BIZCOMMUNITY

Security in the age of digital transformation

By Kim Andersen

17 Aug 2015

The quickening pace of change in business today is forcing companies to transform themselves digitally, in new and innovative ways. It's requiring them to shake off traditional, legacy-based approaches to IT, and think more like those new-age competitors that were 'born digital'. The name of the game is to digitise and transform business processes - embracing new ways of connecting with customers, partners and others in the value chain. However, by doing this, organisations are also faced with new complexities from a security perspective.

In listed companies, studies have shown that data leaks and security breaches have a clear relationship to share price. Once all other variables have been controlled for, research indicates that organisations typically see a 10% mark-down in their share price, even eight months after the security breach occurred.

Stuart Miles via freedigitalphotos.net

Prevention is not always possible

So, security perceptions have a direct impact on shareholder returns. This reality often causes CIOs to take the most conservative approach possible, looking to lock-down, protect and prevent incidents with strong firewalls and policy-driven approaches to security. But in the new digital economy - where ecosystem-based networks and the world of APIs means deeper integration into partners, suppliers and customers - the 'prevention' approach is simply not always possible. We advocate a more pragmatic approach to security: that of detection and quick response, rather than an attempt at prevention. Data is now hosted in new ways, exposed to external parties in new ways, and extended to users via new (often mobile) devices.

Traditionally, staff inside the organisation were protected by, but also restricted by, firewalls and strong-arm IT policies. To compete in a changing environment, the emphasis needs to shift towards empowering staff to take ownership of security, by giving them the knowledge and tools to make the right decisions. With this change in mindset, organisations unlock opportunities to find these "white spaces" of business possibility - new efficiencies, new markets, and new relationships. In being able to work with and share data more easily, they can collaborate, find solutions, find new opportunities, and get closer to customers.

A fresh look at IT security

However, harnessing the power of Big Data and transforming it into knowledge requires a fresh look at IT security.

The old	The new
Prevention-based approach	Detection and rapid response
Limiting staff by “locking things down”	Empowering staff (knowledge and awareness)
Restricting any channels to the outside world	Embracing new business/communication channels
Secured ‘silos’ of information	Collaboration across business units

So, how do organisations deal with the threat of increasingly severe penalties for data leaks (such as the forthcoming POPI Act) for instance, while at the same time readying the business for the new world of open-platforms and real-time integration?

The first step is to accept that any security system is fallible; and to shift the focus to rapid response alerts that minimise any the damage and return the organisation to a state of business-as-usual. Perfection is something that cannot realistically

be achieved. Even some of the world's most prestigious companies - like Apple, MasterCard and Sony - have fallen victim to attacks. Previously, breaches were considered to be an exception. The new model requires us to view them as something endemic to the digital age - something that can be mitigated and immediately addressed, but not prevented entirely.

Organisations should adopt a more refined, granular approach to data access. Instead of blanket policies, data access should consider who needs to access data, at what times, and under what conditions. By using permissions, signing in and out, and using audit trails, organisations can build what we call a 'programmatically controlled' approach to data security.

Ultimately, now is the time to invest more in security than ever before. Threats are on the rise, and their natures are shape-shifting at very rapid rates. With the right approach and the appropriate solutions, organisations can position themselves to capitalise on the benefits of open innovation needed for digital transformation, while responding in real-time to any new security threats.

ABOUT KIM ANDERSEN

Kim Andersen, Account CTO at T-Systems South Africa

- [BizTrends 2016] Digital transformation: top 10 technology trends of 2016 - 18 Jan 2016
- Digital transformation: threat or opportunity? - 15 Oct 2015
- Taking a bi-modal, multi-sourced approach to digital transformation - 17 Sep 2015
- Unlocking the true value of your organisation's information - 25 Aug 2015
- Security in the age of digital transformation - 17 Aug 2015

View my profile and articles...