
Delivering on identity and access management

Does authorisation provide the link?

By Jon Collins, August 2009

Originally published on



The following article was originally published as part of the Freeform Dynamics advisory column on CIO Online. This is focused on the business impact of development in the technology industry. Original articles can be accessed at www.cio.co.uk (registration required).

At a recent panel event involving senior security managers and chief information security officers from a number of industries, Identity and Access Management was cited as one of the top priorities. Participants gave a number of reasons, which can be distilled into three categories: more efficient and less fragmented delivery of IT services; facilitation of better collaboration with customers and partners; and the necessity to demonstrate compliance with data protection legislation.

All of which would be great - if only identity and access management hadn't proved impossible to implement. As one participant stressed, "We're five years down the line, and it still hasn't delivered." Worthy of note: that's not meaning, "delivered on its promises" mind, that's, "delivered at all." So, what is it that makes identity and access management so hard to do?

We can consider this question from both the IT and the business perspective. Considering IT in general, and security-related topics (such as identity and access management) in particular, the challenges faced in deploying such capabilities cannot be helped by our innate desire to concentrate on the 'how' rather than the 'what'.

Identity and access management requires implementers to understand two complex areas at the same time - first, the (rapidly changing) roles and requirements of a large number of individuals; and second, the diverse hotchpotch of new and legacy systems that may be in place. Wouldn't it be great if there could be a system to just resolve all of that? The answer has to be 'yes' - but while the requirements for such a system may be obvious in principle, the practicalities of implementation have defeated all but a minority of organisations.

It is understandable, and indeed desirable, that the IT industry has looked hard at how to resolve some of the technical and philosophical issues around delivering identity and access management. Initiatives such as the claims-based architectures espoused by the likes of Microsoft, together with cross-industry efforts such as OpenID, are to be welcomed. However the one thing they cannot do; is circumvent the complexities at the heart of deploying identity and [access management on an industrial scale](#).

So what are the options? Should we turn perhaps to the business, and insist that it gets its own house in order before IT automates what is required? It's here that we reach the nub of the matter from the business perspective: in a word, churn. As soon as we reach any understanding of who

has access to what and why, such information almost immediately becomes out of date. Organisations large and small depend on pools of contractors and temporary staff; management roles change; hiring, firings, maternity provision and job shares are part of the fabric of modern industry.

Meanwhile, the boundaries of organisations public and private are today more like semi-permeable membranes than fortress walls. We see this in pharmaceutical companies creating innovation ecosystems, just as in borough councils and local health authorities looking to provide services and "deliver individual outcomes" to what is often a highly transient population.

While it is not absolutely clear what is the answer, we can perhaps identify where it may be found - not in the complexity of systems and applications that need to be accessed, nor in the constantly changing pool of people and roles that need to be identified and trusted. Rather, we could look at the interface between the two - or more importantly, the specific event during which authorisation is made between a specific individual and a specific service.

Managing authorisations may hold the key. There are examples of where we already have this licked - consider e-banking for example, where it would be highly undesirable to have anything other than a working solution - and banking IT experts will be quick to point out that it was no easy job to get the smorgasbord of back-end systems integrated into what appears to be a quite straightforward interface.

Drawing on the banking example, for added impetus, we can look to legislation and compliance. Both industry-applicable regulations such as [Sarbanes Oxley](#) and national laws such as the data protection act require that authorisation of access to a given data set is in some way controlled. In other words, many organisations have no choice but to make this happen: it's the law.

Let's remember, it isn't necessary to deliver everything, all at once. In conclusion, it is perhaps time to dispense with ill-fated attempts to provide blanket policies and approaches, however attractive they may seem at the outset. Instead, we can focus first on how to enable responsible individuals to provision access to higher priority systems and higher risk data. If and when this has been enabled, then other, lower priority systems can be brought into the fold.

About Freeform Dynamics



Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

As part of this, we use an innovative research methodology to gather feedback directly from those involved in IT strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream business and IT professionals.

For further information or to subscribe to the Freeform Dynamics free research service, please visit www.freeformdynamics.com or contact us via info@freeformdynamics.com.

Terms of Use

This document is Copyright 2009 Freeform Dynamics Ltd. It may be freely duplicated and distributed in its entirety on an individual one to one basis, either electronically or in hard copy form. It may not, however, be disassembled or modified in any way as part of the duplication process. Hosting of the document for download on the Web and/or mass distribution of the document by any means is prohibited unless express permission is obtained from Freeform Dynamics Ltd.

This document is provided for your general information and use only. Neither Freeform Dynamics Ltd nor any third parties provide any warranty or guarantee as to the suitability of the information provided within it for any particular purpose.