WHITE PAPER: CA IDENTITY & ACCESS MANAGEMENT

The Evolution of Identity and Access Management

AUGUST 2007

Bilhar Mann
CA SECURITY MANAGEMENT

Table of Contents

Executive Summary

Challenge

The role that the IT professional plays in Identity and Access Management (IAM) continues to move forward at a rapid rate, and IAM has become a key tool in the organization's security and risk management efforts. Many organizations however, are not realizing the potential of a fully evolved IAM solution.

Opportunity

Forward looking organizations view identity and access management as more than just a security and risk management tool. By making it an integral part of their company DNA, an evolved IAM solution can act as a service that truly enables business growth.

Benefits

An integrated and mature IAM solution allows an organization to become more operationally efficient, to mitigate risk and satisfy compliance, and to provide consumers, employees and partners access to the information and services they need to be successful.

SECTION 1

The Evolution of Identity and Access Management: From Gatekeeper to Enabler of Business Growth

"It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is the most adaptable to change." [1]

—Charles Darwin

Over the past decade, the role that IT plays in the corporate landscape has evolved at a pace that Darwin would find astounding. In an effort to survive, the fittest IT professionals have rapidly adapted a business-savvy persona, and, in most cases, business people are rapidly becoming more IT proficient.

Similarly, the role that the IT professional plays in Identity and Access Management (IAM) continues to move forward at a rapid rate. Where once its function was perceived as "keeping bad guys out" (and occasionally resetting passwords), IAM has become a key tool in the organization's risk management efforts. Companies have now reached the point where it has become nearly impossible to define where business functions end and IT functions begin.

Savvy IT professionals with evolving roles recognize that IAM can be even more. A recent study by *CIO Magazine* found that nearly 47% of CIOs describe the primary focus of their organization's IT strategy for 2007 as "Viewing IT as an enabler of business growth." This far and away outshined, "Improving IT performance" (25%) and "Reducing IT costs" (12%).[2]

Enabling business growth is not just the charter of CIOs, but of all IT professionals.

So how does IAM evolve beyond gate keeping and risk management into an "enabler for business growth?" The answer is that the IAM solution (and all security functions, for that matter) needs to become so tightly integrated into every aspect of the business that it essentially becomes part of the company's DNA. Unless it is truly encoded into the essence of the organization, IAM will become a vestigial organ and never fully realize its potential as a service that helps people both within and outside the organization get their jobs done securely, efficiently and cost effectively.

To better understand how this can be accomplished, we need to take a look back and see how IAM has adapted to meet the changing business climate.

1 Source: Origin of Species by Charles Darwin, (publ. 1859)
2 Source: CIO Magazine, "Role and Influence of the 21st Century CIO," September, 2006.

SECTION 2

In the Beginning: Efficiency through Automation

Most companies first encounter with an IAM solution arose from the desire to satisfy two very basic business needs—improving security and saving money.

As businesses began to turn to automation in an effort to get faster, cheaper and better results, the need to secure transactions became more important. At its simplest, all data driven processes need to be protected, and the more cost effectively a company can do that, the better off they are.

Consider, as an example, the Department of Welfare for one of the larger industrial states in the U.S. In early 2002, they were running into problems as their automated claims functions were becoming very difficult to navigate. For the system to properly pay claims, some 60 partners required access to data and applications stored in as many as 300 discrete, secure silos—each with its own user account and access policy—throughout the organization's IT infrastructure. The system was time consuming, costly and inefficient to use and support.

Building appropriate security into each application, managing access rights in a rapidly changing department, and supporting users who couldn't always recall multiple passwords and procedures, made poor use of an already taxed IT department's fiscal and intellectual resources. Moreover, it was also making it extremely difficult to follow security policies that had been put in place to protect sensitive personal data.

The IT department initially deployed an IAM solution within one of the applications that provided services for approximately 10,000 contractors and employees located in various offices throughout the state. That number has since grown to include more than 25 applications regularly accessed by more than 35,000 users, including employees, business partners and the public at large, making a solid IAM solution even more important.

The benefits of such an IAM implementation are easily quantifiable: dramatically reduced IT overhead as accounts are created and maintained in a centralized fashion, and improved security as the potential loopholes created by multiple accounts are closed.

In this particular example, an interesting thing happened on the way to saving time and money. While initially looking at IAM as a way to better deploy their resources, two other significant benefits were realized. By simplifying the access process, they saw a dramatic increase in end user and client satisfaction. By tightening security loopholes the Department of Welfare began to better prepare itself to meet increasing compliance issues surrounding client privacy, data integrity and security, and reimbursement documentation. They also took an important step in the direction of using IAM as a risk management tool.

IT user management processes, simplifies auditing and reporting, helps achieve operational efficiencies, assists in regulatory compliance and helps ensure uninterrupted business operations.

SECTION 3

The Rise of Risk Management

The more integrated IAM becomes in everyday business functions, the more IT evolves from dealing with machines to dealing with people. Throughout history, the biggest risk with all

manner of security has been the people, not the equipment. Just ask the citizens of Troy. Their walls were high enough and their gates were plenty strong. Bad decisions by well-meaning people led to bad results.

