The Age of Intangibles/Cyber

The changing nature of risk overall is inherently tied to the increasing proportion of intangible risk.

The value of intangible assets has skyrocketed, and the risks associated with them are also accelerating. Globally, cybercrime is expected to cost in excess of USD 6 trillion annually by 2021.

By comparison, the cyber insurance market today is roughly USD 6 billion in gross written premium. The projected cyber loss amounts are not absorbable or sustainable in the current insurance market and, most urgently, that disparity creates a staggering protection gap for businesses with mounting exposures.

In this age of digitization, businesses are innovating faster in an effort to transform and improve the customer experience. As a result, they struggle to identify the scope of intangible assets, the extent of what is at risk and how to best protect themselves. Digital assets can feel nonlinear – like a "black box" – to many businesses trying to assess their exposure.

COVID-19 has introduced even more complexity, and the new risk landscape reinforces the importance of reassessing the value of this changing asset base.

This dynamic is compounded by new threats that are manifesting quickly.

The insurance industry has also been challenged. We operate in a world where we think of risk in known, measurable terms. Intangible risk, with cyber being the largest, feels different. The exposure is not geographically contained like a natural catastrophe and is not as explicitly calculable as a burning building.

Despite historical profitability and forecasts of hypersonic product growth, the reinsurance industry's cyber growth trajectory has tapered off over the last two years and is showing signs of growing pains. According to Marsh JLT Specialty data, only 42 percent of businesses purchase a cyber product, and many of those may not be sufficiently insured.

This flattening market trend is directly at odds with the heightened threat environment and the increased valuation of intangible assets and is contributing to the expanding protection gap for businesses.

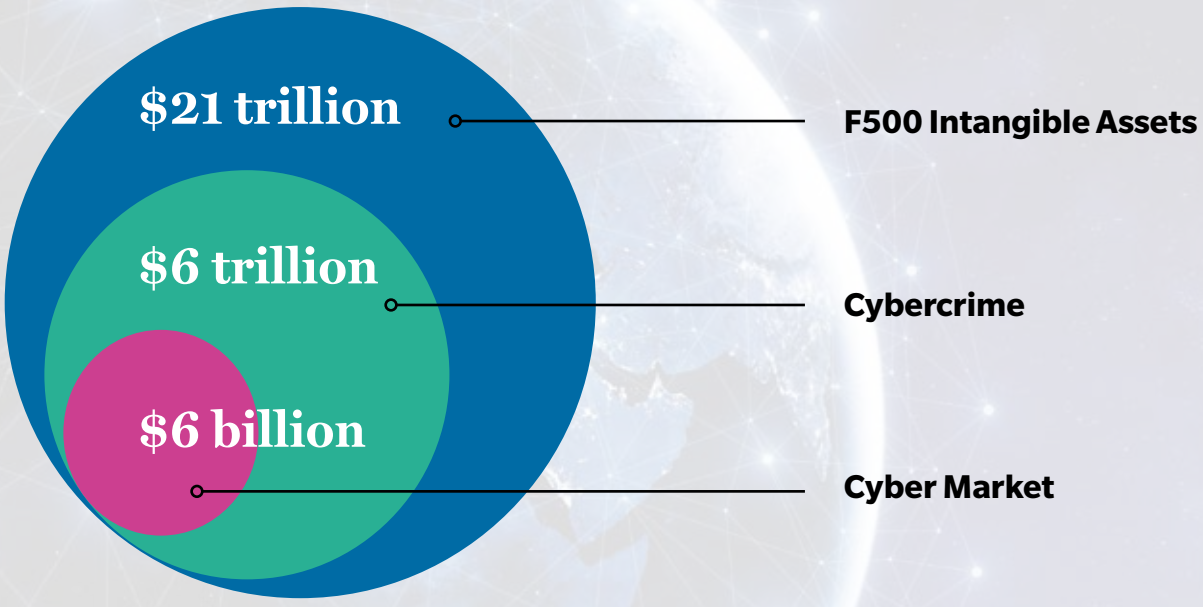
One critical market hurdle to more robust cyber insurance industry growth is maintained profitability, which has come to a juncture due to developments around ransomware.

Since 2009, Guy Carpenter has modeled the cyber industry trended and developed loss ratio selection at 50.3 percent through 2018 on a premium weighted average.

But ransomware attacks have ramped up since 2018, becoming an exposure game-changer, materially threatening the profitability of this line of business and creating a notable industry response. Profitability plays a critical role in promoting product expansion, innovation and sustainable market growth. Without it, the development of cyber risk transfer solutions will be stunted further.

The proliferation of ransomware is creating reimagined loss emergence for (re)insurers and blurring the lines between attritional and catastrophic cyber loss. The trend is moving

The Changing Nature of Risk



away from individual business impact and instead looking at strain characteristics.

Ransomware has progressively become a loss driver across the industry, and recalibrated pricing strategies reflect the growing risk. Guy Carpenter is working closely with our clients to share updates on the threat landscape, deliver cyber industry insights, construct relevant modeling scenarios and design reinsurance placements to protect these portfolios. With its confidence shaken, the industry is adopting risk mitigation and underwriting strategies in order to course correct from the impact of this ubiquitous loss driver.

A Change on the Horizon?

Ransomware payments and their reimbursement under insurance policies are controversial because of their potential for moral hazard and the possibility that such payments will fund criminal, terrorist and/or state-sponsored cyber actors.

Addressing this issue, on October 1, 2020, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) published an advisory that reiterates the prohibition against U.S. businesses and persons conducting business or paying funds to any person on the "Specially Designated Nationals and Blocked Persons" list. U.S. companies can be sanctioned for violation of OFAC's rule even if they do not personally execute a transaction or know that a payment is being made to a prohibited organization or person. The advisory highlights potential sanction risks in the payment of cyber extortion demands and encourages companies and their advisors to report cyber extortion attacks to law enforcement and to contact OFAC immediately if they believe a request for a ransomware payment may involve a prohibited organization or person.

While it is too soon to say whether change is imminent to applicable laws or regulations in relation to these payments, the advisory does remind U.S. companies, ransom payment facilitators and cyber insurers that a regulatory framework on ransomware already exists.

This framework may be further utilized by insurers as they consider future underwriting strategies for ransomware and the insurability of the extortion demands.

It is necessary to maintain the viability and sustained health of the cyber market in order to broaden the range of available intangible risk transfer solutions.

Ransomware attacks have ramped up since 2018, becoming an exposure game-changer, materially threatening the profitability of this line of business and creating a notable industry response. Profitability plays a critical role in promoting product expansion, innovation and sustainable market growth. Without it, the development of cyber risk transfer solutions will be stunted further.

The 2019 Marsh Microsoft Study concluded that the benefits organizations reap from new technological developments supersede the risks. COVID-19 has brought that concept to life. Businesses today depend more on digital assets than ever, which pushes the upward valuation of intangibles even higher.

But, especially in our current risk environment, the cyber (re)insurance industry must be solidly positioned to support and solve for this expanding protection gap.

Developing a robust cyber risk transfer market equipped to handle sizable loss events means:

1. Creating well-defined, forward-looking product options for intangible risk
2. Driving adoption of those products
3. Demanding innovation in response to the morphing risk landscape.

But, it also means developing a relevant and sustainable market. This market has to be equipped to scale and capable of responding to the unpredictable. It also must balance thoughtful product expansion with financial viability, to keep pace with the growth of intangible assets and to meet the risk transfer needs of the business community. ■

Erica Davis,
Managing Director,
North America Cyber
COE Leader,
Guy Carpenter.