



Greig Ross Associates

Bringing Business Clarity and Value to IT

SECURITY WITHOUT COST? INTRODUCING IDENTITY MANAGEMENT

Mortgage lending operations have in recent years become more complex, with multiple locations, outsourcing of functions and multiple regulatory activities. It is becoming essential for lenders to address security issues, particularly regarding the robust management of the right data being accessed only by the right people. The biggest organisations are exploring identity management systems, as a precursor to an IT approach that will quickly encompass the whole industry. Lenders should be aware of the issues at stake, and of the best way forward in mitigating the increasing security risks their complex operations are running.

Within the mortgage industry, where the combined pressure of oversupply and margin erosion is forcing lenders to seek more radical solutions to their operating efficiency, both security and compliance appear merely to add to the cost burden. However, Identity Management has the benefit of not only improving security but of reducing cost at the same time. Sounds too good to be true?

The concept of robust physical identity recognition is of course well known in the FS sector, and at a basic level advances have been made in recent years. Introducers need to check ID as part of fact finding and in accordance with the money laundering regulations; and the CML Handbook states that unless solicitors personally know the signatory of a document there is a requirement to ask the signatory for proof of identity – which must then be carefully checked against ID documents. If proof was needed that better security saves money, refer to the CIFAS identity fraud index which reflects a drop of 18% in identity fraud and 30% in impersonation fraud between 2002 and 2004. CIFAS reports that Banks and Mortgage Lenders are showing reduced index figures, reflecting the strict identity verification procedures they follow and the fact that many accounts are opened face-to-face in branches rather than remotely by telephone, post or on-line.

Traditional checking processes obsolete

So far so good. But the difficulties arise when we move into the world of computers, systems and networks where identities are held as encoded magnetic data and the computer is trying to determine whether a person accessing a file is in fact who they say they are. The rapidly growing number of users, the constant addition of new technology, systems, databases, directories and business applications to the IT environment, and the continual change in the legal environment have made traditional manual processes for managing identities obsolete. This has elevated the importance of identity management in major organisations in both the public and private sectors around the world.

The biggest organisations are only too well aware of the issues and are already looking at methods to address them. Where this technology becomes all pervasive is in the ripple effect where any partner company doing business with a larger organisation will also be



Greig Ross Associates

Bringing Business Clarity and Value to IT

expected to abide by these same rules and use the same technology. The risks for slower organisations are clear: their partners will abandon them in favour of more like-minded, security conscious and risk averse organisations.

The agile organisation

As more business is conducted electronically larger organisations are becoming more attracted to agile, change responsive companies. While many enterprises struggle with complex IT environments that isolate data and resources from the people who need them, agile enterprises create an environment where people communicate and collaborate easily both internally and externally and always have the tools and information they need to work effectively. According to a recent article in CIO Magazine the business benefits of agility included, “improved customer service levels, faster time to market with new products and a greater ability to take advantage of new revenue opportunities”. (CIO.com, “The Agile 100”)

The agile business must be supported by an agile foundation that:

- enhances system security
- provides better access to information held in business applications
- improves productivity and service levels
- reduces management and service costs

The rise of Identity Management

Every decision that is made to provide people with access to your business and every effort made to deliver services or content to people is based on identity. You should not deliver resources or information to people unless you know who they are, how they relate to your business and what they need and are entitled to get from you. Because of security concerns, regulatory legislation and potential cost savings, identity management is “climbing the corporate importance meter”. Corporations can no longer ignore the need to manage a user’s identity from creation to deletion, which ensures logging and auditing of who is on the network and what they are doing, why and when. Burton Group predicts that every organisation will be involved in an identity management project within the next two years.

You may be surprised that such disciplines do not already exist. In many organisations senior executives have relied on their trusted IT people to ensure that this was imbedded in all systems from day one. Unfortunately in many companies simple to use technology was not available and many basic security features were hard coded into systems right across the enterprise.

To try to understand the problem consider an employee’s telephone number which will be found in many different systems, spreadsheets and files throughout an enterprise and

1 Trainers Brae, North Berwick, EH39 4NR.



Greig Ross Associates

Bringing Business Clarity and Value to IT

in other parts of the business group or external partner organisations. After departmental reshuffles, promotions, renumbering systems and company mergers very few of the telephone numbers recorded across all of these systems are accurate. Since people use telephone numbers as identifiers in its simplest form, not being able to find the correct person when you dial the number can cost time and cause confusion resulting in inefficiencies.

The problem of proliferating passwords

More concerning is that the same issue relates to more important identifiers such as passwords where individuals have different passwords for different systems. It is not unusual in some organisations for some people in an organisation to have between five and ten passwords. Standard Life has reported that each of their 13,000 employees throughout the world first logged on to their workstation, then the mainframe, and ultimately as many as ten separate applications each of which required separate password control. We recently came across a person within a company who had eighteen passwords. Such situations lead to confusion, mistakes, time loss and more dangerously opportunities for fraud and impersonation. Employees inevitably resort to writing passwords down or sharing them with colleagues, and Help Desks are inundated each day with requests to reset people's passwords. In that same organisation the Help Desk had eight people whose job was simply to reset passwords.

