$495 USD / free to TM Forum members

2012 | www.tmforum.org

IDENTITY & ACCESS MANAGEMENT

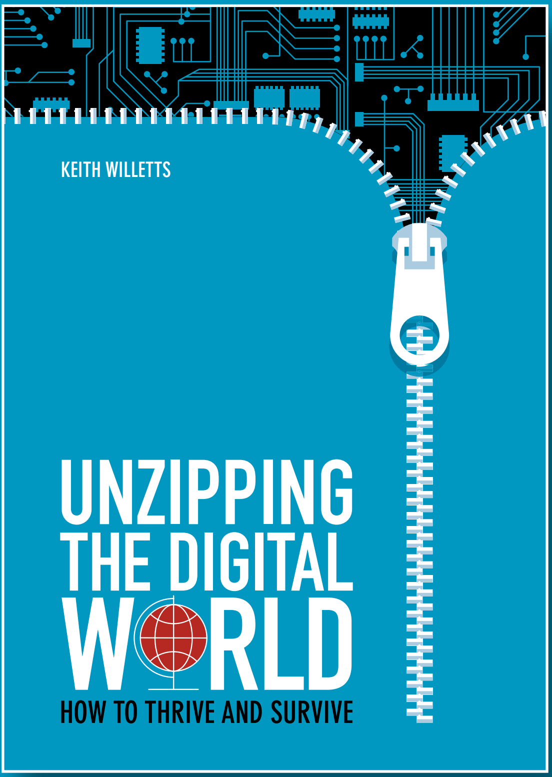
tmforum QUICK INSIGHTS

DRIVING THE BUSINESS CASE

UNZIPPING THE DIGITAL WORLD

A NEW BOOK BY KEITH WILLETTS

AUTHOR, TM FORUM CO-FOUNDER AND CHAIRMAN, COMMUNICATIONS WEEK TOP 25 INDUSTRY VISIONARY, BRITISH COMPUTER SOCIETY AND BT GOLD MEDAL AWARD WINNER.



KEITH WILLETTS

UNZIPPING THE DIGITAL WORLD

HOW TO THRIVE AND SURVIVE

A 'digital tsunami' is feeding on itself driven by cloud, mobile broadband, smart devices and a mushrooming 'internet of things' enabling every sector of every business to rethink how business is done - almost anything that can be digital will be. Willetts unzips the market with a 'no holds barred' picture of what today's giants need to do to thrive and survive in the rapidly expanding digital world and presents a practical series of steps on how to exploit the massive opportunities the digital economy presents.

"TWO THUMBS UP! THE FUTURE FOR OPERATORS WILL COME FROM EXPLOITING NEW SOURCES OF REVENUE IN THE DIGITAL WORLD WHICH ARE SO WELL SET OUT AND EXPLORED IN THIS BOOK."

PAUL BERRIMAN, CHIEF TECHNOLOGY OFFICER, PCCW

www.tmforum.org/unzippingthedigitalworld

IDENTITY AND ACCESS MANAGEMENT
DRIVING THE BUSINESS CASE

TM Forum's research reports are free to all employees of our member companies and can be downloaded from our website once they've registered.

Report author:
John Williamson
john.williamson20@btopenworld.com

Publications Managing Editor:
Annie Turner
aturner@tmforum.org

Editor:
Claire Manuel
cmanuel@tmforum.org

Production Assistant:
Aideen Greenlee
agreenlee@tmforum.org

Creative Director:
David Andrews
dandrews@tmforum.org

Commercial Sales:
Mark Bradbury
mbradbury@tmforum.org

Senior Publisher:
Katy Gambino
kgambino@tmforum.org

Client Services:
Caroline Taylor
ctaylor@tmforum.org

Head of Marketing:
Lacey Caldwell Senko
lsenko@tmforum.org

Report Design:
The Page Design Consultancy Ltd

Vice President, Research and Publications:
Rebecca Henderson
rhenderson@tmforum.org

Advisors:
Keith Willetts, Non-executive Chairman, TM Forum

Martin Creaner, President and Chief Executive Officer, TM Forum

Nik Willetts, Chief Strategy Officer, TM Forum

Published by:
TM Forum
240 Headquarters Plaza
East Tower, 10th Floor
Morristown, NJ 07960-6628
USA
www.tmforum.org
Phone: +1 973-944-5100
Fax: +1 973-944-5110

ISBN: 978-0-9857635-4-1

Executive summary

Identity and access management (IAM) is a big business, getting bigger by the day. According to market intelligence company International Data Corporation (IDC), the global IAM market was already worth $4 billion in 2010 and, according to technology research firm Gartner Inc., it could be worth $11.9 billion by the end of 2013.

It's not difficult to understand why IAM is looming large in the security calculations of industry, enterprise, government and even private individuals. In Section 1, we examine what IAM is, its various components and why it matters. The short answer is, as borne out by a raft of research, that it is not being addressed properly by most organizations, despite the evident serious consequences of failure to do so.

The obvious starting point is the pervasiveness of ICT, electronic networking and the Internet in supporting and enabling the functioning of many aspects of modern life in many societies around the world. With that comes a greater need to be able to identify and authenticate individuals accessing systems and resources, exchanging information or performing transactions.

The consequences of unauthorized accidental, malicious or criminal access to networks and resources can include serious disruption of operations, damage to corporate reputation or brand, major financial loss and, in the worst-case scenarios, potentially catastrophic impairment to a nation's ability to function normally.

At the same time, changes in the way that IT, networking and communications capabilities are provisioned and consumed are broadening the opportunities for IAM mechanisms and systems to be compromised. Notable here are the growing mobilization of the workforce, the developing phenomenon of people using their own mobile terminals and appliances in the workplace (the so-called practice of 'bring your own device', or BYOD), and the increase in the use of enterprise social networking – the report looks at their ramifications for IAM in Section 2.

