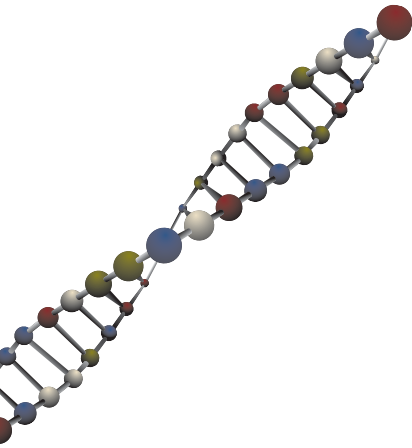


Information security breaches survey 2004



Identity management

The access challenge

A key requirement of effective information security is controlling access to information. Businesses need to make sure the right people have access to the right systems at the right time. It is equally important to block unauthorised people.

Identity Management involves robust controls to make sure that users:

- are who they say they are;
- can see only the information that is appropriate; and
- are set up on systems when they join, and deleted from systems when they leave, efficiently and promptly.

Identity Management



The increasing complexity of IT systems makes it difficult to control user access. As more businesses open up their systems to customers, business partners and suppliers online, the challenge increases.

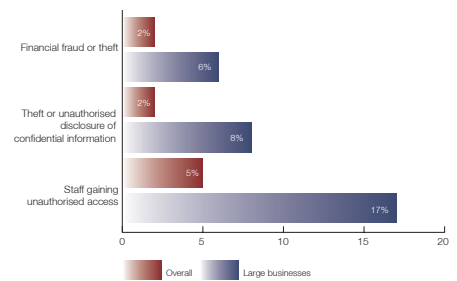
However, building the business case to tackle this problem is not always straightforward. While 53% of businesses found it easy to build a business case for aspects of Identity Management such as data protection and encryption, 29% found it difficult. These figures are low relative to other aspects of security.

There is increased regulatory focus on internal control and privacy around the world. Many UK companies need to comply with the Data Protection Act. Some are also subject to US laws. These further increase the need for effective Identity Management.

Unauthorised access is causing problems

7% of UK businesses had security breaches in the last year associated with weaknesses in their Identity Management. One in five large businesses were affected.

What proportion of companies had a security incident in the last year?



The most common breach related to Identity Management involved staff gaining unauthorised access to information. On average, companies affected reported roughly one such incident a month.

A retailer commented that staff contractors were a particular risk, due to their high turnover and low company loyalty. Yet tracking and controlling their access to sensitive information was nearly impossible.

Roughly one in ten large companies had a significant fraud or breach in confidentiality. Over half of all companies affected said it was their worst incident of the year (outweighing virus infections, etc.). Over half of these rated the incident as very or extremely serious.

Confidentiality breaches tended to cause major disruption over a long period (more than a month in 15% of cases). Remediation and investigation involved significant staff time (10-20 man-days on average). These breaches also resulted in the largest direct cash expenditure of any security incidents. 15% caused more than £100,000 of legal fees, investigation costs and fines.

1 in 6 frauds, and a third of confidentiality breaches, led to customer complaints. While none in our survey reported adverse media coverage, the risk of reputational damage from these incidents is high.

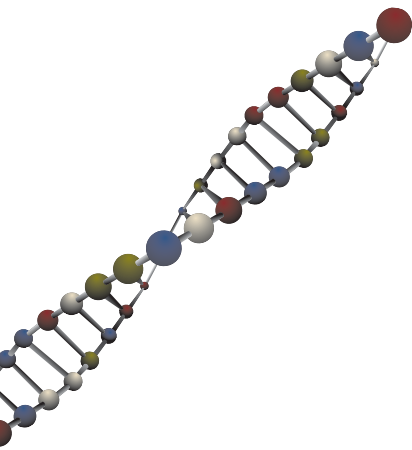
DTI recommends

- Think carefully about who should have access to your IT systems.
- Allow access to systems on an as-needed basis, and review it periodically.
- Consider automation if you have many users accessing many systems.
- Consider whether you need more than just passwords.

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

in association with:





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



Complexity is driving user provisioning

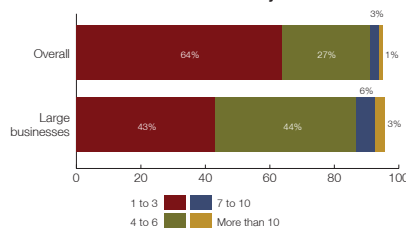
Why do companies' access controls fail to prevent these incidents? One reason is that the sheer number of users and systems in some organisations puts their user administration process under strain.

As a result, new joiners are not set up on a timely basis, and so end up sharing someone else's ID. Leavers are not removed from systems. Transfers between departments lead to accumulation of excessive access rights.

The average user often needs to access several different IT systems for their daily work. The bigger the company, the more systems each individual uses.

As a result, companies are increasingly automating the process for granting, changing and removing access. 16% of all businesses and 31% of large ones do this.

How many systems does the average staff member use to do their job?



Some have also automated the provisioning process. Here, authorisation of a user access request triggers the automatic set up of the required access rights on the relevant systems. While only 3% overall have implemented this, one in four businesses where staff use more than ten systems have done so.

Tellingly, none of the respondents with automated provisioning had suffered any breaches leading to financial fraud or penetration into their systems by an outsider.

One in two small companies handle user administration on an ad-hoc basis, with no formal process. In contrast, 85% of large companies have a formal process.

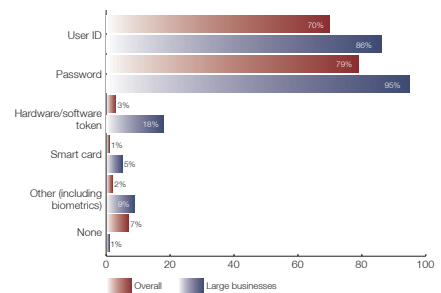
Single sign-on - the Holy Grail?

Single sign-on, where a user has a single user ID and password across all systems has been a target for many. Users find this less painful and are less likely to choose easy passwords or write them down.

44% of small companies use single sign-on. They typically have few systems and rely solely on Windows sign-on. In contrast, only 1 in 5 large companies have single sign-on; a further two-fifths use a central directory for some systems ("reduced sign-on").

Under single sign-on, a breach can enable unauthorised access to all the systems a person uses. Strong authentication (i.e. two-factor, with tokens, smart cards or biometrics) can mitigate this risk. Unfortunately, this is quite rare. Businesses with single sign-on alone, without strong authentication, had a higher than average incidence of unauthorised access.

What techniques do systems use to authenticate users?



While only 6% overall use strong authentication, roughly a quarter of large businesses do so. They seem to be reaping the benefits. Only 3% of them had an unauthorised access breach, compared with 20% of other large companies.

Internet banking is grappling with these issues. At first, most used simple passwords. Now, users must answer extra questions that change with each log-in.

A retail bank suffered a wave of "phishing" attacks, where fraudsters send out e-mails asking customers to enter their passwords into a fake web-site. The bank is now seriously considering rolling out two-factor authentication to its customers.

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 04/612