Is cyber insurance relevant for my client yet?

by **David Dickson**
Safeonline

In a word, **yes**! However, one word would not make for an interesting article and you could be excused for branding me as yet another insurance market commentator, espousing the importance of this 'emerging coverage.'

I do believe, however, that the amount of attention that cyber risk is attracting in the media is justified and that we are fast approaching the 'perfect storm' for cyber insurance. Not only are attackers becoming smarter, increasingly agile and more commercial with their dark-trade, but global regulatory frameworks and increased public perception about the importance and integrity of privacy mean businesses will need to proactively respond. Cyber security protocols and protections will need to be prioritised, and businesses will need to also plan for their own version of the perfect storm; which can leave companies vulnerable to irreversible financial and reputational damage.

Luckily for our clients, the insurance market continues to analyse, assess and respond. Despite that, there remains a few growing pains for everyone involved. Here are a few key things for to look out for in 2019 and beyond.

David Dickson

Heads up the technology, cyber and media insurance team at Safeonline; a specialist Lloyd's broker and Brokerslink member based in London, UK. Safeonline remains one of Lloyd's largest independent cyber brokers in terms of GWP into the market and have been product innovators and risk management specialists in this space since 1999. The team that David manages works with brokers and clients from around the world to assist with their cyber insurance placements; from the US and Canada, to Latam, the Middle East and South East Asia. Prior to joining Safeonline in 2015, David managed the international technology and cyber insurance practice at Howden Insurance Brokers in London.
As well as his commitments to Safeonline, David has served as an innovation advisor at Lloyd's Labs since its inception, and is an active committee member on the British Insurance Brokers Association's (BIBA) Cyber Focus Group.

The (continued) rise of Ransomware

Over the last few years, we have witnessed a meteoric rise in ransomware incidents and the propensity of these attacks to spread globally in a matter of minutes. That said, there have not been any incidents that have caused worldwide catastrophic losses – yet! Recent work by the Cyber Risk Management Project ('CyRim' 2019) estimates that global infection by a contagious malware could cost more than $193bn (almost twice the economic damage of Hurricane Katrina in 2005) and affect more than 600,000 businesses, both large and small; 86% of whom would be completely uninsured. Ransomware disseminates via infected emails, quickly spreading through connected networks and devices, encrypting data along the way, often bringing companies of all sizes to a standstill. Gone are the days of when this perpetrator was a human; these attacks are almost entirely done by bots these days. However, the human side of the hacker remains with many of the perpetrators setting up call centres to "help" companies re-gain access to their data via the payment of a ransom; usually via an untraceable cryptocurrency exchange. The costs for a company do not stop here though; the reduced productivity during this down time, the IT-costs involved with repatriation of data and system-integrity, along with the supply-chain disruption and reputational damage all weighs heavy on the mind and balance sheet of the victim's business.

The adage of "it's not a question of 'if' you get hacked, but when" remains true. Businesses need to ensure they are better prepared for ransomware attacks. From preventing the likelihood in the first place, through intensive employee awareness schemes, to ensuring any 'downtime' is minimalised through effective and regularly tested back-ups and by putting the right type of cyber insurance in place to respond efficiently to an attack.

Cyber insurance policies have evolved to include 'pre,' 'during' and 'post' event services. Some policies provide businesses with measures to help quantify the frequency and severity of a company's cyber risk. Other policies come with free or discounted access to other risk management tools, such as military-grade encrypted back-up providers and/or network monitoring tools. It is fair to say that cyber insurance is moving away from just being a response and remediation policy, towards being a more tangible risk management-tool. I expect this evolution to continue in 2019 and beyond.

