Flying blind in an invisible war

Nathan Desfontaines, Cyber Security Manager at KPMG South Africa

The prevalence of cyber threats is forcing companies to make tough decision and quickly, otherwise they stand to lose direct control of data security.

From coherent mobile information security policies to comprehensive cyber security strategies, the list of what is required from businesses to adequately protect ever-increasing volumes of data is growing.

This is because the number of threats, including mobile malware and hacking, is also increasing. Mobile attacks, custom-designed malware and the threat that wearable technology, such as smartwatches, as examples of what businesses will have to be aware of in 2016.

Why do organisations need to treat cyber security as a key IT element rather than 'another' business risk?

Businesses need to move away from believing that cyber security is a point in time exercise - a fad that is "hyped up", or that the threats of cyber-attacks will go away. Once businesses can do this, then we can start to embrace the benefits technology has enabled within the business while dealing effectively with the very real threat of cyber-crime. When it comes to protecting the businesses information from potential cyber-attacks, businesses need to understand what their "Crown Jewels" are. By knowing what the business has and what it is worth - both to the business and to outsiders – only then will the business gain a better understanding of what information needs to be protected. Trying to achieve 100% security across all facets of the IT estate is a challenge and is bound to dilute the focus on where it really should be – the critical information assets of the business.

What are the toughest security challenges for businesses today?

A constant challenge that businesses face today is having an effective threat intelligence capability assessment, plan and response in place. Most companies would not know if they were being attacked and in most cases, for those who do, they are unable to detect and effectively respond to a breach. The reality is that technology in isolation is not going to ensure a business's readiness to respond to a breach. Businesses need to have a balanced model of full business IT security including; skilled people, embedded practical processes and, a "fit-for-purpose" technology that enhances the ability to detect and respond to a possible breach.

What do you consider to be a comprehensive cyber security strategy?

A comprehensive cyber security strategy therefore should start with a detailed classification of the business' data – as you can't protect what you don't know you have. This classification should be followed by an all-inclusive threat intelligence capability assessment so that an effective post-breach response plan can be developed – and continuously updated, as necessary – as without these, the business is essentially "flying blind in an invisible war".

What could be the consequences to not defending your company from threat intelligence processes?

Aside from a possible legislative, or regulatory financial impact on a business as a result of a cyber-attack, businesses are becoming increasingly concerned around both the financial and reputational impact to their operations and their environment. When considering the financial cost – as well as the potential revenue losses as a result of the reputational risk - involved with responding to a

breach, businesses need to consider all aspects of the breach, such as; the financial and reputational impact of repairing recovering, remediating and responding to the breach.

Although breaches do not always directly affect revenue or stock prices, businesses must also consider other possible effects of a compromise to their information assets. For instance, some attackers are driven by direct financial loss to the business or financial gain to themselves, whereas other attackers are motivated by a reputational agenda and building a name for themselves, while some just enjoy the thrill of testing their ability without a particular agenda or malice in mind.

Businesses therefore should not discount the high probability of being subject to a cyber-attack on the basis that they do not believe they are an attractive target – the reality is that merely by being a "connected" business, one is a target.