

Who's having an identity crisis?

In the second of our three-part series on aspects of defending your enterprise systems at a time when cloud technologies are radically transforming ICT environments, Decipher Works Principal Consultant Stefan Halvarsson discusses the critical role of identity management in securing your organisation's information infrastructure.

In *How to let the good guys in and keep the bad guys out?*, my colleague Michael Leonard discussed access management, and how to overcome its challenges in a cloud computing environment. Identity management is a closely allied topic and organisations often seek to meet both sets of challenges within the same solution. In this paper we're going to focus on the specific demands of identity management and new issues arising when your users need to access SaaS applications.

Why is effective identity management so important?

Identity management is often misunderstood, but fairly straightforward; you need to determine who should have what access to which applications and resources, and who should not, according to your unique business rules and risk management posture.

Thus identity management is the process of managing the information you use to identify different users, controlling their access to your systems and data – wherever and however they are located or hosted – and determining their privileges, and delegating their administrative authorities.

The complexity in even small or medium-sized organisations – let alone larger enterprises – results from user lifecycles being in constant motion, because today's workforces are highly mobile, staff turnover is high, and individual roles and responsibilities often change. Throughout this lifecycle, users are given new responsibilities or transfer within the organisation, and their access privileges must be reviewed, approved and updated to match their new responsibilities, while previous privileges may need to be suspended or removed.

In today's organisations, identity management must not only determine access to your in-house system; increasingly, cloud-based applications are adopted by the business to perform mission-critical activities, so you now need to manage identities across SaaS and externally hosted systems.

If you also manage the identities of your customers or suppliers, this adds further layers of complexity. For example, specific customers may qualify for higher credit levels, or users at your suppliers are given privileged access to your supply chain applications.

In this White Paper...

- Managing identity throughout the employment lifecycle
- The value of establishing identities for short-term users and contractors
- Why segregation of duty is critical
- How to track and audit individual use of powerful shared accounts
- The best approach to successful identity management implementation projects
- Achieving rapid ROI and stakeholder support with a 'quick win'

While accurate authorisation is always important, speed in processing changes to access levels can be just as mission-critical. So the process for setting up new accounts/passwords and changing access levels must be timely, as delays can lessen your organisation's agility and speed to market.

Ultimately, the ability to manage identity and access data is fundamental to corporate oversight and governance requirements for information security. The ability to audit events and generate accurate, relevant reports is key to reducing the effort involved in meeting a range of compliance regimes: legislative, accounting, industry and your own internal (and often dynamic) security policies.

How identity management typically works

Without an automated and effectively implemented identity management system, organisations must manage user identities manually – which involves detailed processes which are usually time-consuming, costly, inefficient and inherently risky. The principal areas where identity is managed illustrate the size of the problem.

New starts

How many new employees spend the first few days of their new job reading hardcopy training manuals rather than getting hands-on experience in their new role? Without an accurately-defined 'identity' in terms of application access allowed and the types of transactions the new user is permitted to perform – along with formal authorisation from their supervisor or manager – manual processing of a new employee can take several weeks, with misunderstandings of the new role and errors in paperwork often resulting in multiple account reconfigurations.

Contractors

Similarly, manually processing appropriate access for contractors for periods ranging from weeks to months – whether they are working on premises or off-site – can be time-consuming and potentially risky. When contractors are paid by the hour or day, any delays in giving them the access they need to enterprise systems can represent a significant cost. Once their engagement ends, their access and rights must be rapidly deleted from all relevant systems.

Short-term visitors

Identity management may also have an increasing role at visitor sign-in areas such as the reception desk. Consider the following examples:

- A maintenance engineer from your service provider needs short-term administrator privileges to apply updates, troubleshoot or remediate your systems
- A customer meeting with a sales executive and needs temporary internet access
- A business partner visiting your procurement team needs to reconfigure supply arrangements within your ERP system or SCM portal

Who is actually working for you?

Effective identity management enables you to know exactly who is working for (or with) you, and the levels of access they have to your systems, in a single, auditable security log – without massive manual processing and tweaking of multiple systems on an individual basis.

