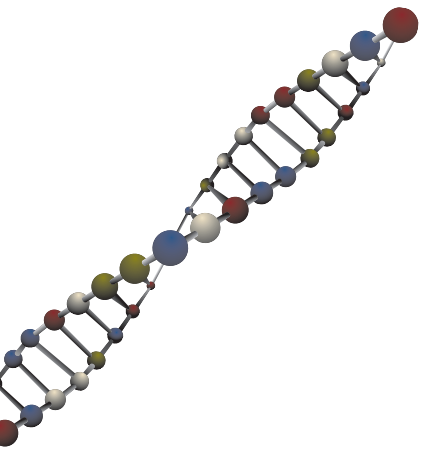
PRICEWATERHOUSECOOPERS

dti

Information **security** breaches survey 2004



DTI recommends

- Use remote access only where there is real business benefit and acceptable risk.
- Deploy extra authentication for remote access users.
- Protect data transmissions (e.g. through VPN).
- Protect sensitive data on portable devices (e.g. laptop computers and PDAs).
- Educate users about the risks associated with remote access, as part of granting them access.

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

in association with:

SafeNet™ The Foundation of Internet Security

Remote access

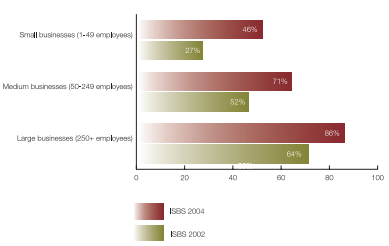
Anywhere, any time

Over the last two years information systems have become an essential part of UK business. 85% of UK businesses now have a web-site and 93% make use of e-mail. Among large businesses these figures are even higher.

In this business environment the need to access data and information systems is growing. More individuals within businesses require more access from more locations than ever before. For frequent travellers, support personnel and sales staff, reliable remote access to data has become a necessity rather than an option.

Over half of UK businesses now provide their staff with access to their systems over the Internet or by direct dial-up. More large businesses are deploying remote access than small ones. However, all sizes of business have significantly increased their use of remote access since 2002.

How many UK Businesses provide remote access?



Adoption of wireless networks has also mushroomed over the last two years. In 2002, only 2% of UK businesses had a wireless network. This has now risen to a third of companies. Large businesses are again more likely to be early adopters, with nearly half doing so.

Personal Digital Assistants (PDAs) are also being used to provide easy access to business information on the move. 35% of businesses now use PDAs, with the figure rising to 57% for large businesses.

Increasing security exposure

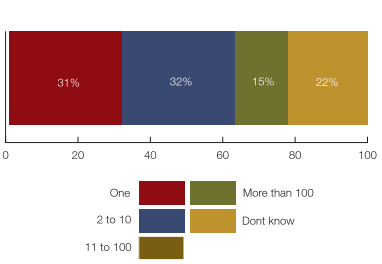
Increased deployment of access enabling technology is leading to an increase in related security incidents. These breaches are a growing concern for UK businesses.

One company had a big increase in the number of viruses after rolling-out remote access to users. Most at fault were the people connecting their own PCs and PDAs to the network.

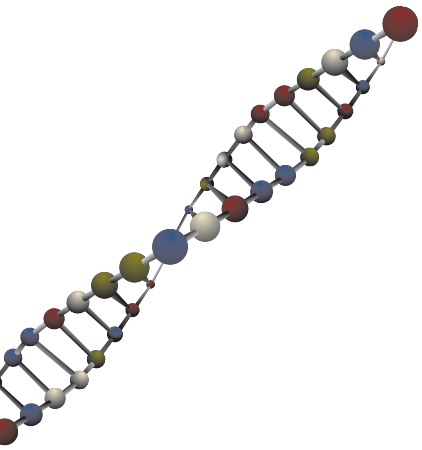
Wireless networks are becoming a focal point for external attack. 8% of businesses with wireless networks claimed to have suffered from attempts to gain unauthorised access. Significantly, a further 23% did not know whether they had been probed.

For those that suffered unauthorised access attempts the number of incidents was low. Nearly two-thirds of businesses reported no more than 10 attempts. By contrast, one in seven identified over 100 attempts. A further fifth could not quantify the number of unauthorised attempts.

How many unauthorised attempts to connect through a wireless network did affected businesses suffer?



Given this, it is not surprising that actual penetration of systems by outsiders (by any means) has quadrupled over the last two years. While remote access is not the only route hackers use to attack networks, they often cite it as the easiest route in. Several businesses reported very serious breaches of this kind.



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%.

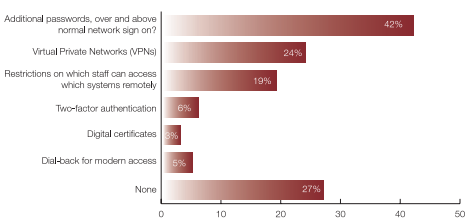
For more information, please refer to the Information Security Breaches Survey Technical Report (URN 04/617). This is available from 27 April 2004 and can be downloaded from **www.security-survey.gov.uk**

Slow adoption of security controls

One might expect that, given the threats, anyone implementing remote access would deploy additional security controls. The survey indicates that often this is not the case.

Of those businesses that are providing remote access, a quarter used no additional controls. These companies are relying on their normal network password controls to defend them. Often these passwords are easy to crack, exposing a chink in the perimeter defence.

What additional security controls are deployed by UK businesses providing remote access?



Large businesses tend to deploy better controls. They are twice as likely to use a VPN as small companies. Three times as many used two-factor authentication or digital certificates. Only 9% of large businesses with remote access had no additional controls in place.

A similar picture emerges for wireless networks. Only one in five used Wired Equivalent Privacy (WEP) or other additional encryption to protect their information from unauthorised disclosure. Over half of wireless networks had no additional security controls at all.

Very few organisations have woken up to the risks posed by PDAs. 58% of businesses that use PDAs have no security measures in place to protect the business data on them. Large companies are a bit better, but even here 38% have no controls. Most of the controls that have been deployed are policies on usage rather than technological protection.

Convenience without awareness of risks

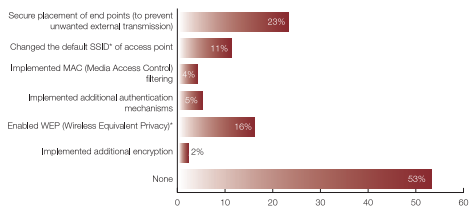
Three main factors appear to be behind the slow deployment of security controls in the area of remote access and accessibility technology.

Firstly, many of those wanting the remote access are seemingly those least aware of the additional risks it creates. In addition, they are often senior or influential personnel with the power to authorise access.

Secondly, the majority of businesses are not performing sufficiently detailed analysis of their security incidents to identify those associated with remote access.

Finally, businesses are not fully aware of the controls available to provide protection. Consequently, the security controls are often inappropriate. For example, only 2% of wireless networks have deployed MAC (Media Access Control) filtering.

What additional security controls are deployed by UK businesses making use of Wireless Networking?



* The SSID is an identifier attached to packets sent over a wireless LAN which functions as a 'password' for joining a particular radio network. WEP encrypts signals to avoid disclosure to eavesdroppers.

To gain the benefits offered by remote access, businesses need to act now to reduce the associated risks to an appropriate level.

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 04/615.