How to safeguard business in the burgeoning cybercrime era

A more connected world has lead to a more vulnerable world as more data is regularly exchanged between employees, clients, and suppliers as well as families and friends using technologies that were designed to share information, not to protect it.

© jes2ufoto via 123RF

There is a greater need for more human involvement and understanding when it comes to the use of technology.

A wake-up call

As the world reels from onslaught of the WannaCry ransomware attack, many are left asking “how could this have been prevented or at least more quickly contained?” While few of the global stock exchanges and other financial systems were affected, the long-term ramifications are yet to be understood. Experts say that despite the attacks slowing over the weekend, this respite will likely only be brief, and Microsoft itself, has warned that governments around the world should treat it as a “wake-up call.”

What companies must realise, is that fighting cybercrime is not just about having the right preventative software in place, it’s about having the right cyber risk management team and relevant, proactive plans and processes in place.

Shifting mindsets

Henry Peens, associate director: risk advisory, and Deloitte South Africa’s cyber leader, says that in order to become truly resilient to cyber attacks an organisation must shift its mindset and change how it views cyber risk and its potential impacts. “It is not just a matter of technology controls, and it’s not just the CIO’s responsibility,” says Peens, “It requires business transformation that broadens the scope of involvement at the top levels of the company, with a focus on overall business risk.”

Bringing people back into technology

By gaining a broad understanding of attackers’ motives and planning proactively by anticipating potential high-impact scenarios, organisations will be able to reprioritise and refocus their investments with the aim of mitigating likely outcomes.

Cathy Gibson, director: cyber risk services agrees, saying that it is critical to bring the right business and technical leaders together to evaluate organisational readiness: “The team must be able to develop a list of high-risk cyberattack scenarios that is relevant to their specific business. It is imperative that the members of the team collectively understand the businesses strategy, products, revenue streams, operations, technology, regulation, and the company's cyber risk program, to identify their both their crown jewels and the greatest risks”

Fast-moving cyber attacks wreak havoc worldwide
15 May 2017

An understanding of the organisations’ processes and activities, in conjunction with the underlying technical environment, will allow the team to model the threats to their specific environment and draw a more realistic picture of the direct and intangible business impacts should the organisation be compromised.

In doing so, the organisation can establish a reasonable level of investment in various areas of its cyber risk program. The reality is that an organisation’s budget will never be big enough to prevent every possible incident, but in following a risk-based approach, the organisation will be able to consider and proactively prepare for a number of possible attack scenarios and consequences.

Ensuring your readiness

If you base your organisation’s incidence response plan on narrow assumptions, it could fall short during a crisis. Once you have identified what is truly most important to the organisation, you are able to create a readiness plan that includes all the people needed to protect, defend, and recover those things should they be compromised.

Peens says that by establishing broad-based cyber-awareness and engagement across your organisation, you will improve your team’s ability to collaborate and react when the cyber incident alarm goes off.

Cyber readiness is not a reactive process, it is a proactive plan of defence. Whether they originate from within or outside of your business, and whether they are aimed at IP, trade secrets, operational disruption, fraud, or data theft, cyber attacks typically extend well beyond the technology domain and can have deep and long-lasting effects on an organisation.

Concludes Peens, “It is critical for every organisation to change the kinds of conversations they are having about cyber risk, and to institute some variation of a secure, vigilant and resilient approach that can ultimately improve their ability to survive and thrive in the face of increasingly likely cyber attacks.”