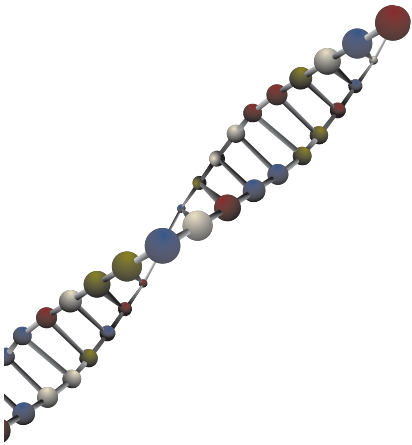


Information security breaches survey 2004



Executive summary

Since 1991, the Department of Trade and Industry has sponsored research into information security breaches to help UK businesses better understand the risks they face. The Information Security Breaches Survey 2004 (ISBS 2004), is the seventh such survey, and has been managed by PricewaterhouseCoopers.

The survey results show that the UK is now firmly in the Information Age, with companies of all sizes embracing the use of the Internet. This is changing the way that business operates, improving efficiency and customer service.

However, a side effect of this increased connectivity is greater exposure to information security issues. Indeed, this survey shows that security problems have now become a fact of business life, and not something that happens to someone else. As organisations struggle to contain these threats, the number of security incidents continues to rise.

It is encouraging, however, to note that information security remains a high priority at board level. More companies than ever have a security policy in place, and those that have adopted BS7799 have found it has yielded real benefits.

It is also pleasing that many companies have drawn upon the guidance the Government, in particular my own Department, has issued to help them address their information security concerns. Our work in this area will continue and form a key part of the Government's agenda for promoting e-business in the UK.

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

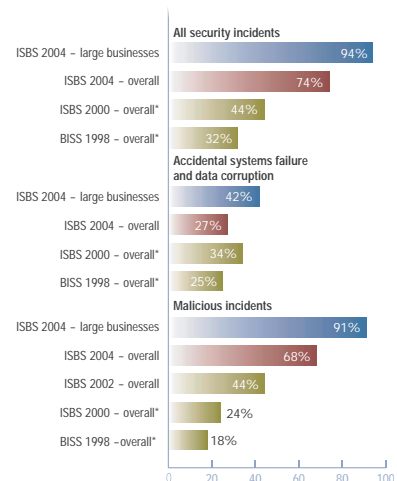


*Stephen Timms MP
Minister of State for Energy, e-Commerce
and Postal Services*

April 2004

- The business environment continues to change with increased use of the Internet.
- Greater connectivity has increased the exposure of UK businesses to security threats.
- As a consequence, the number of UK businesses that suffered a security breach continues to rise.

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



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

- The cost to UK business is significant.
- Some progress has been made in putting security controls in place.
- However, there is still considerable room for improvement.
- One root cause is that many companies lack the expertise to address this complex, changing area.
- Another cause is that spend on information security, while increasing, is still relatively low and is seen as a cost rather than an investment.

DTI recommends

- Draw on the right expertise to understand the security threats you face and your legal responsibilities.
- Integrate security into normal business practice, through a clear security policy and staff education.
- Invest appropriately in security controls (to mitigate the risks), or in insurance (to transfer them).
- Check your key security defences (such as operating system patches, disaster recovery plans, etc.) are robust and up to date.
- Respond to security incidents efficiently and effectively, to minimise business disruption.

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

in association with:



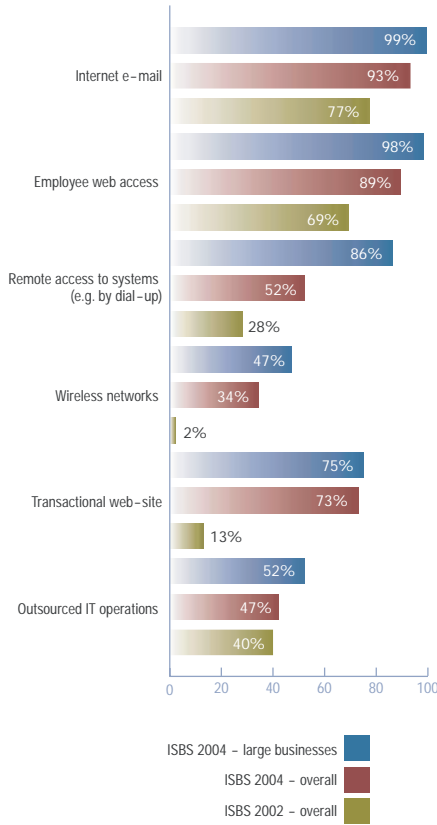
Computer Associates



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

Roughly nine-tenths of UK businesses now send e-mail across the Internet, browse the web and have a web-site. Most web-sites now allow customers to initiate transactions online. Small and medium-sized businesses tend to use a simple externally hosted online store, or just allow customers to e-mail orders in. Web-sites of larger businesses tend to be a fully integrated channel into core business systems.