To illustrate this, consider an accounts payable department with 60 staff. If identity management is a manual, rather than automated process, the manager is typically presented with a list of staff with access rights to the organisation's accounts payable systems quarterly, half-yearly or even annually. At that point he or she is required to review and recertify perhaps 70 current users on your records and their various rights to enact transactions.

This creates the risk that some 10 extraneous individuals have the ability to process payment transactions after they have changed roles, or even left the company, over a period of several months – allowing them plenty of time to do plenty of damage.

- An application supplier arrives to demonstrate new functionality requiring internet/email access on their own laptop, or to log in to train your staff directly on your own systems

All of these scenarios, and many others, present significant challenges if user identity is a manual, rather than automated, process.

Changed roles

Increasingly flexible workplaces result in individuals constantly changing roles. This can create a nightmare for organisations reliant on manual identity and access management, because new roles frequently call for changed application access rules.

For example, when a finance department employee is promoted, they may require higher levels of access to your financial systems but, at the same time, there may be transactions they are no longer permitted to perform under your internal (and/or external) compliance requirements. These rules must be applied simultaneously and immediately, and involve reconfiguration of access privileges within multiple systems, wherever they reside.

Leaving users

Perhaps the most important consideration in managing user identity, inefficient de-provisioning of access can lead to serious security risks if an employee retains access after they have left your organisation. If manual processing leaves you unable to de-provision access efficiently, it can result in potentially hostile terminated employees (or staff leaving to join a competitor) with the ability to access your in-house or cloud systems for hours, days or even weeks after they have left your employ.

Critical identity management issues

Apart from managing the entire lifecycle of employees and shorter-term users outlined in the previous section, there are two more complex and important roles of identity management that need to be understood.

Segregation of duty

The general principle of segregation of duties ensures that a single person does not have the ability to conduct all processes within a transaction. Also known as 'separation of duties' or 'separation of powers', it avoids deliberate abuse of their power by individuals as well as preventing them from making significant inadvertent errors.

The underlying principle – that the greater the number of people that need to be employed in a process, the less likely the error or fraud is likely to occur – is deeply embedded within accounting standards and compliance regimes. Two practical examples include:

- **Human Resources:** Staff responsible for modifying the Employee Master File have no access to the payroll system, be involved in the payroll process, distribute payroll cheques or make hiring or termination decisions.
- **Procurement:** Purchase requisitions are to be reviewed and approved by someone other than the employee initiating them. Conversely, managers responsible for authorising purchase orders are incapable of initiating them.

Why segregate duty?

Notable failures to segregate duties in the global banking industry illustrate the complexity and importance of the task:

- **Barings Bank** collapsed in 1995, after Singapore-based trader Nick Leeson was able to hide losses of over £820 million within its systems.
- In 2008, French bank **Société Générale** lost €4.9 billion due to failings in its risk controls systems, and was additionally fined €4 million by French regulators.
- In November 2012, the UK financial regulator fined Swiss bank **UBS** £29.7 million pounds for system and control failings that allowed a London trader to incur over US\$2.3 billion in trading losses – and resulted in the resignations of the UBS CEO and the two co-heads of UBS Global Equities.

Less spectacular examples appear before our Magistrates, County and Supreme Courts around Australia every day.

Further precautions, including segregating tasks across different departments and physical locations, can also help mitigate risk. When duties straddle a range of applications, individual roles must be stringently identified and applied across all of them – whether within your core systems or relevant SaaS applications.

Shared accounts

Typical examples of shared accounts familiar to the ICT team are access to server administration. Other shared accounts may exist within the organisation, such as administrator rights to specific applications – including the control of access levels within cloud-based SaaS applications, where license purchase negotiations and access are managed by business managers rather than the ICT department.

In both cases, multiple users in the company know the password of these shared accounts – which means that the organisation cannot audit precisely who is reading what data or making which changes. With security industry research indicating that increasing number of system breaches originate from insiders, this has become an unacceptable risk.

Applying privileged identity management to shared accounts can remove, or at least mitigate, this risk. The various users will not need to know the password of the shared accounts they access, which allows for strong passwords. Their check-out and check-in process is logged and audited, so the organisation can trace usage and activities within a shared account to an individual.

Implementing identity management – successfully!

