THE Open GROUP
www.opengroup.org

INTERVIEW WITH JAMIE LEWIS
CEO & RESEARCH CHAIR, BURTON GROUP

Jamie Lewis
CEO & Research Chair, Burton Group

Q: Why should people care about identity management?

A: The demand for identity management is a function of business drivers, a function of what the business objectives are and how they are requiring the usage and/or deployment of the identity technology. So the specific reasons vary by company.

For example, we see customers who implemented password management to increase the effectiveness of their helpdesks; they are saving money by reducing the number of helpdesk calls because users can now manage and reset passwords on their own, through password management mechanisms. Or we see clients who are getting requests from their customers who want to integrate their process with web-based single sign-on or other federation technologies – so these companies are meeting customer requirements that way.

Regulatory compliance plays a big role as well – that's a part of what I characterize as the stick side of the equation rather than the carrot. Financial services, healthcare, pharmaceuticals, and a variety of other businesses are under significant regulations that require them to do specific things with identity to be in compliance with the regulations.

Sarbanes-Oxley, for example, has provisions requiring a public company to be able to show how it managed access privileges that users have for accessing financial data about it. Regulatory compliance is probably one of the biggest drivers for why people are looking at identity management today.

Another good example is related to employee termination. A lot of companies may have policies that if an employee leaves a company, they should turn off all access that the employee had within 24 or 48 hours or some other specific amount of time. But if somebody has been with the company for any length of time, it's pretty hard to know how to find all of the accounts they had, much less to turn them off in a short period of time.

So it's about automating this kind of lifecycle management process, which relates back to the regulatory compliance – making sure that you can actually do it, and prove that it had happened. And then save some money along the way by making operations more efficient.

Regulatory compliance is probably one of the biggest drivers for why people are looking at identity management today.

Q: Would you consider identity management a growth area?

A: Absolutely. We are not a quantitative research firm, so we don't have estimates for how many dollars and how big the market is and so on. But if you look at the relationship that identity management has with the business objectives as I just talked about, and if you agree with the assumptions that identity management and identity-based security mechanisms are a basic requirement for electronic commerce, for distributed system supply chain management, and for the integration of business processes along the lines that cross application platforms and cross company boundaries, it becomes pretty clear that it is a huge growth area that will

grow pretty substantially over the next three to five years. We just need to figure out how to get identity management substantiated and managed.

Q: When you think of architecting a system using identity management, what do you see as the main problem?

A: The biggest problem that most customers face is that they have a lot of identity management, and that it's pretty fragmented. Every operating system, every application, every system they have deployed over the years has some level of identity management function in it. It might not be very functional and it might only apply to that one system, but it's there, so you are creating accounts, passwords, and privileges in many, many different systems.

If you look at the relationship that identity management has with business objectives ... it becomes pretty clear that it is a huge growth area that will grow pretty substantially over the next three to five years. ... Without identity management, the value of the information that can flow through freely would be very low.

So the biggest challenge is how do you bring all those things together, and create a holistic, integrated way to manage identity across all of those systems. That's an easy thing to say and very hard to do. It's a big systems integration task. Figuring out how to do that, in the absence of standards that are supported by a large number of products, represents a pretty significant problem.

I do believe that politics often become a part of the problem: Any time you start talking about identity information and how you name things, there are people inside many companies that feel like they have a vested interested in that discussion – from human resources to people who own the applications and have all their identity information in them, there are a lot of different stakeholders in the company that you need to bring together to solve that problem. It's a largescale problem that involves a lot of different people. So it's both politics and the technology. And sometimes the politics is much bigger than the technology.

Q: So you could say that identity management is one of the prerequisites of The Open Group concept of Boundaryless Information Flow™?

A: Absolutely. If you say "boundaryless" to a security architect, it usually scares them; they view it as a bad thing. But I understand completely what you mean when you say "Boundaryless Information Flow". We see those boundaries becoming a lot more porous nowadays. But the only way to ensure that the information that is flowing across those boundaries is the right information, is to make sure you know who is doing what, when, and where. That's what identity management is about – through policy to be able to say who can do what, when they can do it, and how they can do it. And to put some logical controls around information that moves across those different boundaries. So you are absolutely right, it's a prerequisite.

The other way to put it, is that without identity management, the value of the information that can flow through freely would be very low. If you are browsing the web and if you are downloading marketing materials, you don't care so much about the security of that information – on the contrary, you want it as widely propagated as possible. But when it comes to financial information, you don't want that information propagated – you only want the right people who need it to see it. To ensure that, you need identity-based security mechanisms built on sound identity management that will allow you to create accounts based on identity, assign privileges based on identity, change accounts, and tie policy to identity.

Q: What trends do you see in the identity management architecture? You mentioned Service Oriented Architecture (SOA) and the related hype. So what do you see as the big positive trends?

A: I talked about market trends of consolidation. There used to be a lot more vendors with lots of often overlapping products, and customers were somewhat hesitant to make big bets based on small vendors who might not be making money and might not be around in a couple of years. The industry consolidation that occurred has been largely positive – it has created fewer players, but enough to have competition, and all of them being bigger companies that you know you can bet on. That's one trend.

The biggest challenge is how you ... create a holistic, integrated way to manage identity across all of those systems.

From an architecture point of view, people have understood that they can't try to solve the whole problem at once. Instead, they are picking specific problems like password management, or some lifecycle management project for a smaller number of applications to focus on. For example, let's say there are 15 applications in your organization that are causing 70% of your compliance headaches. If you focus on solving provisioning for those 15 applications you make huge progress. Although you don't solve your whole problem at one time, if you solve that particular issue, you solve a large part of your problem and create momentum for solving the next issue after that.

About SOA, I think people are understanding the link between web services and identity-based security: They understand that without identity-based security, web services won't work. So I think as people are starting to look at how to use web services in end-systems integration, they are realizing that is an important part of how they build applications. So we are seeing that trend getting into tools. That's a good way to do that as well.

Federation is another one. Again, it is not solving the whole problem at once, but we are starting to see more and more situations in which it is used. For example, a big financial services company – a client of ours – was asked by one of its biggest customers to provide web-based single sign-on for its employees coming into the financial services company's portal. We see a lot more of that and we see federation really picking up steam in a lot of different places.

Q: Where do you see identity management standards heading, and how do you see the play of open standards *versus* proprietary systems?

A: Open standards are a prerequisite for many of the things I talked about. Although we'd like it to move faster, when you look at developments like SAML or Liberty, there has been a lot of progress over the last three to four years. The web services framework, some of the basics for web services like SOAP, WSDL, and WS-Security, those are all standards now. Those are good signs. Also, Microsoft and Sun came to agreement to bury the hatchet and make friends a while back, and we certainly hope to see some concrete results from that. I think we probably will, and that there will be some convergence and coexistence of those standards. So in respect to the federation, I don't think customers have to worry about which one to use, and don't have to wait to see how it works out because the coexistence and convergence are already a reality in many ways. Coexistence first, and then convergence later. And I think that's a good thing.

Thank you.