Non-compliance: leading organisations down the rabbit hole

By Simeon Tassev

10 Oct 2018

PwC's latest Global Economic Crime and Fraud Survey 2018 ranks South Africa as the second most targeted country in the world when it comes to cyber attacks. The survey also shows that many organisations are preparing for the inevitability of cybercrime, with over 25% of respondents believing cybercrime will be highly disruptive and impactful on their businesses.

Simeon Tassev, is managing director and QSA at Galix Networking

Although cybercrime is destructive, the increase in incidents is achieving one positive: people are finally talking about the risks, understanding the dangers of their organisation's face, and putting strategies together to prevent cyber attacks. One of the ways businesses can achieve this is to ensure they comply with regulatory standards.

The role of compliance in preventing cybercrime

With the General Data Protection Regulation (GDPR) in full effect, and the pending Protection of Personal Information (PoPI) Act, becoming compliant is imperative for businesses. These regulations incorporate obligations that organisations need to meet with regards to the safety, privacy and security of personal information. They specifically outline requirements for dealing with data storage, incident responses and creating security awareness which, in turn, has created new roles within the business, such as data privacy officer and security response teams.

Although these regulations can be relatively vague, and often don't outline precise tools or measures that businesses should be taking, organisations who interpret them by doing the bare minimum are likely to find themselves on the receiving end of a data breach and having to disclose this to the world. Both GDPR and PoPI demand that businesses be transparent about data breaches by taking the necessary steps to advise any relevant parties of data loss, as well as what they are doing to recover or respond to an attack.

Basic cyber hygiene practices that go a long way

Doros Hadjizenonos 9 Oct 2018

When it came to the recent Liberty data breach - their quick notification to customers and third parties was met with alarm and generated a very public outcry, putting them at the centre of a media storm which likely cost them a fair measure of business.

However, it was also proof that Liberty's compliance strategy is mature, and that they are prepared to adhere to the requirements laid out by both GDPR and the PoPI Act. It showed that they were proactive in alerting customers and related parties of the breach, pre-empting speculation before they had to read about it in the news.

It's important to note, at this point, that no organisation can be 100% protected against cybercrime. For a large organisation, the challenge of protecting data becomes even more complex and enormous. Every business has the capacity to improve – and performing a compliance exercise helps them achieve the best measure of where they are and what they still need to do.

Do we need to comply with all regulations?

In a nutshell, yes, if the provisions laid out in a regulation touches your business. However, there are standards which make it easier to comply with various regulations – standards which encompass most of the requirements of requirements laid out by GDPR and PoPI, and which offer more structure in the face of the vagueness of some of the regulatory conditions.

For example, Condition 7 of the PoPI Act deals specifically with the security safeguards that businesses should have in place. However, it does not stipulate specifics, and terms like 'appropriate' and 'reasonable' leave the condition open to a measure of interpretation. This provides loopholes for businesses that wish to do the bare minimum. It also leaves many businesses wondering where to even start…

Avoiding the high cost of poor cyber resilience

Brian Pinnock 2 Oct 2018

Complying with a more mature, rigorous standard such as The Payment Card Industry Data Security Standard (PCI DSS), can ensure that there are no loopholes, help you better comply with other regulations and help to improve overall data security. More importantly, it outlines steps and provides frameworks for businesses to follow so that they have a better idea of where to start, and how to cover all angles.

Compliance is not an easy task to undertake and the larger the business, the more difficult the task. Working hand in hand with a partner who understands an organisation's specific needs and constraints can ensure that a business not only covers all their bases but reaches compliance that much quicker.

A partner will be able to help a business identify which processes and controls are already in place, what they need and how they can be incorporated to form a holistic strategy. They will also help businesses to effectively combine their people, processes and technology in such a way that compliance becomes an almost natural progression, rather than a sudden change.

Compliance is critical, and will soon be expected of every organisation within South Africa and across the globe. Starting now is important; starting with a partner makes it easier.

View PwC's Global Economic Crime and Fraud Survey 2018

ABOUT SIMEON TASSEV

Simeon Tassev is the director of Galix, a reseller of Mimecast Solutions in South Africa
- Cybersecurity awareness is no longer a generic exercise for business - 7 Feb 2023
- Understanding cybercrime's true impact is crucial to security in 2021 - 3 Feb 2021
- What can we do to stop ransomware attacks on governments? - 16 Dec 2019
- Cyber security professionals are no Darth Vader - 19 Mar 2019
- How to create a cybersecurity culture - 16 Jan 2019

View my profile and articles...