BIZCOMMUNITY

Security in the business context

By Jayson O'Reilly

16 Dec 2014

The past few years has seen information security undergoing a radical transformation. A discipline once seen as no more than a necessary evil, security tools have become an integral part of the business strategy.

There is no doubt that innovation is now a vital part of the business strategy too, and at the core of all critical innovations is the secure exchange of information.

Reliant on data

Information is the currency of the new economy. All businesses are reliant on the data we create and share, and at the same time, we find ourselves at war with unseen criminals who are trying to steal that information. The goal of any security business is to protect the data and manage the risk.

CSOs who are succeeding, are driving closer relationships between business innovation and security, and a large part of this is having a good security strategy in place.

Without the strategy, business innovation will not happen, and the company will be at risk. Moreover, too often we see the case where the business and security teams operate as disparate entities, and security is applied as an afterthought, instead of being built into the strategy from the ground up.

What they don't realise is that it's far more effective and far cheaper to build security in from the start, rather than slap it on at the end. Security practitioners need to work with the business, to understand what the key business objectives are, and ensure that security is built in accordingly.

Find out what the risks are

A good place to start is to take a risk-based approach. Understand what the risks are, and how important information security is to the business. The understanding of risk needs to be an element in all investments and in all operational processes. This needs buy-in from the executive team or it will be entirely ineffective.

Companies need to find the balance between what they are prepared to spend on security tools and measures, versus an acceptable level of risk. Risk will never be wiped out entirely. Decide what the most valuable business assets are, and start protecting those first.

Determining what the most sensitive and valuable data is, and where it lives, is the first step towards preventing data loss, as is determining who has access to that data, and ensuring principles of least privilege. Understanding risk is crucial when deciding which tools and measures to implement to prevent data theft or loss, and it is now that security practitioners need to balance the amount they are willing to spend with the amount of risk they are willing to accept.

Business must be able to answer questions around what controls should be implemented, who is allowed to access, move and edit data, as well as what to do should these policies be ignored, or should there be an attempt to change or send this data outside the organisation. These are all elements to establishing what the reasonable and acceptable risk threshold is, and can be quite the balancing act between costs, risks and not smothering innovation and productivity.

Ultimately, it is about supporting the main business initiatives while meeting compliance requirements. Security must be seen in the business context.

ABOUT JAYSON O'REILLY

As MD of @Vance Cyber Security, Jayson O'Reilly is responsible for maintaining agility, putting clients first, and addressing cybersecurity challenges through thought leadership - and most importantly, ensuring that customers do not subscribe to the madness of doing the same thing while expecting a different result.

- Risk, security teams must collaborate - 28 Dec 2018
- Why privacy and security matter - 23 Nov 2018
- Next-generation firewalls demand built-in intelligence - 27 Mar 2015

View my profile and articles...