Trip Report

Gartner Identity & Access Management Summit 2009

23 – 24 March 2009 | London, UK

Under the firm hands of Gartner Summit Chairs Ray Wagner and Ant Allan, over 300 attendees from across Europe were given the full breadth of latest knowledge and insight into IAM. The audience represented 28 countries and came from across all industry sectors with a particularly strong presence from financial services this year.

This Trip Report provides you with a snapshot of key thinking, essential discussion topics and core take-aways that you can consider now you have returned to the office.

Gartner Opening Keynote: Enabling Governance and Risk Management in an Age of Business Challenges

Earl Perkins, Research VP

We are entering an age of accountability that fundamentally changes how enterprises work. Organizations need accountability in terms of the access employees, partners, and customers have to sensitive systems and information – and to assure accountability. This is where IAM lives – supporting and assuring the required transparency enterprises will require.

IAM should be part of governance, risk and compliance management within the organization if we are to mitigate operational and reputational risk. Despite best intentions, IAM still needs to be a part of the policy-setting process, the creation of the appropriate frameworks and processes, even before addressing the issue of technology.

To 'sell' IAM to the organization the key is to speak in language they understand; risk-based IAM economics formalize reporting on the cost of failure and limiting exposure from bad decision-making, and to change a general awareness of the risks into specific actions. IAM reduces risk, improves efficiency, supports sourcing, austerity programs and allows the setting of robust baseline benchmarks. It allows a move from coarse-grained "awareness" of access toward a finely-grained, precise and contextualized knowledge.

As an appropriate decision cycle think of the 'seven Ps': Principles, policies, practices, processes, people, products, and production. Begin at the strategic level (principles) and translate it down to the operational level (production); start by setting the principles you wish to answer, set the policies for people and processes to execute, codify behaviours into actual practices, then control those practices with specific processes, assess your people in terms of the skill sets needed and the organizational needs, and finally consider the products (technology) you need and then production – what you actual create at the end of it.

Governance Risk and Compliance Management (GRCM) is entering mainstream use, but effective GRCM requires effective IAM. This increasing importance and alignment means enterprises are now participating in decisions…But means you can now capture more requirements, gain more support, and change the dialog within your organization.

Premier Mastermind Interviews: IAM in the Downturn: What is the Impact on End-User Organizations and Vendors?

Gartner Research VP, Ant Allan, discussed with **Bill Mann**, SVP Business Unit Strategy, Security Management at **CA** and **Mike Davies**, Director, Identity and Authentication Services at **Verisign** responses to the present downturn and how to protect IAM projects.

Ant: *Will organizations continue to invest in IAM as overall budgets are being cut back?*

Bill: Companies will continue to invest… security projects are going to be sold on the merits of business value and on reducing risk. If the project can't provide those answers then the project shouldn't take place. IAM is fundamentally about knowing and being able to audit who has access to what, where and when.

Ant: *Is this an argument management will pay attention to?*

Bill: In the past the mistake has been made that people have talked too much about the technology and not enough about the business risk. The link has to be made explicit and then technology feeds into safeguarding and defending against that reputational risk.

Ant: *Are there particular strategies that can improve communication of this message?*

Bill: Transparency and accountability are key. Management leading an IAM project need to ask what are your valuable assets? Where is your customer data? Have you defined roles and identities? They need to answer the basics not just run through a standard process.

Ant: *Within this climate where budgets are tighter and people are being asked to make changes…What should people consider for their overall IAM projects and challenges?*

Bill: You need to be transparent and you need to ask the right questions. Focus on things where you can achieve quick wins that can help you understand what you have inside your organization. Focus on protecting privileged users before getting into more complex elements. Show upper management that you have protected the organization against disaster.

Ant: *If you already have a project underway – and haven't focused on getting the principles right before purchasing the product…Could it be appropriate to freeze the project and concentrate on areas where quicker wins could be achieved?*

Bill: Ultimately if you can't demonstrate that you are providing value and reducing risk then you shouldn't proceed. Be pragmatic. If the project isn't on track then shelve it. Provisioning is a great example of an area where if you haven't exercised role management then it probably isn't going to track properly right now. Go do the role management piece then return to it.

Ant: *There's a still a lot of proprietary products and standards – there are few simple interfaces. Where's the driver for development?*

Mike: The demand has to come from end users. Things have developed this way because the standards have come about to solve a particular problem. It's a good ambition to federate and create links between different standards…but it's a difficult job and will happen bit-by-bit.

Ant: *Is this a good climate to embark on that kind of work?*

Mike: We've seen a lot of people pulling back from implementations; pulling back into core products and services, focusing on key customers. The point is that the contraction is done; it's time to look to the future. It's not that the 'green shoots' are here but they're starting. That could accelerate the work in this area.

Ant: *If organizations have had to scale things back and put things on the back burner, how do they ensure they are kept 'shovel-ready' so when the budget is back they can go ahead?*

Mike: The standards are so important. Having adopted a standard for one part of IAM the next time you need to implement something you already have the skills. You should use standards in a modular approach on each of project so you can implement quickly later on. It's easier to hire someone with the appropriate familiarity with a specific standard.

Ant: *Is it a good approach to take right now if you have to cut something? For organizations to favour projects that will give the best foundation for future development?*

Mike: As one of many factors involved, definitely, if you can use a project as a poster-child for how you could adopt technology in the future across many different projects, then yes.

Gartner Identity & Access Management Summit 2009

europe.gartner.com/iam

Guru Keynote: Optimizing Identity for the 21st Century

Baroness Susan Greenfield, one of the world's foremost experts on the human mind, explored the ways in which identity may be shifting under the impact of 21st Century living.

She pointed out how the essence of human identity is a feature of the physical brain, but is not just being dictated by the genes. Nurture can in fact trump nature.

