

# Identity Management for the Security Professional

By Mark MacAuley

**Looking at what IdM is in the context of your business, why you may or may not need it, and what implementing a solution is really about, will help you be more successful with your efforts.**

If you were to ask six people from six different groups within your organization what Identity Management is and what it will do for you, I'm willing to bet you would get six different answers, probably more. Identity Management (IdM) is an IT initiative, not always well defined, that sometimes ends up doing what its users want for more than what they originally thought it would cost. Looking at what IdM is in the context of your business, why you may or may not need it, and what implementing a solution is really about, will help you be more successful with your efforts. Proper use of IdM should be defined by the organization, not by industry standards.

Many companies over the past four or five years looked at Identity Management as a way to audit for meeting compliance criteria, as well as to introduce a user-centric layer of application access control and process. A lot has changed in the IdM space, thankfully, and it is important to security professionals to understand what's out there.

I will explore some key points that come from having worked with a Fortune 10 company and three other Fortune 100 companies directly, and having spoken with over 100 organizations on three continents about Identity Management. Much of the time I have spoken about what a deployment really means, which approaches seem to work, and which others definitely don't.

## Questions for Identity Management

Here is a series of questions which, once answered, will provide you far more focus – and save you at least \$100,000 in implementation costs.

1. Will you manage identity at the network layer or at the application layer?
2. What will the organization receive from implementing an identity management solution? Be very specific. Answers such

as “avoiding an insider breach” or “SOX compliance” are inadequate. “Not paying \$500,000 to our PR agency after an insider breach” or “saving \$50,000 on our next SOX audit” are better.

3. What do you ultimately want to accomplish for your organization by implementing an Identity Management solution? Improve user account management? Automate IT processes? Zone segments of users and infrastructure? Remove anonymity from your network and applications?
4. Will the Identity Management solution add another layer of security to the mix, or create new risks?
5. Who will own the implementation and ongoing support? Local IT? Risk management? The corporate CIO?
6. Who else needs to be represented and involved with vendor selection, besides the security team, and when will you involve them?

I have not included justifications for return on investment (ROI) here. Any ROI discussions I undertook, and even models I developed as a consultant, were wrong. They were wrong because they assumed a return at the early stages of the project – but the return really starts getting measured at the end of a project. They were also based on data and situations that were static, not fluid as in real life. The way to approach a money discussion is to look at peer organizations, either in size or industry, who may have had a breach, and see what their costs were post-breach or post-incident. That is, don't take the vendor perspective, necessarily.

Problems like credit monitoring, market capitalization losses, and other real and measurable costs are easy to see and to justify against. Compare those to the reduction in cost of call center calls, or damage to the brand – which is what a lot of vendors bring to the table for data in various forms. Do some homework, and quantify the savings on what you know about your organization. It will pay in the long run.

## Question One

There is a reason the first question I put forward is that of deciding between the network layer and the application layer. The answer will have significant impact on the outcome of the project. It will accurately tell you why Identity Management is important to your organization, who should be involved, and what you should budget for it. It will also help the rest of the organization explore whether managing application access is enough. So ask yourself: Does it make sense to deploy an IdM solution at the application layer, or the network layer?

### Application layer

Here are the steps you will need to factor into your project plan for the application layer.

1. Discovery will be challenging. You will need to inventory and prioritize all the applications you'll provision. Write down who owns each application and how to reach them.
2. Sign license agreements after you have an accurate inventory, so you buy what you need from the vendor if at all possible.
3. Document the "as is" and "to be" business process that will be built into the provisioning system. Get sign-off on this process from all stakeholders and application owners.
4. Technical design happens next. Review with the security and legal departments to ensure that any holes are uncovered, before you start writing code and configuring applications.
5. Once design is signed off on, it is time to map design and process. Start building a solution in your development environment.
6. Run it through development, staging, testing/UAT, and production processes, and then launch.
7. Repeat for every application in the inventory, although parallel build cycles are possible depending upon size of teams.

Take care to note that the application-layer approach may require years for large organizations. The per-application costs I have seen range from \$50,000 to \$100,000, including licensing, services and labor.

### Network layer

Here are the steps you will need to factor into your project plan for the network layer.

1. This segment of the IdM space is fairly new – less than 2 years old – so companies are not as well established. You will want to pilot every shortlisted vendor solution. This will give you a sense of your approach being correct, and also how accurate the claims are.
2. Most discovery for this class of products is automatic and is application – and process-agnostic, since you're in the network layer. There is huge political benefit here, and discovery will take hours or days at most.
3. You will be introducing another layer of hardware to your environment, since most vendors are appliance-based. This will change, as the juggernauts in the router world want this functionality and code ported to their hardware platforms.

The network layer approach will protect and control access not just to applications, but to three layers: networks, servers and applications.

The approach is also much faster, with implementations requiring only a few days or one to two weeks. Fully deployed solutions will run \$30,000 to \$500,000 for *every* application, user and device.

## Questions Two through Six

With your answer to Question One behind you, Questions Two through Six should move right along. They are the reasons of justification, and will ultimately help determine the budget, who needs to be involved, and who will have to live with the project once it is completed. These are not trivial questions; but with an understanding of what the two approaches are, these questions become easier because you know who to ask and involve from the outset of the project.

They are also important because this is where you will have the opportunity to understand the politics, which I believe to be one of the most overlooked areas. If you decide to take the application-layer approach, you will need to rely on the application owners to give you data – but only so that you can go on to build an application or layer of functionality that they don't understand, on top of "their" application. When you undertake this, in many cases you'll encounter reluctance and pushback.

Spend more time on process than on the code and the technology. That is, completely think through the process you want to implement, not the technology you want to implement. The solutions available today are flexible enough to support and reflect your process, and not the other way around – so get your process right.

The most successful IdM implementation in which I participated at a Fortune 10 company focused entirely on getting the "to be" process right, and then implemented the technology to support the process. Not only did the company succeed in being the first to say it had met the compliance directive or audit, but it also met the next two pieces of the directive – access management and provisioning and deprovisioning.

## Conclusion

You have a choice. Do you want to manage and enforce access by user, or do you want to manage network, infrastructure, and application access by user and/or device? Don't forget that a machine has an identity too. I believe this is why some are starting to aggressively analyze Network Admission Control (NAC). Furthermore tokens, while a mature solution, don't provide a machine ID or machine authentication – which is a risk area in and of itself.

The future of Identity Management through the eyes of security professionals will see convergence of NAC (machine health), identity-based access control, and layered security. We need to know who is on our network and accessing our infrastructure and applications, and what device they are doing it with – is it a compliant or healthy device? Fortunately, the technology is catching up to the business needs, and the convergence seems to be happening quickly to support a more secure enterprise.

## About the Author

*Mark MacAuley is a member of the ISSA, IAPP, InfraGard, and the IISFA. Mark runs a blog at <http://identitystuff.blogspot.com> and has consulted on and sold identity management solutions for the past four years. He lives in New England and is currently the Northeast Manager at Trusted Network Technologies. He can be reached at [identitystuff@gmail.com](mailto:identitystuff@gmail.com).*