlighted user management as a major area for improvement. User ids and passwords do not get cleaned up when temporary staff leave, because there is no process or requirement for managers to notify HR.*

Identity management provides businesses with the opportunity to significantly reduce overall IT and operational costs. It seems likely that many UK businesses will implement identity management over the coming years.

## Security Practices in Place - Technology

### Are UK businesses that provide remote access using virtual private network (VPN) technology?

Figure 68



### Identity management

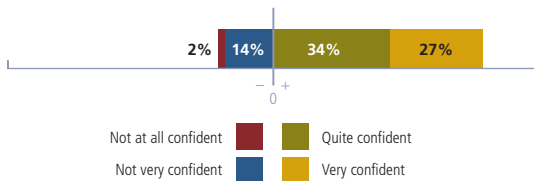
Figure 69



# Security Practices in Place - Technology

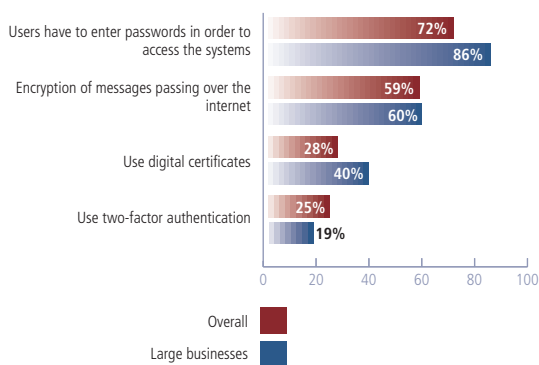
**How confident are UK businesses that sufficient controls are in place to prevent/detect all security incidents relating to e-procurement and EDI?**

Figure 70



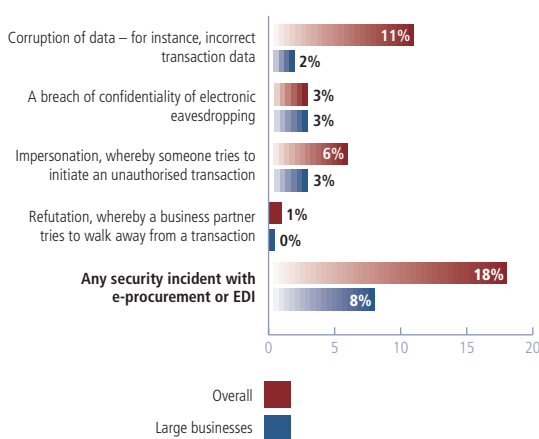
**Which of the following controls over e-procurement or EDI do UK businesses currently have in place?**

Figure 71



**What security incidents have UK businesses suffered in the last year relating to using e-procurement or EDI?**

Figure 72



## E-Procurement and EDI across the Internet

Electronic data interchange (EDI) is the exchange of data between computers, in a form that allows for automatic processing without manual intervention. Simple trade messages are created by using the standard international identification codes for goods, services and locations. The use of translation software means that EDI can take place with no restrictions on the hardware and software and it enables organisations to communicate with each another in a more cost efficient manner. EDI used to take place over proprietary networks, but increasingly it is now carried out over the Internet.

A related business activity is e-procurement, where users in one organisation purchase products or services from other organisations through a purchasing portal. E-procurement is facilitated through the use of EDI messages passing across the Internet.

While 61% of the UK businesses using e-procurement or EDI across the Internet are confident that sufficient controls are in place to prevent or detect all security incidents associated with it, 16% are not confident. Compared with other areas in the survey, respondents were least confident about the security over their e-procurement and EDI activities.

72% of UK businesses carrying out e-procurement or EDI over the Internet (86% of large businesses) require users to authenticate themselves (e.g. through passwords) to gain access to EDI/e-procurement systems, and only 25% require two-factor authentication. This is surprisingly low, and perhaps explains the 6% of organisations that have suffered impersonation, where someone tries to initiate a transaction in someone else's name.

