

# A STRONGER IDENTITY FOR ACCESS MANAGEMENT

Press Release

23rd August 2017



In our ever increasing digital age, we are finding that we need to work even harder at governing and protecting data and information. Philip Yazbek, industrial psychologist at consulting firm Bizmod, says that how we govern and protect starts with who and how we access data and information.

Organisations need to ensure that their identity and access management is properly secured and managed. Yazbek says that the global cyber-attack that hit 150 countries worldwide (SA included) in May should be a

wake-up call to not only organisations, but to our government agencies as well, confirming that our information security is still very vulnerable.

“Organisations can have all the necessary firewalls and security controls in place, but if they are not controlling and monitoring identity and access management (IAM) they are leaving the doors open for cyber criminals,” warns Yazbek.

## HE CITES RECENT CYBER SECURITY RESEARCH WHICH HAS REVEALED SOME STARTLING INFORMATION:



In South Africa, data breaches costs SA firms R28,6 billion per annum. (IBM & Ponemon Institute, 2016)



Breaches are usually discovered long after they have occurred. In 2015, the average amount of days it took from when the incident occurred until it was discovered was 146 days (Mandiant Consulting, 2016)



In most breaches, legitimate user credentials were used, where 63% involved weak, default, or stolen passwords. (Verizon DBIR, 2016)



Employees can be your biggest risk. It was found that 43% of data loss was internal, half being intentional, the other half accidental. (Intel Security Report, 2015)



90% of ex-employees retain access to their former employers’ software applications. Another 49% were shown to have logged into a company account after no longer working there. (Intermedia, 2014).

“Employees move around in an organisation; they may move across roles or up in the ranks and by doing so accumulate access rights along the way, says Yazbek. “It may even become a form of entitlement to be a super-user with avant-garde access.”

Yazbek says that this is why corporate governance for identity and access management control is so critical. In the past, before the advent of smart devices, cloud networking and VPN access, IAM was simpler because systems were mainly computer based and were easily controlled in closed networks. Now, people are connecting on different platforms – PC, mobile devices to the cloud – and various operating systems (Android, IOS, Microsoft), so the architecture has had to evolve to cater for this, making IAM and how it is governed more complex.

Yazbek concludes, “While we assume that people have the integrity to not abuse their privileges and only use the access they need, the onus is on the organisation to ensure this is controlled.”

For media queries please contact Tandi Robertson from REPUBLIC PR on 072 774 5054 or tandi@republicpr.co.za

For more information visit [www.bizmod.co.za](http://www.bizmod.co.za)