

# Only authorised users welcome



**Some corporations find the responsibility of securing data a burden, but Neil Chaney finds out why user provisioning can make it easier**

**W**ith internal attacks on systems becoming ever more frequent, and the necessity for data accuracy increasing under corporate compliance legislation, I decided it was time to examine whether centralised user provisioning could secure information cost-effectively.

One man told me, tongue-in-cheek, "I would have the most secure network in the world if I didn't have to let my employees use it." OK, that's obviously not a feasible option, but you can understand his concern when you consider the following real-life situations.

A leading utility company determined that around 6,000 members of staff had access to elements of its confidential, online corporate information. Unfortunately, it had only 4,000 current employees – the remainder no longer worked for the company.

In a recent survey conducted by Novell, six per cent of former employees who lost their jobs due to an unpleasant termination or layoff would reportedly seek revenge against their ex-employer by planting a logic bomb or by deleting critical files. Four per cent admitted to Novell that they would release a virus on their employer's network – as the saying goes, you do the math.

Jason is a senior employee at a bank. He has access to 11 computerised business applications, each of which require a secure login and password. But Jason cannot remember all those passwords, or which password applies to which

application, so he writes them all down – somewhere. He just cannot remember exactly where.

Jenny is a systems administrator at a large telecommunications company. With the recent cutbacks, she is overworked and highly stressed. When Richard joined Jenny's company, Jenny should have taken the time to register him with the appropriate security level on each individual application to which he needed access.

Unfortunately, Richard's boss had only defined Richard's requirements as "similar to Paul's." With no simple way of confirming which applications Paul had been granted access to, Jenny did the easiest thing and cloned Paul's access rights for Richard. However, this



**Ensure that only those who need to have access to information get it**

**Neil Chaney,  
Open Systems Management Inc.**

erroneously and irresponsibly gave Paul access to the company's billing system. From that day forward, Richard, his friends, and his friends' friends received their home telephone access for free.

#### **Making the company responsible**

In today's automated environment, stories about people who gained access to something that they should not have and abused the privilege are common, but the stakes are getting higher. In the U.S., legislation such as the *Sarbanes-Oxley Act of 2002*, the *Gramm-Leach Bliley Act of 1999 (GLBA)*, the *Health*

*Insurance Privacy and Accountability Act (HIPAA)* and the *California Database Security Breach Information Act (SB 1386)* provide for criminal and civil penalties against the officers of companies who fail to take adequate action to protect information. In Europe, the amount of legislation (*Basel II*, *Higgs*, and so on) is the same, if not greater.

Senior directors of companies now have to certify the integrity of their financial records – all this in an environment where, according to the Carnegie Mellon University CERT Coordination Centre, the number of cybersecurity incidents pretty much doubles each year. It has reached the stage where company directors have started refusing to certify financials until the security of their financial systems is verified.

So how can the directors of our corporations ensure that all the necessary measures are taken to secure key information and the systems and networks that store, manipulate and transmit it? Especially when every sizeable organisation employs a Jenny or a Jason?

Identity management is the key, and one of its fundamentals is to ensure that only those who need to have access to information get it. This requires a central repository of authorised user information and automated, controlled registration and de-registration of those users across the applications.

The software available to perform this task is called user provisioning, and it is one of the basic building blocks of identity management. The good news is that utilising user-provisioning software should not only improve service levels, security and auditing, but it will pay for itself within a timeframe that even the

◀ most jaundiced finance director would consider good value. In fact, “Identity and access management (IAM) solutions, which can offer three-year return on investment (ROI) figures in the triple-digit-per cent range, are becoming essential tools for the effective management of user account and access rights information across heterogeneous IT environments, for web and non-web applications,” according to Roberta Witty’s Gartner Group report *ROI drives Identity and Access Management Implementation* (3 December 2002).

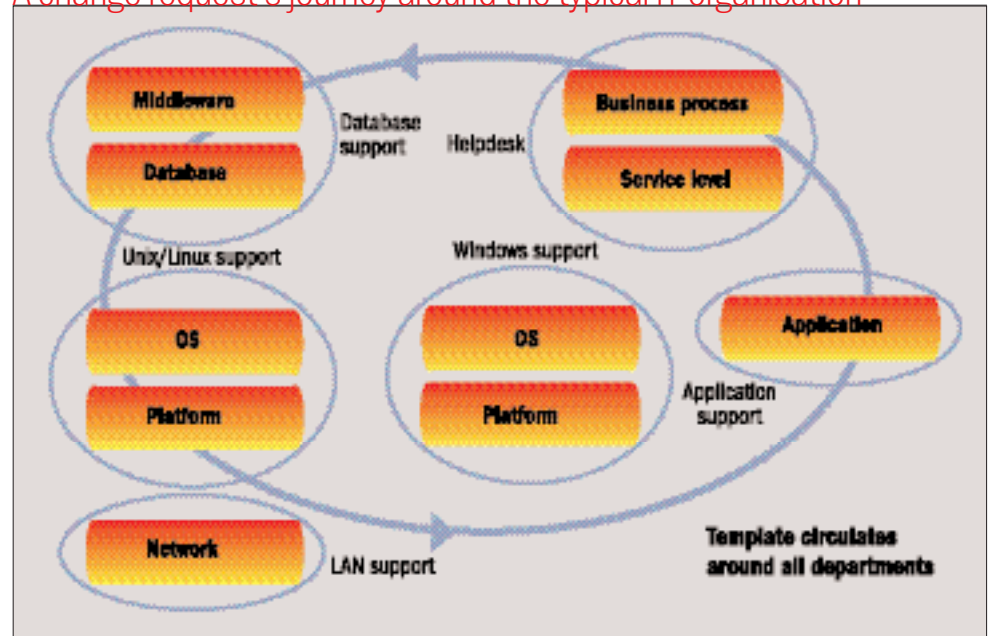
### Making the case

Without user-provisioning software, the task of registering and de-registering users will normally fall to the experts, like Jenny, for each element of the IT infrastructure – DBAs will perform user-administration tasks for databases, UNIX administrators for UNIX, Windows administrators for MS Windows, and so on.

