BIZCOMMUNITY

Impact of BYOD and BYOA on corporate security

Late last week business leaders sourced from a range of industries - including education, medical and IT services - joined representatives from Integr8 and Cisco Systems at the Saxon Hotel to discuss the impact of Bring Your Own Device (BYOD) and Bring Your Own App (BYOA) on corporate security.

Both of these are realities in the workplace today and their increasing relevance has forced decision makers to assess seriously whether or not their corporate security strategies can manage these influences.

Paul van Niekerk

Participants at the interactive session included Paul Beyleveld, representing Cisco Security, Andre de Kock, IT manager: Medhold; Chris Baird, CFO: Medhold; Paul van Niekerk, general training manager: NetCampus (member of the Business Connexion Group); Jan Roux, CIO: Integr8 and Bennie Strydom, chief sales officer: Integr8.

In the knowledge that the forces of internet connectivity, mobility, smart devices and consumerisation of IT continue to combine, delegates delved into the dynamics of who or what is actually driving BYOD & BYOA and what approach should businesses take to effectively address concerns - particularly security.

80% of BYOD unmanaged

Statistics from global research companies, including Gartner, Checkpoint, Ovum and IBM, support the notion that mobility has now permeated businesses.

According to research, 75% of companies say there are more than twice as many personal devices connecting to corporate networks now than there were two years ago, more than 10 billion personal mobile devices are expected to be in use by 2020 and 80% of BYOD activity is going unmanaged. Furthermore, 1.2 billion smartphones and tablets are expected to be sold in 2014.

Roux peppered the session with leading questions that fuelled discussion over issues such as the relevance of Mobile Device Management (MDM), policy drafting and implementation, perception of the market, productivity and risk management.

"Mobility enables productivity and efficiency through real time communication," claimed Chris Baird, CFO, Medhold. "The question of whose device it should be is a corporate decision based on acceptable risk levels in selling sensitive company data."

Introduction of policy is first step

Given the advent of mobility in the workplace and rising wave of apps into the market, risk is inevitable in terms of BYOD and BYOA. However, as far as security strategy is concerned, delegates felt that policy introduction was the first point of departure to ensure that risk could be mitigated.

The point that Baird raised was that risk could never be entirely eradicated, but should be mitigated. It was agreed that the introduction of policy was the first point of departure to successfully do this.

Beyleveld emphasised that there is technology in place to empower businesses to minimise and control risks, but that it is critical to consider business requirements and align policies with these requirements.

As an example, some businesses have enforced a technology policy and framework that allows employees, when they are at work or on premise, to access the corporate network off a flash drive. Everything is on the drive and works off a server as long as they are connected. When they leave, the device is 'cleared' and not accessible to the network. It eliminates remote access and thereby reduces the risk of anywhere access.

Skills and training

Bennie Strydom

De Kock referred to the need for awareness around security backups, on training and skills development within the corporate in order to ensure that critical resources such as corporate IP are adequately protected. "We have to also think about the introduction of POPI and the implications for the market."

In the education space, there is genuine progress being made added Beyleveld. "There are universities that are issuing tablets to students, as a resource through which they can source electronic textbooks... these institutions are also capitalising on getting students, BYOD is a model for revenue generation."

Finance is another vertical that continues to make strides in handling mobility in the workplace. Established service providers have adapted strategies to empower employees with the relevant access to networks and a model for the controlled application of mobile devices and applications.

Low percentage of uptake

Roux posed the conundrum that if the majority of companies do see value in embracing BYOD & BYOA, why is there such a low percentage of real uptake? Fear of the unknown and misperception of what can actually be done to control BYOD were cited as two potential reasons.

Integr8 and other representative companies present voiced their opinions of why it is critical that policy drives the accessibility of data, use of devices and application in the workplace. There was agreement that control was a central issue, as were ownership of the device and the implications of setting restriction.

Ultimately, according to Integr8 and many of its partners, there is sense in taking specific steps when it comes to BYOD and BYOA. Firstly, it is important to decide on whether or not the business will block it, to realise that there is no 'one solutions fits all' and there must be a genuine and clear understanding of what the risks will be to adopt, that policy generation must be proactive and there must be effective communication to the rest of the organisation.

Once these steps have been taken, the process of security management, control mechanisms, implementation and support can be initiated.

Participants in this roundtable discussion left the session with a greater sense of ease over BYOD and BYOA thanks to the insight gained.