Embracing the cyber insurance opportunity

Significant rewards await forward-looking insurers that get it right

Paul Merrey, KPMG in the UK
Matthew Martindale, KPMG in the UK

Paul Merrey

Matthew Martindale

Digital technology in today's increasingly interconnected world is forging perilous new threats to businesses everywhere. AI, the Internet of Things, robotics and augmented reality are among the rapidly emerging innovations unleashing not only exciting new levels of communication, automation, mobility and convenience but also unprecedented potential for cyber-related disaster.

Businesses of all sizes are struggling to identify, assess and respond to an explosion of digital threats and targeted cyber attacks that could paralyze their operations at any moment. From tangible assets such as property to intangible assets that include intellectual property (IP), customer data and reputations, organizations in every sector are becoming dangerously exposed to an array of emerging cyber risks.

Financial services and retail businesses, for example, are already a focus of organized cyber crime, while ransomware and distributed denial-of-service attacks are increasingly being used against organizations in industries such as healthcare, media and entertainment. Public sector and telecommunications businesses, meanwhile, are considered highly susceptible to espionage- or terrorism-related cyber attacks.[1] Digital technology has also opened the door to business system failures that can inflict massive physical damage, accidents and theft.

As organizations are quickly learning, sometimes at high costs, cyber risk is now much more than a data breach and the nature and sophistication of potentially catastrophic cyber attacks keeps evolving.

Cyber crime is high on the agenda of business executives, and they are making progress in implementing security measures. KPMG's 2017 Global CEO

[1] *Closing the gap — insuring your business against evolving cyber threats*, KPMG in the UK, DAC Beachcroft and Lloyd's insurers, June 2017.

Outlook reveals four in 10 CEOs (42 percent) feel their organization is now adequately prepared for a cyber-event, compared to just 25 percent in 2016. As a result, the issue ranks fifth among business leaders, versus number one in last year's survey.[2]

We see strong signals that many CEOs are moving beyond a generic view of cyber risk to develop risk, resilience and mitigation plans in the context of the parts of their business that could be most seriously affected. The risk remains very much top of mind and the need for vigilance remains high. Cyber insurance is an important way for CEOs to protect their organizations.

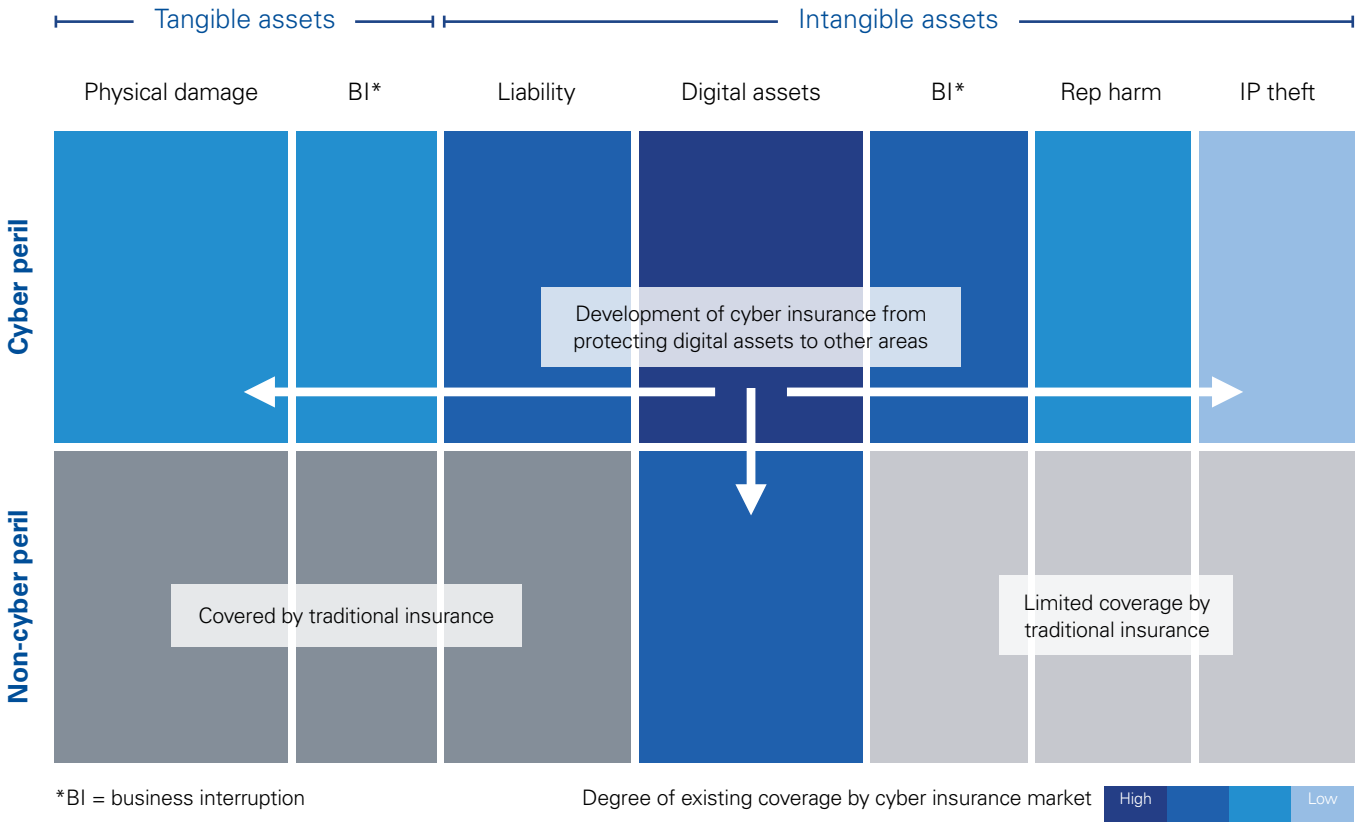
As the scope, frequency and impact of cyber-related incidents soar, huge new opportunities exist for insurers positioning themselves for growth in the cyber insurance market.

