Exploring Secure Identity Management in Global Enterprises

A Joint Study by Novell Worldwide Services, Stanford University and
Hong Kong University of Science and Technology
March 2003

Executive Summary

Secure Identity Management (SIM) is an important topic of discussion among security specialists and executives. A study conducted by Novell Worldwide Services, Stanford University and Hong Kong University of Science and Technology dissects this topic by examining the key drivers of SIM, in terms of security and efficiency improvements across an account lifecycle, and outlines the most critical obstacles to SIM adoption.

Key Business Drivers for SIM

IT managers report that a lack of clear access policies and approval structures inhibit secure and efficient account creation. Without automated communication and management tools for stakeholders and IT managers, companies are suffering from major security vulnerabilities and operational inefficiencies.

The study reveals that enterprises do not enforce – or often even instate – appropriate password rules. Without convenient account and access management, users have to cope with the burden of maintaining redundant account information. Consequently they create workarounds that put corporate security at great risk.

Revoking access rights can take more than two weeks. Most IT managers state that they do not have the tools to revoke rights in a timely fashion.

Obstacles to SIM Adoption

There is currently a lack of support, understanding and executive mandates surrounding SIM. A perception of high cost and high technical complexity of SIM implementations causes hesitation among IT managers. Lack of integration with existing systems, processes and organizational structure are seen as further obstacles.

Conclusion

After certain underlying prerequisites, such as awareness and sponsorship, are satisfied, SIM can be successful with a comprehensive and iterative approach to both the IT and organizational redesign.

According to the following study this is what is happening at the world's leading companies:

- A secretary unknowingly gives away access to the company's most valuable sales leads.
- 8 out of 10 times, passwords are written on the back of a person's business card.
- A former employee still charges expenses to the company billing system.
- IT Helpdesks spend 30% of their time solving simple password related problems.

These dilemmas are not exclusive to the companies portrayed in the following study. Large corporations everywhere are struggling to regain control over their information systems. After empowering employees, customers and partners with more and more information systems, companies are now asking themselves: "Who needs access to what information?" This is not an easy question to answer, but by neglecting it, enterprises suffer serious security vulnerabilities and organizational inefficiencies.

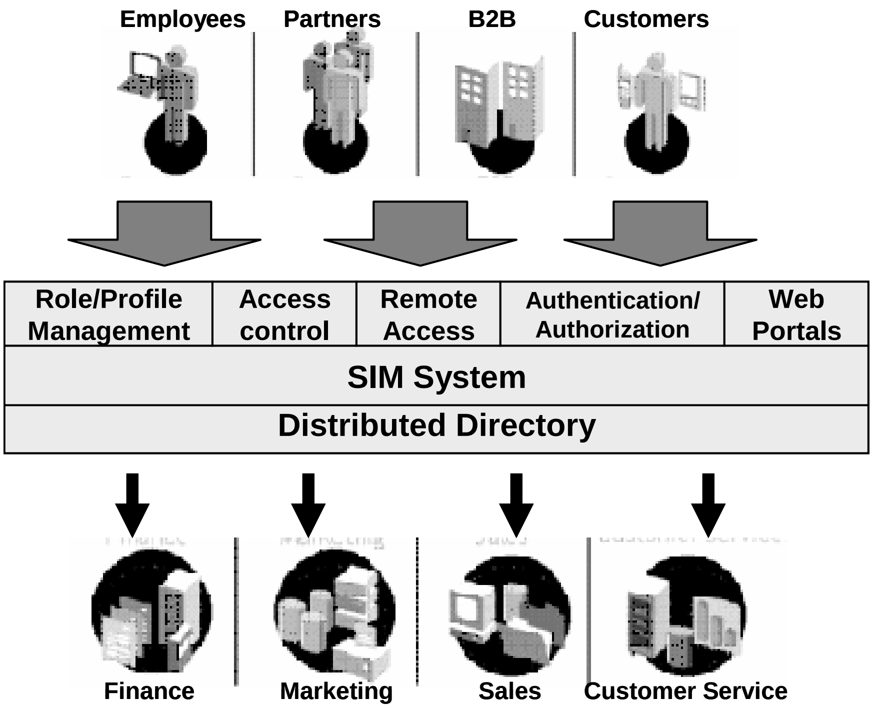
A Study of Secure Identity Management

In February 2003, Stanford University and Hong Kong University of Science and Technology conducted a joint study of enterprise Secure Identity Management. The study consisted of a statistical analysis of 200 Global 2000 company survey responses and over 30 individual interviews with IT executives and IT managers in North America, Europe and Asia. Companies shared their current technologies, processes and attitudes regarding the management of user access rights.

