dimension data

accelerate your ambition

The new cybersecurity: *enabler of innovation*

For as long as there have been connected networks, the focus of IT security has been on controlling access to enterprise data and resources. While perfectly understandable, this is by definition a defensive posture.

As networks become more complex and enterprises grow increasingly reliant on digital business, it is imperative that IT adopts a new approach to security that safeguards assets while also facilitating transformation.

Fortunately, many enterprises are moving toward embracing a proactive, risk-management strategy where cybersecurity becomes an enabler of innovation and an accelerator of digital business. In a 2015 CSO survey, 75% of responding chief security officers said they had spent more time in the previous three years advising senior business executives on security issues than before, with 80% expecting the amount of time spent talking to the business side about security to increase further in the next three years.[1]

'Security is no longer an afterthought, but a business issue,' CSO concluded in its survey report. 'As new projects/processes are implemented, executives are concerned about security and thus are looping in their CSOs to help make business decisions.'

Outmoded architecture, outmoded security

Legacy IT systems simply cannot support the competitive needs of enterprises in the digital economy, where mobility, agility, flexibility, and scalability are the key drivers of success.

'In the digitised economy, successful organisations are building agile and adaptive technology infrastructures that allow real-time collaboration, data sharing, and superior customer engagement.'

Digital data is generated, transmitted, and received by an expanding number of devices, including smartphones, tablets, wearables, medical equipment, and the Internet of Things. The challenge of storing, managing, and providing reliable and rapid access to this data and backend IT services gave rise to cloud computing. This has forced IT professionals to reconsider their fortress mentality by accepting (albeit reluctantly) that enterprise data, business applications, and even IT infrastructure can be secure in a remote, hosted location.

In the digitised economy, successful organisations are building agile and adaptive technology infrastructures that allow real-time collaboration, data sharing, and superior customer engagement. These super-networked digital enterprises require that a myriad of networked devices, systems, and people are able to easily and safely share data and use remote services. But accomplishing this is difficult if not impossible if enterprises retain a device-centric, perimeter-based view of security that relies on rigid controls and firewalls to prevent less-secure systems from connecting with databases and services.

A new paradigm for risk management

The balancing act is not easy. Retail, for example, surpassed financial services as the top target for cybercriminals, according to the NTT 2016 Global Threat Intelligence Report. To survive, however, retailers in the digital, mobile economy have no choice but to allow customers and partners access to backend services and systems.

[1] CSO State of the CSO Survey, IDG Research Services, 2015

‘To survive, however, retailers in the digital, mobile economy have no choice but to allow customers and partners access to backend services and systems.’

Similarly, healthcare providers are sharing more data than ever before in order to improve collaborative care, while increasing patient engagement through portals and mobile apps that give health consumers a way to digitally check information, pay bills, and make appointments – all of which must be accomplished while meeting stringent HIPAA rules for protecting patient privacy. Returning to paper health records and phone-based data exchange is not a viable option.

What’s needed for these sectors and others in the connected world of the future is a proactive, managed approach to cybersecurity designed to protect entire IT ecosystems – regardless of the types of systems, apps and devices that are connected to the network – now and in the future.

A proactive cybersecurity strategy that enables enterprises to anticipate and thwart breaches before they occur isn’t possible without the right strategy, tools, and skill sets.

That combination, though, is hard to come by even in the largest enterprises. In addition, most enterprise IT departments are busy enough trying to keep their networks running while supporting the goals of the business.

That’s where managed security services providers can prove invaluable. An experienced managed security services vendor will have IT pros with security expertise in every part of the stack.

And in the event of a breach, they can deploy Computer Emergency Response Teams to quickly eliminate vulnerabilities and begin recovery.

Enterprises that are able to manage risk in a way that protects data as it travels from endpoint to endpoint – no matter the origin or destination – will gain a competitive advantage because they will be able to innovate without unnecessarily exposing their data or networks to cyberthreats.

Partnering with a managed security services vendor allows enterprises to confidently explore new opportunities in the mobile, data-driven economy without exposing their digital assets to harm.

Dimension Data’s cybersecurity managed services help digital enterprises manage risk intelligently and cost-effectively. To learn more, visit this page.