In addition, the rise of what can be generally termed cloud computing adds further challenges, which are examined in Section 3.

Section 4 outlines how current approaches to IAM so often fail, which as is to be expected in such a complex and changing world, is often down to a combination of factors rather than inadequate technology.

In Chapter 5 we look at industry standards that can be deployed to address IAM issues.

Clearly, using improved and automated systems to reduce the risk of interference with operations, financial losses and damage to reputation isn't the only consideration driving IAM up the agenda of IT, networking and communications communities. Implementing better IAM capabilities holds the promise of enhancing enterprise IT efficiencies and quality, lowering operational expenditure (OpEx), and increasing workforce productivity through wider but controlled access to systems, resources and data. In the case of being able to grant wider, managed access to outsiders, such as self-service customers, there's the potential for enhanced customer relationships and satisfaction, and higher revenues.

Nor is better IAM just a 'nice-to-have'. In an increasing number of markets, enterprises and organizations now have to comply with legislation relating to privacy, confidentiality and data protection and retention, the adherence to which can be jeopardized should IAM systems be breached. To the list of consequences of compromised IAM can be added potentially heavy penalties for breach of statutory obligations.

Section 1

What is IAM and why is it important?

Identity and access management (IAM) is basically an activity that is concerned with the control of access to ICT systems, resources and assets that is accomplished by: allocating and authenticating the rights and attributes of individuals; enforcing the rules and policies that permit or deny access; and auditing, logging and reporting the activity of system users.

In this context, identity is the digital representation of data relating to a specific individual, whether they are an employee, partner, supplier or customer. Identity management is about setting up and controlling the roles and access entitlements of these individuals, with the ideal being to associate one digital identity with one individual. However, given that the needs and circumstances of users change – for example, following corporate acquisitions and mergers, staff reductions and changes in supplier or partner relationships, IAM systems need to be able to track identities, and modify, curtail and retire their privileges as appropriate.

IAM systems can have a number of attributes and components, some of which overlap or are subsets of others. Among the most common are:

- High-level policy-based management. This is software that uses rules or logic to control access to, and administer the use of, IT and network resources.
- Directory services. These handle the storage and management of critical data such as user profiles, accounts and passwords.
- Passwords and password management.
- Account and resource provisioning.
- Authentication. A set of technologies and mechanisms that are employed to establish whether users are who they claim to be.
- Authorization and access management. The processes by which it is established that users are authorized to undertake particular actions and are granted access.
- Access governance, or the granting of access in line with internal or external security requirements.
- Identity lifecycle management.
- Single Sign-On (SSO), by which a user performing a single action for authentication and authorization can access multiple systems. Single Sign-Off is the reverse process.

On the supply side there are vendors who offer what are designed as full suite IAM solutions, along with a larger number of other vendors who offer point systems that address one or more specific aspects of the IAM requirement. Some IAM suppliers, including IBM, Oracle and Microsoft, are 'household' names, active in multiple IT sectors. Others, including CA Technologies, Courion Corporation and RSA, are less well known outside of the IAM industry and tend to emphasize particular competencies. Among them, respectively, for these three companies are: content-aware IAM (or control of usage as well as access); access governance; and authentication. There are also

> *"Identity is the digital representation of data relating to a specific individual, whether they are an employee, partner, supplier or customer. Identity management is about setting up and controlling the roles and access entitlements of these individuals."*

system integrators offering 'mix and match' solutions. Meanwhile, a growing trend is for the provision of IAM solutions from the cloud on an on-demand, subscription basis. This particular business model has its attractions and its challenges (see Section 3).

In any event, all such vendors are targeting a significant global IAM market opportunity that, according to a forecast from analysts at market intelligence company TechNavio, will grow at a compound annual growth rate (CAGR) of 8.2 percent over the period 2011 to 2015.

Why should we care?

As indicated previously there are a number of reasons why demand for better IAM capabilities is on the rise. Beefing up IAM defenses to avoid major financial loss is a particular incentive here. For obvious reasons, enterprises and organizations that have been damaged by a compromised IAM system aren't that ready to publicize the fact or quantify the damage. However, it has been widely reported that weakness in the IAM systems of Société Générale may have contributed to that institution's loss of around $7 billion through the actions of a rogue trader in 2007/2008.

Privileged Access Management Report: Survey Results and Best Practices is a recent research report sponsored by access management software specialist FoxT and carried out by information security research company Echelon One. This includes the statement that:

"As enterprise breaches become more sophisticated, the potential for successful compromises by insiders, rival corporations, and governments increases without proper server access controls in place. Failing to secure contextual authentication and authorization to critical data, and control elevation to privileged accounts without sharing passwords, can easily result in scenarios where rival corporations are able to access product development plans, patents, and engineering data and win the race to a competitive market offering. The ramifications of these scenarios pose huge financial threats to the enterprise in the near and short term once intellectual property is compromised."

"The threats organizations face continue to become more aggressive and expose them to a range of losses from intellectual property, customer lists, strategic plans and trade secrets," says Bob West, CEO and founder of Echelon One. "Failing to control access to mission critical servers and data creates both economic and national defense issues we need to address immediately."

While it may be difficult to accurately quantify the overall dollars or other associated damage costs to organizations that result from compromised IAM, a recent HP survey carried out by the Ponemon Institute furnishes some insight into the scale of the opportunity for unauthorized or unintended activity that lax

"There are a number of reasons why demand for better identity and access management capabilities is on the rise. Beefing up identity and access management defenses to avoid major financial loss is a particular incentive."

Better access policy management will help improve core security monitoring

IAM mechanisms provide. *The Insecurity of Privileged Users* study focused on more than 5,000 IT operations and security managers across Australia, Brazil, France, Germany, Hong Kong, India, Italy, Japan, Korea, Singapore, Spain, the U.K. and the U.S. It found that:

- Some 52 percent of respondents indicated that they are at least likely to be provided with access to restricted, confidential information beyond the requirements of their positions.
- More than 60 percent reported that privileged users access sensitive or confidential data out of curiosity, not job function.
- Customer information and general business data were at the highest risk, and the most threatened applications included mobile, social media and business unit specific applications.

