

Information security breaches survey 2006

Executive summary

DTI recommends

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

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

and

www.getsafeonline.org

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

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

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

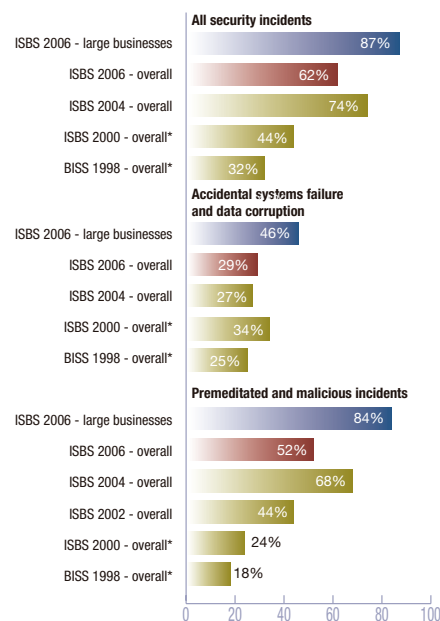
Access to security expertise continues to pose an issue for the UK business community, so the launch earlier this year of the UK Institute of Information Security Professionals is very welcome. The big increase in the use of external guidance and specialists to supplement in-house capability is also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



Alun Michael MP
Minister of State for Industry and the Regions

- IT systems in general, and the Internet in particular, are increasingly important to business operations. Given this, the priority attached to information security remains high.
- The priority given to security has translated into action. Security controls have improved and confidence in those controls is high.
- The improved controls appear to be having an effect; the number of companies affected by security incidents appears to have stabilised.
- The cost, however, remains considerable.

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.

- Many UK businesses are a long way from having a security-aware culture. Security expenditure is either low or not targeted at key risks.
- New technologies pose a particular security threat for the future.
- Despite the high levels of confidence about current security, UK companies are more concerned about tomorrow's security than ever.

in association with:

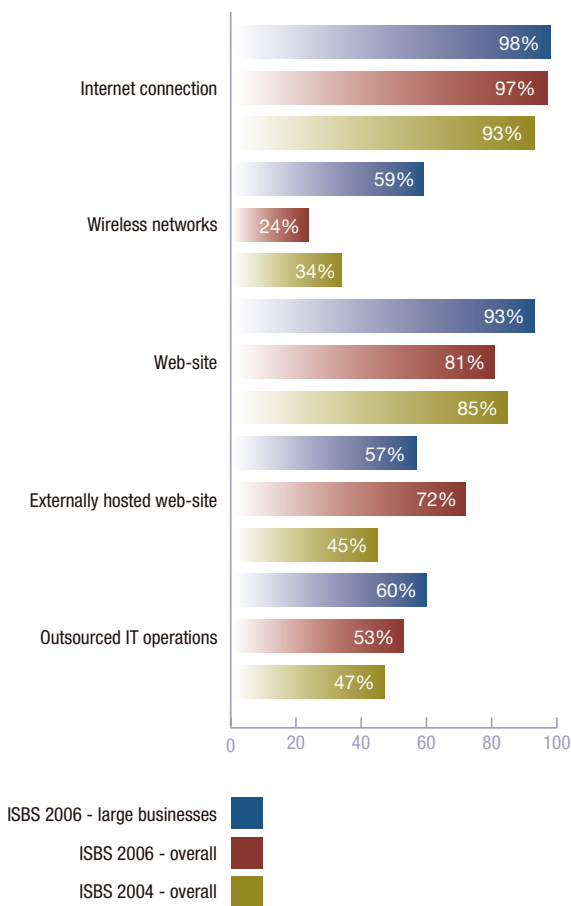
IT systems in general, and the Internet in particular, are increasingly important to business operations. Given this, the priority attached to information security remains high.

Nearly every UK business makes use of the Internet; 97% have an Internet connection and 88% of these are broadband. Roughly four-fifths of companies have a web-site, of which 89% are externally hosted.

Increasing volumes of online business raise firms' dependency on IT; only one in six small companies could operate their business without their IT.

Over half of all businesses outsource some of their IT operations. Offshoring is also growing, particularly in larger companies.