Only 59% of UK businesses using e-procurements/EDI encrypt messages passing over the Internet. This is also surprisingly low, and, given this, it is perhaps not surprising that 3% have suffered a breach of confidentiality.

Digital certificates bring a whole new degree of integrity to communication by enhancing on-line validation and security. Digital certificates authenticate the identities of both the sender and recipient and provide proof of the content and delivery of a communication in addition to guaranteeing that the exact message received was the message sent. Digital certificates are ideally suited to e-procurement and EDI, but only 28% (40% for large businesses) are using them. This may explain the 11% of organisations that have had transaction data corrupted, and the 1% that have suffered refutation (where a business partner has tried to walk away from a transaction).



## Emerging Technologies

A number of technologies of the future are emerging at present. These pose new security opportunities and threats to the organisations that adopt them.

A lot has been written about how biometrics are going to revolutionise the security industry. From the results of this survey, this is unlikely to happen in the next year in the UK. Only large businesses are currently using biometrics at all, and only 3% of large businesses do so. The use of biometrics is growing rapidly, with a further 7% of large businesses planning to adopt them in the next year. However, the overall usage levels are likely to remain low for some time.

Another security technology that has been much talked about in the last few years is Public Key Infrastructure (PKI). After several years of relatively little uptake, there are signs that the UK could be on the brink of widespread adoption of digital certificates. 28% of organisations carrying out EDI or e-procurement (40% of large businesses) are now using digital certificates, as are 14% of organisations that provide employees with remote access (21% of large ones). The challenges with digital certificates remain, principally the cost of setting up a secure certification authority. For this reason, most UK businesses are likely to be best served by outsourcing their certification authority requirements to a trusted third party.

One large business switched from using secure access tokens (which provided adequate security) to PKI (which was more expensive) for remote access because users had been taping their tokens to their laptops. Moving to digital certificates (as soft tokens) made life easier for the users, without reducing the effective level of security.

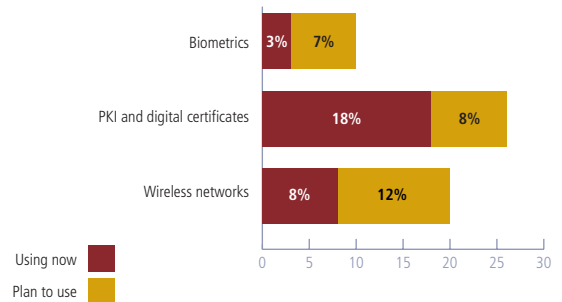
Another growing technology is the wireless network. 2% of UK businesses (and 8% of large organisations) are currently using wireless networks and a further 3% (12% of large businesses) plan to implement them over the next year. However, this technology may prove to be a security time bomb. Only 47% of organisations using wireless networks currently encrypt the traffic over those networks. Without encryption wireless transmissions can be intercepted, as has been the subject of recent newspaper articles.

One organisation recently cancelled their wireless pilots in the UK and the US after they found that companies in the office space next to them could access their wireless network.

## Security Practices in Place - Technology

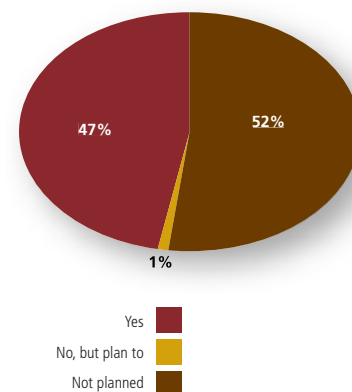
### Are large UK businesses using emerging technologies?

Figure 73

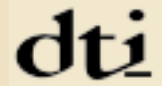


### Are large UK businesses encrypting wireless network traffic?

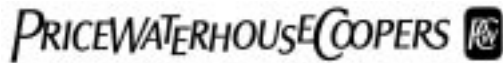
Figure 74



## Sponsoring Organisations



The Communication and Information Industries (CII) Directorate within the Department of Trade and Industry (dti) works with industry and the science base to improve the global competitiveness of the UK's communications, information and electronics businesses, thereby enhancing the competitiveness of the UK economy and improving the quality of life in the UK.