Cyber insurance and closing the gap

Unfortunately, as cyber risks and attacks proliferate, many organizations and their insurers are discovering alarming gaps in the coverage provided by traditional insurance policies. Cyber insurance has traditionally focused primarily on digital assets such as customer data. Now, the global industry is starting to respond to the changing market by expanding into adjacent insurance lines across both the intangible and tangible asset space — a trend that will no doubt continue as the industry matures.

As the scope, frequency and impact of cyber-related incidents soar, huge new opportunities exist for insurers positioning themselves for growth in the cyber insurance market. For those that get it right, the rewards will be significant in a market that is predicted to be worth more than USD10 billion in global premiums by 2020.[3]

Cyber insurance is expanding into adjacent areas



Source: *Seizing the cyber insurance opportunity*, KPMG International, 2017

[2] *Disrupt and Grow: 2017 Global CEO Outlook*, KPMG International, June 2017, kpmg.com/ceooutlook.
[3] *Seizing the cyber insurance opportunity*, KPMG International, 12 July 2017, https://home.kpmg.com/xx/en/home/insights/2017/06/seizing-the-cyber-insurance-opportunity.html.

The immediate challenges for insurers include the need to enhance their cyber capabilities, unravel the complexity of modeling and pricing, and redefine their organizational structures. Cyber insurance has a unique opportunity to lead the crucial shift from products to innovative new solutions that create new advantages for insurers and customers alike. Forward-looking insurers are evolving their focus from property and assets coverage to providing a full spectrum of services across these three key categories:

1. **Understanding risk.** Insurance providers are working with technology companies to leverage their deep know-how in customer use cases and software and hardware vulnerabilities.

2. **Preventing risk.** Businesses remain slow to implement preventive measures due to low awareness and recognition of the value of such services — even when offered free of charge. Incentives could drive up implementation in this area. Ultimately, a move towards preventative services is likely to lead to a decrease in overall premiums and claims.

3. **Responding to cyber incidents.** Insurance players have already established partnerships to provide a variety of cyber incident response services. Customer take-up rates for these services have been relatively low but industry participants expect the industry to see expansion in this area as customer awareness of the added value gradually grows.