A request to add a new user will need to pass through all such departments, and each expert or system administrator will need to do their bit in registering the user for the software they’re responsible for. The process is both error-prone and time consuming.

With mistakes often made in the registration process, due to the complexity of the task and the supply of erroneous information by business users, the helpdesk gets overwhelmed with user administration requests, cannot fulfil its

### A change request’s journey around the typical IT organisation



service level agreements, and end users can only rarely gain immediate access to the business applications and processes they need. The result is lower productivity and increased frustration.

User-provisioning software prevents this by centralising the user administration function. It works on the principle that a person is granted access to applications according to their role in the organisation. For example, anyone who is a member of a marketing team based in San Francisco will receive access to the centralised CRM system and the San Francisco-based email and office server.

User-provisioning software at its most basic will register an individual on every application, database, middleware and operating system to which they need to be granted access, based on the entry of the user’s name, their department, and the definition of their company role(s).

With a predetermined set of business rules, the users’ profiles are set up and the minimum access requirements that they need to do their job are efficiently granted. Access of individuals who leave is immediately disabled.

The result is that access to applica-

### Some do’s and don’t’s when choosing a vendor...

- DO define what you are looking to accomplish before buying any software. You might be able to accomplish your goals through process improvements alone;
- DO get an external consultant to help you identify qualitative and quantitative goals that are achievable. Then use the output as the basis for your return on investment (visit [www.cosuser.com/downloads/COSuser%20RUMA.pdf](http://www.cosuser.com/downloads/COSuser%20RUMA.pdf) for an example);
- DON’T take it for granted that your vendors know what they are talking about – this is a new market for most vendors and market analysts. Check reference sites and experience;
- DO try to phase any implementation, and arrange for payment by results;
- DON’T be overwhelmed by all the current talk of emerging standards, because it is primarily dictated by the vendors. To see a glossary of buzzwords, standards and links to standard bodies and vendors, visit [www.identitymanagement.co.uk](http://www.identitymanagement.co.uk);
- DO choose flexible software. Your company’s requirements might have several unique elements (think about that home-grown application that only your organisation knows how to register users on). How are you going to ensure that these unique applications will fit into the picture?
- DO make sure that you can continue working if the worst happens and the user-provisioning service goes down;
- DO be wary of the cost of importing and cleaning existing user information into the central repository, because this can cost you a lot more than the software. Stipulate that your vendor will take responsibility, or be aware that you will have to do it. If so, know exactly what you will have to do in advance;
- DO consider your directory or metadirectory strategy. It is highly probable that the user-provisioning solution you choose will have to integrate with your directory services;
- DO make sure that you choose a solution which does not have to work in real time. Real-time solutions tend not to be scalable and can interrupt production systems when it is inconvenient.

tions is restricted to users who need to have it and, even then, the access is granted only at the appropriate level. Links from an identity management system through to a corporation's human resources system are common.

This level of automation removes a huge administrative cost burden from the organisation, and the Burton Group has reported: "Today, manually administered environments require at least one full-time equivalent for approximately every 500 to 1,000 users."

This level of automation also enables new employees to be productive as soon as they join the company, rather than having to wait days to be set up across all the different applications they need to do their job.

Another benefit of a centralised user administration is that all user administration transactions are audited so that directors can prove their governance, and any bypassing of the role-based system can be quickly highlighted.

The central repository of authorised users then allows other benefits to be layered on top. Password synchronisation is

one example. Depending on the organisation's policies, a user making a password change anywhere can have that password propagated across all their applications. This means there is only one password to remember, which in turn means it does not normally get written down and stolen. Each password can be strengthened and changed more often.

Web browser-based workflow engines are often linked to user-provisioning software, so end users can easily request new accounts, passwords or shares, and have those requests routed automatically to the appropriate managers for authorisation before being committed to the system. This eases the workload of the organisation's help desk while also improving service and enabling the end user to be a lot more self-sufficient.

Some user provisioning packages will also track the physical and intangible assets, such as laptops, mobile phones or home telephone lines, that are supplied to users. When users leave the organisation, they are not only disabled from all applications, but a comprehensive report of items that need to be cancelled

or reclaimed is produced for those who need to take the appropriate action. Goldman Sachs claims to have paid for their user provisioning project purely out of reclaimed assets.

#### What's the catch?

So are there any drawbacks? Not really, provided that you take a process-led approach to your user-provisioning project. As with any process engineering, you should never underestimate the importance of senior management buy-in and monitoring, to prevent politics getting in the way of a successful implementation, of consultation and planning across departments, to gain their cooperation and acceptance, and of a phased implementation plan and strong project management.

If you do all this, and pick the right vendor, you can enjoy the benefits that are driving user provisioning forward as one of the fastest-growing sectors of the security software market. ■

*Neil Chaney is founder and CEO of user provisioning solutions provider Open Systems Management Inc.*

neil.chaney@osm.co.uk  
phone: +44 1344 638000  
fax: +44 1344 638011

www.cosuser.com

Open Systems Management, Inc  
Two Union Square, 601 Union Street  
42nd Floor  
Seattle, WA  
98101 USA

Open Systems Management Ltd  
Kings Ride Court  
Kings Ride  
Ascot  
SL5 7JR, UK