Although organisations of all sizes can benefit from an identity management solution, there is widespread (and justified) concern over implementing them. In the past, many projects ended up behind schedule and over budget, delivering significantly less than intended ROI.

Failed technology is rarely the cause of these unsuccessful projects. While the causes are varied, most can be attributed to the following factors:

- **Initial scope:** trying to do everything at once
- **Shortcuts** that ultimately leading to later problems
- **Lack of expertise** in terms of the technologies being deployed, as well as how they best integrate with your existing ICT infrastructure, current standards and best practices
- **Inadequate insight** into (and factoring in of) your current costs, business processes, security policies and compliance requirements
- **Insufficient support:** executive participation, validation and buy-in

How will your business benefit?

Given the mounting costs involved in keeping up with increasingly dynamic user access requirements to both in-house and cloud-based systems – as well as an increased focus on information security and compliance – it is not surprising that identity management is becoming a priority for many organisations, and not just the largest.

Ticking all the boxes

The acknowledged best approach is to take the time to develop a logical, phased approach to identity management, starting with a quick win that achieves immediate cost savings and visible results for both the ICT team and users.

- **Thoroughly understand** your current situation, unique capabilities and constraints
- **Seek expert guidance** in the various identity management technologies more likely to be successful in your environment, and best practices for their cost-effective implementation
- **Conduct role modelling** to increase accuracy and speed configuration of role-based access
- **Gain stakeholder support** by demonstrating benefits fast

Go for a ‘quick win’

Implementing identity management can represent a major, though worthwhile project, so the best approach is to address a particularly problematic or costly area to deliver rapid ROI and user acceptance.

Password synchronisation is a ‘quick win’ for many organisations. Enabling users to access all the applications they need – seamlessly and securely – will dramatically enhance their satisfaction, improve ICT service levels and reduce support desk effort in retrieving or resetting lost passwords to multiple in-house and cloud systems.

You’ll then be able to leverage this success to automate additional aspects of managing internal or external user identities by way of a phased approach to additional functionality, based on your specific business imperatives: compliance, service levels and/or administrative cost reduction.

For those ICT teams that appreciate the value, but have difficulties in building a business case, we recommend scoring a 'quick win' to prove business value, while staying focussed on the comprehensive benefits of implementing an identity management system:

- **Improved productivity and user satisfaction** through synchronised passwords and on-demand access provisioning, changes and de-provisioning of employees, contractors and even short-term visitors
- **Automation** of routine manual user administration and processes across applications
- **Decreased daily ICT administration and help desk costs** including savings from eliminating discrete, customised identity administration for individual applications
- **Centralised enterprise-wide** control over user administration processes, with more granular access management through use of roles
- **Elimination of inconsistencies** across multiple platforms due to human error
- **Reduced risk** of users gaining unauthorised access levels and former employees retaining access to your enterprise systems
- **Improved compliance posture** with centralised views and automation of business processes for verifying identities and granting access rights
- **Support** for reliable, simplified governance/compliance reporting
- **Improved business flexibility** from faster time to market and a centralised, standardised security infrastructure to support rapid rollout of new internal and external systems

How to get started

Decipher Works can analyse your security challenges to help you achieve fast, cost-effective benefits from an identity management system. We'll then work with you to get the most from your investment, by extending deployment to deliver additional business benefits.

Read the other papers in this series:

- > *How to let the good guys in and keep the bad guys out?*
- > *Real time threat intelligence, PCI compliance and reporting*



Stefan Halvarsson is a managing partner in Decipher Works and senior technical advisor working across multiple clients. He has 20 years' professional IT industry experience in Australia and Europe, across both public and private sectors. His expertise is in Identity and Access Management, with an impressive track record in defining, designing, configuring and delivering complex IAM solutions.

About Decipher Works

Decipher Works specialises in helping medium-to-large organisations enhance their information security infrastructure to reduce risk, cost and maximise return on their IT investment.

A certified IBM Security Systems business partner with a strong focus on solving our client's specific business issues, we draw on our deep industry experience to design, deliver and manage customised IT security solutions offering rapid ROI. Our team of consultants has an extensive track record in successfully implementing business-driven security, identity and access management systems and complementary application integration and software development services.

Phone 1300 724 880

Email services@decipherworks.com.au

Web www.decipherworks.com.au