KPMG

Seizing the cyber insurance opportunity

Rethinking insurers' strategies and structures in the digital age

Thriving on disruption series

As our world becomes increasingly digital, insurers have an opportunity to address the real risks that cyber poses. To become cyber leaders, insurers need to enhance their cyber capabilities and rethink their organizational structures. For those, that get it right, the rewards could be sizeable.

Paul Merrey
KPMG in the UK

Matthew Smith
KPMG in the UK

Matthew Martindale
KPMG in the UK

Arturs Kokins
KPMG in the UK

Global Strategy Group

KPMG International

Commercial lines insurance is characterized by complex buying processes in a large and valuable market, making the sector ripe for disruption, with technology acting as both an enabler and accelerator. We believe disruption is likely to be fueled by seven key trends, each of which will be discussed in a series of articles that examine the likely market impact and resulting opportunities from each. This paper's topic is highlighted in blue:

1. The rise of risk aggregators
2. Demand for new products and solutions as businesses develop different risk profiles
3. The future of excess capacity
4. **Customers demanding broader solutions, rather than just insurance products**
5. Collaborative development of solutions to meet emerging customer needs
6. Cognitive computing advancements creating value through sophisticated analytics
7. The changes to business models and requirements for more agile operating models.

In this paper, *Seizing the cyber insurance opportunity*, we explore how the cyber insurance market epitomizes an industry shifting to broader solutions.

The historical role of an insurer as someone that merely protects is changing, as customers demand broader solutions that prevent incidents from happening in the first place – and offer support during and after a crisis. This is especially important for cyber insurance, where companies are struggling to get their heads around threats that can literally paralyze their businesses.

Over the following pages we look at the evolving nature of cyber insurance, the huge opportunities this brings, and the implications of building a cyber-oriented insurance company.

To give us a better idea of insurers' views and concerns about cyber insurance, we held separate discussions with approximately 20 industry practitioners and executives from across the value chain, including insurance carriers, managing general agents (MGAs), brokers and reinsurers. Their responses have informed the thinking in this paper and we would like to thank them for their contributions.

Rethinking insurers' strategies and structures in the digital age

Technology brings a new range of threats to both tangible (e.g. property) and intangible (e.g. reputation) assets, many of which are not covered by established insurance policies, leaving organizations of all types dangerously exposed to the impact of cyber perils.

Cyber insurance, as it has historically been defined, has focused primarily on digital assets, such as customer data. However, with the scale, frequency and impact of cyber incidents increasing, many traditional insurance lines like home, property, energy and aviation are transitioning by proxy to cyber insurance.

Our discussions with industry experts support this trend and predict that the cyber insurance sector is undergoing several waves of development to expand from digital assets to encompass physical assets, as well as other asset classes such as reputation, intellectual property and business interruption. The faster the insurers can unravel the complexity of modeling and pricing these risks, the quicker they can seize a share of this exciting, expanding market, which could be worth more than US$10 billion of global premiums by 2020.[1]

This represents a significant opportunity, but also a big challenge for insurers, who need to move their cover from products to managing risks, preventing incidents, and responding to incidents. Insurance companies are creating teams that focus on cyber insurance risks but we recommend that they should adapt their organizational structures to ensure that cyber is integrated into everything they do, possibly creating stand-alone cyber insurance centers of excellence that bring together cyber risk modeling, crisis management and digital platforms. Ultimately, as customers start seeing value in integrated solutions to protect against cyber incidents across all asset types, insurance companies might consider shifting their department structures away from a focus on assets (e.g. property, motor, aviation) to a focus on perils (e.g. cyber terrorism), thereby challenging the status quo of traditional insurance.

In today's digital world, almost all insurance lines are impacted by cyber

Most businesses are under-insured and/or under-prepared for emerging cyber risks.

Technology has become an integral part of our lives, with emerging innovations like artificial intelligence, the internet of things, robotics and augmented and virtual reality impacting homes, workplaces, transportation and leisure. This is creating new levels of e-mobility, automation, smart buildings and even smart cities.

But these developments bring new threats, and the insurance industry is playing catch-up to keep pace with the rapid rise of cyber risks. According to research from Allianz, annual worldwide losses attributable to cyber-crime are close to US$500 billion[2] – a figure set to quadruple to more than US$2.1 trillion by 2019.[3] Yet yearly global cyber premiums are estimated at just US$2.5 billion – a mere 1 percent of total commercial premiums,[4,5] (and this modest figure only represents cover for a narrow range of risks – mainly digital assets). Furthermore, it is estimated that 60 percent of FORTUNE 500 companies currently lack any insurance against cyber incidents,[6] primarily due to a lack of cover currently available for many types of cyber risk.