2018 – a huge year for privacy regulation

The General Data Protection Regulation (GDPR) took effect in May 2018 and has already been instrumental in changing the way people, companies and governments appreciate data privacy. Google (January 2019) has been the recipient of the first major fine under the GDPR (c. €50m) and we can expect further fines and penalties in the near future. It is not just the EU who are changing the dynamics of data privacy though; within the last twelve months, at least ten other countries have moved to implement similar laws, including: Brazil ('GDPL'); Australia ('NDB scheme') and Canada ('PIPEDA'). In the US, California, who are often seen as the pioneers of data privacy regulation, will also implement GDPR-like stringent measures in their Consumer Privacy Act of 2018, when it takes effect in 2020. Cyber insurance often affirmatively offers coverage for regulatory fines, penalties and investigations, where insurable by law. Whilst the insurability of these fines and penalties will likely be established in the courts, cyber insurance is still active in helping companies prepare and evaluate their business practice in light of the new regulatory climate. Mandatory breach notification is likely to affect most companies worldwide, regardless of where they are based or operate, however most businesses are still woefully unaware of what they would and should do, in the event of a data breach: *Who*

to notify? How to notify? Who should we call? Lawyers? An insurer? An IT security company? Whether businesses like it or not, these are the questions that they will have to answer should they have an issue. Prudent businesses will look to insurance providers to help them to answer these questions and for risk awareness, management and transfer.

> “It is fair to say that cyber insurance is moving away from just being a response and remediation policy, towards being a more tangible risk management-tool. I expect this evolution to continue in 2019 and beyond.”

More players, more capacity, more coverage

When our CEO, Chris Cotterell, started Safeonline in 1999, he was one of only a handful of insurance brokers in the world selling cyber insurance; and there were fewer than five insurers offering cyber products. As we have become increasingly reliant on technology, both at home and at work, the opportunity for crime and the vulnerabilities we face have proliferated. The insurance market has responded as the risk emerged and grew. As such, today there are close to 200 capacity providers across the globe, including insurance companies, Lloyd's syndicates and MGAs; most of whom claim to have a 'market leading cyber product.' There are also more brokers (from those who admittedly "dabble" in the coverage, to full on specialists) than I can count. In the last five years or so, the increased competition across the globe has caused the market to dramatically soften, causing prices to drop and coverage to broaden. The average cyber policy of today is incredibly different to the first iteration in the late 1990s; focussing primarily on 'internet liability.' Today, cyber policies continue to evolve at almost the same speed as the threats and crimes against which they are aiming to protect. That said, the industry still seems somewhat undecided on whether 'cyber' should be treated as a product or a peril. What this now means is that some insurers are starting to provide coverage such as contingent property damage and bodily injury in cyber policies, whereby this would usually be considered part of general liability coverage. The same can be said of social engineering and other types of 'digital crime' which can also be found in some broad property and crime policies.
To further confuse policyholders, some traditional business package policies are now extending to provide cyber extensions. This can cause conflict with stand-alone cyber policies; causing issues with sub-limited coverages, the possibility of two sets of breach-response and claims teams being involved in a loss, and potentially triggering 'the other insurance' policy condition. The message to cyber prospects and policyholders in 2019 and beyond needs to be clear. Do not be too prompt in disregarding stand-alone cyber policies in the wake of obtaining cyber extensions elsewhere. Many of these packaged policy providers will be inexperienced in handling cyber claims and might not have in place the rapid and streamlined response services needed.

For prudent companies, cyber insurance should be seen as a 'must have,' especially in light of the increasing and evolving risks, greater privacy legislation and growing number of coverage options. However, our role as client advocates and advisors is crucial and the message is clear; seek specialist coverage from specialist providers, via a broker who understands the client's needs and what the insurance providers can offer. The role of the broker for cyber insurance has never been more important and neither has the message we are communicating. If a business has a presence online, collects or processes data, and/or relies on a system or network to derive an income, then cyber insurance is absolutely relevant. With the tightening of privacy legislation across the globe, the continued evolution of cyber risks posing a threat to all, and premiums being at an all-time low, this is the perfect time for businesses to purchase cyber insurance. •