In our modern world, people and their behavior still pose the greatest threats to the security and integrity of all kinds of data. It's no longer just enough to manage access. IT departments are increasingly being asked to document the digital activities of everyone who makes contact with data or applications. In addition, requests to both manage and document access to data are coming fast and furious from a number of different sources both within and outside of an organization.

Internally, pressure to remain compliant starts from the top. The Board of Directors and Corporate Counsel are looking to minimize risk and exposure. High-profile security breaches have cost corporations dearly, both on a fiscal level and with their brand reputation. These events have left everyone scurrying to make sure they are covered. Once it was determined that the cost of compliance is less than the cost of potential exposure, the CIO found himself, or herself, in the risk management business.

The finance department gets into the act as CFOs and their reports look to documentation as a tool to help improve utilization, track ROI and measure organizational efficiency. Line of business management also wants to know about efficiency, but they are primarily concerned with getting the most out of their applications. Tasked with P&L responsibilities, they need to know if they are getting what they are paying for and if the applications they need to do their jobs are available when they need them. If not, they want to know who's responsible. Having the right IAM policies, processes and procedures in place can help avert the fire drill that comes with trying to find those answers, meeting the internal needs more efficiently and at less expense.

Clearly, adapting to working with all of these internal business functions is crucial to the survival of IT professionals. It's the cost of complying with continually expanding external regulatory requirements, however, that has made IAM such a critical component of risk management.

Analyst firm IDC cites regulatory compliance as the leading driver of IAM spending in 2006 and expects that trend to continue with the total IAM software market exceeding $4 billion in revenue by 2009. [3]

In the U.S., Sarbanes-Oxley (SOX) and the Health Insurance Portability and Accountability Act (HIPAA) get most of the press, but the Gramm-Leach-Bliley Act (GLBA), the Federal Financial Institutions Examination Council (FFIEC), and Payment Card Industry Data Security Standard (PCI) also make compliance a complex and expensive business.

For companies doing business outside of their own country, global regulations such as the U.K. Data Protection Act (DPA), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), Sarbanes-Oxley for Japanese companies (J-SOX), and a host of ISO standards, create even more demands on IT departments to produce the goods when it comes to proving their data security.

3 Source: IDC White Paper sponsored by CA, Beyond Compliance: CA Enables the Enterprise to Meet Demands Today, Provides Flexibility for the Future, #205749, March, 2007

A global producer and distributor of TV and movie programming with more than 5,500 employees operating in 67 different countries, uses hundreds of different applications to create, edit and distribute content. Controlling access to extremely valuable content was a significant IAM challenge, and corporate compliance directives handed down from their Asian headquarters required significant implementation resources. As a global company, they were also faced with a host of domestic and international compliance regulations.

To streamline provisioning and user management processes and to improve overall auditing functionality, they turned to an IAM solution that featured integrated single sign-on, roles-based access control and a self-service infrastructure. Almost immediately, security policies for more than 3,000 users were enforced through centralized authentication, authorization and access controls. This improved overall security, accountability, user experience response times and IT efficiency, while making auditing for regulatory compliance simpler.

With an IAM solution architected as an integral part of the IT infrastructure, rather than as an add-on afterthought, the daunting task of implementing and enforcing a strong security policy across multiple locations on several continents became dramatically easier. This company has quickly and easily implemented a distributed solution through their IT support hubs and data centers across the globe and continues to add an average of three new applications into the IAM service every six weeks.

Enforcing security and corporate compliance, and automating the audit and documentation processes, are perfect examples of how an IAM solution can serve as a risk management tool. As with the earlier example, end user satisfaction was a further benefit as the people requiring access to digital content and applications were able to get that access quickly and easily. When they did have issues, the IT team was better equipped to help them.

The Future: Connecting People with Services

It's clearly established that an IAM solution ultimately needs to be baked into the DNA of an organization in order to keep data and applications secure and to more easily prove regulatory compliance. Like a police officer, an IAM solution needs to both protect and serve. A comprehensive IAM solution acts as a service when it seamlessly and efficiently connects people with precisely the data and applications they need to accomplish their goals.

Our "data anytime, anywhere, any place" world has increased security and risk management requirements, while adding access and integration issues that never existed before. A fully-grown and fully-deployed IAM solution will enable the business to balance integration and appropriate access, properly protecting the silos where data is stored while making them transparent and accessible to authorized users.

It's no secret that financial service institutions often lead the way in implementing cutting-edge physical and logical security procedures, and using IAM to accommodate end user customers is a strong example of how it can truly act as a service.

In Europe, a group of leading financial services companies offer a wide range of personalized banking, financial, insurance and consumer credit solutions to approximately 1 million customers through a network of more than 500 branches. Their centralized information systems consisted of a mainframe connected to more than 750 severs at various branches and third party vendors.

This financial institution wanted to extend service beyond the branch and begin offering home-based banking to their customers. However, the combination of distributed environments and Web-based applications offered a significant IAM challenge. As expected, each system had its own built-in authentication and security mechanisms which proved to be ill-suited to an environment where access was extended beyond the confines of the bank's internal infrastructure.