How has the business environment changed over the last two years



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

Personal Digital Assistants (PDAs) are also being used to provide easy access to business information on the move. A third of businesses (and half of large ones) now use these devices.

Finally, adoption of wireless networks has mushroomed over the last two years. In 2002, only 2% of UK businesses had a wireless network. This has now risen to a third.

However, a side effect of this increased connectivity is greater exposure to information security issues

The threats continue to evolve, with new viruses and vulnerabilities being identified every week. The average UK business now receives roughly twenty viruses a year, and has its web-site scanned or probed many times.

Large businesses are attacked more, receiving on average a virus a week.

At the same time, dependence on electronic information and the systems that process it continues to increase. 87% of UK businesses are now highly dependent compared with 76% two years ago. Over half store highly confidential records on computers. Security breaches are potentially more damaging than ever.

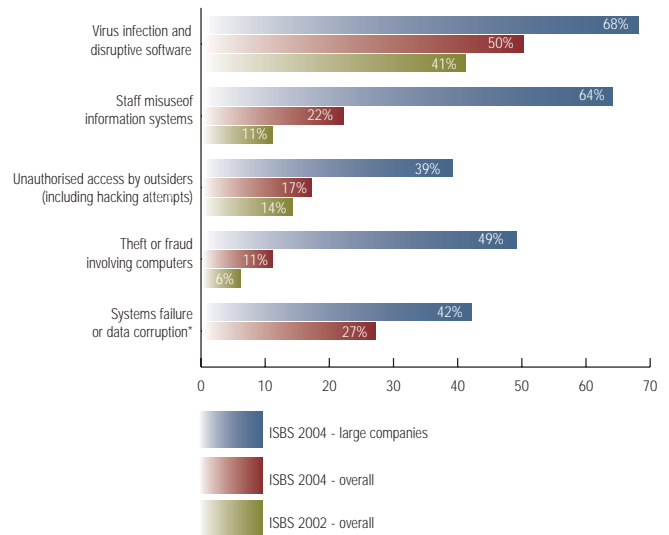
As a consequence, the number of UK businesses that suffered a security breach continues to rise

The sad reality is that security problems have now become a fact of business life, and not something that happens to someone else. As organisations struggle to contain the threats, the number of security incidents continues to rise.

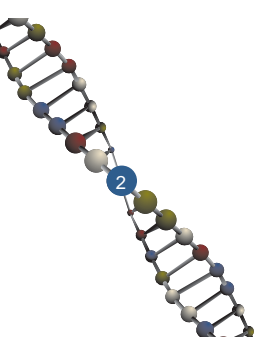
Malicious incidents are driving this increase. These include viruses, unauthorised access, misuse of systems, fraud and theft. Two-thirds of UK businesses had at least one of these breaches in the last year. This is an increase from just under half two years ago. It continues the high rates of growth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

Virus infection and inappropriate usage of systems by staff were the cause of most of the incidents. Viruses also caused the greatest number of serious breaches.

What type of breaches did UK businesses suffer?



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



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

The security breaches are not isolated instances. The average UK business now has roughly one security incident a month. Large companies have roughly one a week.

In addition to these incidents, many organisations reported unsolicited e-mail ("spam") as an increasingly significant issue for their business. A third of UK businesses cited it as a major issue, and most reported growing volumes. While not a security breach per se, spam is clearly disruptive and many IT and security staff are grappling with how best to address it.

The cost to UK business is significant

The average cost of an organisation's most serious security incident was roughly £10,000. In large companies, this was more like £120,000. The impact on availability was by far the biggest contributor to this cost, with some organisations suffering a very major disruption to their business operations for more than a month.

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

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

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

Respondents were significantly more pessimistic about the future outlook for information security breaches than they were two years ago. They believe that incidents will happen more often in future, and that they will be harder to detect.

Some progress has been made in putting security controls in place

Information security is firmly on the board agenda. Three-quarters of companies rate security as a high or very high priority for their top management or board of directors. The priority is highest in large businesses, with five in six considering it important.

Some progress has been made in putting security controls in place. For example, the number of UK businesses with a security policy continues to rise. One third of all companies, and two-thirds of large businesses, now have one.

UK businesses have also clearly understood the need to ensure outsourced operations are secure. Most companies that outsource their IT operations have Service Level Agreements that clearly set out their information security requirements.

However, there is still considerable room for improvement

In the 2002 survey, we highlighted ten key action areas for senior management. Progress against these is patchy. There appears to be a disconnect between the apparent priority and what is done in practice.