According to HP/Ponemon, many respondents claimed to have well-defined policies for individuals with privileged access rights to specific IT systems. However, almost 40 percent were unsure about enterprise-wide visibility into specific rights, or whether those with privileged access rights met compliance policies.

The study also looked at how organizations attempt to maintain control over the IAM issue in different ways. Twenty-seven percent said their organizations use technology-based identity and access controls to detect the sharing of system administration access rights or root-level access rights by privileged users, and 24 percent said they combine technology with process. However, 15 percent admitted access is not really controlled and 11 percent said they were unable to detect sharing of access rights.

“This study spotlights risks that organizations don’t view with the same tenacity as critical patches, perimeter defense and other security issues, yet it represents a major access point to sensitive information,” comments Tom Reilly, Vice President and General Manager, Enterprise Security Products, HP. “The results clearly emphasize the need for better access policy management, as well as advanced security intelligence solutions, such as identity and privileged user context, to improve core security monitoring.”

> *“Almost 40 percent of respondents were unsure about enterprise-wide visibility into specific rights, or whether those with privileged access rights met compliance policies.”*

Section 2

New technologies and working practices muddy identity and access management waters: enterprise mobility, bring-your-own-device and social networking

Today the IAM landscape is being significantly impacted by changes in the way that IT, networking and communications capabilities are provisioned, procured and consumed. In the process, the role of IAM has become more critical.

One trend much in evidence in recent years is the mobilization of the workforce. From relatively modest beginnings that had managers and employees making use of their mobile phones for voice applications, email and calendaring, the service remit of enterprise mobility systems has expanded dramatically, and the numbers of people that can be classified as being part of the mobile workforce has rocketed.

The repertoire of present-day enterprise mobility systems can encompass voice, data, email and applications unified on a single terminal, with enterprise access and data automatically and seamlessly made available via the most appropriate network or terminal. Some proponents see a partnering role for the fixed network in an enterprise version of fixed-mobile convergence (FMC), while others add to the mix Voice over IP, mobile Internet access and Web 2.0 tools such as blogs, wikis and social networking. Then there are applications such as asset tracking, field force automation, enterprise resource planning and customer relationship management.

In terms of the numbers of people involved, the updated *Worldwide Mobile Worker Population 2011-2015 Forecast*, a 2012 analysis from IDC, estimates the world's mobile worker population will reach 1.3 billion by 2015: this represents 37.2 percent of the total workforce. IDC believes the most significant gains will be in the emerging economies of Asia-Pacific thanks to continued, strong economic growth. The Americas will experience a slower growth rate due to a protracted economic recovery and high rates of unemployment.

"Despite recent market turmoil, mobility continues to be a critical part of the global workforce and we expect to see healthy growth in the number of mobile workers," says Stacy Crook, Senior Research Analyst for IDC's Mobile Enterprise Research program. "Our forecast shows that the worldwide mobile worker population will increase from just over 1 billion in 2010 to more than 1.3 billion by 2015."

The bring-your-own-device (BYOD) phenomenon can be considered as a further development of enterprise mobility. BYOD, which is the practice of people bringing their own consumer mobile devices to use at work rather than relying on what the company IT department supplies, is gaining considerable traction in some geographies. The U.S. and Asia-Pacific are two such.

In May 2012 Cisco Networks announced findings from the *Cisco IBSG Horizons Study* of 600 U.S. IT and business leaders. This found most organizations were enabling BYOD in the enterprise, with a very sizeable 95 percent of respondents saying their organizations permit employee-owned devices in some way in the workplace. This study also concluded that the average number of connected devices per knowledge worker was expected to reach 3.3 by 2014, up from an average of 2.8 in 2012.

In the same month British service provider

Enterprise social networking looks set for significant growth, especially among larger organizations

BT released findings from BT-commissioned research into attitudes towards BYOD, interviewing 2,000 IT users and IT managers in 11 countries. This analysis suggested that Asian IT managers are the world's most bullish on the benefits of BYOD. While 80 percent of IT professionals worldwide thought that enterprises with a BYOD policy hold a competitive advantage, that number rises to more than 90 percent in China, India and Singapore. When it came to implementing BYOD, 96 percent of Chinese, 91 percent of Singaporean and 86 percent of Indian IT managers said their organizations had, or will have done so in the next two years, well above the global average of 81 percent.

Social networking is another new activity being enthusiastically embraced by many enterprises and organizations. As noted by the authors of The Radicati Group's 2011 analysis *Social Networking Market, 2011-2015*, social networking services are used both by consumers and businesses to build communities and interact with their contacts through textual communication, media content sharing and collaborative features.

In the case of enterprise social networking, The Radicati Group points out that there are both internal business-to-business (B2B) and customer-facing business-to-consumer (B2C) collaboration communities. The first variety allows users "…to interact, share content and collaborate on projects through features like shared blogs, wikis, document sharing and group management". The second involves "…social interaction between businesses and customers, allowing customers to join in on business-related conversations and interact with business representatives".

Enterprise social networking looks set for significant growth, perhaps especially among larger organizations. According to Gartner Inc., fewer than 30 percent of large organizations will block employee access to social media sites by 2014, compared with 50 percent in 2010. Gartner also calculates that the number of organizations blocking access to all social media is dropping by around 10 percent a year.

"Even in those organizations that block all access to social media, blocks tend not to be complete," observes Andrew Walls, Research Vice President at Gartner. "Certain departments and processes, such as marketing, require access to external social media, and employees can circumvent blocks by using personal devices such as smartphones."