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



Given the increased dependence on IT systems, it is encouraging that firms continue to take information security seriously. Three-quarters of UK businesses rate security as a high or very high priority to their senior management or board of directors. The priority is consistent across all sizes of company. Companies that are heavily dependent on their IT systems are nearly twice as likely to assign a high priority to security as those that do not.

The main objectives of information security expenditure remain the preservation of confidentiality, integrity and availability; nine-tenths of businesses rate these as important. Protecting customer information and compliance with the Data Protection Act are seen as increasingly important. Enabling business opportunities and improving efficiency tend to be less significant drivers for expenditure, with only two-thirds considering these as important.

Financial services companies and the education sector are most likely to hold highly confidential data. Manufacturing firms are more likely to hold sensitive data than two years ago; nearly two-thirds do so now, in comparison with less than half in 2004.

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

The number of companies with a formal security policy has never been higher. Nearly three times as many have a security policy as did six years ago.

Security policies are being supported by increased information security expenditure, some of which is spent acquiring external expertise. The average UK company now spends 4-5% of its IT budget on information security. Almost every UK business makes some use of external guidance or expertise to supplement their in-house security capability.

Policies and increased expenditure are leading to better adoption of security controls: Almost every organisation backs up its critical data and three-quarters store these backups offsite. UK businesses have also reacted strongly to the disruption caused by viruses in 2004. 98% of businesses now have anti-virus software, four-fifths of firms update their anti-virus signatures within a day and 88% install critical operating system patches within a week. Companies are also deploying other controls over their Internet e-mail; 86% filter incoming e-mail for unsolicited messages (spam).

The investment in security made by UK businesses has translated into progress against all five key recommendations made two years ago.

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

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

UK businesses appear to believe that the extra investment in security is worthwhile; three-quarters of them are confident or very confident that they have identified all significant security breaches in the last year.

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

62% of UK companies had a security incident in the last year, down from 74% two years ago. Large businesses have also seen a reduction, down to 87% from 94%.

Malicious incidents were responsible for the large increase in 2004; they now account for the reduction seen in 2006 (down to 52% from 68%).

The 2006 figures still remain higher than 2002 levels, so it is too early to assume the reduction represents a long term downward trend.

The cost, however, remains considerable.

Despite the reduction in the number of firms suffering breaches the actual number of reported incidents is rising. The median number of incidents suffered is roughly eight a year. This has increased from two years ago. The cost associated with security incidents has also risen. In 2004, the average cost of a UK company's worst incident was roughly £10,000; it is now £12,000.

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

	ISBS 2006 - overall	ISBS 2006 - large businesses
Business disruption	£6,000 - £12,000 <i>over 1-2 days</i>	£50,000 - £100,000 <i>over 1-2 days</i>
Time spent responding to incident	£600 - £1,200 <i>2-4 man-days</i>	£1,750 - £3,500 <i>5-10 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.)	£500 - £1,000	£3,500 - £5,000
Damage to reputation	£100 - £400	£5,000 - £10,000
Total cost of worst incident on average	£8,000 - £17,000	£65,000 - £130,000

Large businesses are more likely to have security incidents (87%), tend to have more of them (median of 19 per year) and their breaches tend to be more expensive (£90,000 on average for the worst incident).

For firms overall the cost is roughly 50% higher than two years ago. In contrast, large businesses have seen a 20% reduction in the average cost. Overall, the cost of security breaches to UK plc is up from two years ago, and is of the order of ten billion pounds per annum.

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

Despite the overall increase in security expenditure, roughly two-fifths of businesses still spend less than 1% of their IT budget on information security. To justify expenditure and spend effectively, businesses need to carry out security risk assessments. However, only 44% of companies have done this in the last year.

There is a correlation between security expenditure and those firms that perform risk assessments. On average, those that carried out a risk assessment spent 7% of their IT budget on security. The average expenditure for those that did not was only 4%. It seems likely, therefore, that those that have not assessed the risks are under-investing in their security.

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

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

Investment in security standards and related qualifications is also low. Just one firm in eight has security qualified staff. Three-fifths of UK businesses are still without a security policy. Only one in ten firms is aware of the contents of the BS 7799 standard.

