KPMG

MATCHI·BIZ

Cyber Insurance – How Insuretechs Can Unlock The Opportunity

Not just digital, also physical - and intangible assets

Cyber risk is not just a wholly digital risk – it spills over into the physical world of tangible assets as well, e.g. hacking into a fire protection sprinkler system could lead to flooding and damage to physical property. An integrated view of cyber is critical to fully address the range of risks that it can give rise to. Cyber risk is a bridge between tangible and intangible assets, which leaves organisations exposed to a much wider scale of damage, which is not often adequately insured since Cyber Insurance has historically been focused on digital assets, such as client's personal data or transactional data. The increase in cyber attacks along with its wider impact has led insurers clients and insurers to rethink the knock-on effect on other insurance lines like personal (reputation), property (physical damage), intellectual property (competitor information) etc.

The unfolding of Cyber Insurance developments from a single focus on digital to encompassing other asset classes is a nascent one, with current insurers struggling to use traditional methods to model these risks, especially in the light of minimal, and unrepresentative, data. Those who do, will be well positioned to grab significant share of what is growing market.

Intangible assets comprise a growing proportion of value

Between 1975 and 2015, the value of intangible assets as a proportion of total enterprise value (among S&P 500 companies) increased from 17% to 87%[1]. The increase in insurance cover for these assets have not followed suit – due, in part, to the inability of insurers to develop innovative products to insure such assets, e.g. universal methods of brand valuation were absent for many years. Consider the brand value of Coca Cola which is a substantial portion of the value of the company, yet the actual product has been largely unchanged for decades.

From protection to prevention

Cyber Insurance is a relatively recent development in the insurance sector, having been around only since the 1990's. Telecom and professional services companies used this to protect themselves in the event of accidental transfer of malware to clients or the loss of confidential client information. It took the form of a traditional insurance policy with very little specific information on the quantum of payments related to the risk event. The emergence of new cyber risks has created a much more complex landscape and insurers now are no longer expected merely to offer cover after the events but also to assist in the prevention of such risks materialising. It is also expected that insurers will assist post the event to prevent further deterioration or escalation of the consequences.

Companies, on the other hand, are also increasingly crafting multi-pronged responses towards cyber threats. Previous findings suggested that companies may be complacent about cyber risk prevention in the presence of a covering policy. However, the nature of the attendant reputational risks (which itself is difficult to insure against) has elevated the issue towards preparation for the inevitability of cyber risk events. This increased awareness has led to better preparation towards understanding and addressing cyber risks, beyond the tweaking of policy cover elements[2].

A huge opportunity for growth

Predicted to rise from **US$2.5bn** in **2015** to **US$7.5bn** by **2020**, reaching **US$20bn** in premiums by **2025**

Although still a relatively small market, the growth is fuelled by increased and varied cyber risks as well as the growing value of intangible assets. Penetration levels are still relatively low: <15% in the US but <1% in other regions of the world, so there is potential for significant growth[3].

This is both an opportunity and a challenge since insurers have to migrate from a mindset of providing cover to one of actively managing risks, including prevention and event based responses.

2015
global revenue was
$100bn
taken from all segments of the cyber service range (i.e. from risk mitigation to risk transfer and post-incident solutions)

70%
from companies offering risk mitigation services
mostly software or hardware security solutions. The insurance and reinsurance markets were estimated to account for only 2%[4].

However, the growth rate of the Cyber Insurance industry is ten times that of the cybersecurity sector: Global Cyber Insurance premiums are $3-4bn growing at 50% annually vs $70-80bn industry growing at 5%[5].

Companies are under insured - and vulnerable

Global annual losses attributable to cyber-crime are close to US$500bn and is expected to quadruple to more than US $2.1trn by 2019. Yet yearly global cyber premiums are estimated at US$2.5bn which is only 1% of total commercial premiums - and this is focused mostly on digital assets[1].

It is estimated that 60% of FORTUNE 500 companies currently lack any insurance against cyber incidents – mainly due to the lack of adequate Cyber Insurance solutions[1].

Intangible assets are largely uncovered, even though reputational damage post a cyber event (like a data breach) is the single biggest cyber concern of corporate executives, according to KPMG's 2016 Global Consumer Loss Barometer.