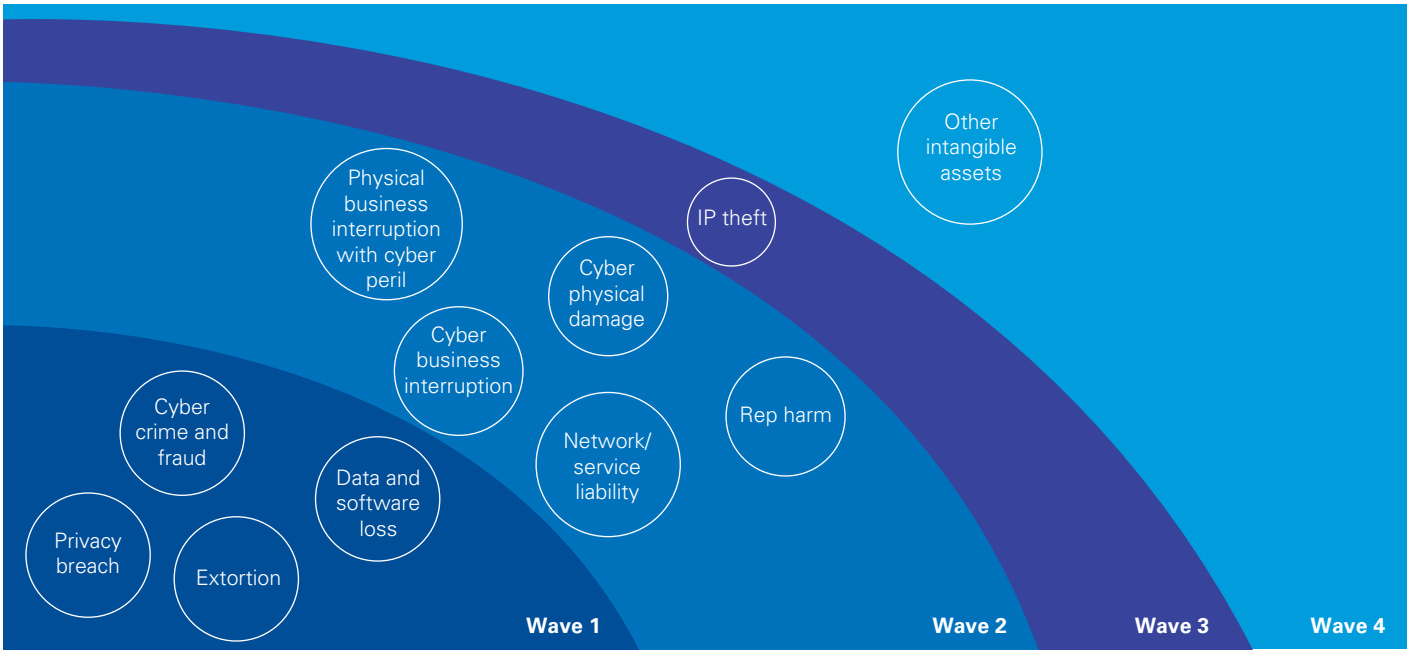
A 'wave' of opportunity

As insurers seek to expand coverage and introduce innovative solutions, industry experts anticipate that the development of cyber insurance is about to undergo several critical 'waves.' From an initial focus on digital assets, the sector is expected to expand to encompass a range of new products covering other asset classes, as well as addressing non-cyber perils in traditional insurance. Each wave represents an increasing level of complexity and insurers have no time to lose in transforming for the future.

Wave 1: Strengthening core digital asset propositions with crisis management

Cyber propositions that focus on losses related to digital assets — such as data breaches, cyber crimes and data losses — are likely to remain the core of any proposition set. But as competition increases, players face growing pressure to differentiate their services. That makes Wave 1 a critical period, as success should help insurers not only establish competitive advantage in the core cyber insurance market but also provide a platform to progress through subsequent waves. The focus will need to be on developing integrated crisis management solutions that improve customer experience, drive top-line growth, generate market intelligence to model risk more effectively and enhance underwriting capability.

The four waves of cyber insurance development



Wave 2: Enhancing risk modeling to expand coverage to assets with cyber triggers

As risk-modeling capabilities evolve, insurers should be able to expand their offerings into other cyber areas. In the short term, cyber insurance will diversify into areas such as business interruption and network and service liability. Business interruption is a particularly critical area, with most businesses reporting some business interruption loss following a cyber incident. In the medium- to longer-term, as risk-modeling capabilities improve, insurers can start addressing losses to other intangible assets caused by a cyber peril, arising from issues like reputational harm. While these areas are more complex and may take longer for insurers to add to their portfolio, they could become the new sweet spot for cyber insurers.

Wave 3: Insuring the 'uninsurable'

As the traditional cyber insurance market becomes more saturated, and broad crisis management solutions become the new norm, insurers need to push the boundaries of risk modeling and develop new products serving untapped areas. One such product could be IP theft insurance. This could be addressed by developing an innovative parametric cover: instead of measuring the actual loss caused by an IP loss, the insurer and the insured would agree on a specific payment to be triggered in case of a loss event, irrespective of the value of the loss.

Wave 4: Transitioning from cyber to intangible asset insurance on non-cyber perils

Some market participants see cyber insurance as closely related to broader intangible asset insurance. A natural future evolution of cyber insurance could, therefore, include damage to intangible assets with non-cyber perils, such as reputational harm due to product recall, which is rarely covered by traditional insurance. To succeed, insurers would need to develop new capabilities, build a better understanding of non-cyber perils and leverage their crisis management services.

The insurance industry is at the threshold of a major shift that poses real challenges, but the payoff promises to be significant for insurers willing to rethink strategies and offerings for the digital age. ■

Contributors

Paul Merrey
Partner, Strategy
KPMG in the UK
T: +44 20 76945276
E: paul.merrey@kpmg.co.uk

Paul specializes in strategy advice to the insurance industry, and has significant experience in strategic options assessments and growth strategy development. He is currently leading KPMG's work on strategy within the Lloyd's and London market, supporting the Vision 2025 ambitions. Prior to joining KPMG, Paul spent 10 years at Prudential plc, where he was latterly Group Head of Strategy and M&A. He qualified as a Chartered Accountant with PwC and has an MBA from Warwick Business School and an MA from the University of Oxford.

Matthew Martindale
KPMG in the UK
T: +44 20 76942989
E: matthew.martindale@kpmg.co.uk

Matthew leads KPMG's cyber security service offering for Insurance and Investment Management markets within the UK. He joined KPMG in 2000 and has been principally involved in delivering cyber security advisory and assurance engagements. In addition to his consultancy work, Matthew worked in an operational role as the Chief Information Security Officer.

> Cyber propositions that focus on losses related to digital assets — such as data breaches, cyber crimes and data losses — are likely to remain the core of any proposition set.