No room for complacency: The need for better cyber security

Insurance CEO Outlook

January 2018

More than three quarters of insurance CEOs see cyber security as more of an opportunity than a threat. And rightfully so. In fact, in my opinion, that number is surprisingly low.

Let's start with the obvious opportunity: cyber insurance. It has already become a booming business for many insurers and all signs suggest that policies and revenues in this area are climbing steadily. And it's not just commercial policies that are being written. Insurers are also exploring how they can extend their capabilities into new and emerging areas such as protecting the connected home, automated vehicles and personal information.

But cyber security is more than just an opportunity to create new revenue streams. It is also critical to maintaining existing ones. Indeed, any insurance company worth their salt is currently busy working to digitize their enterprise and create new front-end platforms to get closer to their customers. And that requires a keen focus on delivering really strong cyber security. Simply put, if you can't offer your customer a secure digital experience, you probably won't keep your customers.

In much the same way, a strong cyber security stance is also key to a wide range of other relationships and business requirements. Regulators, in particular, are increasingly focused on insurers' cyber preparedness and controls. So, too, are a wide range of other stakeholders including shareholders, boards, public interest groups and the media.

Not ready yet

So it is somewhat worrying that, according to KPMG International's recent survey of CEOs, more than half (57 percent) of insurance respondents said they were only 'somewhat' prepared for a cyber event. And only 26 percent said that cyber security is one of their 'top of mind' risks. This seeming lack of concern is reinforced by their investment expectations: just 28 percent say they will 'significantly increase' investment into cyber security over the next 3 years.

To be frank, my experience and my conversations with leading insurance organization CEOs suggests that these respondents must have been feeling particularly optimistic when filling out our survey. Certainly, every major insurer that I work with has already had an unexpected wakeup call and now takes cyber very, very seriously.

Some have suffered their own breaches. Some have learned from watching the experience of others and want to avoid a similar fate. Most recognize that, if they don't improve on their own, the regulators will do it for them.

> “Some insurers have suffered their own breaches. Some have learned from watching the experience of others and want to avoid a similar fate. Most recognize that — if they don’t improve on their own — the regulators will do it for them.”

Not an easy task

There is no denying that most traditional insurers face an uphill battle when it comes to cyber security. The reality is that insurers come from a classic paper-based business model that is struggling to make the jump into the digital world.

They are working in a difficult IT environment; many are running mainframes and systems that were developed in the 1970s and 1980s; most preside over a mess of legacy systems that have been tied together with fixes that are akin to duct tape and crazy glue.

They know it will take significant work to remediate their past issues. And it will take even more work to create the right long-term programs to properly protect their business from this ever-evolving and growing risk. Yet many are now starting to make significant progress on their journey to cyber readiness.

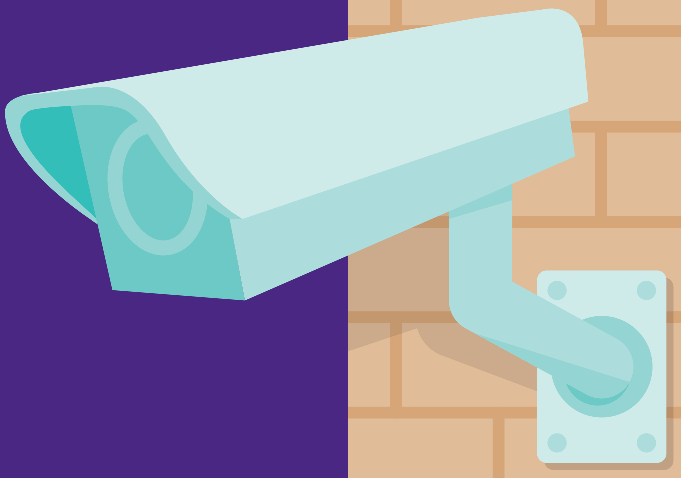
My work with leading insurance organizations suggests that there are a number of actions that insurers should be taking if they hope to thrive — or even survive — in the new environment.

Time for action

One of the most important steps is to **improve the understanding and awareness of the risk at the executive and board level**. Many insurers struggle to identify, articulate and measure their cyber risk in the current environment. And that means their boards and executives are not able to challenge the activities and plans being created by the business. In part, this requires boards and executives to work closely with their ‘three lines of defense’ to improve awareness and understanding. But it also requires boards and management teams to have regular discussions and debates on the topic rather than simply waiting until an issue arises or a regulator asks questions.

Boards and executive teams should also be taking steps **to prepare for the likely eventuality that they will suffer a debilitating attack**. They should be running regular ‘desktop’ exercises that simulate a cyber-attack and they should be thinking carefully about how they will react and respond. Will they pay a ransom? Will they disconnect their systems from the internet until investigations are concluded? What will be the impact on employees, customers and shareholders? Conducting these exercises in a safe and controlled environment will allow decision-makers to move quickly and decisively when an attack does occur.

At the same time, those responsible for cyber security within the organization (likely the Chief Information Security Officer or CISO) should be **working closely with the business to identify and assess the risks, goals and solutions for cyber security**. They need to help the business identify which programs and platforms are critical to the running of the business and then work with the business owners to understand the vulnerabilities of each. Then they need to be having mature conversations with the business about what needs to be done, and at what cost, to secure those systems without reducing business flexibility.



To the secure goes the spoils

My work with leading insurers and other financial services organizations clearly indicates that there are no quick fixes or silver bullets. It is a journey that will take time, resources and patience. It will require boards and executives to have enough awareness to be able to challenge the decisions being made by the business. And it will require the business to be in the 'lead'.

But let's also remember that the opportunities created through a strong cyber position and robust controls are massive and vital to future growth. You simply cannot win in today's environment without it.

I believe that the most successful organizations going forward will be the ones that are able to create a smart balance between corporate opportunity and operational risk. They will be the ones that are able to protect their reputations and grow their business. They will be the ones that build trust with clients and regulators. And they will be the ones that are best positioned to seize new market opportunities when they arise.

So if your organization is not finding that balance, I'd humbly suggest that it's time to start rethinking your approach to cyber security.

Contact

Matthew Martindale
Partner
Cyber Security, Financial Services
KPMG in the UK
T: +44 20 76942989
E: matthew.martindale@kpmg.co.uk

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor 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.

Designed by Evalueserve. Publication name: No room for complacency: The need for better cyber security. Publication number: 135114-G.
Publication date: January 2018