In many organisations the process of inducting a new employee is called Provisioning, because of the multiple resources and services the employee requires such as registering their computer, providing access to the correct printer, ensuring they gain access to the correct networks, access to the accounts system and the payroll system etc. Creating new employees in each of the systems they require access to is typically a long, manual process inherently subject to mistakes and inaccuracies. Sometimes these are rectified right away, and sometimes they are only discovered when the person moves to a new department or leaves.

Similarly it is not unusual to find that some identifiers are left on systems long after people have left the company. Hackers call these 'worm holes', and use them to gain access as if they are legitimate system users.

Cost of managing inefficient identity processes

The costs in administering and trying to stay on top of all these elements of identity security is enormous. To determine whether your organisation is typical of most businesses you should request a report from your IT Manager which asks questions such as:

- How many employees have more than one login identity and password?
- On average how many identities does each person have?

1 Trainers Brae, North Berwick, EH39 4NR.



Greig Ross Associates

Bringing Business Clarity and Value to IT

- How much time is spent and what is the annual cost for giving employees access to the systems they use?
- What is the cost of managing password resets?
- How many ex-employees still have access to your systems?

IDC provide a simple example of how security logging costs can be cut, as well as a frightening insight into the hidden cost of inefficient security management:

1. Each year the average large company with four to eight applications spends 0.83 hours per user managing passwords
2. For 5,000 users this requires more than two to four full time help desk workers dedicated to password management alone
3. 70.4 percent of all users call the help desk at least once per month to get help with a password, at an average of 25.2 minutes per call
4. For 5,000 users this translates into 1,478 hours in lost user productivity per month.

The implications of Sarbanes Oxley

Whilst Sarbanes Oxley is not clear in prescribing a solution to the compliance issue it does make clear what obligations a company is under in order to be compliant. The internal controls referred to ultimately break down into a series of processes that companies must adhere to in the preparation of financial reports, as well as the protection of the information that goes into the making of the reports. U.S. Companies and those supplying and working with U.S. Companies are increasingly recognising Identity Management as an important ingredient in helping to ensure Sarbanes Oxley compliance. Maintaining transactional and security audit trails is increasingly being sought by such organisations in the light of this legislation.

Key elements of effective Identity Management solutions

Provisioning for starters, leavers and movers

Provisioning effortlessly manages the identity lifecycle of each person starting, leaving and moving around your organisation. This is achieved through an automated workflow process based on pre-defined business rules. As a result users are granted access (and as appropriate have rights withdrawn) to all of the resources they need, with continuous auditing ensuring compliance.

Manage identities effortlessly

Identity Management streamlines the process of managing a user's identity across all connected systems round the clock from any web browser. This reduces costly manual updates for various data bases, systems and applications and lowers administration costs

Employee Self Service

1 Trainers Brae, North Berwick, EH39 4NR.



Greig Ross Associates

Bringing Business Clarity and Value to IT

With an Identity Management solution in place, further efficiencies can be achieved by allowing policy based self service. Typically this allows employees to reset passwords based on a centrally controlled security policy. In addition employees can be allowed access to certain fields of their own identity and be allowed to change details, such as personal address, phone numbers etc.

Single Sign-on and Smart ID

It is a considerable relief to employees to have only a single password to allow them access to all the systems they require. It is then relatively straightforward to operate regularly changing passwords routines – perhaps on a monthly basis. Advanced Identity Management systems permit company users to sign on only once using the company standard smart ID card, reducing costs further.

Reporting & Compliance

Recently regulatory compliance has become a critical issue in the highly regulated world of financial services. Organisations must prove compliance with government regulations to reduce their risk and liability. Customers and partners also want assurance that companies they do business with are complying with security regulations, which is why a complete secure identity management solution must include auditing and reporting. Such reports should ensure that security policies are being enforced, and collect and report on real time monitoring and ‘big picture’ views. The information should be collected and stored in a “non-repudiative” data store log where event data can be viewed to determine compliance with corporate policies and government regulations.

Where do you start?

The starting point is by asking the right questions to discover whether or not your business has an issue and where the problems and challenges lie. From recent research it appears that most businesses going forward require an identity management solution. Indeed it may become a fundamental necessity to demonstrate that this technology is employed within your organization. The next stage is to conduct a properly managed project plan. Some organizations take six months to implement this type of technology whereas large organizations may take several years to fully roll it out across the group. The longer the delay in introducing this technology the larger the problem that is being stored up.

The choice of identity management systems can be a bit of a maze and it is often difficult to comprehend the entirety of identity management solutions. It is obviously important that a business does not select an inappropriate solution that does not match the infrastructure or its needs. It is important to take appropriate advice from the start on such matters as using a single solution that works in many different technology environments, across multiple locations and takes account of current and future organizational and technology plans.

1 Trainers Brae, North Berwick, EH39 4NR.



Greig Ross Associates

Bringing Business Clarity and Value to IT

Developing an identity management infrastructure both for people and technology is the only way to successfully manage the heterogeneous, distributed, siloed organisation that makes up a typical business today. The goal is to create a critical service in identity that can be applied right across the organization which results in the benefit of having better control, visibility and security while continuing to streamline operations with partners and external customers; seamlessly linking applications; and driving down costs by reducing help desk calls via self-service and sharing administrative costs with partners.

Identity management is about managing each and every one of the unique identities, the rights these identities have, and the privileges associated with enterprise users in a centralized and policy-driven manner. These efforts usually include single sign-on, password management, user provisioning, and user, group and organizational management.