While cover is low, cyber risk is undeniably a major concern for business. In KPMG's 2016 Global CEO Outlook, chief executives cite cyber security as the number one risk facing their companies. However they also recognize that there is more work to be done in this area, with 72 percent of CEOs not feeling fully prepared for a cyber event.[7]

The types of cyber-attacks against businesses vary from sector to sector and are constantly evolving. For example, the financial services sector finds itself a focus for organized cyber-crime, and retail is increasingly being targeted. Ransomware and distributed denial-of-service attacks are increasingly used against businesses with healthcare, and media and entertainment particularly targeted. Meanwhile, the public sector and telecommunications sectors are highly susceptible to espionage-focused cyber-attacks.[8]

Traditional insurance players are increasingly realizing that cyber risk is much more than a data breach. As the following diagram shows, digital technology has introduced a wide range of additional threats that impact existing insurance cover, where hackers and/or system failures can cause physical damage, accidents and theft. Such a trend offers cyber insurers the chance to take market share from established players.

Exhibit 1: Examples of how emerging cyber risks are shifting the focus of traditional insurance towards cyber

Home	Property	Energy
— Smart home radio signals are intercepted and replayed to open a property's doors and commit a robbery	— A smart warehouse's thermostats are breached, causing a significant increase or decrease in temperature, leading to a major loss of products — A sprinkler system or waterworks are accessed in a malicious or unauthorized way, causing flooding and physical damage — Operational technology is accessed to change product ingredients or manufacturing designs, causing liability or product recall.	— A drilling system is breached, making it overheat and causing a fire — An internal oil rig email system is accessed in a malicious or unauthorized way, infecting computer networks offshore.
Motor	**Aviation**	**Seaborne**
— A communication system between self-driving vehicles gets accessed, sending false signals and causing widespread passenger fatalities.	— An in-flight entertainment system is accessed to steal personal passenger information — A smartphone app is used to access a plane's steering system and cause a crash.	— A yacht's navigation system is accessed, forcing the yacht off course, and a ransom is demanded to return control or to unlock the navigation system — Wi-Fi networks are breached to steal financial information / personal photos, access bank accounts, and read / write private emails.

Cyber insurers are entering adjacent areas

Growth opportunities in an under-insured market.

