Insurance Times

HOT TOPICS Ardonagh | Broker Survey | Claims | Discount rate | Insurtech | Top 50 Insurers | Brexit | M&A | Cyber

Silent cyber: the danger lying buried in your insurance policy

6 September 2018

Expert view: ThoughtRiver's chief legal intelligence officer Martin Davidson (pictured) looks at how AI can help cyber insurance

The analysis of insurance policies has traditionally been manually completed using small sample sets, making it open to inaccuracies, with a long and expensive process to manage variations. With artificial intelligence technology, large volumes of policies can be reviewed at one time using proven, reliable science, providing insurers with a more accurate picture of where their exposures lie, most notably cyber.

Cyber risk is a growing problem. Estimated to cost the global insurance industry more than $2.1trn in losses every year by 2019, it's a problem that's not going to go away any time soon.

While most of the risks associated with cyber are obvious, including cyber liability and data breaches, it's only when companies look more closely at the small print in their insurance policies that they realise they have a problem. Given that cyber is a relatively new risk, many insurance policies will not have cyber coverage explicitly written into them. This phenomenon is known as 'silent' cyber or non-affirmative cyber risk: potential cyber-related exposures contained within an insurance policy which are not expressly covered or excluded. Up until now, most insurers have simply taken samples of their policies to identify these risks, but because it's impracticable to check every single policy, particularly with a large portfolio, there's a huge margin for error.

Failure to pick up on these exposures can be catastrophic. In the worst case scenario insurers can be saddled with billions of pounds in losses or even wiped out by a big event that they didn't expect their policies would respond to.

An example of this would be a cyber attack on an industrial plant's control system that results in a boiler exploding, causing widespread property damage and business interruption losses. If the company wasn't explicitly covered or excluded under its policy wording, its insurer could be on the hook for multi-million or even billion-pound claims. Worst still, a single attack affecting many companies can trigger multiple policies that were not intended to cover cyber, resulting in large losses all at one time. Worse still, recent research has revealed that most companies are woefully unprepared: 72% of bosses surveyed in KPMG's Global CEO Outlook said they are not ready for the cyber security threat, while Allianz estimated in 2016 that 60% of Fortune 500 firms lack any coverage for cyber attacks.

"Data security and intrusion is a far bigger issue than it was even five years ago," said Tim Pullan, founder and chief executive of one of the pioneering new technologies, ThoughtRiver. "Alongside the corporate scare stories such as the cyber attacks on Sony and Target, the biggest problem for insurers is just trying to quantify the risk."Added to that you have the increased regulatory crackdown on issues such as silent cyber. But that has only brought with it a heightened awareness of the problem and how it should be addressed."

Among the lines most likely to be affected, according to PwC, are professional liability, property and aviation, as well as casualty. Meanwhile, a scarcity of historic data and the rapid evolution of cyber as a risk make it increasingly difficult to quantify the extent of the problem, not least within the insurance policy itself. As a result, the PRA in July last year put out a Supervisory Statement urging insurers to tackle silent cyber exposures through more robust wordings and exclusions, specific limits and rating. Lloyd's of London has also called on its syndicates to assess the impact of various cyber attack scenarios to gain a "consistent view of accumulation risk – including silent cyber".

That's where revolutionary new artificial intelligence software comes in. In the case of ThoughtRiver, the insurer uploads its policy portfolio using the automated technology to ask cyber related questions which identify and quantify exposures before producing a report – all at the push of a button.

The fact that it can check every single policy held by a company both quickly and efficiently means that it is far more accurate than current estimation methods. In this way it can help not only insurers and reinsurers who may have latent cyber exposure, but also brokers, and their clients struggling to get to grips with their risks and insurance policies. “This new technology enables insurers to be more scientific about the way they manage their risk across vast volumes of policies,” said Pullan. “There’s also significant opportunity for companies to understand their exposures and where they may have gaps in their policy for which they need additional coverage.

“Among some of the most common areas of exposure are in data theft and property liability. But that’s not to say there may be other areas that a company had never previously considered could be exposed to this risk.” ThoughtRiver’s customer data is held securely on dedicated databases, while subscription accounts are located on dedicated virtual servers. Access is controlled and restricted.

Developed over three and a half years and launched last year, ThoughtRiver is commercially available for insurers, reinsurers and brokers. For more information or to book a demonstration visit www.thoughtriver.com.