Up.

UNIQUE PERSPECTIVES

Liberty Specialty Markets

CYBER

LIBERTY'S CYBER CELL UNDERPINS SUSTAINABLE UNDERWRITING

As COVID-19 forced more businesses to embrace flexible working, it gave cyber criminals a new avenue to exploit. Could the market accommodate a threat that was transforming at such speed and scale? Jon Rigby and Matthew Hogg discuss.

Authors

Jon Rigby CBE
Chief Cyber Officer & Air Vice-Marshal (Retired)
United Kingdom

Matthew Hogg
Strategic Head of Cyber Underwriting
United Kingdom

> "Since the global cyber-attack from NotPetya in 2017, cyber claims, particularly due to ransomware attacks, have risen, as have expectations of insurance cover."

The nature of the cyber threat is changing at a rate unlike any other peril such as natural catastrophe or systemic risk with a global, cross-class impact. Organised crime gangs use cyber extortion as a means for revenue generation. According to Bitdefender's 2020 Consumer Threat Landscape report in 2020 ransomware attacks increased year on year by 485%, while the incidence of malware rose 72%.

Criminals attack businesses worldwide 24/7, but they only need to find one victim. Businesses on the other hand, need to successfully defend a threat every time one materialises to remain unscathed. What began as a few crude attacks on retail outlets has become a steady stream of targeted, sophisticated attacks on a wide range of industries which are vital to ensure a nation's economic and financial stability, such as health and financial services.

Given our increased dependence on IT, the consequences of a cyber event – in terms of business continuity particularly – are increasingly severe. The insurance industry is facing both an increased likelihood of cyber events, coupled with significant, cross-class impact.

In addressing this challenge, cyber insurers lack the wealth of historical data available to their colleagues in other classes, for example managing natural catastrophe risk.

Industry is under strain

Since the global cyber-attack from NotPetya in 2017, cyber claims, particularly due to ransomware attacks, have risen, as have expectations of insurance cover.

As the volume of ransomware demands have grown, law enforcement and regulators have become uncomfortable about the validity of ransomware claims payments. Currently, this money goes from the risk protection industry to the insured, but ultimately may end up in the hands of organised crime gangs, a situation which may not be allowed to prevail longer term, as justice systems around the world begin to act, with politicians, law enforcement and regulators openly and actively engaging in seeking to limit the ransomware threat.

Regulators are on the move

While the payment debate continues, Lloyd's, the Prudential Regulatory Authority (PRA) and others are keen to see carriers take action more broadly, clarifying what level of cyber cover is available within general liability policies and eliminating additional residual exposure – often referred to as 'silent cyber'.

All books are potentially impacted by cyber risks with some more than others. There is clearly value in achieving this clarity of cover as a matter of principle, as guidance/regulations issued from the PRA and Lloyd's have achieved better outcomes.

In property classes, cyber cover is more frequently excluded and then for some classes written back to varying degrees of materiality. We estimate around 60% of first party lines within the London Market are now on full cyber exclusion. Some 20%-30% carry minor levels of cyber write-back – for example to provide mandatory protection against fire and explosion triggered by a cyber event. A minority of classes, however, continue to offer significant business interruption cover through writebacks. This is where Liberty Specialty Markets (LSM) likes to focus. For each class we specify the preferred treatment and then monitor the performance on the policy to ensure that our approach is prudent and reasonable.

The Colonial Pipeline outage in May 2021 is an example of how hackers can exploit a weakness and how property policies are potentially exposed to cyber events. Cover against risks on this scale needs to be carefully reviewed to ensure that pricing and reserving are set at the right level to accommodate the risk.

Liability classes are another area requiring a more tailored approach. In the case of Directors & Officers (D&O) and Professional Indemnity (PI), protection against cyber threats is a key part of what a D&O policy delivers, where a class action is brought against a board following a failure to take appropriate action to protect against an attack. Third party cover for such an event is a legitimate expectation in the PI space – the challenge for the insurance industry is to ensure that we are clear about the liability and that we rate and manage the risk appropriately. We want to make the cover explicit and intrinsic to the policy.

Financial institutions (FI) is another sector frequently targeted by hackers, with one report saying the sector is hit 300 times more frequently than others. Cyber cannot be excluded from FI wordings so it needs to either be fully affirmed or excluded with a material write-back.

Unique approach needed

As the cyber threat continues to evolve, so LSM has flexed its approach.

In 2019 we created a 'cyber-cell' to strategically manage all aspects of cyber underwriting within both cyber-specific and general lines. Within the cell we have underwriting, exposure management, data, intelligence, and operational expertise. Our multi-disciplinary team is there to set a clear and consistent cross-class cyber strategy that empowers our class underwriters to manage and underwrite risks either via specialist standalone cyber cover or better, more informed protection within their existing covers.

Recognising that we need to actively monitor and manage our exposures to remain an effective risk transfer partner for our customers, we are focused on ensuring that we look at each risk through three lenses: class, industry and insured. We are developing a consistent approach to risk across the portfolio, so that we do not offer levels and types of cyber cover limits within a general class that we would not be prepared to offer on a standalone policy. Transparency and consistency are essential to support our insureds. Carriers who are inconsistent in their policy will be 'picked off' as coverage is eroded, capacity withdraws, and brokers have to work harder to secure placements.

What does the future hold

We are focussed on the systemic and catastrophe risk associated with the cyber hazard and are systemically reducing our exposure, just as we would for earthquake or windstorm. However, for the moment we are of the view that it is not the big cyber events that threaten to derail less regulated markets. NotPetya, the biggest international threat so far, generated an insured loss of $3bn-$6bn. Large data protection fines are yet to top $0.5m. Instead, the threat to underwriting sustainability is more insidious and will come not from an event, but from the attritional impact of smaller losses accruing on policies month after month. For now, this threat will come from ransomware, but cyber has shown us that new threats and methodologies will continuously emerge to threaten our insureds' prosperity.

Alongside underwriting discipline on a cyber standalone and cross-class basis, supported by multi-disciplinary modelling, the future will require more effective sharing of data between clients and their insurers and between the insurance community. We are yet to establish the historic bank of insight that underpins risk modelling in other classes. In the meantime, our focus will be to use a combination of our own and commercial platforms to understand exposure and set strategy.

As the cost of capital rises, and the risk to carriers grows, judgement, knowledge and data will be required to enable these risks to be written sustainably. Our key consideration is that we take steps now to ensure that we can protect both LSM and our insureds from the impact of a systemic cyber event, impacting multiple classes and regions. State actor malware leaking into the private sector could be the trigger, or simply the continued sophistication of attacks. ■

> "Transparency and consistency are essential to support our insureds."

GET IN TOUCH

Jonathan.Rigby@libertyglobalgroup.com
Tel: +44 (0)7500 331216

Matthew.Hogg@LibertyGlobalGroup.com
Tel: +44 (0)20 3758 0368

libertyspecialtymarkets.com