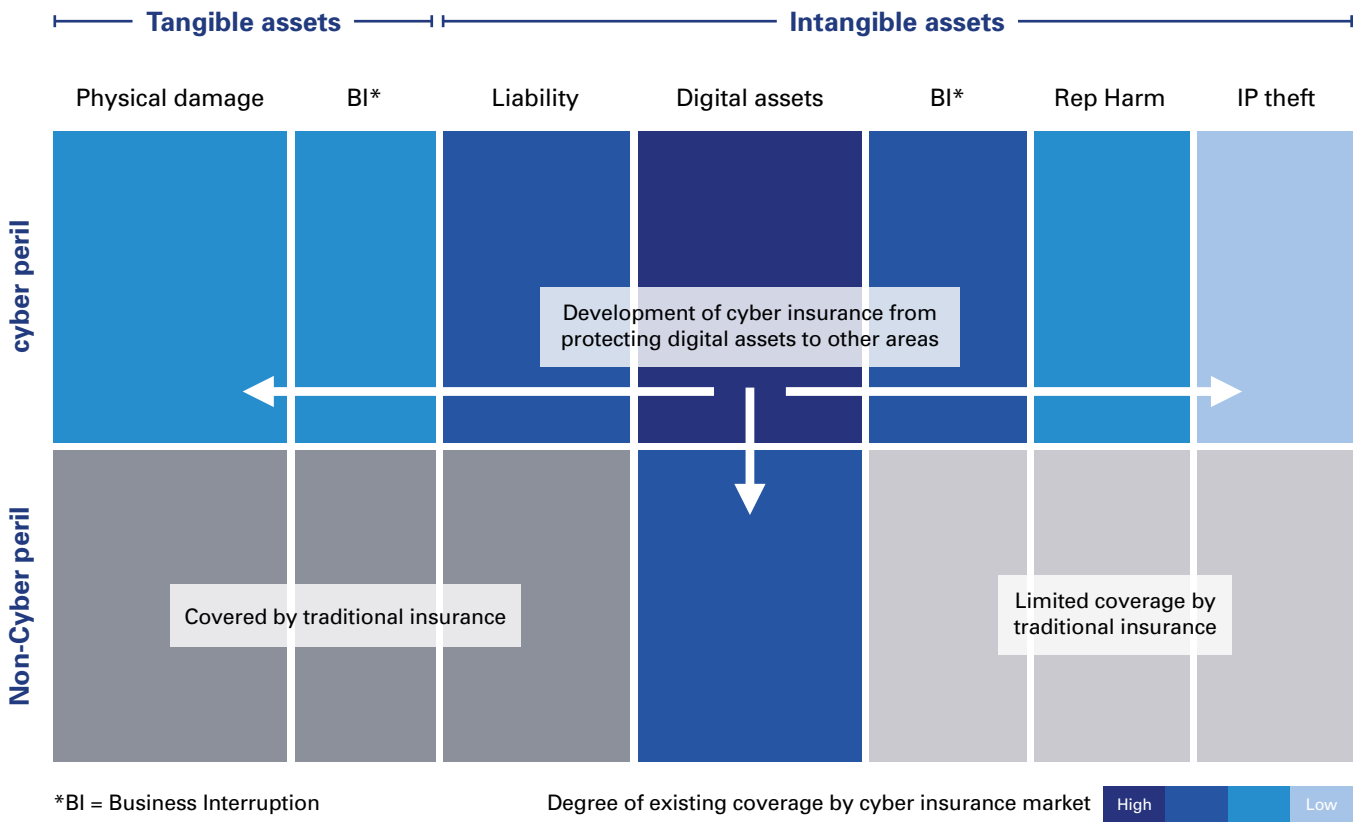
The global cyber insurance market is expanding quickly, with annual growth of around 20-25 percent. It is predicted to rise from US$2.5 billion in 2015 to US$7.5 billion by 2020, reaching US$20 billion in premiums by 2025.[9,10] This growth is driven by both regulatory changes (especially in Europe, where new EU rules are expected to follow the US example of imposing heavy fines on companies that suffer data breaches[11]), and an increasing awareness of threat types and levels among businesses. However, these estimates account primarily for traditional cyber insurance products, such as data breach, cyber crime and fraud, extortion, data and software loss and network and services liability – in other words, products meant to protect digital assets against losses caused by cyber perils. We believe these market growth predictions may be under-estimated.

There are other asset types, particularly other intangibles, which are similarly exposed to cyber perils but are often left uninsured, or are sometimes intentionally or unintentionally covered by non-cyber insurance product lines. Between 1975 and 2015, the value of intangible assets as a proportion of total enterprise value (among S&P 500 companies) rocketed from 17 percent to 84 percent.[12] Most of these intangibles are currently uninsured, even though damage to organizational reputation following a breach is the single biggest cyber concern of corporate executives, according to KPMG's 2016 Global Consumer Loss Barometer.[13]

When you take these assets into account, the 2020 cyber insurance market could exceed US$10 billion if insurers develop the right solutions to address these risks.* This trend also has implications for traditional insurance, as in the future, a growing proportion of risks are likely to be picked up by cyber insurers as they expand from protecting digital assets into adjacent areas (see Exhibit 2).

* This projection covers both, a) traditional insurance products, such as privacy breach, cyber-crime and fraud, extortion, data and software loss and network & services liability – in other words, products meant to protect digital assets against losses caused by cyber perils, which we forecast to be US$7.5 billion in global premiums by 2020; and b) other asset types (such as reputation and intellectual property) that are similarly exposed to cyber perils but are often left uninsured, which could exceed US$2.5 billion in global premiums by 2020.

Exhibit 2: Cyber insurance is expanding into adjacent areas



— The cyber insurance market started in the digital asset space.
— As data and risk modeling capabilities have improved and awareness of the scope and nature of cyber perils increased, the industry has started to expand into adjacent insurance lines across both the intangibles and tangible asset space – a trend we expect to continue as the industry matures.

