Facing the cyber threat in the insurance sector

Insurance CEOs may need to go back to basics to ensure their cyber investments are protecting against the right risks in the right way.

Insurers confidently deal with massive risks every day. But when it comes to their cyber security, they are not so confident. According to a recent survey of more than 100 insurance CEOs, less than one-in-five believes their organisation is fully prepared for a cyber-event. And 42 percent think cyber security is their most pressing risk, far outweighing their concerns about other key risk areas such as regulatory risk.

Clearly, cyber security is at the very top of the executive agenda. And our data suggests that CEOs plan to devote significant investment towards improving their cyber security stance over the next few years.

While this is certainly encouraging news – more investment is urgently needed – our experience working with large insurance organisations suggests that CEOs may need to take pause to rethink their cyber security program if they hope to achieve real results from their investments.

The pressure rises

Insurance CEOs have good reason to worry. In comparison to other financial services sectors – banking in particular – the insurance industry has lagged in cyber investment, focus and capabilities. In part, this is due to urgency: banks were getting pummelled by cyber-attacks and needed to move quickly to protect their reputations, customers and bottom lines. The cyber war has traditionally been much quieter on the insurance front.

All signs suggest this is about to change. As other financial sectors become more secure, attackers are moving on to find weaker targets and this is bringing insurance companies into the firing line, and the stakes are very high as insurers hold enormous amounts of data on individual health and personal property for example. At the same time, regulators have started to ask insurance CEOs difficult questions about their cyber resilience position. And they have not always been happy with the answers they have been receiving. Letters have been flying between CEOs and regulators.

Insurance CEOs also increasingly see cyber security as a basic requirement for doing business. Many are now starting to develop cyber insurance policies, seizing the opportunity to better mitigate losses due to customer cyber events. But they are recognising that – to be a credible player in the cyber insurance market – they need to start by getting their own house in order. At the same time, they are realising that shifting customers to digital channels depends on maintaining customer trust and that, too, requires strong cyber security discipline.

As a result, forward-looking insurers are now working to improve their capabilities and create alignment between their internal and external cyber risk management activities.

Gaps emerge

Let us be clear: insurers have not been ignoring their cyber security responsibilities. The vast majority have made significant progress over the past few years and most now boast important capabilities, controls and processes. They are certainly not an 'easy target'. But they are also far from secure.

Likely the greatest challenge facing insurers comes down to a lack of basic discipline: key security patches are not implemented; access management (particularly off-boarding of employees and contractors) is not controlled; information and IT asset registers are out of date; and rapidly emerging threats are not being properly tracked. This is largely about keeping up the rigour around the controls and processes that are already in place.

Many insurers are also struggling with inconsistent and fragmented cyber security capabilities across lines of business and markets; often the legacy of years of M&A activity. So while, in most cases, cyber capabilities have been decentralised, resulting in significant control challenges at the Group level, our experience indicates that cyber security must be managed at a centralised level (allowing for adaptation by business units and markets to suit unique circumstances and requirements).

Most insurers will also need to focus on honing their response and recovery capabilities. To date, most have been lucky to avoid a full-scale security crisis. But this has allowed some organisations to grow complacent and let their plans and processes become stale. Far too few organisations run regular drills or maintain updated roles and responsibilities.

Time to get serious

If insurers are serious about improving their cyber security position, the first thing they need to do is spend some time assessing the current situation. They, and their executive committees, must improve their awareness of the risks, the existing controls and the gaps in their position. They must understand the urgency of the situation and articulate that urgency across the organisation. And they must put cyber security at the top of their personal agendas.

Before investing significant sums into cyber security, our experience suggests that insurance CEOs may want to focus on five key areas:

1. **Ownership:** Cyber security is a business issue, not an IT issue. CEOs will need to find ways to ensure the business is taking ownership of cyber security and that discipline is being maintained. Some of the more successful insurers have elevated their Chief Security Officer to report directly to the COO, creating clear line of sight between the business and the risk.
2. **Capabilities:** Clearly, new and improved cyber security capabilities will be required. But CEOs will also want to assess their current 'pockets' of cyber security excellence and work to ensure those capabilities and best practices are shared across the enterprise. Leading insurers are starting by ensuring that their existing capabilities are being properly utilised.
3. **Awareness:** Improved awareness from the C-level down is key. In particular, insurers will need to focus on improving their understanding of their ecosystem of third party participants – non-affiliated agents, outsourced service providers and other non-employees with access to data – to manage their risk in a consistent manner.
4. **Organisation:** CEOs will need to work with their business leaders to understand the right balance of centralised and decentralised services to most appropriately meet the cyber risks in each market. Creating the right structure for robust and consistent cyber security is key to fielding a responsible (and defendable) response.
5. **Preparedness:** Successfully activating a response and recovery program takes practice, commitment and clear lines of responsibility. From 'red teaming' exercises that simulate the way an attacker behaves through to improved employee training and more frequent drills, CEOs will need to carefully consider how the ensure their organisation remains prepared.

Set the pace or risk falling behind: Insurance CEOs speak

This article is from our *Set the Pace or Risk Falling Behind* article series.

In 2016, KPMG interviewed more than 100 CEOs at some of the largest insurance companies around the world. We asked them about their greatest challenges and their business strategies. We talked about their investments into growth and innovation, and explored their greatest risks.

In our article series we present the findings of our research and provide context and ideas to help insurance executives make the most of the changing environment. The series of unique articles focuses on key themes such as transformation, data and analytics and customer-centricity and offers new ideas and actionable tips in emerging areas such as automation, partnerships and cyber security.

To read other articles in the series visit kpmg.com/au/insuranceceos

Contact us

Martin Blake
Partner, Insurance Sector Leader
T: +61 2 9335 8316
E: mblake@kpmg.com.au

Jackie Sharp
Insurance Client Director
T: +61 2 9335 7418
E: jackiesharp@kpmg.com.au

Gordon Archibald
Partner, Technology Risk
T: +61 2 9346 5530
E: garchibald@kpmg.com.au

kpmg.com.au

March 2017. VIC N15214LOB.