The pros…

The benefits of generally mobilizing the enterprise are numerous. Comprehensively mobilizing enterprises holds out the prospect of simultaneously reducing costs, increasing productivity, making better use of 'dead' spots in time, improving responsiveness and customer service, and achieving a better balance between work and leisure time.

The potential advantages of BYOD are also readily understood. Inter alia the BT-commissioned survey referenced above indicated that:

- Over 80 percent of IT managers think that enterprises with a BYOD policy hold a competitive advantage over other organizations.
- 64 percent of IT managers think that having a BYOD policy will enable employees to be more productive.
- 48 percent think it will also allow employees to work more flexibly.
- 47 percent think it will enable employees to serve customers better.
- This sentiment is shared by employees – 42 percent of employees using their own device for work believe that they are more efficient and productive as a result.

Added to the foregoing, even if subsidizing the use of employee-owned consumer devices, there's the possibility of employers saving money. Technology refresh-wise, consumers may be willing and able to replace their mobile phones or tablets at a quicker rate than their employer can afford to. Then there's the prospect of greater employee satisfaction.

In principle, enterprise social networking can likewise be a powerful force for corporate good.

The use of internal B2B platforms can enhance employee productivity, speed up decision-making and usefully flatten management hierarchies. In the background is the notion that social networking simultaneously empowers the individual and yet promotes greater corporate cohesion.

Again, the use of enterprise B2C platforms can strengthen customer engagement, improve brand promotion and tap into the strengths of personal and group recommendations that social networking can facilitate. In the Global Trust in Advertising Survey announced by Nielsen in April 2012, 92 percent of consumers around the world said they trust 'earned media', such as word-of-mouth and recommendations from friends and family, above all other forms of advertising. The same survey suggested that 58 percent of online consumers trust 'owned media', such as messages on company websites, and sponsored ads on social networking sites were deemed credible by 36 percent of respondents.

The cons...

As you might anticipate, though, the benefits outlined above come with a potentially hefty price tag. The phenomena of enterprise mobility, BYOD and enterprise social networking all raise issues of security that have implications for the IAM industry.

In the case of enterprise mobility, a security vulnerability clearly arises from the circumstance that sensitive corporate and personal data can be held on devices or removable storage media that can be stolen or lost. In part this has driven the expansion of a mobile device management (MDM) market that business information provider Visiongain believes could be valued at over $3.54 billion by 2016, with the greatest growth accounted for by the enterprise segment, which could be worth $2 billion.

Added to this, though, misplaced or misappropriated devices that fall into unauthorized hands could be used to access additional data and applications on enterprise networks. Concern to avoid such an eventuality has helped stimulate the development of a mobile IAM (mIAM) sector. One player in that sector is IBM, with the IT giant proposing mIAM as part of a three-part solution it calls 'Mobile Security Intelligence'. IBM's mIAM offering is one element of Data, Network & Access Security, with the two other components of the overall IBM system being Mobile Device Management and App Dev & Test.

IBM's account of mIAM is as follows:

"Mobile Identity and Access Management (mIAM) solutions are employed to authenticate and authorize users and their devices. In a mobile environment the identity of the user as well as the device needs to be verified. Access to enterprise systems needs to be guarded to avoid unauthorized access to enterprise data or applications. As mobile devices are multi-purpose devices that are often shared, with most mobile apps connected to back-end systems to deliver content or functionality, a solid mIAM solution is a must-have for any enterprise that is serious about their overall security posture."

If anything, BYOD further complicates the IAM challenge. IT departments may not always have full oversight of which individuals are using which terminals. Where there is a mixture of employee- and company-provided devices, different levels of access and entitlement may need to be set up for each type. Different devices may also have different degrees of vulnerability to nuisance, malicious or criminal cyber activity.

Accordingly, despite the benefits suggested by the BT survey instanced above, BYOD makes IT managers nervous. BT says only

The trend toward a bring-your-own-device enterprise is creating new concerns for IT managers

one in 10 think that all BYOD users recognize the risks and less than one in five believe all users understand the access/permissions related to their mobile devices. It appears IT managers are nervous with some justification. Of employees who use their own device for work, one in three sees "no risk" in using their own device in a work context, and just a quarter recognize the significant risk they pose to company security.

Also in May 2012, Juniper Networks released results from its first-annual Trusted Mobility Index. Among the findings of this study was the somewhat alarming statistic that the trend toward a BYOD enterprise is creating new concerns for IT managers, with nearly half of all respondents using their personal device for work (41 percent) without permission from their company.

"BYOD environments are increasingly becoming the norm for many enterprises and an important enabler of employee productivity and improved user experience. However, one of the barriers to adoption is the lack of confidence that IT can eliminate the potential risks of unauthorized access and security breaches," summed up Chris Crowell, President and CEO, Enterasys Networks, on the occasion of that company's launch of its Mobile Identity and Access Manager. Among other things, the Enterasys system is designed to provide device-, user- and location-specific network and application access, granular enforcement of policies based on user and device profiles, and automation of policy and provisioning capabilities.

The growing adoption of enterprise social networking is likewise adding to the IAM load although, in the view of Gartner, such activity can actually be used to improve IAM practices and capabilities. The research firm argues that identity data and social media platforms can expose organizations and users to a wide variety of security threats, but organizations can also use this identity data to improve support for their own IAM practices and the ambitions of business stakeholders.

Gartner has identified three significant impacts of social media on IAM:

- Personal trust misaligned with corporate trust. Employees who participate in online social media continually make judgments about the degree of trust they should place in the platforms and in other participants, and they adjust content, structure and vocabulary to match their risk assessments. These assessments and the fundamental inputs to their assessment process may not align with corporate expectations for risk management. As a result, employees may say and do things on social media platforms that violate corporate policy or are otherwise counter to corporate expectations.
- Public content supports identity intelligence. The collection of identity data by public social media on a massive scale enables improvements in the production of identity intelligence. This pushes IAM programs to discover the user profiles accessed by staff and to maintain capabilities for accessing external services in order to harvest identity data.
- Identity data can be leveraged for IAM. Social media provide a mechanism for verifying the identity of employees, job candidates and customers, and a cloud identity platform for performing IAM for other applications. IAM programs can use social media for identity verification and to extend identity services to internal and external applications via a semi-trusted social platform.

