Why privacy and security matter

By Jayson O'Reilly

23 Nov 2018

The 2018 Data Threat Report from Thales and 451 Research found that only 13% of organisations will not be impacted by privacy regulations. This is a big drop from the 28% of companies who said the same in 2017.

With the number of data breaches increasing at an exponential rate, it's become apparent that no organisation is safe. That's without mentioning wider issues around how organisations are using people's data. When it comes to cybersecurity and data privacy, there are almost endless scenarios to consider.

Both cybersecurity and privacy are categories of corporate risk, and they must be addressed to meet compliance requirements and minimise the possibility of brand damage in the event of a breach. However, many companies see corporate risk as something that needs to be managed through the minimum budget required to address it.

Privacy and data security best practices

The stakes have never been greater than they are right now with respect to the collection, use, retention, disclosure and

disposal of personal information. A number of agencies, including the National Institute of Standards and Technology (NIST), have been promulgating updated guidelines and recommendations for privacy and data security best practices in a variety of industries, and companies are being encouraged to establish internal policies and procedures.

A new approach to better information security

Jayson O'Reilly 5 Oct 2018

These policies should include a top-level information security and privacy policy, a risk management programme, an acceptable use policy, access compartmentalisation, communications monitoring, breach reporting, a document retention policy and outsourcing policies.

While it may be easier said than done to implement new policies and best practices, companies are faced with the additional challenges of evaluating and deploying new technologies that simultaneously may both hinder and help privacy initiatives. For example, blockchain provides the ability to record transactions in a decentralised fashion but raises complex issues in terms of privacy regulations.

Integration of IoT

The IoT is adding even more complications. As devices of all kinds become increasingly integrated with IoT, so does information, all kinds of information, including intellectual property and personal information. Given this backdrop, it is often easy to get lost in the details of cybersecurity and privacy and forget why security and personal privacy matter in an increasingly digital world.

Privacy is important because damage to brand reputation equates to customers walking away from a company and the loss of revenue. It is important because people expect the companies they interact with to be protecting their data.

It is customers who are the ones applying pressure when it comes to data protection, and regulations like GDPR are transforming consumer data best practice across all sectors. They are also playing an important role in placing the power firmly back where it belongs: in the hands of the consumer.

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...