A policy on risk

The cyber insurance industry is holding companies to a high standard, say Brunswick's WENDEL VERBEEK and SOFIA MATA-LECLERC

A spate of high-profile breaches in recent years has led to a booming market for cyber insurance. PwC predicts the global market will reach $7.5 billion by 2020. That kind of growth brings considerable influence and is making the insurance industry a significant force that is reshaping expectations for companies around cybersecurity preparedness.

"Three years ago, cyber insurance wasn't that common," says Kristy Harris, Manager of Corporate Insurance at Southwest Airlines. "It's now come to the forefront in response to these high-profile breaches."

According to Moody's Investors Service, more than 50 insurers globally offer standalone cyber coverage. That number is expected to grow as companies, and by extension underwriters, increasingly focus on mitigating the risks associated with a breach.

In some cases, underwriters have had to scramble to catch up with their clients in understanding the complex operations that make cybersecurity protection effective. Increasingly, however, cyber insurers themselves are driving the discussion, wanting more sophisticated security plans tailored to each company's risk profile.

"A few years ago when we were talking to cyber insurance underwriters, we found that some didn't differentiate between company business models, or take into account the different risks," Harris says. "They have come a long way since then. They are learning to underwrite the risk better, getting more comfortable assessing risk. And we're seeing more expansive coverage as a result."

Data breach insurance is fairly narrowly defined, but can cover forensics, communications and legal support, network interruptions, and fallout from lawsuits. "People think cyber insurance will help cover anything digital, but that's not the case," says Harris. "The big 'a-ha' moment for us at Southwest was trying to insure against someone stealing our loyalty reward points. Theft of assets is a crime loss – not a cyber loss. Psychological cons and impersonation losses aren't covered either."

> "Tell me more about how you are addressing risks culturally as you go. I am looking for companies who are investing in – and changing – behavior"
>
> **MARCUS BREESE**
> **Hiscox London Market**

Insurers' expectations are helping to drive cyber policy for companies. One of the first things a cyber underwriter will want to see is a security incident response plan that goes well beyond IT. Specific levels of responsibility should be included, with triggers to ensure the right people are involved at the right time.

"I get concerned when it seems that a client's IT guys are kept completely separate, in a dark dungeon somewhere," says Laila Khudairi, Head of Cyber at insurer Tokio Marine Kiln. "In the event of a breach, there may not be a proper escalation process."

An effective cybersecurity plan needs to be able to involve the entire company, says Marcus Breese, Cyber and Professions Line Underwriter for Hiscox London Market. "Tell me more about how you are addressing risks culturally as you go," he says. "I am looking for companies that are investing in – and changing – behavior."

It is critical that insurers see multiple stakeholder perspectives represented – customers in particular. If affected parties feel they have been treated well, they are less likely to sue or to take their business elsewhere, Khudairi says.

Since cyber's risk landscape shifts constantly, a security plan needs to be regularly put through its paces, says Erica Constance, Senior Vice-President and cyber expert at Paragon International Insurance Brokers in London. "I would expect companies to test these procedures annually, at least," she says. "Things are going to change."

Regulation is one area that is already changing. The 1998 UK Data Protection Act "was created before the first text was sent, so it doesn't take into account that our lives are now played out online," Constance says. In 2018, the EU General Data Protection Regulation will come into effect, and companies active in Europe will be required to report certain breaches and review their practices.

All the pressures companies face are echoed by cyber insurers. "Crisis communications preparedness is a larger consideration, and it affects more than the policy's premium," Khudairi says. "It ultimately determines whether or not we will underwrite the risk."

WENDEL VERBEEK is a Director in Brunswick's London office advising on financial and crisis communications. **SOFIA MATA-LECLERC** is a Director in San Francisco, specializing in crisis, cybersecurity and corporate reputation.