Identity and access management

Pressure to manage access effectively

To operate effectively, businesses must grant the right access to the right people at the right time. They also need to prevent the wrong people gaining access. To achieve this, companies have to set up appropriate access rights for their users. They also need to ensure systems check the identity of users when they try to gain access. Together, these techniques are known as identity and access management. The complexity and diversity of today’s computer systems make this a major challenge for many UK businesses.

Increasingly, a company’s users extend beyond their own staff. Greater adoption of transactional web sites is driving the need for stronger access control management over third parties.

In the past, many businesses that sought funding for identity and access management projects justified the expense in one of two ways. The first was reducing the cost of user access management, and the second was enabling new business ventures using the Internet. In 2006 these remain important justifications for identity and access management projects. However, compliance with laws (such as the Data Protection Act) is even more important.

Which identity management related objectives are important drivers of security expenditure?

Unauthorised access incidents continue

Overall, levels of identity management related incidents are consistent with 2004. Among large companies there is a small increase; in one in five, staff had gained unauthorised access to data.

How many UK businesses had security breaches last year?

While the incidence of fraud is low, when frauds do occur they tend to have a worse impact than any other type of security incident. The greatest impact of these incidents is on reputation and remediation costs. In addition, several small businesses incurred direct losses of between £10,000 and £50,000 as a result of fraud.

One large bank’s worst incident was a serious financial fraud that cost millions of pounds. Several small businesses suffering fraud had to spend more than £10,000 (e.g. in legal costs) to recover the situation. A fifth of firms affected by confidentiality breaches spent more than £1,000 on remedial action.

A retailer said loss of confidential credit card data was their most serious security incident. Most worrying of all was the damage to the firm’s reputation.

In 2006, one in eight confidentiality breaches led to adverse media coverage; in 2004, none did. Large multi-nationals are particularly concerned by this. Laws in some jurisdictions (e.g. California) require public disclosure of privacy breaches.

Identity theft and phishing are increasing issues, particularly in financial services and telecoms providers; several businesses reported daily attacks.

DTI recommends

- Think carefully about who should have access to your IT systems.
- Allow access on an as-needed basis, and review it periodically.
- Consider strong authentication for high risk systems.
- If you have a large number of users, automate the set-up and removal of access rights.
- Adopt an integrated approach to identity and access management.

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

Information security breaches survey 2006

Enabling business opportunities
Improving efficiency or cost reduction
Compliance with laws and regulations

Staff gaining unauthorised access to data
Staff obtaining and misusing confidential information
Financial theft or fraud using computers
Impersonation or phishing attacks

In 2006, one in eight confidentiality breaches led to adverse media coverage; in 2004, none did. Large multi-nationals are particularly concerned by this. Laws in some jurisdictions (e.g. California) require public disclosure of privacy breaches.

Identity theft and phishing are increasing issues, particularly in financial services and telecoms providers; several businesses reported daily attacks.
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.

### Piecemeal adoption

More UK businesses are using strong authentication techniques (such as hardware tokens or digital certificates) than ever. This is one reason why the number of incidents has not risen more. However, single factor authentication continues to prevail; four-fifths of companies still rely on passwords alone.

**What techniques are used to authenticate users?**

![Diagram showing the percentage of businesses using different authentication techniques.

Software tokens, where a small file is placed on a user’s computer, have been adopted by many firms as a relatively cheap way of increasing their security. Telecoms and technology companies are the highest adopters. A quarter of them use software tokens or certificates; this is four times the overall uptake.

A technology firm said they needed to demonstrate that they used strong authentication to satisfy their customers.

Unfortunately, use of software tokens and certificates alone does not seem to provide better protection. More firms using these suffered from unauthorised staff access than equivalent sized firms without them. This contrasted with other forms of strong authentication (such as biometrics) where users had fewer incidents.

The number of user IDs each person needs to do their job has not changed much. A third of users in small businesses have only one user ID and password. In large firms 70% use between two and six IDs. Large businesses with more complex systems are not adopting single sign-on. Instead they are taking a more pragmatic ‘reduced sign-on’ approach.

### Comprehensive Identity Management provides benefits

Firms that use electronic requests but not automated user provisioning were more likely to suffer unauthorised access by staff. In contrast, those using fully automated provisioning had fewer such incidents. Automated user provisioning is providing security and efficiency benefits. Unfortunately, its use remains the exception rather than the norm, possibly because of the set-up costs.

Even rarer is the adoption of all the pieces of the identity and access management jigsaw. Just 1% of businesses combined strong authentication, single or reduced sign-on and fully automated user provisioning. None of the firms in this position had a single identity management related security incident. It is not an easy journey, but it does appear worthwhile.

A large manufacturer said that after three years it was finally gaining both security and efficiency benefits from its identity management project.

Firms with online businesses increasingly have to manage user IDs for their customers as well as for their staff. The growing threat of identity theft and fraud requires businesses to adopt stronger identity and access management techniques.

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 2006, URN 06/805.