The following report reveals the key results of this study in order to help CIOs and CSOs think about Secure Identity Management issues in their own organization.

Secure Identity Management Overview

Companies claim that they are starting to address these dilemmas with solutions most popularly referred to as Secure Identity Management (SIM). These solutions typically consist of a distributed directory service that maps account information between users and the company's multiple information systems, as depicted in the diagram below. Users are assigned to access rights based on responsibilities and could be given a unique, universal ID and password that they can use to sign on to multiple systems at once.



With this network architecture in place, companies are starting to overlay software and web interfaces to manage identity and access information. For example, user provisioning solutions provide, maintain and revoke user access across multiple applications and data stores within the company. Remote access and extranet access management solutions allow employees, customers and suppliers to log into information systems from outside the company firewall. These fundamental applications enable companies to further augment their security with cutting edge technologies such as biometric authentication using, for example, fingerprint recognition.

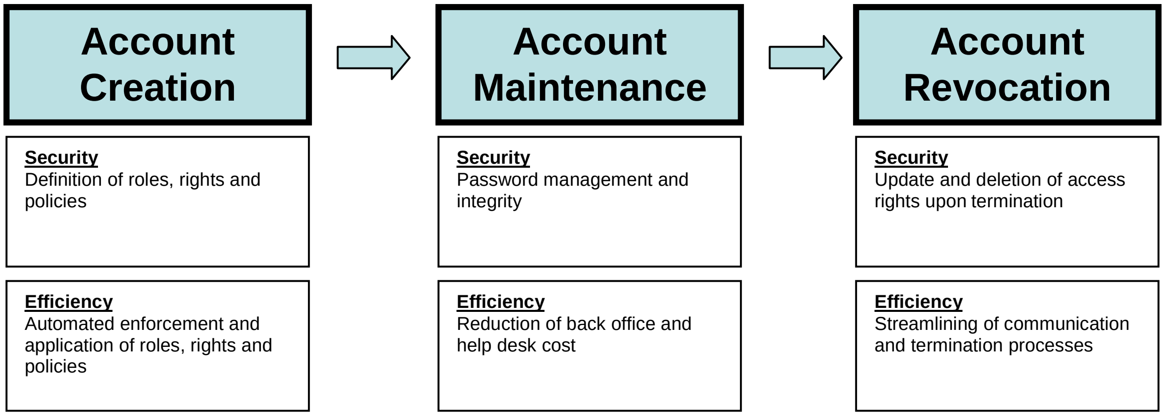
Key Business Drivers for SIM

Of all the factors that drive the demand for SIM solutions, such as disparate information systems and regulatory pressures to ensure data integrity, companies unequivocally cite security risks and efficiency gains as their most pressing concerns.

Security risk management: Companies recognize the need to manage security risks and protect assets. Some have even created the role of Chief Security Officer (CSO) to carry out this mandate. Safeguarding the resources from malicious attacks means that CSOs and CIOs need to find a way to better manage, track and revoke access both within and outside company firewalls.

Efficiency improvement and cost reduction: Inefficient and labor intensive processes cost companies time and efficiency. Making manual changes to numerous application directories and databases to update a user's information can be extremely time-consuming and cost-prohibitive for IT organizations.

The study carefully explores how these business drivers necessitate SIM across the three main phases of the user account lifecycle: account creation, maintenance and revocation. The presentation of study findings will follow the framework depicted below. In the second half of this report, the obstacles to successful SIM adoption are presented, along with a summary of recommendations.



Account Creation

Security
Definition of roles, rights and policies

Efficiency
Automated enforcement and application of roles, rights and policies

Account Maintenance

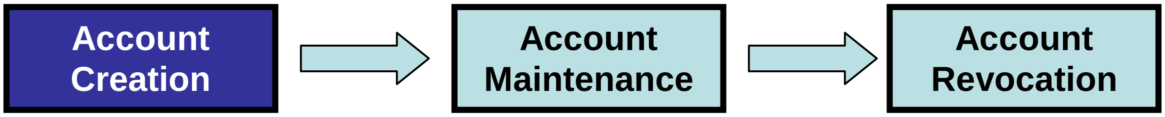
Security
Password management and integrity

Efficiency
Reduction of back office and help desk cost

Account Revocation

Security
Update and deletion of access rights upon termination

Efficiency
Streamlining of communication and termination processes



Providing your employees with access

The first step in ensuring security is providing users with appropriate access to resources based on their role in the enterprise. However, lack of automated, rule-based processes and systems make it difficult, if not impossible, to provide appropriate rights – leaving companies exposed to considerable security breaches and operational inefficiencies.

