The cost of forgotten passwords
Barbara Gengler
MAY 25, 2004
This report appears on australianIT.com.au.

FORGOTTEN or lost passwords can cost companies big bucks. Technology researcher Gartner estimates it costs $US14-$US28 ($20-$40) for companies to reset a password.

Cox Communications, a US cable group, says its costs are probably not that high, which is just as well because one-fifth of calls from its 20,000 employees are to reset a password.

Even if Cox was paying only $US10 on each password reset — that’s $US70,000 a month, or $US840,000 a year.

The rapid rise of threats such as hacking, electronic theft, spam, viruses and worms clearly shows the need to identify who is sending information and who is using computer resources.

There is no shortage of technologies that can be used for identifying people. Some of them can be used on their own, while others have to be combined to make them effective.

IDC analyst Brian Burke says his company expects identity management and web services security will revitalise the IT sector over the next few years.

IDC expects the identity management market to reach nearly $US4 billion by 2007, up from almost $US600 million in 2002 — 46 per cent compound annual growth.

Gartner, another technology research group, says the variety of vendor and product choices has combined with market-speak and complex end-user environments to create confusion.

There is no single approach to identity management because the strategy must reflect specific requirements of each business and the technology it uses, Gartner says.

One company seeking a piece of that pie is Alacris. Its products are designed for customers seeking higher levels of security and identity assurance.

Conrad Bayer, chief technology officer at Alacris, says the web-based management capabilities it offers support complex processes, which in turn provide a high degree of trust in the management of digital identities.

The term identity management has become grossly overused in the past two years as vendors have latched on to it while providing very different services, he says.

RSA Security offers a range of products to its 13,000 customers.

Its authentication options include tokens, one-time user access codes, smart cards and digital certificates. These tools identify users and devices before they interact with mission-critical data and applications.

Brian Breton, senior product marketing manager at RSA Security, says the first thing a system should do is verify that the person using it is assigned an identity.

The next technology in the process is access control, which compares the identity against a set of business rules and resources, he says.

Effective identity and access management programs reduce labour costs while maintaining a secure environment.
Rainbow Technologies applies cryptographic systems to hardware keys and USB two-factor authentication tokens.

It uses these in conjunction with other tools to provide secure remote access.

It offers a secure socket layer virtual private network (SSL VPN). It also has a public key accelerator for SSL-enabled servers using the internet. Another vendor, Courion, uses self-service identity management tools to reduce support costs.

Its products offer password reset and synchronisation, digital certificate registration and profile management.

Courion chief executive and president Chris Zannetos says bank security gave him ideas.

"We stole more from the banking world than self-service," he says.

"We learned they had to provide an interface for employees and customers at different levels of capability.

Banks tried to create monolith applications by linking technologies to different functions.

"We link directories, database security systems and auditing systems to automate the process of setting up accounts."

This report appears on australianIT.com.au.