How insurers can position themselves for future cyber market growth

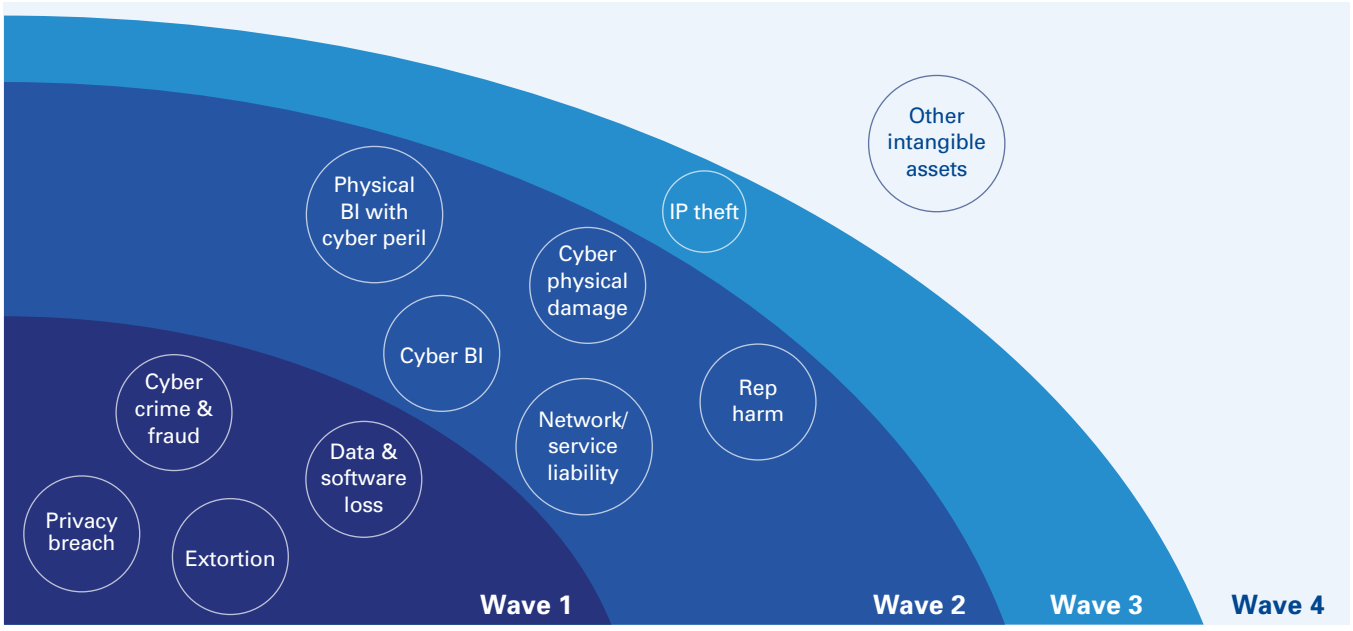
Managing the increased complexity of modeling and pricing tangible and intangible cyber risks.

As insurers seek to expand coverage and introduce innovative solutions, we, along with the industry experts we spoke with, expect the development of cyber insurance to undergo several waves (see Exhibit 3). 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 of the waves represents an increasing level of complexity. To accelerate their progress along the risk spectrum, insurers need to gain a better understanding of these new risk areas to enhance their risk modeling. Currently, the data for many pricing and reserving decisions is either not readily available, or is disjointed. Better data, more readily accessible, should help to create accurate models that drive more informed decisions.

Getting these basics right should help to improve the accuracy and reliability of loss forecasting, pricing and risk capital allocation, to cope with major loss events.

Exhibit 3: The four waves of cyber insurance development



Wave 1: Strengthening core digital asset propositions with crisis management services

Cyber propositions that focus on losses related to digital assets, like data breach, cyber crimes and data loss, are likely to remain the core of any proposition set. These are 'bread and butter' products of most cyber insurers and should keep bringing significant revenues in the short-to-medium-term. However, as competition gradually increases, players are likely to come under growing pressure to differentiate their service propositions.

We believe that Wave 1 is 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. By focusing on developing integrated crisis management solutions, they could improve customer experience to drive top-line growth, generate market intelligence to model risk more effectively and enhance underwriting capability.

Wave 2: Enhancing risk-modeling capabilities to broaden coverage to other assets with cyber triggers

As risk-modeling capabilities evolve, insurers should be able to expand their offerings into other cyber areas. We see this wave occurring in two separate stages.