> ***"We don't know who has access to what and who has access to change things."***
>
> --Product manager, best-in-class networking company

When asked for the ideal scenario, this manager stated that the first thing he would like to see is "a system where all the access policies are described and all access rights are logged - when, where, who gave authorization, etc." At the most fundamental level, many of the companies studied are struggling to even understand how access rights should be assigned and provisioned in their organizations.

Recommendation: The first step for companies to manage security risks is to define clear security policies and to give managers visibility to carry out these policies.

Companies, lacking access policies and visibility, also state that they experience difficulty establishing authorization structures. The study shows that in several organizations, manager approval is not required for employees to get access to critical information systems. For example, an intern at a large software company was able to create an account by merely calling a secretary, allowing the intern the ability to edit and download the company sales lead database. Companies are giving the people, like IT associates, inappropriate authority and responsibility over their most critical intellectual assets. An IT specialist at one of the largest banks in Asia admitted that, with the power he has, he regularly has to "fight temptations".

Recommendation: Companies need to establish and enforce an authorization and approval structure.

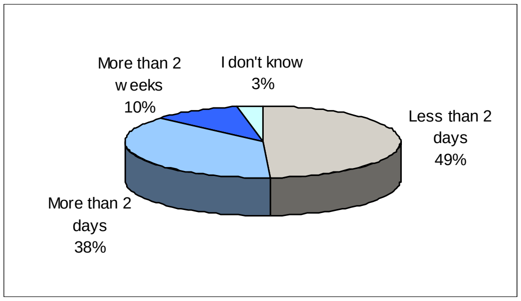
Even if the managers have the authority, visibility and policies to decide appropriate access rights, they also need automated tools to communicate decisions. An IT manager at a global apparel manufacturer and retailer explained that employees were often given inappropriate access rights by mistake, citing human errors as one of the most common reasons. For example, when a new employee requests a network account, IT associates have to track down that employee's manager to find out which drives, databases and folders that employee will need to access. This exchange of vital information often occurs over the phone or in the hallway, and is then manually inputted to various systems every time a new employee joins the company.

Recommendation: Companies need to minimize manual communication by establishing a mapping of new users to their managers, their roles and their access rights.

Q. How long does it take a new hire to get access to all the systems he/she needs?

48% of companies take more than two days.
10% of companies take more than two weeks

Provisioning of access rights is not only a security concern, but also a major cost issue for companies. A long-time access management expert states that it is very common for companies to take up to a week for a new employee to be completely set up on all systems.



Several companies blame this lag time on organizational inefficiencies and technical difficulties. Staff absence and poorly defined IT responsibilities caused an employee at a global transportation company to wait over a month to obtain his access account. In a similar fashion, the IT department at an apparel manufacturer told a buyer that technical difficulties were the reason for her not getting appropriate access rights for two months.

Recommendation: These anecdotes and statistics reveal a huge potential for companies to gain greater efficiency and reduce time to productivity. Companies need to analyze and track the cost and productivity related to activities such as access provisioning. This enables companies to estimate the potential benefit of a formal SIM system.

Business Case 1: Productivity Gain – Giving Access

Assumptions:

Productivity loss, due to lack of access	25%
Avg. lag time to obtain access	1 week (per survey results)
Avg. cost of employee	$40,000 (www.payscale.com)
Number of employees	10,000
Avg. annual employee turnover	15%

Potential productivity gain per new employee:

1/50 years * 25% productivity reduction * $40K cost per year = $200

Gross potential productivity gain per company:

10,000 employees * 15% yearly turnover * $200 saving per employee = $300,000

Account Creation

Account Maintenance

Account Revocation

Maintaining system security

Once employees are given appropriate access to company information systems, they need to uphold security while going about their daily activities. The study shows that poor password management is a major security risk and cost which companies face. This is the case because employees are frustrated by loosely enforced rules and an excess of account information.

It is a common rule that users should create passwords that are robust and hard to deduce. For example, passwords should include numbers and letters, and should not be words found in dictionaries. However, several IT managers state that password creation rules like these are not strictly enforced, allowing users to use obvious passwords such as their birth date. Another general practice is to require employees to change their passwords regularly, but upon further investigation, several IT managers admitted that users "recycle" passwords between systems; for example an IT user can use the same password from a previous period for a different system. There is no global password policy to ensure password security across different systems.

Recommendation: Set up and enforce clear password policies that mandate robustness, unique renewal and confidentiality.

