BERR | Department for Business Enterprise & Regulatory Reform

2008 INFORMATION SECURITY BREACHES SURVEY

Executive summary

SURVEY CONDUCTED BY

PRICEWATERHOUSECOOPERS

IN ASSOCIATION WITH

symantec.

hp

THE SECURITY COMPANY INTERNATIONAL

EXECUTIVE SUMMARY

As dependency grows, ...

UK businesses continue to grasp the opportunities provided by new technology. The broadband revolution has allowed companies to increasingly use the Internet to reach their customers and enable their staff to be more mobile. Their IT activities now extend beyond traditional physical network boundaries.

97%	have a broadband connection to the Internet.
93%	have a corporate website.
54%	allow staff to access their systems remotely.
42%	use a wireless network.
17%	use Voice over IP telephony.
5%	have moved some of their IT operations offshore.

The larger the company, the more likely it is to have adopted these business practices. For example, six out of seven very large businesses now offshore some IT operations.

All of these practices have increased significantly since two years ago. This trend is likely to continue. For example, 30% of companies will be using Voice over IP telephony by the end of 2008.

As a result, IT systems and information security are more important to UK companies than ever before. For the first time, small businesses believe security is as high a priority for them as large companies.

84%	are heavily dependent on their IT systems.
81%	believe their board gives a high or very high priority to information security.
77%	see protecting customer data as a very important driver of their expenditure.

Controls are improving, ...

This is translating into real improvements in controls, particularly in basic disciplines such as anti-virus and backups.

99%	back up their critical systems and data.
98%	have software that scans for spyware.
97%	filter incoming email for spam.
97%	protect their website with a firewall.
95%	scan incoming email for viruses.
94%	encrypt their wireless network transmissions.

It is not just technical controls that have improved. Companies increasingly realise that their people, while their greatest asset, can be their greatest vulnerability, and so need to be educated on security risks. Businesses are investing more in their security, especially those that think hardest about where to spend their money. The general level of awareness is rising, and the focus now needs to be on changing and measuring actual behaviour. With increasing awareness comes a move away from the traditional user ID and password and towards stronger authentication techniques such as smart cards or biometrics.

Over the last six years, the security landscape has changed dramatically.

2002	2008	
27%	55%	have a documented security policy.
2%	7%	of IT budget spent on security (on average).
20%	40%	provide ongoing security awareness training to staff.
5%	14%	use strong (i.e. multi-factor) authentication.
5%	11%	have implemented BS 7799/ISO 27001.

BS 7799 is the British information security management standard that formed the basis of, and is equivalent to, the ISO 27000 series of international standards.

EXECUTIVE SUMMARY

Leading to fewer reported incidents, ...

After the peak in 2004, the number of companies reporting a security breach has returned to roughly the level seen in 2002. However, attitudes and controls in some companies mean that incident statistics are probably understated. For example, companies that carry out risk assessment are four times as likely to detect identity theft as those that do not. In addition the average seriousness of incidents has increased, so roughly a quarter of companies had a serious breach, the same as in 2006.

	Small (<50 staff)	Large (>250 staff)	Very Large (>500 staff)
Companies that had a security incident in the last year	45%	72%	96%
Average number of incidents, median (mean)	6 *(100)*	15 *(200)*	>400 *(>1,300)*
Average cost of worst incident in year	£10k to £20k	£90k to £170k	£1m to £2m

The most striking feature is the decline in reported virus infections. Virus infection has dropped from the largest cause of security incidents (which it has been for the last decade) to fourth place out of five. The number of companies infected has fallen back to levels last seen in 2000. In contrast, unauthorised access by outsiders is not declining and remains at four times the level seen in 2000.

	Overall	Large businesses
Number of companies affected	↓ 25%	↓ 20%
Average (median) number of incidents suffered by affected companies	↓ 30%	↓ 20%
Average cost of each incident	↑ 25%	↑ 30%
Total cost of security incidents	↓ 35%	↓ 20%

The total cost to UK plc has dropped by roughly a third compared with two years ago, returning to the levels seen in 2004. An indicative estimate of the overall cost is in the order of several billion pounds a year. Companies are generally pessimistic, with only 17% expecting fewer security incidents next year.

But some big exposures remain.

Confidential information is increasingly at risk, especially in large businesses, where:

13%	have detected unauthorised outsiders within their network.
9%	had fake (phishing) emails sent asking their customers for data.
9%	had customers impersonated (e.g. after identity theft).
6%	have suffered a confidentiality breach.

Many companies are not doing enough to protect themselves and their customers' information.

10%	of websites that accept payment details do not encrypt them.
21%	spend less than 1% of their IT budget on information security.
35%	have no controls over staff use of Instant Messaging.
48%	of disaster recovery plans have not been tested in the last year.
52%	do not carry out any formal security risk assessment.
67%	do nothing to prevent confidential data leaving on USB sticks, etc.
78%	of companies that had computers stolen did not encrypt hard discs.
79%	are not aware of the contents of BS 7799/ISO 27001.
84%	of companies do not scan outgoing email for confidential data.

To protect your business in this changing world:

1. **Understand the security threats you face, by drawing on the right knowledge sources.**
2. **Use risk assessment to target your security investment at the most beneficial areas.**
3. **Integrate security into normal business behaviour, through clear policy and staff education.**
4. **Deploy integrated technical controls and keep them up to date.**
5. **Respond quickly and effectively to breaches, e.g. by planning ahead for contingencies.**

This executive summary and a separate 32 page technical report are available in electronic form from:

www.security-survey.gov.uk.

Printed in the UK on Mega Matt paper which is made from 50% recycled and 50% chlorine-free pulp from countries that operate strict reforestation policies.

Department for Business, Enterprise & Regulatory Reform. www.berr.gov.uk

First published April 2008. URN 08/787.