"Organizations need now to turn their attention to the impacts of social media on identity and access management," concludes Walls.

Section 3

The cloud and its implications

Web-based cloud computing, in which software, applications and processing power are accessed and bought in on an as-needed subscription basis, is proving a big hit with government agencies and commercial enterprises of varying sizes. One often cited estimate, from Forrester Research, predicts a market worth over $241 billion in 2020, up from $40.7 billion in 2010.

In principle the cloud brings a number of benefits to users, including lower capital expenditure (CapEx) and operational expenditure (OpEx), shorter implementation timelines, open-ended system scalability, and ready access to specialist expertise and technology refresh.

There are, however, non-trivial concerns about cloud security that stem from a weakening of the end-user organization's control of access, the sharing of resources with other, sometimes unknown, parties, and the disconnect between in-house hardware and off-site applications. It's worth noting, though, that public cloud computing has the potential to improve the general security posture and capabilities of some organizations. Smaller ones, in particular, can profit from access to better skill sets and more advanced technologies than their in-house provision might otherwise cost-justify.

In the context of IAM, the cloud is something of a mixed blessing.

On the one hand, the attraction for end-user organizations is that cloud-based IAM can save time and money, improve security and reduce risk. This can be achieved through:

- lower CapEx and OpEx, equaling lower total cost of ownership (TCO);
- shorter system implementation times;
- transfer of responsibility for maintenance, support, trouble shooting and technology updates;
- access to a wider pool of expertise, both technical and regulatory.

On the other hand, in the case of the public cloud and the shared community cloud, there's the rider that access control is often now at one remove from the end-user organization. As a number of observers have pointed out, it's unlikely that most businesses and other organizations would be willing or able to locate and operate access solutions at the cloud service provider's premises.

As such the cloud presents IT departments with an access dilemma, acknowledges Centrify Corporation, a company whose identity and access management products are designed to enable organizations to control, secure and audit access to cross-platform systems and applications using Active Directory.

"The cloud brings a number of benefits to users, including lower capital and operational expenditure, shorter implementation timelines, open-ended system scalability, and ready access to specialist expertise and technology refresh."

"Many organizations are facing a Catch-22 when it comes to migrating applications to the cloud. They get the biggest ROI by moving business-critical apps that need to scale rapidly and on-demand," reasons David McNeely, Director of Project Management, Centrify. "But these are precisely the applications that need the tightest security and access controls."

But Catch-22 or not, cloud-based IAM is set to grow in popularity if the findings of a recent survey by Courion are on the money. This survey canvassed more than 400 companies worldwide and found that 64 percent were using cloud-based applications to achieve cost and efficiency advantages. It also indicated a big opportunity for IAM vendors offering alternatives to traditional implementation methods.

More than 50 percent of respondents handled IAM manually and 70 percent identified benefits of IAM in the cloud as including: improved speed of business operations; usability; cost; and access risk management. Courion believes this suggests that companies that provide alternatives to overcome the long implementation cycles and high costs associated with traditional IAM deployments are positioned to make inroads into a growing market.

Additionally, with more than 80 percent of respondents allowing access via mobile devices, there was significant opportunity to improve IAM operations as enterprises become more open and potentially exposed to greater access risk.

Again, according to a Gartner estimate referenced by cloud security company Symplified, IAM as a service (IAMaas) will account for 20 percent of all new IAM sales by the end of 2012, compared with less than 5 percent in 2011.

"With more than 80 percent of respondents allowing access via mobile devices, there was significant opportunity to improve identity and access management operations as enterprises become more open and potentially exposed to greater access risk."

Section 4

Why existing identity and access management systems can fail

There are many reasons suggested for why and how IAM systems can fail to achieve the objectives sought by their architects, operators and owners. Perhaps surprisingly, given the complexity of the tasks involved, few commentators believe technology weaknesses are the main causes of IAM failures. Rather, in the view of many, lack of success boils down to planning, process and people shortcomings. Among what might be termed the high-level candidates here are:

- inadequate investment commitment to the project;
- failure to align IAM technical requirements and capabilities with overall business objectives and goals;
- poor project management and the absence of clarity about what the solution is meant to achieve;
- lack of integration with other IT systems and organizational processes;
- difficulty of getting different departments with different agendas singing from the same song sheet;
- insufficient IT skills and competencies to manage the considerable customization effort often required when large organizations try to implement comprehensive IAM solutions.

At a lower level, the HP/Ponemon analysis cited earlier offered a number of observations about some specific privileged user challenges facing organizations implementing IAM systems. These included:

- top barriers to enforcing privileged user access rights are the inability to keep pace with change requests, inconsistent approval processes, high costs of monitoring and difficulty in validating access changes;
- areas for improvement include monitoring privileged users' access when entering root-level administrative activity, identifying policy violations and enforcing policies across an entire organization;
- nearly 80 percent of respondents reported that deploying a security information and event management (SIEM) solution was critical to governing, managing and controlling privileged user access rights.

Interestingly, based on the responses, the study suggested that the potential for privileged access abuse varies from country to country, with France, Hong Kong and Italy having the greatest potential, and Germany, Japan and Singapore having the least.

Some specific shortcomings in existing arrangements were also identified in the FoxT/Echelon One survey, notably the absence of automation, the inability to centralize operations, and the lack of enforcement mechanisms. The findings and commentaries of that survey of 327 information security professionals include:

- Manual enforcement of privileged-user access and passwords remains prevalent among 37 percent of enterprises polled: Failure to automate access-management controls results in the sharing of privileged passwords. Once passwords are shared across multiple accounts users begin taking administrative shortcuts, enterprises are unable to track actions back to a specific user. Manual enforcement of privileged-user access represents an opportunity for data compromise and is the number-one compliance risk.

