The malware maelstrom

Davis Kessler and Nadia Bagijn of Travelers reflect on the value that having a standalone cyber policy can bring to businesses navigating today's data-driven world

Q What does a strong first line of defence look like for firms in 2020?

A In our experience, cyber-security needs to start at the top. An overall awareness of cyber risks that emanates outward from the management and board level can serve to emphasise the culture of cyber appreciation and build that critical awareness.

Above all else, our experience, backed by numerous independent studies, shows that it is us – people – who are the weakest link. Human error is an ever-present threat. This is why staff training is critically important. However, training in a vacuum tends not to be the best approach. If you have employees who are trained yet don't really see the management taking a serious approach to risk control, there is a tendency for them not to follow suit. Whereas if they see that their leaders truly buy into the culture of cyber awareness, employees feel empowered to act in a more positive way.

In terms of cyber coverage and the insurance policy a firm may be interested in, it pays to be mindful of what a standard liability policy will and won't offer. Generally speaking, standard insurance covers that do not have a specialist cyber policy attached will leave gaps – most often on the first-party breach response side. This means that should you have an incident and need to bring in an IT forensics firm, this can quickly become costly, and expenses such as this generally are not going to be picked up under a standard liability policy.

Davis Kessler
Travelers

Following five years of private legal practice, Davis Kessler joined Travelers' product development team in the US in 2012 and quickly began focusing on cyber coverage issues. In 2018 he transitioned to Travelers Europe to help develop its standalone cyber proposition and has led the cyber-underwriting team since launching that product in May 2018.

Nadia Bagijn
Travelers

Nadia Bagijn is the head of financial institutions at Travelers. She joined the company in August 2016, having previously been an underwriting manager at Liberty for 18 months. Prior to this, Bagijn spent over 11 years with AIG in Australia, the UK and the US in various roles. She obtained a master's degree in corporate finance and banking from the University of Technology, Sydney.

The other crucial element that a dedicated cyber insurance policy will bring – particularly if you're a smaller or mid-market-sized firm – is the breach response factor. Cyber insurance is different from a lot of other lines of insurance in that it is not merely a pool of money that will pay loss but acts in a similar way to a service contract.

Cyber insurance policies will come with pre-vetted access to a number of expert providers who can guide customers in the event of a cyber incident. A good policy will come with 24/7 access to the right experts who know how to quickly identify and correct issues and get the firm back up and running. For example, if a customer's website has been brought down and is made unavailable, Travelers has relationships with vendors who specialise in mitigating this type of attack and are there to get the customer's website back online as quickly as possible.

A dedicated stand-alone cyber policy will provide cover that a professional indemnity policy does not provide – things such as offering access to the right vendors at a moment's notice after a breach. For instance, we have a 24/7 hotline our customers can contact. If there has been a breach, which leads to business interruption, then every minute matters, so having a vendor at your fingertips is valuable.

And, just as importantly, a separate cyber policy would have a dedicated limit to respond to cyber events. When a firm relies solely on their PI insurance, thinking that covers their cyber needs, they're not only leaving gaps in coverage, but they are at risk of drawing down their PI insurance limit, which they may need later for more traditional claims. This goes back to the point that companies need to be aware of their exposures, and what their existing insurance policies can and cannot provide.

Q Why will some companies not have the right insurance cover in place?

A I think there is a continued level of complacency and lack of appreciation on many levels. We have often seen a mentality of, 'It won't happen to me.' A lot of this comes down to an education gap, and it is the job of us as insurers and brokers to help close this gap.

Our experience, along with industry publications and government stats, show that firms of all types

and all sizes are getting hit with cyber fraud. Criminals are opportunists; if they can breach into a large bank the prize may be bigger, but they would need to breach much tougher controls. If it is easy to defraud a single employee at a small to mid-sized firm, that is a quick win. And that is what we see happening time and again.

These kinds of breaches can often be a case of one click and it's done, and this will go unnoticed for a while. We have seen some claims where this happens, and only then do customers begin asking about specific crime and cyber coverage and how it is going to respond to the likes of a cyber breach. I think it will take a while for risk and asset managers to truly accept that it can and will happen to them, and that they should have response plans – and the right kind of insurance cover – in place pre-incident.

Q What is the minimum level of cyber-security that firms should have, and how can they minimise losses if a breach does occur?

A It comes back to this culture of cyber awareness and the need for direction to come from the top. Employee training is certainly key and the right security is also important. When we are underwriting a prospective customer, we look at the human element and the security controls in place to ascertain what is sufficient.

For larger companies, such as banks, we would expect more robust controls in place and greater incident response preparation, such as hypothetical exercises that take you through a 'live' event. While smaller entities may be more constrained with their budget, they should not be complacent and should still take certain precautions. There are resources available to improve one's cyber-security posture online. We have free guides on our Travelers website, and there is also a large amount of government-created information.

In terms of resilience in the event of an actual incident, it comes down to preparation. Having a response plan, clearly defined roles and responsibilities, making sure the people who are going to manage in those roles know what they are expected to do, and knowing which third parties you need to contact are all important and relatively straightforward measures to have in place. And it may seem a bit counterintuitive in this digital era, but make sure you have the response plan available as a hardcopy; the plan won't be any use if it is only on electronic files and computers were to be locked down with malware.

> *With a specialist cyber policy, customers are able to get the right cover and access to the right expert help, meaning they can react better and faster in the event of an attack*

Q What are the common exposure areas likely to be in 2020?

A An area we are seeing a lot of claim activity in is ransomware. One of the best protections against this is to have good, secure backups in place. That way, if ransomware does infiltrate the defences in place, you can revert back to a safe place within your IT network. But all too often we see cases where the backups get impacted by the same virus, and then the company's whole network is impacted.

New data protection laws (focusing attention on an individual's privacy rights), the growth of cloud computing and social media, corporate 'bring your own device' policies, and business email all raise risk levels – and make dedicated cyber cover essential. If a company supports transactions made from its website, having mirrored websites would be something else we would also approve of.

This is especially true for hedge fund managers as they need to access information and be able to trade immediately. Regaining access to their system as quickly as possible is vital. The risk of not being able to perform a trade on time could well be catastrophic.

A cyber event also brings with it the potential of reputational damage. If a firm gets hacked and is unable to trade for a period of time, these clients may go elsewhere due to their concerns about internal security and the company's ability to manage its fund. With a specialist cyber policy, customers are able to get the right coverage and access to the right expert help, meaning they can react better and faster in the event of an attack – certainly more so than if they relied on cover that is not specialist cyber protection. With our CyberRisk cover, customers have access to specialist professional advice and teams, including breach coaches from our expert partners, Pinsent Masons. HFM