UK businesses are also overlooking other key areas of security. A quarter of companies do not carry out any background checks when they recruit staff. One in eight organisations does nothing to educate their staff about their security responsibilities. Few firms are well prepared to react to major security breaches when they do occur. Three-quarters of UK companies either lack disaster recovery plans or have not tested them in the last year.

More than half of UK businesses are dependent on the physical security of their premises alone to protect their PCs and laptops (and the data that is on them) from theft. Only one in seven encrypts the data on hard discs.

New technologies pose a particular security threat for the future.

New threats and greater use of emerging technologies represent a risk to the security of UK businesses. These threats already exist, but are likely to increase in the future. UK businesses are slow to adopt the controls to reduce the threat.

For example, while anti-virus and patching disciplines have improved, a quarter of UK businesses are not protected against spyware; this is software (typically downloaded from the Internet) that logs and transmits information without the user's knowledge. As a result, one in seven of the worst malicious software incidents in the last year related to spyware.

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 and interactive surveys.

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%.

The 2006 survey was managed by PricewaterhouseCoopers for the DTI and was sponsored by Microsoft, Clearswift, Entrust and Symantec.

For more information, please refer to the Information Security Breaches Survey Technical Report (URN 06/803). This is available from 25 April 2006 and can be downloaded from www.security-survey.gov.uk



UK companies are also poorly placed to deal with identity theft; only 1% have a comprehensive approach to identity management (authentication, access control and user provisioning). 84% say there is no business requirement to improve this. As more customers and suppliers are granted direct access to corporate systems, this will represent an increasing exposure.

Three-fifths of companies that allow remote access do not encrypt their transmissions; businesses that allow remote access are more likely to have their networks penetrated than other companies.

Three-fifths of businesses do not block staff access to inappropriate web-sites and only one in six scans outgoing e-mail for inappropriate content. Most worryingly, 30% of transactional web-sites do not encrypt the transactions that pass over the Internet.

The adoption of appropriate security controls is not keeping pace with the growing use of emerging technologies. Although more authorised wireless networks are protected than two years ago, one in five is still completely unprotected. A further one in five is unencrypted. Two-fifths of companies that allow staff to connect via public wireless hotspots do not encrypt the transmissions.

Removable media devices can hold large volumes of data, and reduced prices have made devices such as USB tokens and MP3 players affordable to all. Despite this, 55% of firms have taken no steps to protect themselves against the threat posed by removable media devices.

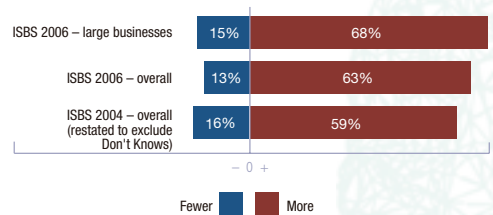
A similar story emerges for instant messaging; two-fifths of companies that allow its use have no controls in place.

Adoption of Voice over IP telephony is currently low, but many firms plan to implement it over the next year. Only half of the companies that have implemented Voice over IP telephony evaluated the security risks before doing so.

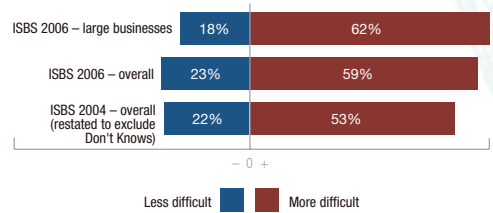
Despite the high levels of confidence about current security, UK companies are more concerned about tomorrow's security than ever.

UK businesses appear to recognise that their ability to identify current threats does not mean they are immune from future threats.

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



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



Nearly two-thirds expect there will be more security incidents in the next year than in the last. Three-fifths of companies believe it will be harder to detect security breaches in the future. This pessimism is consistent with the view that UK businesses are winning yesterday's battles, but are not preparing the foundations for defeating a more technology focused form of guerrilla warfare.

Overall, the five key recommendations made in the 2004 survey appear just as relevant today. However, in the light of this year's survey results, we have emphasised the importance of adopting an integrated risk-based approach to information security, including consideration of emerging technology. Without this, UK businesses are likely to become increasingly exposed in tomorrow's security landscape.