In the short term, we expect cyber insurance to diversify into areas such as business interruption and network and service liability. These areas appear to be the natural progression from the digital asset space as they are significantly less complex than other lines. Business interruption is a particularly critical area from the customer perspective with 60 percent of businesses reporting some business interruption loss following a cyber incident.[14]

In the medium-to-longer-term, as risk-modeling capabilities continue to improve, insurers are expected to 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. Similarly, we expect cyber physical damage cover to become more popular to address tangible asset-related losses, as cyber insurers start stepping into traditional insurance territory.

Wave 3: Insuring the 'uninsurable'

There are areas that are currently perceived to be uninsurable, even though they expose businesses to potentially significant losses. As the traditional cyber insurance market gets more saturated, and broad crisis management solutions become the new norm, insurers need to push the boundaries of risk modeling and develop new products in untapped areas. One such product could be intellectual property (IP) theft insurance. This could be addressed by developing an innovative parametric cover, so, instead of measuring the actual loss caused by an IP loss, the insurer and the insured would agree on a specific payment that would be triggered in case of a loss event, irrespective of the value of the loss.

Wave 4: Transitioning from cyber to intangible asset insurance to cover 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, be harm to intangible assets with non-cyber perils (e.g. reputational harm due to product recall), which is rarely covered by traditional insurance. To succeed in this segment, insurers would need to develop new capabilities, build a better understanding of non-cyber perils and leverage their crisis management services. This may be a challenge; but the subsequent opportunities could be sizeable.

Shifting cyber insurance from products to solutions

Integrating new technology and building relationships with third-party response providers.

Today's organizations are so reliant on technology that any cyber breach can be catastrophic. Yet the scope of many current cyber products is limited to after-the-event reimbursement. Businesses are looking for more than just products; they want broader solutions that prevent incidents from happening in the first place, along with support when loss events arise. Risk assessment, prevention and crisis response could become an essential part of any customer-centric offering across most classes of business, particularly for intangible assets. Cyber insurance has a unique opportunity to lead this shift from products to solutions and can be at the forefront of new and exciting customer offerings.

To help businesses manage cyber crises and maintain business continuity, insurers need to build a mix of internal capabilities and external (sometimes exclusive) partnerships with third-party providers – something we are already beginning to see. This should help them provide a full spectrum of services across three key categories: understanding risks, preventing risks and responding to incidents.

Understanding risk: Insurance providers are partnering with technology companies to leverage their deep know-how in customer use cases and software and hardware vulnerabilities. Such a model could provide insurers with much-needed intelligence on key risk factors to help them model and price offerings more effectively, enabling them to cover a greater spectrum of cyber perils. Making these partnerships work, keeping them cost-effective, and leveraging them across all business lines, is a substantial organizational and cultural challenge.

Preventing risk: Our discussions with a number of major insurers suggest that businesses are slow to implement preventive measures. This is, again, due to low awareness and hence low recognition of the value of such services – even when offered free of charge. One way to address this challenge is to provide additional incentives in the form of premium discounts, on the grounds that it should reduce incidents and, therefore, payouts. Ultimately, a move towards preventative services is likely to lead to a decrease in overall premiums, but also bring down loss ratios. Even if this were to occur, it would still remain critical that insurance companies continue to invest in strengthening risk-modeling capabilities, to get comfortable with the new world of lower premiums and potentially reduced claim volumes.

Responding to incidents: Insurance players have already established partnerships to provide a variety of cyber incident response services. However, to date, customer take-up rates for these services have been relatively low (as they have been for preventative services). This is also thought to be primarily due to a lack of understanding and awareness of the benefits and scope of propositions. Industry participants expect the industry to see expansion in this area, as customer awareness of the added value gradually grows.

Rethinking the organizational structure

Becoming tomorrow's insurance company.

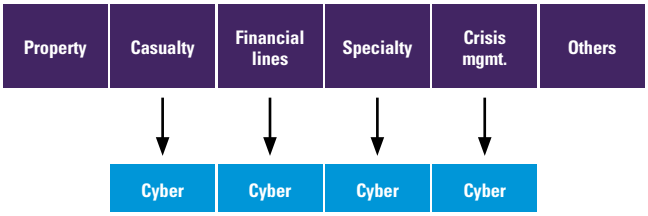
Today's underwriters typically have in-depth experience and expertise in their chosen, specialist (tangible) asset class, whether it's motor, aviation, property or energy. But they are often far less confident when it comes to evaluating the impact of cyber on these tangible assets. Consequently, many exclude cyber risks entirely from their policies or do not account for potential 'silent' cyber exposures. This leaves the door open for significant future losses and could allow more agile, specialized cyber providers to gain market share.

