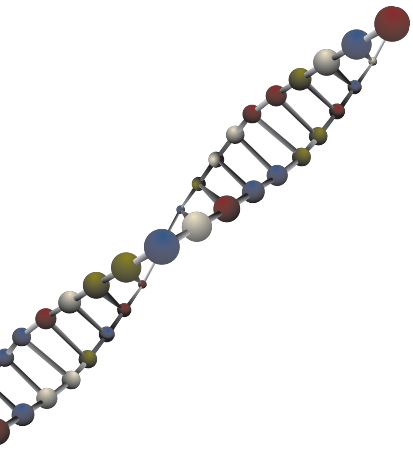
PRICEWATERHOUSECOOPERS

dti

Information **security** breaches survey 2004



DTI recommends

- Deploy firewalls on all network connections.
- Consider other intrusion prevention countermeasures to protect important systems.
- Put a monitoring or testing process in place to check for vulnerabilities.
- Co-ordinate intrusion prevention with other security countermeasures such anti-virus.

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

in association with:

McAfee® SECURITY

Intrusion **prevention**

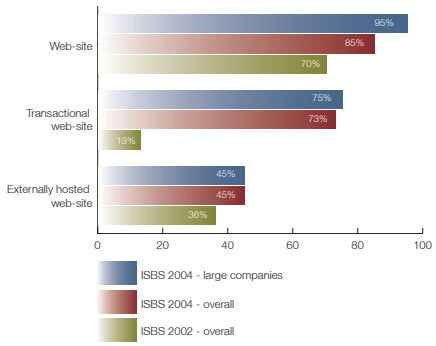
The need for Intrusion Prevention is clear

Over the last two years use of the Internet to provide and support business functionality has grown.

Web-sites are common for large businesses, with their use by small and medium sized businesses showing significant growth compared to previous years.

Particularly noteworthy is the growth of transactional web-sites. This may be one of the reasons, particularly for SMEs, for the increase in the number of businesses using external service providers to host their web-sites.

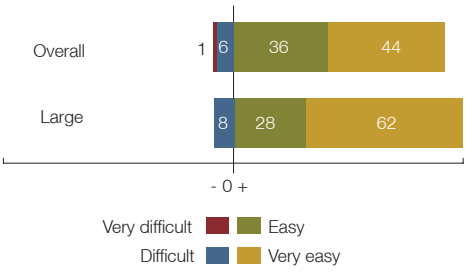
The changing business environment



Other recent studies in this area have also shown an increase in the volume of business conducted through web-sites.

Given this, the potential for security incidents leading to business disruption has increased. It is unsurprising that businesses find it relatively easy to justify expenditure on intrusion prevention.

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



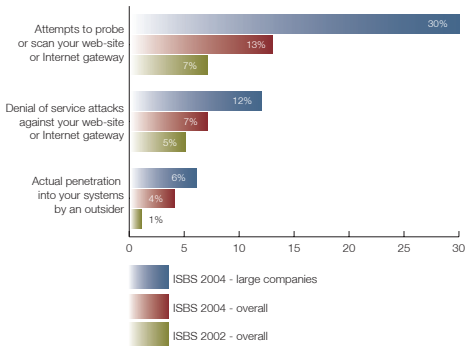
Increase in attacks on web-sites

The number of small businesses reporting hacking attempts remains relatively low but has risen significantly. Given the increased business dependence on web-sites the speed of the rise is worrying.

One in three large companies reported probes against their web-site. These figures are likely to be understated. As we will see later, some businesses reporting no scans did not have the processes and technology in place to be sure of this.

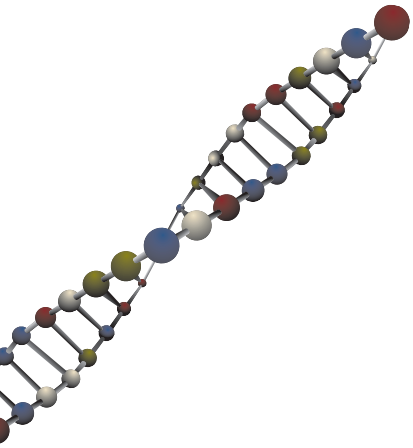
Businesses that had been scanned reported an average of one probe a week. After probes, outsiders had penetrated the systems of 4% of companies, four times as many as two years ago.