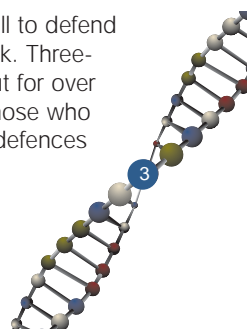
How much progress has been made against the top ten actions identified two years ago?

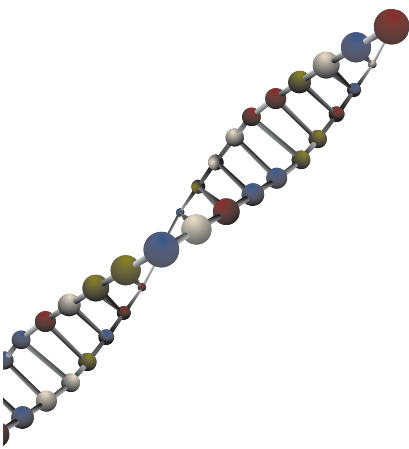
	Status	Trend since 2002
Staff education		↔
Security policy		↑
Security skills		↔
Investment in security		↑
Managing systems change securely		↑
Up-to-date technical security defences		↓
Legal compliance		↔
Contingency plans		↓
Insurance cover		↔
Security audits		↔

Virus protection is a good example. Almost every business is now aware of the need to protect its business against viruses. 93% have implemented anti-virus software, and 59% of them now update this software immediately a new virus signature is identified.

Despite this, half of UK businesses (and two-thirds of large ones) were infected by a virus in the last year. Increasingly, viruses are bypassing traditional anti-virus software and targeting vulnerabilities in computer operating systems. Processes for keeping these up to date with the latest security patches are often weak.

Businesses also tend to rely solely on their firewall to defend their Internet gateway and web-site against attack. Three-quarters of in-house web-sites have a firewall, but for over half of these this is their sole defence. Many of those who host their web-site externally do not know what defences their service provider has against attack.





The information security breaches survey has over the last decade formed an integral part of the DTI's programme to help UK businesses address the issue of information security.

The survey takes place every two years and involves telephone interviews with 1,000 businesses of all sizes across all areas of the UK, plus a series of face to face interviews.

Based on the total sample of UK businesses in this survey, we are 95% confident that the margin of error for our sampling procedure and its results is no more than +/- 3%.

For more information, please refer to the Information Security Breaches Survey Technical Report (URN 04/617). This is available from 27 April 2004 and can be downloaded from www.security-survey.gov.uk



Despite their many issues, user ID and password are still the dominant mechanism for authenticating users' identities. However, a third of large businesses have moved to some degree of two-factor authentication, and have seen a reduced level of unauthorised access breaches as a result.

New users of remote access, Internet e-mail and web access tend to have adopted them without implementing any controls. Worryingly, only half of all wireless networks have security controls in place.

Contingency planning is not much better. Fewer than one in ten businesses (and only a quarter of large ones) have tested their disaster recovery plans to see if they would work in practice.

So, why is more not being done?

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

Three-quarters of businesses are confident that their technical security processes are sufficiently good to prevent or detect all significant security breaches. Given the weaknesses in these controls, it appears that some do not fully appreciate the risks they are running. Only one in ten companies (and only a quarter of large ones) has staff with formal information security qualifications.

In theory, the UK should be leading the world. After all, in December 2000, the British Standard for Information Security Management, BS 7799, was adopted as an international standard, ISO/IEC 17799.

Overseas companies are increasingly using ISO/IEC 17799 to structure their security processes. In the UK, however, neither overall awareness of BS 7799, nor the number of businesses that have implemented it, has increased over the last two years. The survey shows that those organisations that have implemented BS 7799 have found that it has yielded real business benefits.

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

Companies now spend on average 3% of their IT budget on security compared with

2% two years ago. Large businesses spend roughly 4%. Overall levels of investment in security are still considerably below a reasonable 5%-10% benchmark level.

The averages mask a mixed position. Roughly a quarter of companies are investing in security at, or above, benchmark levels. In large companies, this rises to roughly half. The majority of businesses, however, are still spending less than 1% of their IT budget on security.

One factor behind the underinvestment is that security is often seen as an overhead rather than an investment. Less than half of all businesses ever evaluate their return on investment (ROI) on security spend. This has not changed significantly since two years ago.

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

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

Taking action to secure your business

While there is no magic wand solution, passive resignation is not the answer. There are simple steps that businesses of all sizes can take to reduce the likelihood and impact of future incidents. The five main recommendations on the front page are a helpful starting point.

Above all, this survey shows that too many organisations have waited until an incident hits them before putting counter-measures in place. Don't wait until the horse has bolted before closing the stable door.