To cope with the increasing blurring of boundaries between traditional product lines and cyber insurance, organizations are creating small teams of cyber experts. But, given the pervasive nature of cyber perils, each separate underwriting team will need to increase its knowledge. In the short-to-medium-term, we believe that insurance companies could benefit from a more collaborative, internal approach to measuring the likelihood and impact of cyber related threats across product lines.

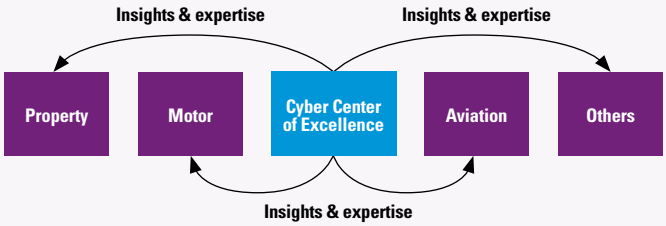
Establishing a standalone cyber insurance business unit – possibly as a Center of Excellence – could bring together and develop critical skills and capabilities like cyber risk modeling, crisis management and digital platforms. These could be applied across business lines and help insurers move through the four waves outlined earlier in this paper, eventually entering into uncharted territory including reputational harm and intellectual property theft.

The creation of a separate stand-alone cyber capability could also help organizations support the shift from product to solution, and the development of both preventative and incident response services. While these services are not currently widespread, either in terms of availability or customer uptake, industry participants increasingly expect these to become critical components of a successful offering, eventually establishing themselves as a new industry norm.

Today's insurance company



Tomorrow's insurance company



Organizational structure

— Cyber typically sits in a broader casualty or financial lines department, and sometimes in a specialty or crisis management department, largely due to the limited scope of current cyber cover.

— From an organizational perspective, creating a standalone cyber department could increase the internal and external profile of this fast-growing business line and help in attracting the best talent

— A separate cyber insurance department could act as a Center of Excellence to provide insights into cyber perils and support risk modeling for other lines of business increasingly impacted by cyber perils

— The cyber Center of Excellence could align with, or work closely with the internal Chief Information Security Office that is protecting the organization from attack.

Service offering

— Current cover typically focuses on data breach, with limited extensions to cover other cyber-related perils

— Most cyber insurers focus on the cyber product itself and do not offer comprehensive crisis management services

— Preventative services are still not widely used, as busiensses are often not willing to pay for them. And, if they are introduced, it could dramatically increase the complexity of the offering, as the customer would have to establish a host of preventative measures to satisfy the terms of the premium. This could cause the customer to opt for another insurer providing a simpler, more traditional product

— Insurers are not confident enough with cyber risk-modeling capabilities to offer preventative services free of charge. Only a few market players have developed a strong cyber response offering to maximize the added value to customers.

— A stand-alone cyber business unit would also focus on developing critical competencies (cyber risk modeling, crisis management services and digital platforms) that could be leveraged to maximize value across other business lines

— One competency – crisis management services – will be core to success in data breach and other cyber insurance segments

— A strong service offering will soon turn from a competitive differentiator into a new norm

— Partnerships will be key as specialized third-party service vendors could provide a broad spectrum of support throughout the crisis management process, including enhancing understanding of cyber risk through cyber maturity assessments, penetration tests, threat assessments, and desktop cyber security exercises. In addition, 'post-bind' services focused on maintenance of the cyber risk, like annual threat briefings, desktop cyber exercises and Board level briefings, could help bridge the gap before the response services get involved

— In the longer term, as more cyber talent becomes available, underwriting teams might build their own niche cyber capabilities, such as cyber property risks, cyber aviation risks, and cyber energy risks

— Data collection, analytics, and sharing will become increasingly important to maximize the value of core business activities.

Challenging the traditional insurance status quo

Eventually, the proliferation of cyber threats and incidents could even impact the traditional structure of underwriting classes, with insurance companies potentially shifting their department structures away from a focus on assets (e.g. property, motor, aviation) to an emphasis on perils (e.g. data breach or cyber terrorism), thereby challenging the status quo of traditional insurance. Such a transition would mean that the underwriters of the future would need to be experts in specific peril types and be able to assess the likely resulting impact on both, tangible and intangible assets.