- Potential for insider fraud is widespread, with 76 percent of respondents unable to automatically administer user accounts across multiple servers: Potential for access creep emerges when enterprises cannot automatically administer user accounts across the entirety of their server farm. Access creep results when employees accrue unmanaged access rights throughout their careers at an organization, resulting in more privilege than is established by their positions. Without central consoles that can administer user accounts across multiple servers, IT is unable to manually administer each individual user account within the organization due to a lack of available resources and staff.
- 73 percent of respondents reported that they are unable to centrally define the access rules and policies necessary to map access to employee role: Enterprises that are unable to centrally define rules and policies create the opportunity for user-access controls to change from server to server, enabling data compromise and accelerating the operational costs of manual enforcement.
- Enterprises lack the critical infrastructure to enforce server access: 42 percent of those surveyed are unable to implement multi-factor authentication, and 37 percent are not able to define and enforce granular authorization rules: The inability to automatically authorize and enforce who can access which servers, and even what commands they can execute based on the context of the request, leaves enterprises open to the risk of a data breach.

“The inability to automatically authorize and enforce who can access which servers, and even what commands they can execute based on the context of the request, leaves enterprises open to the risk of a data breach.”

Section 5

Standards key to improved identity and access management

As well as improvements in areas such as those suggested by the HP/Ponemon and FoxT/Echelon One analyses, it's generally recognized that better standardization of the various aspects of IAM would pay dividends in the form of lower total cost system ownership, faster ROI and reduced implementation lead times.

Standardized management system models, interfaces and best practices in particular are key to achieving many of the objectives of the IAM community. Unlike proprietary solutions, standardized approaches can be replicated, recycled and reconfigured to meet evolving needs without major reworking and re-engineering for each new project.

A number of standards are commonly used in the IAM industry. Among them are:

Lightweight Directory Access Protocol (LDAP), originated at the University of Michigan. Hitachi ID Systems defines LDAP as follows: "It is a network protocol, based on TCP, with optional support for SSL Encryption, that is used to access a hierarchical directory of information on a directory server. LDAP is considered to be lightweight because it is based on a simplified version of X.500 directories."

The IETF's Web Authorization protocol (OAuth). One of the definitions provided by the OAuth community is: "OAuth provides a method for users to grant third-party access to their resources without sharing their passwords. It also provides a way to grant limited access (in scope, duration, etc)."

Security Assertion Markup Language (SAML) developed by the Organization for the Advancement of Structured Information Standards (OASIS). OASIS has defined SAML as follows: "SAML is an XML-based framework for communicating user authentication, entitlement and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application."

Another OASIS development, eXtensible Access Control Markup Language (XACML), is described by that organization as follows: "In a nutshell, XACML is a general-purpose access control policy language. This means that it provides a syntax (defined in XML) for managing access to resources."

TM Forum's Frameworx suite of standards (see page 18) provide the blueprint for effective business operations. The suite has been developed by the Forum's unique online Collaboration Community and is constantly refined and extended to meet new and changing needs. A number of the specifications and models the Forum initially developed for the service provider industry have wider applicability in the context of improving IAM for enterprises and other organizations in general. This is not that surprising, as many of the IAM concerns and requirements of service providers are identical to those of enterprises and institutions operating in different sectors.

The requirement to have to work with diverse legacy IT systems and processes, the diversity of which may proliferate following acquisitions and mergers, along with the switch from a single-entity 'closed' business model to a federated, supply chain model, is shared by both service providers and other types of businesses.

Following privatization and market liberalization, many network operators and service providers have merged or been bought out by others. Networks are now more and

TM Forum has identified the need for a standardized and centralized provisioning and auditing mechanism for users

more assembled using solutions sourced from multiple suppliers. At the same time, where there was once end-to-end ownership of all components of service, today it's common to find that there is a multi-tenanted delivery chain and that the service itself can be the product of collaboration between infrastructure, content and merchant parties, and even involve end user input. With all this has come greater need for, and reliance on, IAM.

Multi-vendor communications and mobile networks in a typical service provider environment are now managed using multiple proprietary user management systems (UMSs) supplied by operational support system (OSS) companies. In order to move towards a more secure, consistent and efficient management of network components, TM Forum has identified the need for a standardized and centralized provisioning and auditing mechanism for users – in this instance operator personnel – and their entitlements, working on these management systems. Added to this is a requirement for individual service providers to be able to implement specific authorizations based on local situations.

In pursuit of these objectives, the Forum established the Enterprise Identity Management (EIM) team as part of the TM Forum Interface Program (the work of the Interface Program feeds directly into the Integration Framework, a key element of Frameworx). Members of this team are concerned with the security aspects of network management, and are responsible for the definition and implementation of the interface between the Central User Management System (UMS-C), from which a service provider can provision access rights and authorities, and multiple Local User Management Systems (UMS-L), which actually implement the access rights and authorities.

In particular the EIM team is working on the deliverables for Telecom OSS Operator User Management and for Single Sign-On/Off.

Telecom OSS Operator User Management Release 1.0, or TMF615, specifies an interface by which it is made possible for service providers to consistently provision access rights and authorities across the system for operator users. It also deals with auditing the results of the provisioning operations.

The first commercial implementation of TMF615 deployed in a multi-supplier OSS environment involved Vodafone D2, Ericsson and IBM. In this case study two possibilities were examined – the implementation of TMF615 directly in the Ericsson OSS and, for other systems not yet supporting the standard, the creation of a trouble ticket via JSR91 TM Forum Interface Program Trouble Ticket Interface to support the manual procedure for user provisioning. For more details of this pioneering work, please see page 29 of the *TM Forum Case Study Handbook 2011*, which is free for all employees of TM Forum's member companies to access from www.tmforum.org/CaseStudyHandbook11 once they've registered on our website.