What proportion of UK businesses suffered security web-site related security in the last year?



Three quarters of businesses that reported system penetration rated it as their worst security incident of the year (worse than virus infections etc.). Over a third described the impact as very serious. One might expect the primary reason for this to be financial loss or service disruption. In fact, the main reason quoted was the time spent on investigation and remediation. A quarter took between 2 and 10 man-days effort.

A financial services organisation explained that the main impact of an attack was not direct damage. Instead, it was the time spent investigating the cause, analysing the damage and performing remedial work.



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.

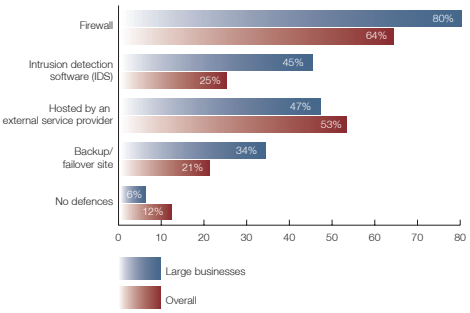
Based on the total sample of UK businesses in this survey, we are 95% confident that the margin of error for our sampling procedure and its results is no more than +/- 3%.

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**

Reliance on firewalls and external hosting

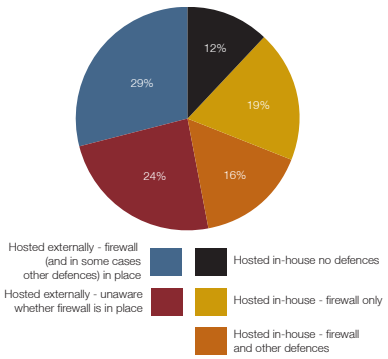
Businesses are deploying a range of intrusion prevention techniques to protect their web-sites. Firewalls predominate. Three-quarters of in-house web-sites have a firewall, but for over half of these this is their sole defence. The larger the business, the more likely it is to protect its web-site with a firewall as well as having intrusion detection software.

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



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

Differences between internal and external hosting



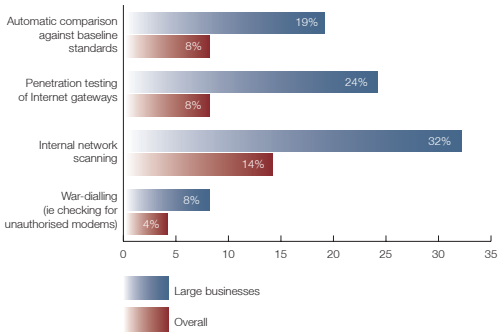
One security officer commented that this presents a dilemma. Handling their web-site security in-house is not working. Their intrusion detection software is still not simple enough. Everyone is too busy to look at the deluge of 'noise' it produces. On the other hand, outsourcing security to a managed security services provider does not feel right. They want to be in control.

Misplaced confidence?

Despite the increase in network security incidents, businesses remain broadly confident in the effectiveness of their defences. 72% of businesses are quite, or very confident that their technical processes are able to prevent or detect security breaches.

This confidence would be encouraging were it based on effective monitoring. However, this is often not the case. Many organisations do not test their network security. However, large businesses are increasingly using security tools to scan their systems. Some scans check the configuration against baseline standards. Others test for vulnerabilities that are visible from inside or outside the business.

How do UK businesses check compliance with their security policy?



Business that carry out these checks reported more attempts to probe their web-site security. However, they reported less actual penetration of their systems by outsiders. The fear is that businesses without these monitoring and intrusion prevention processes may have a false level of comfort. Scanning and hacking activity may not be detected until it is too late to react.

Increasingly, viruses and worms are exploiting network security weaknesses. This is another reason to invest in effective intrusion prevention. Co-ordinating anti-virus and network security approaches is essential here.

This report is printed on Mega Matt paper which is made from 50% recycled and 50% chlorine-free pulp from countries that operate strict reforestation policies.

Department of Trade and Industry. April 2004. URN 04/614