Insurance company of the future

While the shift from assets to perils could be a significant transition for the overall insurance industry, it may not be as radical as it may originally seem.

Furthermore, with the scale of opportunity appearing to be commonly accepted across major players, there is a sizeable prize available for those insurers willing to rethink strategies and structures for the digital age.

KPMG's cyber insurance practice

Cyber insurance is turning many parts of the traditional insurance market on its head, infiltrating existing asset categories and creating new ones. With its extensive experience, KPMG can help insurance companies navigate the uncertainty by adapting to evolving consumer and regulatory demands, and embracing new technologies to outpace digitally smart new competitors.

We are helping to pioneer the shift in cyber insurance from products to solutions, and work with clients to reshape their organizations to place cyber at the center, as well as providing cyber response expertise to help manage incidents if they occur.

Our efforts are also supported by KPMG's global network of business-savvy cyber security member firm professionals. KPMG's global network of cyber security professionals helps clients understand, prioritize and manage their cyber security risks, so they can take control of uncertainty, increase agility and turn risk into advantage. No matter where organizations are on the cyber security journey, KPMG's teams of cyber security professionals can help.

Reader comments

Actions:

Share with:

Sourcing & notes

1. KPMG analysis based on a range of market sources and market participant interviews.

2. A Guide to Cyber Risk, Allianz, September 2015.

3. Worldwide Cybersecurity Spending Increasing To $170 Billion by 2020, Forbes, 9 March 2016.

4. Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020, Forbes, 20 December 2015.

5. Cyber Insurance and Cybersecurity: The Convergence, Aite Group LLC, June 2016.

6. Can startups disrupt the $20 billion cyber insurance market? TechCrunch, 23 May 2016.

7. 2016 Global CEO Outlook, KPMG International, 2016.

8. Closing the gap - insuring your business against evolving cyber threats, produced in association with KPMG in the UK, DAC Beachcroft and Lloyd's insurers, June 2017.

9. Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020, Forbes, 20 December 2015

10. Cyber risk 2025 – The next 10 years, Allianz, July 2016.

11. Boom in cyber attack insurance predicted to gather pace, Financial Times, 29 December 2016.

12. 2015 Annual Study of Intangible Asset Market Value, Ocean Tomo, 2015.

13. KPMG Consumer Loss Barometer, 27 July 2016.

14. Cyber risk 2025 – The next 10 years, Allianz, July 2016.

Authors

Paul Merrey
Partner
Global Strategy Group
KPMG in the UK
E: paul.merrey@kpmg.co.uk
T: +44 (0)20 7694 5276

Matthew Smith
Director
Global Strategy Group
KPMG in the UK
E: matthewg.smith@kpmg.co.uk
T: +44 (0)20 7694 3060

Matthew Martindale
Director
Cyber Security Lead
KPMG in the UK
E: matthew.martindale@kpmg.co.uk
T: +44 (0)20 7694 2989

Arturs Kokins
Associate Director
Global Strategy Group
KPMG in the UK
E: arturs.kokins@kpmg.co.uk
T: +44 (0)20 7311 3398

Global and regional contacts

Greg Bell
Co-Leader, Global Cyber Security
KPMG in the US
E: rgregbell@kpmg.com
T: +1 404 222 7197

Akhilesh Tuteja
Co-Leader, Global Cyber Security
KPMG India
E: atuteja@kpmg.com
T: +911243074800

Gary Reader
Global Head of Insurance
KPMG International
E: gary.reader@kpmg.co.uk
T: +44 (0)20 7694 4040

Simon Donowho
Asia Pacific Insurance Coordinating Partner
KPMG in Hong Kong
E: simon.donowho@kpmg.com
T: +85228267105

Laura Hay
Americas Insurance Coordinating Partner and National Practice Leader
KPMG in the US
E: ljhay@kpmg.com
T: +1 212 872 3383

kpmg.com/strategy

OLIVER for KPMG

Publication number: 134575-G | Publication date: July 2017

About KPMG's Global Strategy Group

KPMG's Global Strategy Group works with private, public and not-for-profit organizations to develop and implement strategy from 'Innovation to Results' helping clients achieve their goals and objectives. KPMG Global Strategy professionals develop insights and ideas to address organizational challenges such as growth, operating strategy, cost, deals and transformation.