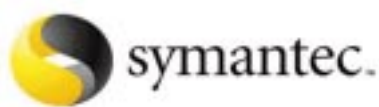


**PricewaterhouseCoopers (PwC)** is the world's largest professional services organisation. Drawing on the knowledge and skills of more than 150,000 people in 150 countries, we help our clients solve complex business problems and measurably enhance their ability to build value, manage risk and improve performance in an Internet-enabled world.

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. We develop and implement security solutions, integrating the leading user management, encryption and authentication products to provide customers and employees with seamless but safe access to clients' systems over the Internet. Our beTRUSTed division ([www.betrusted.com](http://www.betrusted.com)) provides world-class Public Key Infrastructure (PKI) expertise and certification authority services. We also help our clients monitor their security, through penetration testing, security audits and accreditation against standards such as ISO 17799. For more information about PwC's security services, see [www.pwcglobal.com/security](http://www.pwcglobal.com/security).



**RSA Security** is the world's largest Internet security company, with nearly 20 years' experience in helping organisations conduct e-business with confidence. More than 8,000 customers worldwide rely on RSA Security's strong authentication, access management, encryption and digital signature solutions, both to protect against the risks of a security breach, and to enable secure e-business processes. Additional information about RSA Security can be found at [www.rsasecurity.com](http://www.rsasecurity.com).



**Symantec**, the world leader in Internet security technology, provides a broad range of content and network security software and appliance solutions to individuals, enterprises and service providers. The company is a leading provider of virus protection, firewall and virtual private network, vulnerability assessment, intrusion prevention, Internet content and e-mail filtering, and remote management technologies and security services to enterprises and service providers around the world. Symantec's Norton brand of consumer security products is a leader in worldwide retail sales and industry awards. Headquartered in Cupertino, Calif, Symantec has worldwide operations in 38 countries. Additional information about Symantec can be found at [www.symantec.co.uk](http://www.symantec.co.uk).



**Genuity** is a leading Internet infrastructure services provider and the first company in the industry to offer an e-Business Network Platform. Genuity combines its Tier 1 network with its full portfolio of managed Internet services, including dedicated, remote and broadband access, web hosting and Internet security to develop a platform for creating scalable and repeatable managed e-business solutions. With annual revenues of more than \$1 billion, Genuity is a global company with offices and partnerships throughout the US, Europe, Asia and Latin America. Additional information about Genuity can be found at [www.genuity-europe.com](http://www.genuity-europe.com).



**Countrywide Porter Novelli**, one of the UK's top five public relations consultancies, is also number one in crisis communications. It is part of Porter Novelli International, one of the world's leading public relations firms with offices in 97 cities within 55 countries around the world. Additional information about Countrywide Porter Novelli can be found at [www.cpn.co.uk](http://www.cpn.co.uk).



## Top Ten Actions for the Board

Make sure your business:

- creates a security-aware culture by educating staff about security risks and their responsibilities.
- has a clear, up to date security policy to facilitate communication with staff and business partners.
- has people responsible for security with the right knowledge of good practice (e.g. BS 7799) and the latest security threats - consider supplementing their skills with external security experts.
- evaluates return on investment on IT security expenditure.
- builds security requirements into the design of IT systems and outsourcing arrangements.
- keeps technical security defences (e.g. anti-virus software) up to date in the light of the latest threats.
- has procedures to ensure compliance with data protection and other relevant regulatory requirements.
- has contingency plans for dealing with a serious information security breach.
- understands the status of its insurance cover against damage as a result of information security breaches.
- tests compliance with its security policy (e.g. security audits, penetration testing of its web-site).

Most important of all, do not wait for a serious security incident to affect your business before you take action.

