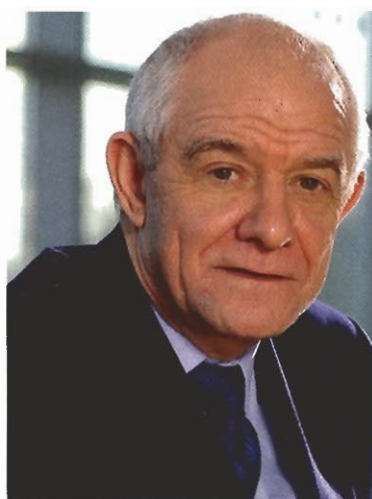




ON THE SPOT IAM



“IAM is not dead in the water, but it is on life support.”

AMIR LUBASHEVSKY, MAGIX
INTEGRATION

IN THIS MONTH'S ON THE SPOT FEATURE, WE ASKED WHETHER IDENTITY AND ACCESS MANAGEMENT (IAM) IS DEAD IN THE WATER OR TAKING OFF? words by **SAMANTHA PERRY**

(From top down) Mike Small, CA Africa; Amir Lubashevsky, Magix Integration; Lewis Taljaard, Novell.



Identity and access management (IAM) has hit the headlines over the past three years as companies battle to get to grips with corporate governance regulations, security concerns, an increasingly mobile workforce and blurring boundaries making

it difficult to determine who is inside or outside the business. You'd think IAM would be a no-brainer, but its complexity notwithstanding, it hasn't been implemented fast or furiously. *Brainstorm* wonders what's up with that?

□ IAM has a wide scope and has been around for a long time, so it's not dead or even just resting. IAM is a journey that organisations travel. And, as they travel, they move in a spiral where adoption of or improvements to one of the key components (authentication, authorisation, auditing and administration) reveals the need to improve another. Compliance and privacy have been recent drivers of demand for certification, attestation and privilege management. Trust is fundamental to commerce and knowing who you're dealing with is essential to trusted e-commerce. IAM is alive and evolving.

Mike Small, principal consultant for IAM at CA Africa

□ IAM is not dead in the water, but it's on life support. Anyone trying to purchase, implement or support IAM as a technology or a product is flogging a dead horse. The only way IAM can work in the real world is if it's integrated into, and forms a holistic part of, the business infrastructure. Furthermore, looking after only the identities of people within the business is just as unacceptable. Real identity management must also protect the data belonging to the broader community, such as customers and partners. IAM can never work as an isolated, standalone concept.

Amir Lubashevsky, director at Magix Integration

When considering IAM, clients find themselves in two minds as to whether it's dragging along or soaring ahead. While some of the early adopters had to pave the way for other companies to learn from their mistakes, the industry has matured over the past two to three years. IAM has demonstrated go-to-market value to corporates as well as tangible cost savings, not to mention many compliance benefits. The top IAM vendors already provide the next generation of IAM, with key aspects such as physical and logical integration, federation, real-time remediation and identity as a service.

Lewis Taljaard, business unit sales specialist at Novell

IAM is becoming a fundamental necessity. The IT world is expanding, exploding with new technologies at a very rapid pace. As our technology grows, so does the need to protect and manage larger numbers of users. The number of electronic identities has increased drastically and has reached a point where manually operated identity management falls short. Companies are increasingly looking to automate and accelerate the complex processes when provisioning new employees, and this trend will continue to fuel the adoption of IAM.

Suria Cronje, channel manager at Comstek

IAM deployments in large heterogeneous environments are complex and would be dead in the water for organisations that still believe IAM is about implementing technologies to counter poor organisation and process controls. IAM brings about



organisational and process changes that have far-reaching consequences in the extended enterprise. Due consideration must be given prior to deploying any solution. IAM failures have been tipping the scale over the past few years, but with the maturity of system integrators and IAM software vendors in this area, success rates are sure to pick up. Organisations that fall into the trap of rushing to deploy solutions, before understanding what business value is to be accrued, usually find themselves spending a fortune, with no way of justifying the spend once the kit is implemented.

Ugan Naidoo, managing consultant at Fujitsu Services SA



Organisations have a continued and growing need for a comprehensive IAM solution, to protect valuable IT assets from improper use and enable approved users to access applications and data while protecting these assets against unauthorised access. Managing user identities and their rights to access resources throughout the enterprise is critical to effective security management. Seems simple, but the solution needs to do this without interfering with productivity, while balancing the security risks with the cost of acquisition and management. It is possible to protect these assets and improve business productivity, to address enterprise security needs while improving user experience and reduce costs, while increasing efficiencies and supporting compliance.

Charles Senabulya, software group director at IBM sub-Saharan Africa

In a world filled with unmanageable risk, the need for an integrated, architected approach to information security has never been greater. Governments, companies and other institutions of all kinds need to be able to assert with 100 percent certainty that the information on which their daily activities depend is safe and secure. Identity and authentication are core components in information security. Without the ability to authenticate the identity of any and all users, there can be no comprehensive security. It's for this reason that The Open Group, the world's leading standards body, has created a workgroup focused specifically on identity management.

Stuart Macgregor, Real IRM CEO