How do you as a **business leader structure** and **secure** your **business operations** in the face of **cybercrime** and **digital transformation**?

Implementing Identity Access Management that enables secure platforms

By Tonderai Kariwo, BSG Principal Consultant

At times, everyone becomes frustrated with the amount of passwords and the hassle of having to remember these, along with the frustration of not getting access, changing passwords and the impact of cybercrime.

Worryingly, for businesses that already face these issues, additional risks often arise that challenge how the typical business leader should structure and secure their business operations. Combining this with the advent of digital transformation, the results are a multitude of complex technology environments.

In recent times the importance of IT security has been called into question as there has been an increase in targeted cyber-attacks which compromise our technology and can prove to be crippling, for example the cyber-attack suffered by Liberty Group.

So what does this mean for business? How does business balance security and the user experience when designing **Identity Access Management (IAM)**? To answer this question, I am going to delve a little deeper into IAM and the important role it plays across Governance, Risk and Compliance, securing your business processes, people and technology.

Exploring the main factors to consider when implementing access control

Having recently been involved in the implementation of an IAM solution at a leading corporate health and insurance company (read the full case study) the key factors that need to be considered when successfully implementing access control were highlighted.

- Take a business-led approach that is accountable for delivery and aligned to strategy, as well as incorporate data insights to inform the decision making. This provides the benefit of introducing Role-based Access Control (RBAC).
- If the back door to your house is left open, it doesn't matter how much security there is on the front door. Understand the complete landscape of infrastructure and technology given that security is only as good as its weakest link.
- Central to your solution design should be job profiles that drive access entitlements at a role-based level.

- Integrate your design to cater for the resolution of identified audit points. This is fundamental to the business strategy and key to ensuring operational compliance.
- Additional to the above is ensuring that a holistic view of the business capabilities are factored in, ensuring that your solution is robust and catered for security, compliance, fraud etc.

When deploying a cloud-based solution take time to understand the application of enterprise security and governance, given the complexity of managing data from the cloud.

Identifying the points of failure to avoid

In our case, when the IAM solution implementation commenced, there were a lot of unknowns and gaps within the HR database and job profiles. There were multiple processes that did not have any identified owners, as well as a multitude of systems within the environment interacting together.

Action needed to be taken to ensure that the many moving parts and parties were identified, mobilised and co-ordinated. It became very clear that business leaders needed to be informed and kept accountable for both the implementation and the impact to the strategy, so as to manage a successful change.

Ensuring that quality data is available is key as this impacts the issuance of access entitlements. We needed to ensure that the access entitlements were accurately aligned to the job profiles that resided within the HR database, so that users would be correctly assigned access entitlements at a job profile level. The data needed to be accurate. Most important was working with the different technology domains to ensure that the data flow was consistent and seamless across multiple systems and data layers especially when managing the solution from the cloud. This meant there were multiple secure options through which to connect to the cloud-based system.

Combining people, processes and technologies

Clearly all three are important given the complexity of the environment and the multitude of technology and people involved to create, manage, authenticate, control and remove a user's permissions, and the way data is accessed by the users.

> Starting with a **risk-based** and **user-centric approach** can go a long way in identifying where the **biggest risk** and impact to users lies, thereby addressing this first when implementing IAM.

This approach creates clarity and structure that is aligned to the end goal and design which in turn provides ongoing business benefit (**People**). The next step is identifying the processes and improvements that are necessary to validate and change in line with the IAM implementation (**Processes**).

Lastly, go about aligning the business requirements, e.g. access entitlements at a job profile level, to the technology capabilities that will manage IAM once the solution is implemented (**Technology**). The aim of this approach is to reduce the risk of security breaches to your technology by securing your platforms through the manner in which users interact with the technology.

Steps to take when implementing IAM

IAM is leading the path in an exciting world filled with endless business opportunities that will reduce risks while implementing security policies and processes. However, it can be daunting to educate, prioritise, pick and implement solutions, and then maintain all of it with thoughtful governance. Practical steps that business would prize in implementing IAM are:

- That business has identified critical process experts to own key processes (for example on-boarding, claims, authorisations, pay-outs) or functionality that will guide the controls and measures supporting access entitlement provisioning to the job profiles
- Enabling internal audit to setup the internal controls that would govern, resolve and report against IAM metrics
- The technical solution be it on premise or cloud is fully understood, the environment including the infrastructure are known and the different integration points are validated will facilitate easier deployment and interaction of the data flows
- Ensuring that there is ongoing alignment to the business strategy and operations that determine the responsibilities within the job profiles and ultimately the correct access entitlements throughout the implementation phases
- Ensuring that key capabilities such as risk-based authentication, behavioural analysis, automated workflows are in place, and allow us to appreciate IAM and the direct interconnectedness to functions such as fraud, security and governance

Maturing our secure platforms through Identity Access Management

IAM as a framework is a continuous practice within the organisation and sits at the heart of how business will continue to strive to build and implement secure platforms that are user centric. At the heart of this continuous practice is understanding the breadth of the business across the business lines, while supporting the CIO and business leaders to appreciate the work involved in implementing IAM in a diverse technology environment, which is consistently changing.

It is imperative to take a risk-based approach to managing the complex work as this prioritises key areas that support business in mitigating potential security risks by eliminating inappropriate user access entitlements. Ultimately, focus should be directly aimed at fostering a positive user experience by replacing costly legacy systems, while creating resilience within the business operations through the implementation and maturity of a robust Identity Access Management framework. ■

Sources: Counting the cost of Liberty's cyber-attack, Moneyweb, 2018

Get in touch

Jurie Schoeman

BSG Chief Executive Officer

jurie.schoeman@bsg.co.za

+27 (0)83 30 27169

+27 (0)11 215 6666

Celebrating 20 years of getting the job done
Getting the job done, with you
20 YEARS