Experience acts on the brain creating a proliferation of new synaptic connections that then create more complex neuronal circuits and assemblies. Even a clone would have a unique brain influenced and redrawn according to what that clone experienced in life. Due to the plasticity of the brain, identity is continually modified and shaped by environment.

Looking into the future, Susan briefly pointed to nanotechnology as a way in which the physical boundaries of the body – the internal world – would be merged with the external world, and likewise how biotechnology is already increasing the homogenization of human generations; blurring the physical lines between young and old. She then focused on the issue of how ICT was merging the cyberworld with reality. She questioned whether it was a wholly positive move with computer games as an example of a sensation-based mode of being based on immediate gratification. She believes that this fails to stimulate cognitive experience and therefore reduces the development of strong conceptual frameworks and content. She linked it also to potentially more risk-taking and the creation of collective identity or even absence of individual identity where the external here-and-now dominates.

Findings from the Gartner European Identity & Access Management Summit

EIGHT OF THE GARTNER IAM ANALYST TEAM DESCRIBE BELOW ONE KEY FINDING AND ONE KEY RECOMMENDATION EACH THAT YOU AS A PROFESSIONAL IN THIS SPACE SHOULD TAKE FROM THEIR PRESENTATIONS ON-SITE.

IAM and the Mobile Workforce

John Girard

Finding: 90% of large enterprises worldwide have remote workers, but many are not managing these workers effectively.

Recommendation: IAM controls will fail unless companies structure HR and management practices to maintain equitable and productive working relationships with location-independent workers.

IAM and Governance, Risk, and Compliance Management

Tom Scholtz

Finding: The IAM program is a key part of the organization's GRCM strategy. Managing the user lifecycle is an important activity, and access management encompasses an important set of risk management controls.

Recommendation: Treat your IAM initiatives as an integrated component of your IT risk management program.

IAM and Privacy

Carsten Casper

Finding: Appropriate protection for personal data depends on a number of factors such as location and sensitivity. The *legal* entity owning the data is legally responsible for protection. On the other hand, it is often the *physical* location that determines who is *perceived* to be responsible.

Recommendation: IAM projects need to balance these different perspectives on the location of personal data. IT organizations should leave questions of regulatory compliance to their lawyers and focus on procedural and technical protection for personal data in transit and in storage.

Identity Aware Networking

Mark Nicolett

Finding: Identity aware networking can augment traditional access control systems by limiting access to resources at the network layer.

Recommendation: Engage your network security organization's network access control project and integrate with your existing IAM policy infrastructure and access management processes.

Identity Intelligence

Mark Nicolett

Finding: Security Information and Event Management (SIEM) augments the audit capabilities of IAM infrastructure by providing broad scope user activity and resource access monitoring.

Recommendation: Reduce labor associated with SIEM report analysis by using IAM policy information to move from simple activity monitoring to exception monitoring of resource access that is based on knowledge of identity, role, status and access rights.

Role Management

Earl Perkins

Finding: Role management is the means to assign accountability to access; entitlement management enforces that accountability. Both work together to deliver accountability assurance.

Recommendation: review current application development, delivery, and operations strategies as one planning initiative.

IAM Services

Earl Perkins

Finding: IAM as a service has entered evaluation, testing, and early adoption phases as a result of maturing solutions for enterprises coupled with increasing needs for scale.

Recommendation: Evaluate IAM as a service for existing assembly and extension IAM projects.

IAM Project Management

Perry Carpenter

Finding: Most IAM related project/program failures are due to poor planning – not technology, vendors, etc.

Recommendation: Know what you want to do before you start doing it! That is, have a vision and a plan before you select a product and begin deploying technology.

Identity Management Best Practices

Perry Carpenter

Finding: Just because a technology has a name doesn't mean that it is functionally complete or suitable for a particular deployment scenario.

Recommendation: Select IAM vendors/ technologies according to tactical and strategic needs. Sound processes and a sound architecture are fundamental to a fit-for-purpose infrastructure.

Gartner Identity & Access Management Summit 2009

europe.gartner.com/iam

Comprehensive SSO

Gregg Kreizman

Finding: Improving user convenience is the No.1 reason that firms consider an SSO solution, followed by held desk call reduction, compliance requirements and shared workstation support.

Recommendation: Make a frank assessment of your enterprise's ability to simplify its target system environment to an acceptable level through attrition and directory integration of new applications, and assess the time frame for doing so prior to investing in tools.

IAM Architecture

Gregg Kreizman

Finding: Enterprises will always be behind the risk management curve if enterprise security is approached tactically.

Recommendation: Link the IAM architecture strategy, requirements and principles with the business via the enterprise architecture, and architect for choice.

Enterprise Authentication

Ant Allan

Finding: As enterprises replace simple passwords in more distinct use cases it becomes harder to find a single new authentication method that consistently provides the right level of assurance, at an acceptable total cost of ownership (TCO), and with appropriate ease of use.

Recommendation: Adopt a consistent methodology to evaluate the relative assurance level, relative ease of use and absolute TCO of candidate methods. Invest in open, flexible authentication architectures to simplify current and future use of multiple methods and reduce the overall TCO.

Consumer Authentication and Fraud Detection

Avivah Litan

Finding: Criminals will compromise credentials used to access your systems often using attack vectors outside your controls.

Recommendation: Protect your data and accounts from unauthorized access through a layered security approach that includes stronger user authentication, continuous fraud detection and out-of-band transaction verification.

SEE YOU NEXT YEAR!

The **Gartner Identity & Access Management Summit 2010** will be held on March 3 and 4, in the Royal Lancaster Hotel, London. We hope to see you again!

Gartner
Identity & Access Management Summit 2009

23–24 March | London