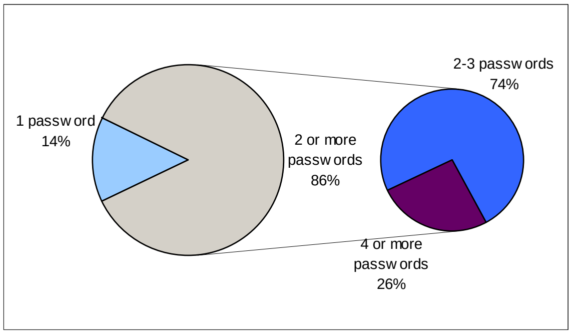
Q. How many passwords do you have to remember on a daily basis?

86% have to keep track of two or more passwords
26% of which have to keep track of four or more passwords

"Eight out of ten times I find users' passwords written on the back of their business card or under their keyboards."

--IT specialist, global apparel manufacturer

Recording passwords in obvious places is only one security-threatening general practice. Given the amount of account information typical employees must remember, it is not surprising that they use workarounds to recall passwords. Survey respondents say that it is common to share passwords among users for even the most



critical systems such as ERP applications. An employee from a large Asian financial company reveals that ten people from his department can access the database using only one password.

Recommendation: Reduce the amount of account information that employees must remember by implementing a universal, well-protected and robust login that allows a single sign-on to access all the systems they need.

Maintaining access rights is also a huge cost block for organizations. One networking specialist, in his 25 years experience, believes that it is usual for IT help desks to spend up to 30% of their time on just password related issues. It is easy to see how the time can accumulate. On average, an administrator needs to manually enter redundant data in four different applications or systems each time a user changes departments or a new user is added. Consequently, these inefficiencies can sum up to millions of dollars wasted for large corporations.

Business Case 2: Help Desk Efficiency

Assumptions:

Helpdesk time spent on SIM related issues	15 – 30% (per survey results)
Employee to helpdesk staff ratio	125:1 (www.rfgonline.com)
Avg. hourly cost of help desk employee	$22 (www.rfgonline.com)
Number of employees	10,000

Annual help desk cost reduction solely due to SIM:

15% to 30% workload reduction * 40 hours * 50 weeks *
$22 hourly cost * 10K/125 employees =
$528K to $1,056K

Account Creation
Account Maintenance
Account Revocation

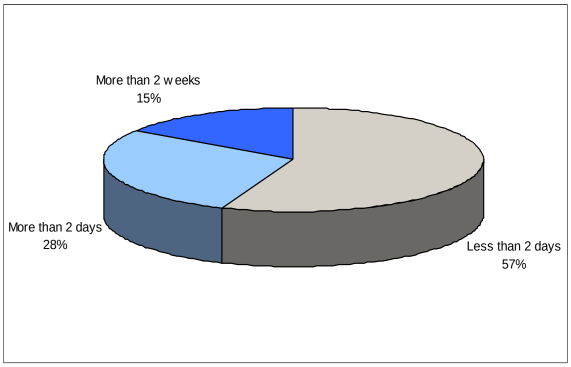
Updating and revoking access rights

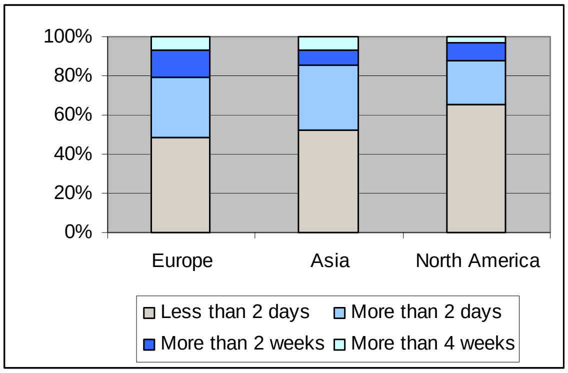
A crucial and sometimes final phase of managing identity and access in companies is the deprovisioning of access rights, specifically, when users leave the company or change departments. The study reveals that companies take far too long to revoke access rights and that in some cases companies do not even revoke access rights at all.

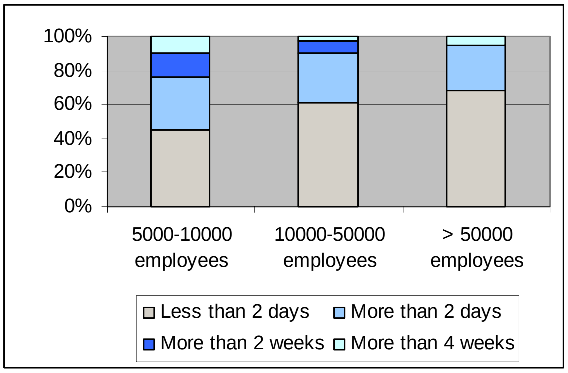
Q. How long does it take your company to revoke an employee's access rights?