Supported user operations of TMF615 were: create, modify, delete and audit. The translator to JSR91 included a database to simulate online resources and storage of the ticket status.

Some impressive results were recorded. The implementation of TMF615 in the Ericsson OSS application reduced provisioning time by 79.2 percent. The participants calculate that where all OSS applications support TMF615, the overall provisioning time will be reduced by about 98.4 percent and the time for a detailed

What is TM Forum Frameworx and how can it help you?

TM Forum's Frameworx suite of standards provides the blueprint for effective business operations, enabling you to assess and improve performance by using a proven, service-oriented approach (SOA) to operations and integration. It has been adopted by 90 percent of the world's largest service providers – and its take-up is accelerating as service providers recognize it is core to their business. Frameworx helps you:

- Understand your customer through a common customer management information model
- Innovate and reduce time-to-market with streamlined, end-to-end service management
- Cut operating costs by enabling highly efficient, automated, industry standard operations
- Reduce integration costs and risk through standardized interfaces and a common information model
- Lower the risks of transformation by delivering a proven blueprint for your business
- Gain independence and confidence in procurement through conformance certification and procurement guides
- Gain clarity by providing a common, standard language
- Build essential partnerships quickly and easily through common processes, information and terminology.

The suite was developed in the Forum's unique Collaboration Community and continues to evolve through the efforts of the Community to meet changing market needs. It is driven by service providers and available exclusively to members, who represent more than 90 percent of the world's communications subscribers.

Frameworx is made up of four components:

Business Process Framework (eTOM)
The Business Process Framework provides efficient, clear and effective business processes that are critical to delivering innovative services quickly, at the least possible cost. It offers a comprehensive, multi-layered view of these processes and is aligned with ITIL. It is supported by off-the-shelf tools to provide a multi-dimensional catalog of the business processes and includes guidelines and process flows ensuring your processes are streamlined and effective across the enterprise and across partners in a value-chain.

Information Framework (SID)
The end-to-end management of service demands the consistent use of data across an enterprise. The Information Framework provides a comprehensive, industry-agreed definition of the information that flows through an enterprise and between service providers and their business partners. It is supported by off-the-shelf tools and provides a common information model, enabling the definition of standardized integration points.

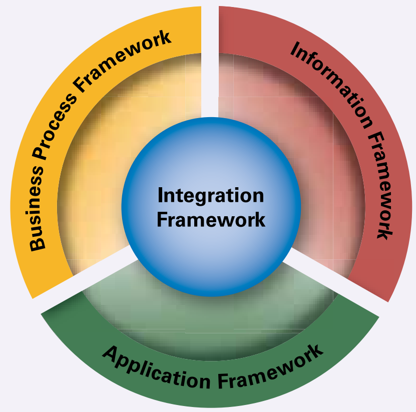
The Application Framework (TAM)
Understanding how your business processes are implemented in your software architecture is essential. This Framework provides a model for grouping processes and their associated information into recognizable applications. It provides a common language and identification between buyer and supplier for all application areas.

It helps in the design of enterprise architecture through a better understanding of your systems architecture plotted against a standardized map.

The Integration Framework
Automation of business processes enables you to significantly reduce costs and rapidly deploy new services. But automation requires interoperability between systems across the entire enterprise and an extended value-chain of partners. The Integration Framework defines how the processes and information behind these systems can be automated by

Available on the App Store

Search and navigate Frameworx with the free iPhone/iPad app



defining standardized Service Oriented Architecture (SOA)-based interfaces. The Integration Framework includes:

- A taxonomy for services and guidelines for the development of Business Services.
- Model driven tooling for the machine assisted production of standard interfaces.
- A repository of Business Services.

Business Metrics
Understanding the performance of your business is a critical aspect of managing transformation. Knowing how you compare to the industry in key operational areas will guide your transformation investment. TM Forum's Business Metrics, mapped to the Business Process Framework, provide a way for you to measure success based on a balanced scorecard that covers:

- Revenue and margin: a view of fiscal performance.
- Customer experience: measures that impact the end-customer's reaction to the service offering.
- Operational efficiency: a view of cost and expense drivers.

Latest release – Frameworx 12
Frameworx 12 has seen the largest number of updates to the Business Process Framework, with over 800 new processes added, especially for billing, charging, policy management, fraud management and value chain management. Other new additions include:

New security capabilities to provide defense-grade security to commercial networks
Frameworx 12 includes three new security user stories that address denial of service attacks, penetration attacks and application misuse. These user stories were mapped in to the Business Process Framework to create new security processes in five areas that serve as a blueprint for organizations to use in establishing their security practices for network defense.

Software Enabled Services
The Software Enabled Services features in Frameworx provide a set of building blocks to enable standards-driven, model-based software solutions. This facilitates development of Frameworx-compliant IT solutions focused on agile service delivery. Benefits will include a rapid time to market for new services and the ability to manage the complete lifecycle in an SOA.

Cloud Service Level Agreement Handbook
Based on requirements from the Enterprise Cloud Leadership Council, this guides service providers on the expectations from their enterprise customers on service level agreements (SLAs). It provides guidelines to ensure your SLA is commercially viable for cloud and may be used by the enterprise to measure the worth of an SLA offered by a vendor of enterprise cloud services, or by the service provider to ensure that the SLA the service provider they are offering is enterprise-grade. It will be free for TM Forum members to download from our website.

New Quick Start Pack for Fulfillment
This accelerates the ability to streamline fulfillment processes for product and service delivery. It provides a common language for working with partners for delivering services, saving time in defining business interfaces, as well as enabling rapid deployment of new services through well-documented processes and a common language.

