INSURANCE ADVISORY PARTNERS
Insurance and Insurtech Experts

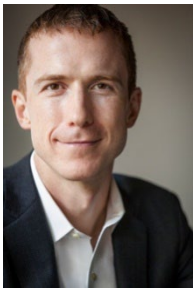
Insurance Advisory Partners

Quarterly Executive Interview

Cyber Risk Q&A

with Pascal Millaire, CEO of CyberCube

Amid the stratospheric rise in ransomware attacks, Insurance Advisory Partners talks to Pascal Millaire, CEO of CyberCube about the opportunity this is creating, and how data-driven risk analytics is helping insurers prevent the ugly duckling of cyber risk turning into a black swan.



Pascal Millaire, CEO of CyberCube, the leading data-driven cyber risk analytics platform for the insurance industry

1. **The cyber insurance market seems to continue to be correcting far more than other lines of commercial insurance. What is your view on the overall state of the market?**

   The cyber insurance market has experienced a substantial increase in rates of ransomware, which has resulted in a deterioration of historically attractive loss ratios, but the market is indeed correcting in an appropriate manner.

   The last couple of years have seen compounding annual rate increases of 30% plus, with some large corporates experiencing increases in rates in excess of 100% per year. This has been combined with more rigorous underwriting standards, greater use of analytics and a tightening of terms and conditions, resulting in reduced exposure for many carriers. Despite these changes, demand from enterprises for cyber remains at an all-time high and enterprises have generally been willing to absorb these premium increases given the worsening cyber risk environment and greater board-level awareness of cyber risk.

   With these positive developments from an insurance perspective, from an underlying risk perspective we are now seeing a leveling off of ransomware frequency and often a decline in severity.

   As a result, this is a market in which insurers are seeing more demand for a product that is more profitable.

2. **Is cyber risk the next Black Swan event in the global insurance industry?**

   Quite possibly. The potential for global aggregation events remains the biggest concern for many insurers but progress is being made rapidly.

   Over the last 36 months, we have observed 36 ‘near-miss’ events, which had the potential to become aggregation events for the global cyber insurance industry. These include cyber attacks against single points of technology failure such as MS Exchange, Solarwinds and Blackbaud.

Analytics from companies such as CyberCube are doing a far better job at identifying these single points of accumulation, providing an understanding of modeled losses and assisting carriers in defining appropriate underwriting and reinsurance strategies. Insurers and reinsurers are also rolling out new policy wordings that ensure carriers aren't covering the sort of systemic nation-state induced losses that the industry cannot absorb.

There is more work to do, but a combination of better modeling and more precise policy wordings means the industry has made major advances on this topic in recent years.

3. **What is the most common factor you see in the insured in successfully underwritten, low loss ratio cyber business? How have cyber underwriting guidelines evolved over time?**

The particular microsegment that insurers underwrite is, and continues to be, one of the most important determinants of underwriting performance. Companies of different sizes, geographies and industries have major differences in claims frequency and severity.

What is changing is the increasing use of company-specific risk indicators to differentiate between risks within a microsegment. For example, insurers noticed the presence of certain risky open ports that were a leading indicator of claims, given certain ports were common entry points for ransomware. CyberCube sees such patterns in our data and have identified an additional nine security signals that lead to even higher incidences of claims frequency.

The underwriting of cyber risk is getting more sophisticated and as a result insurers are becoming more value-adding as partners in holistic cyber risk management.

4. **How does cyber risk correlate with other insured risks? Is aggregated risk being accurately measured?**

Given we haven't seen a major systemic cyber aggregation event, carriers had previously taken very different approaches. These were as extreme as assuming no catastrophe loads for cyber insurance policies (given carriers hadn't seen losses from aggregation events) all the way through to assuming a carrier's exposure to cyber was equal to the sum of limits of all cyber insurance policies that were underwritten. Today, the existence of cyber catastrophe models and analytics that track aggregation against specific single points of technology failure allow far more nuanced approaches.

One of the most important questions is whether cyber risk correlates to broader market risks, as that could be an inhibiting factor for the growth of alternative capital. The academic literature on the topic shows that companies tend to quickly recover from the stock declines associated with a cyber attack directly on a particular company.

The second-order impacts on suppliers are even more muted – particularly as they don't tend to impact the long-term cash flows of the enterprise in question. Outside of outright large scale nation-state to nation-state cyber conflict, which could have correlating market impacts, there is increasing belief that cyber is less correlated to market risks,

which is an important factor in the alternative capital transactions we expect to see over the next couple of years.

5. **There has been a great deal of market growth and recent rumors with cyber MGAs. What does this mean for the overall cyber insurance market?**

   Cyber MGAs have brought technology-first approaches to cyber underwriting that leverage the vast volumes of data available in the public domain on cyber security.

   At the same time, incumbent insurers also have access to many of the same tools in cyber underwriting, which they are combining with diversified balance sheets, deep partnerships, extensive customer bases, sophisticated risk management approaches and insurance capabilities built over many decades in other lines of insurance.

   There is over a trillion dollars a year lost due to cyber crime and internet-connected technology failure. That number is growing and only a small portion is covered by a cyber insurance policy today.

   The growth of cyber MGAs is emblematic of the opportunities for innovation in cyber insurance and frankly the industry needs even more technology innovation from such players. The growth of cyber MGAs is not, however, a sign that incumbent insurers have a limited role to play in addressing this enormous market opportunity.

6. **What is happening in the cyber ILS market and how quickly will it help (or hinder) the overall market?**

   The biggest constraint to the growth of the cyber insurance market is access to sufficient reinsurance capacity and cyber ILS offers the potential for such additional capacity.

   Given the size of the market opportunity to insure cyber risk, there's a case to be made that the cyber ILS market could one day eclipse the size of the natural catastrophe ILS market.

   CyberCube is actively working on a cross-section of such opportunities so do watch this space.

7. **We would be curious to know your views on the overall state of the insurtech funding market.**

   Regular readers of the Insurance Advisory Partners Public Market Comps newsletter (such as myself) will be aware that in a market where the S&P 500 is down 13% over the past year, publicly listed insurtechs are down 58%, with substantially compressed multiples. Clearly such a major change in public markets has an impact on private insurtech funding.

   At the same time, venture capital and private equity investors have raised large funds, which they have committed to deploy in the insurtech and fintech space and so capital is indeed out there.

The difference is the growth-at-(almost)any-cost mindset has been replaced by a more nuanced view of efficient growth, underlying unit economics, asset-light models and underlying SaaS metrics. As such, if you are an insurtech that does have strong underlying fundamentals, you are in a unique position to go after funds that are looking for such insurtech businesses with attractive business models.

8. In conclusion, what will it take to successfully manage cyber risk?

Cyber risk is a once in a generation, if not a once is a century, opportunity for the P&C industry. The winners will be those insurance institutions that embrace new forms of data, analytics and technology and thoughtfully combine them with traditional insurance approaches. I expect cyber risk to be a hotbed of innovation in insurance for many years to come.

INSURANCE ADVISORY PARTNERS
Insurance and Insurtech Experts

Unparalleled Expertise, Experience And Insight For The Global Insurance & Insurtech Industry

An independent, employee-owned investment banking partnership

Focused exclusively on the global insurance & insurtech industry

Provides a broad range of capital raising, M&A and strategic advice to our clients

The Founders have over 70 years of insurance investment banking and operational experience

Our team has worked on hundreds of insurance M&A and capital raising transactions