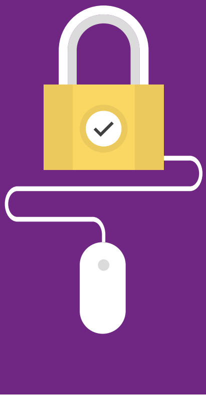
Cyber-security is more than just IT

June 2016



Preparing an organisation for cyber attack requires more than just firewalls and passwords, with strategy and a proactive cultural mindset also being essential factors.

If organisations aren't talking about, protecting against, or prepared to deal with a cyber-security threat on a humanistic level, they are fighting a losing battle, says Stan Gallo, Partner, KPMG Forensic.

"Cyber security is strongly on the radar following the Federal Government's 2016 Cyber Security Strategy, which announced an increased focus on information sharing with business," he says.

Gallo says the last in-depth cyber security review was in 2008 – prior to the introduction of iPads and only a year after the iPhone was first introduced. Since then business has increasingly leveraged technology to increase competitiveness, efficiency and international reach.

"Technology has evolved tremendously, as has the level and complexity of cyber attacks" Gallo says.

Gallo presented on '*Latest developments in cyber security – Insights into what organisations need to do to protect themselves*', at CeBIT 2016, held in Sydney from 2-4 May. He says organisations need to take a practical and holistic approach to dealing with this risk.

"This means being on top of technology development, and incorporating the human element to develop a cyber security mindset in employees, driven from the top down."

He warns the damage of a cyber breach can be both financial and reputational.

"Typically, when we see the money go directly offshore, once it is gone it is very, very difficult to recover. My experience in the last year is that once sent, the only funds that have been recovered are when the banks picked it up early and flagged the transactions as suspicious, halting the transaction in mid-flight."

The scope of threat

Executives need a full understanding of the risks at all levels – from wayward team members to the public, third-party providers, contractors and suppliers. Cyber hackers are not just seeking money, but many aspects of a company's data, including customer information or inside knowledge into business strategy.

Organisations need to understand the breadth of information they hold and how it could be powerful in the wrong hands.

"Is it customer information, user IDs, passwords and other personal information? Is it other confidential information – for example a law firm that holds details about merger and acquisition deals that could be used to unfair advantage?" he says.

While many organisations focus on technical controls, they can fail to focus on the humanistic and cultural aspect of cyber security – particularly the role their own staff play.

"How do we get employees to understand they are doing this [cyber security] for a reason? How do we get them to think twice about those 'too good to be true deals', free USBs, odd emails or invoice scams that crop up and look legitimate?" he says.

What can organisations do?

Many organisations are still 'reactive' to cyber-crime, rather than on the front foot, Gallo says. To make this shift, it is important to understand what you are trying to protect and its value.

"Understand what controls you have in place. Link that to organisational culture and the psychology of the staff and other people who have access to the system including internal, and third- and fourth-party providers," he says.

Stan Gallo, Partner, KPMG Forensic

It is essential to have a risk management process, to understand the damage that could be caused by cyber attack, and to have a recovery and communications plan in the event a breach occurs.

"Software doesn't attack computers, people drive these attacks on computers. While it is incredibly lucrative it is not going to stop."

Sharing information about cyber attacks with other organisations could be beneficial, so that people are not trying to solve the problem independently.

"This information sharing needs to be coupled with IT controls and with a proactive cultural mindset. When those things come together we will have a more secure environment."

Contact us

Stan Gallo
Partner
KPMG Forensic
+61 7 3233 3209
sgallo@kpmg.com.au

kpmg.com.au

Download on the App Store

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

Liability limited by a scheme approved under Professional Standards Legislation.

June 2016. VIC N14116ADV