Customer Experience Handbook
An overview of Customer Experience Management (CEM) in the industry and a summary of TM Forum work to date that is applicable to CEM. It provides recommendations for service providers on how to develop a roadmap for CEM, how to measure and manage customer experience, and provides recommendations to TM Forum and the industry for future direction in development of standards and best practices.

Model Federation Enablers
Designed to allow the Information Framework (SID) to model any kind of resource, including those where the detail of the resource is defined by someone else. In addition, the interface development tooling in Frameworx generates basic interface capability utilizing the Information Framework. As a result the federation capability of the Information Framework will also by implication allow Frameworx interfaces to provide high level management functionality for any kind of resource.

reconciliation of all user data will be reduced by 98.8 percent. The participants also noted that TMF615 facilitates daily auditing with ease.

Meantime, using a translation to JSR91 *TM Forum Interface Program Trouble Ticket API*, the provisioning workflow for all OSS applications was able to be set up completely independently from the support of TMF615. This reduced the user lifecycle audit time by 98.1 percent.

In summary

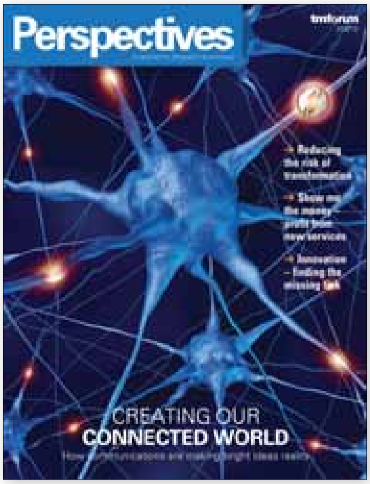
Greater use of standards will help combat issues around IAM, which as we've seen are growing daily in importance. However, using improved and automated systems to reduce the risk of interference with operations, financial losses and damage to reputation isn't the only consideration driving IAM up the agenda of IT, networking and communications communities.

Implementing better IAM capabilities holds the promise of enhancing enterprise IT efficiencies and quality, lowering operational expenditure (OpEx), and increasing workforce productivity through wider but controlled access to systems, resources and data. In the case of being able to grant wider, managed access to outsiders, such as self-service customers, there's the potential for enhanced customer relationships and satisfaction, and higher revenues.

Better IAM is not just a 'nice-to-have'. In an increasing number of markets, enterprises and organizations now have to comply with legislation relating to privacy, confidentiality and data protection and retention the adherence to which can be jeopardized should IAM systems be breached. To the list of consequences of compromised IAM can be added potentially heavy penalties for breach of statutory obligations.

Have you seen our other recent TM Forum publications?

TM Forum's research reports are free to all employees of our member companies and can be downloaded from our website once they've registered. The reports are also available for non-members to purchase online.

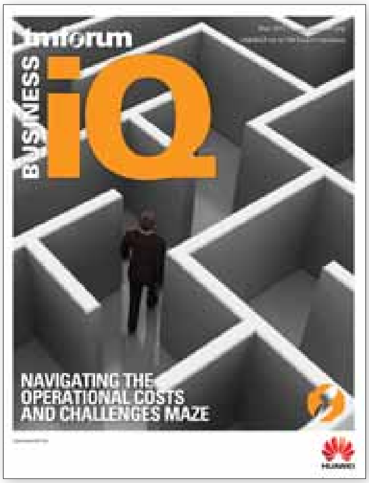


Perspectives 2012

Perspectives is TM Forum's annual publication for senior professionals in the world of digital services.

The theme of this year's edition is our industry's progress to a fully connected digital world. The digital world will impact every business sector on the planet with new business models and markets, which will bring major threats to those who fail to seize the opportunities the digital economy brings. In order to make the most of these opportunities, companies need to be smart and move fast.

With access to some of the industry's leading lights and most sought after journalists and analysts, if you are part of the communications or related industries, whether you sit in the boardroom or stand by the water cooler, make sure that you read *Perspectives 2012*.

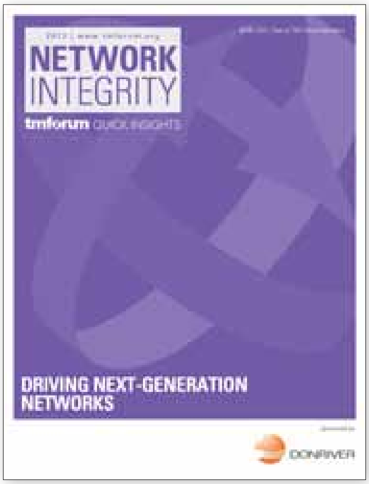


Business IQ:
Navigating the operational costs and challenges maze

TM Forum's *Business IQ* explores the business transformation issues facing our industry right now. Standardized, reusable, recyclable processes and flexible systems and platforms are the key to being able to embrace new business models, launch new services fast and open up new revenue streams.

In this issue, we look at the main aspects of operational costs and challenges. We explore some of the highlights of TM Forum's groundbreaking Operational Cost Model Survey Report, interview industry visionary Dr. Hossein Eslambolchi, and show how TM Forum's Frameworx suite of standards has helped Vodafone D2 blaze the transformation trail.

Also, our select virtual panel of experts discusses cross-industry IT trends and explores how service providers' operational expenditure profile is changing.



Network integrity: Driving next-generation networks

Network data is among the most important information a service provider holds. Its careful management is key to remaining competitive and profitable. Driven by market pressures and new business opportunities, service providers around the world are pushing to rollout new networks, promising greater flexibility while containing costs. Although service providers might incorporate a number of best practices into the deployment effort of these new elements, serious differences in both administrative and operational data can occur.

This *Quick Insights* report introduces the concept of network data integrity. We look at ways to improve data integrity for new and in-service networks, using a combination of managed access control, inventory discovery and reconciliation, and automated audit capabilities across the network lifecycle. We also include some interesting case studies that show the scope for problems with new network deployment, even in an environment utilizing best manual practices.

Visit **www.tmforum.org/researchandpublications** to find out more