43% of companies surveyed take more than two days
15% take more than 2 weeks

European companies, in particular, are slow to update access rights. Over 20% of European companies take over two weeks to revoke access, while only about 10% of North American and Asian companies report this same lag time. This is also true of smaller companies. 54% of companies with fewer than 10,000 employees report lag times of more than 2 days, while 32% of companies with more than 50,000 report this level of responsiveness.







In a supplemental study of former employees, one out of three was able to access part of their corporate network, such as voice mail, email and even sales force applications. For example, an employee at a global investment bank – now working for a competitor – was able to access her voice mail months after she left, giving her access to all internal banking announcements. There are cases of companies taking even years to realize that former employees are still able to access systems remotely.

Recommendation: Companies, need to strive for a shorter and stricter deprovisioning process in order to protect their systems and resources.

"Of an employee's 20 passwords, seven are still active after termination. When three of these are used in the right sequence, he/she has access to the remote server, which is directly connected to everything else and damage can be done anywhere."

--Corporate Security expert, global IT services company

Even companies with efficient deprovisioning processes are not truly effective because they are not able to revoke all access rights. Without an automated user identity management tool, revoking rights becomes impossible because companies do not have visibility into all access rights of a particular user. This can have harmful effects. At a market leading software company, one executive admits that a former employee was able to still charge expenses to the company's billing system six months after he left.

Without an automated user management tool one might think that companies have an auditing system in place – this proved not to be the case. An employee at a globally operating logistics company was granted administrator rights while working at the headquarters in Europe. However these were never revoked when he finished his assignment. This shows a common problem of rights being given to users, but never being followed up by any IT supervisors.

Recommendation: Perform regular audits to clear out old accounts and find security vulnerabilities.

Many companies leave expired accounts intact, because they rely on the company firewalls to keep hackers and malicious former employees out of their network. However, what companies do not realize is that they are still vulnerable if outsiders can physically gain access into the building. Using old accounts and passwords, outsiders can then log onto the network from any machine. An IT manager at a major defense company explains that if a terminated employee was able to get into the building he could use an old account for up to 60 days. Interviews have revealed that it is not difficult to do so – entry badges are often left with former employees.

Recommendation: Account deprovisioning must be enforced, especially in companies that allow network sign-on from any local machine in the building.

Obstacles to Secure Identity Management

Potential Benefits of SIM:

- **Reducing risk** of misuse of company's internal data and applications.
- **Shortening time to productivity** by providing new hire access in a more timely fashion.
- **Reducing IT help desk staffing and costs** by eliminating the need to manually resolve SIM issues.
- **Reducing development cost of separate security modules** for each application by using standardized security APIs shared across systems and applications.
- **Ensuring data integrity** required for regulations like HIPAA, GLB Act, FDA 21CFR11 and FERC.
- **Improving efficiency** of employees by providing seamless intranet and extranet access to applications.
- **Improving convenience** by providing a single entry point.
- **Accelerating time-to-market of web services** based e-business initiatives.

Executives and IT managers at almost 50% of companies surveyed stated SIM as a key priority in their organization. The sidebar highlights some of the benefits that make SIM attractive.

The other half of these companies has not yet realized the pressing need for SIM. The study identifies three main obstacles to SIM adoption: 1) lack of awareness and support at the appropriate level; 2) fear of complex and costly implementation; and 3) poor system integration with current processes in the organization.

Lack of awareness

While employees and IT managers openly speak of identity and access loopholes in their companies, the study shows that many of them do not believe the security threat is significant enough to be on their radar screens. A top security consultant estimates that 15% of CIOs are unaware of any possible security problems, while the rest of the CIOs usually delegate SIM problems to their staff, because they do not see the issues to be relevant at their level.

Complex and costly implementation

Some IT managers attribute the bulk of SIM costs to hardware requirements. Many interviewees who have experience with SIM, however, feel that most of their costs have been driven up by implementation processes. Implementation cost and technical difficulties largely depend on the complexity of a company's existing IT infrastructure. The current tangle of IT systems makes implementing any centralized process or SIM system prohibitively challenging and labor intensive.

System integration with processes in the organization

Most companies face major challenges in deploying identity management because their organizations are becoming more and more complex, and increasingly distributed. In order to gain buy-in from managers across the organization, access management systems need to reflect the company's current power and authority structure. It is common for managers to perceive a loss of power as processes and systems become more centralized. Some companies are therefore hesitant to adopt enterprise-wide SIM solutions for fear of disrupting their fragile power structures.