FIVE PRO TIPS TO ENSURE SUCCESS WITH IDENTITY AND ACCESS MANAGEMENT

By Wayne Olsen, Datacentrix security business unit manager

Identity and Access Management (IDAM) is an essential aspect of an organisation's overall security posture – both from a physical access perspective (office premises, laptops, documents and so on) as well as from a digital viewpoint (data, systems and applications).

Often, this data may be scattered across a number of internal and external systems, so enterprises must have a reliable way of managing a number of identities and permission levels.

However, if IDAM is conducted in isolation from the broader security strategy, it is likely to be less effective and place organisations at risk of access breaches. The result could be loss of consumer trust, brand damage, regulatory fines, and other disastrous consequences.

So, just how can an organisation ensure that their IDAM strategy is best suited to their organisation, achieving optimal results, while making certain that it also remains relevant in the face of an ever-changing threat landscape?

Let's look at the top five tips to ensure impenetrable IDAM in your business:

1. Design your IDAM programme in the context of overall business and technology strategies
The harsh reality is that there's no simple 'plug and play' IDAM solution for any enterprise, no 'one-size-fits-all' approach. The business strategy and objectives, as well as the technology roadmap, will dictate the types of controls that must be implemented to best serve the business' needs.

For instance, in some organisations where a mass of personal customer data is held (such as a bank), a heavy emphasis on data security will be front-and-centre in one's IDAM approach. For a purveyor of luxury goods, then physical IDAM might be the

biggest priority. Software providers might be more focused on how to ensure only authenticated users can access their services (preventing piracy and unauthorised use).

IDAM should certainly not be planned and implemented in isolation. Consider the organisation's broader enterprise architecture – and follow formal project management and software development approaches to ensure alignment with the business and technology strategies.

2. Mitigate the greatest risks early on
In principle, IDAM can alleviate identity abuse and deter fraud, while providing auditing compliance and acting as an impartial 'witness' to sensitive business transactions (providing evidence when needed).

In practice though, the organisation must firstly identify the biggest risks to its business, and place a heavier emphasis on addressing these concerns.

Generally, we see the most effort being poured into high-visibility issues, such as ransomware, hacking, network security, and ensuring regulatory compliance. But there may be some lesser-known threats that are quite specific to your business, which actually pose the biggest risks.

3. Garner support at all levels and disciplines within the organisation
In large enterprises, perhaps the biggest reason for the success or failure of any initiate, technology or otherwise, is the team's ability to corral the support and endorsement from across the entire organisation.

It's critical for an IDAM programme to have the right level of support within an organisation prior to implementation. Technical guys will see bells and whistles, and perhaps become enamoured with the likes of single sign-on. On the other hand, business leadership will understand the importance of regulatory compliance and protecting intellectual property.

Frame the benefits in these various ways, to get all levels of the organisation on board with what could potentially be the introduction of a disruptive technology.

4. Take a structured, phased approach to the rollout
It is crucial to take a structured, phased approach to the rollout, showing business value at every stage. To begin with, individuals must be positively identified and physically verified to create the right level of trust.

Early on, the tasks are likely to be creating frameworks, groups, memberships, duties and roles. Allied to this, data (both structured and unstructured) must be classified, and policies and procedures put in place.

Remember that IDAM maturity is more of a journey than an event. While we might initially focus on 'keeping the bad guys out', the programme should mature, where the angle is more about 'keeping the good guys honest and protecting the innocent from identity abuse'.

5. Plan for growth, agility and flexibility
Here, we come full circle, returning to the need for your IDAM to be woven into the fabric of your broader technology and architecture strategies. In this way, it should be built to evolve, to be continually analysed and improved.

Over time, new types of threats emerge, and new criminal tactics start to take hold. Your IDAM strategy must respond to the ever-changing threat landscape.

Ensure your initial IDAM solution specs include detailed current and probable future functionality requirements – so you can choose a solution that caters for immediate needs, but also has the flexibility to grow, allowing you to toggle new features whenever needed.

While IDAM is a core component of any security technology implementation, and certainly one that can deliver massive benefits, the concern is that these projects can become costly and lengthy if a business is not properly prepared.

To avoid exposing your business to undue risks for lengthy periods of time, Datacentrix can support your business throughout the preparatory and planning phases, through implementation and management, setting your IDAM programme up for success.

Contact Wayne Olsen, Datacentrix security business unit manager on 087 741 5000 or wolsen@datacentrix.co.za