Turning to an IAM solution that offered a single sign-on for Web-based resources, along with a centralized security policy management server, they were able to seamlessly consolidate and control access across a variety of platforms, delivering the data and applications that customers needed to do their home banking.

Internally, the IT staff is able to reduce risk and achieve compliance, integrate internal and third party applications, enhance security and reduce stress on the help desk, with a reliable, easy to use IAM solution.

Externally, people got to do their banking from home, quickly, easily and securely.

Out of the 80,000 users on the system, managers indicated that only 10 initially required some level of help. This seamless transition has helped to grow their online-banking business and strengthen customer loyalty while lowering the cost of transaction processing. All the while, customers were blissfully unaware of all cost saving, efficiency and policy compliance machinations that were going on behind the scenes.

SECTION 4

Conclusions

It can be as simple as making the customer's online experience transparent following a merger or acquisition, enabling a partner to seamlessly connect to an extranet for a joint project or providing the appropriate access to multiple data sources for your customer service team located in another part of the world. A comprehensive IAM solution connects people with disparate data and allows business to continue to grow and in many cases to grow faster than it would have otherwise, and with less risk. Meanwhile, integration activities, maintenance and upgrades go on quietly in the background.

Analysts and IT professionals alike acknowledge that most organizations need some level of outside assistance (be it a consultant, a software vendor, system integrator or all three) to help them evolve their IAM solutions to a point where they are truly offering a service that helps their business grow. There are too many fragmented systems, regulations and compliance issues to do it alone. This often puts IT organizations in a defensive, reactive position. Most need help to properly assess risk and deploy systems that provide the access and documentation required to satisfy all concerned stakeholders.

Those organizations that have "made the leap" to IAM were ready for regulations and are therefore closer to being "enabled" by doing IAM right. However, as mentioned above, regulation acts as a catalyst for all companies to get to this point. The rate of evolution will increase even faster as companies race to comply. Beyond that, some organizations are already beginning to recognize that implementing an IAM solution that acts as a service makes good business sense.

Consider a world of massive interconnected businesses—where every transaction and information exchange is automatic, instant and can be set up on the fly requiring minimal coordination. The

network in essence becomes the equivalent of a massive utilities grid. Plug in any application, employee, customer or partner and you are ready to go. While this is a long way out in any grand sense, it is being done on a smaller scale today with services oriented architectures.

Automated supply chains currently connect multiple partners, vendors, customers, manufacturers and shipping agents, to be adjusted and changed in near real-time. What is perhaps more interesting is that in many cases, these "users" are themselves machines, programmed to perform tasks automatically. These multiple, rapid, automated transactions have enormous potential to boost efficiency, but all of these conveniences come at a price. As the number of processes and transactions increase exponentially, so does the need to secure and document them.

Since the concept of "internal" and "external" user is blurry, a traditional perimeter approach to security no longer makes sense. However, a system built with IAM hardwired into its DNA helps prevent security vulnerabilities that massive multiple transactions create, while enabling IT and business management to assign priority, document, and meter access rights, service levels, and privileges to any level of user, whether human or mechanical.

Those IT-savvy business professionals mentioned earlier need to continue to evolve their thinking about IAM the way their IT colleagues have. An integrated and evolved IAM solution that allows an organization to become more operationally efficient, to mitigate risk and satisfy compliance, and to provide consumers, employees and partners with access to the information and services they need, is truly an investment in the ongoing evolution and growth of the entire organization.

SECTION 5

About the Author

Bilhar (Bill) Mann
Senior Vice President &
General Manager
Security Management

Bilhar (Bill) Mann is senior vice president and general manager of CA's Security Management business unit. Bill is responsible for continuing to build out CA's portfolio of world-class security management solutions and ensuring they are integrated with CA's other Enterprise IT Management solutions. Specific focus areas are identity and access management (IAM), threat management and security information management (SIM).

Bill has 15 years of experience in security management. He joined CA in 2003 to advance its security management strategy and was instrumental in CA's 2004 acquisition of Netegrity, Inc. a leading provider of IAM software. Later, he was named senior vice president of product development for CA's SIM and threat management product families.

Prior to CA, Mann was director of product management at Volera, a majority-owned subsidiary of Novell. As director of business development at Novell's Net Content business unit, he defined a co-hosted content distribution service and established strategic partnerships with key data center hosting companies. Mann joined Novell upon its acquisition of JustOn, Inc., an application service provider (ASP) startup that he co-founded.

Earlier, as director of product management for email and web security firm Worldtalk (now Tumbleweed), Mann launched one of the first integrated web security products for anti-spam, anti-virus, malicious code and content inspection.

Before moving to the United States in 1996, Bill ran a London-based IT consulting firm where he held security-related consulting and engineering positions for major European clients.

To learn more, and see how CA software solutions enable organizations to unify and simplify IT management for better business results, visit ca.com/iam.

CA, one of the world's largest information technology (IT) management software companies, unifies and simplifies complex IT management across the enterprise for greater business results. With our Enterprise IT Management vision, solutions and expertise, we help customers effectively govern, manage and secure IT.

WP05EVOLIAM01E MP31921