Cyber risk is not just about data breaches

Although cyber risk has been associated with digital assets like data breaches, it extends far deeper across multiple other lines of risk. The bulk of the damage due to a cyber event may actually be the physical asset, especially if cyber techniques are being used to gain access to a physical asset. For example:

Home - hacking an alarm system to gain entry to steal possessions.

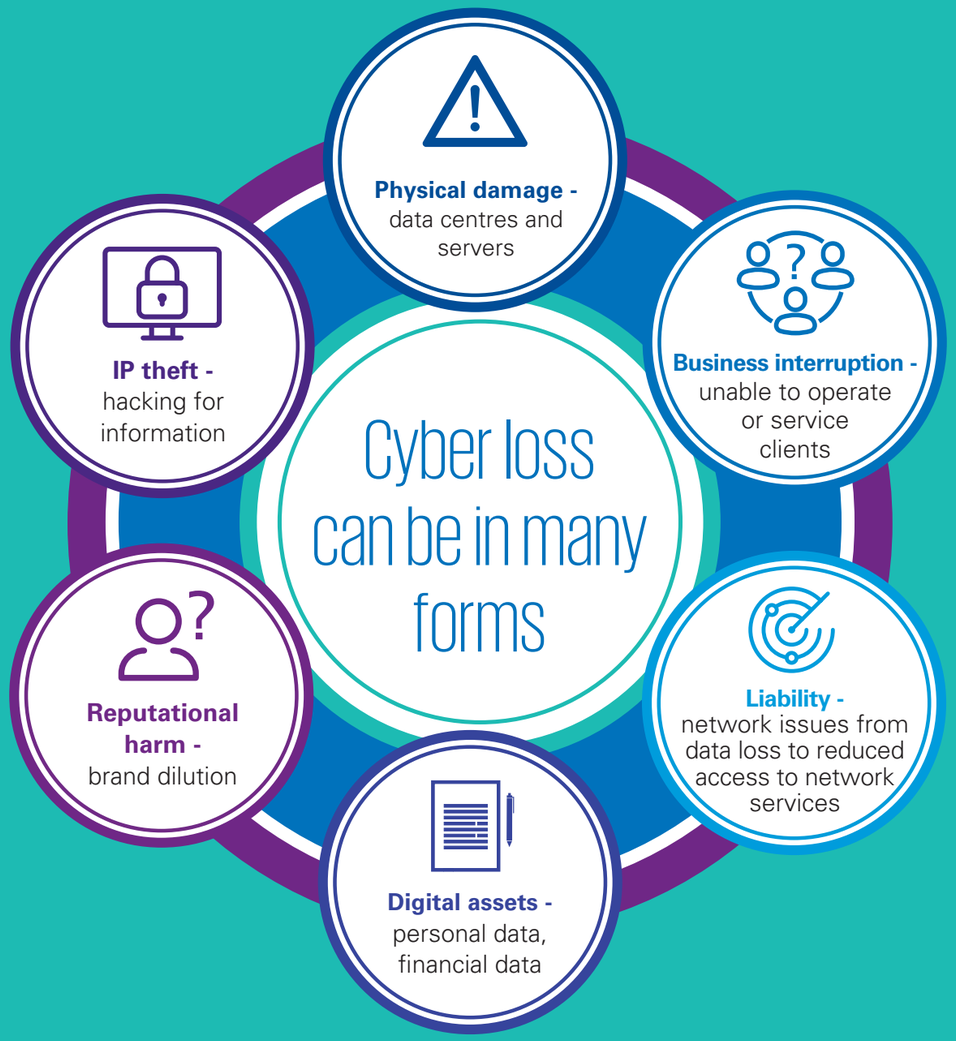
Property - hacking control systems for malicious purposes including sabotage: changing temperatures in competitor warehouses to destroy stock, setting off fire sprinkler systems to evacuate buildings.

Car - vehicle theft by controlling onboard computers to immobilise cars.

Aviation/shipping - stealing customers personal information through on-board internet access.

For these reasons, cyber risk is being recognised as an operational risk and monitored separately from general operational risks.

Cyber loss is both digital and physical



Risk modelling a key competency

The greatest challenge for insurers in developing Cyber Insurance products is the lack of data around cyber-security incidents. Historically, the superiority of risk models led directly to profitability and the ability to differentiate customers on the basis of risk levels. The unwillingness to report cyber events is understandable, given the potential for further reputational fallout which may exacerbate the loss.

A possible solution would be the establishment of anonymised databases for cyber events, which would allow for more rigorous risk modelling.

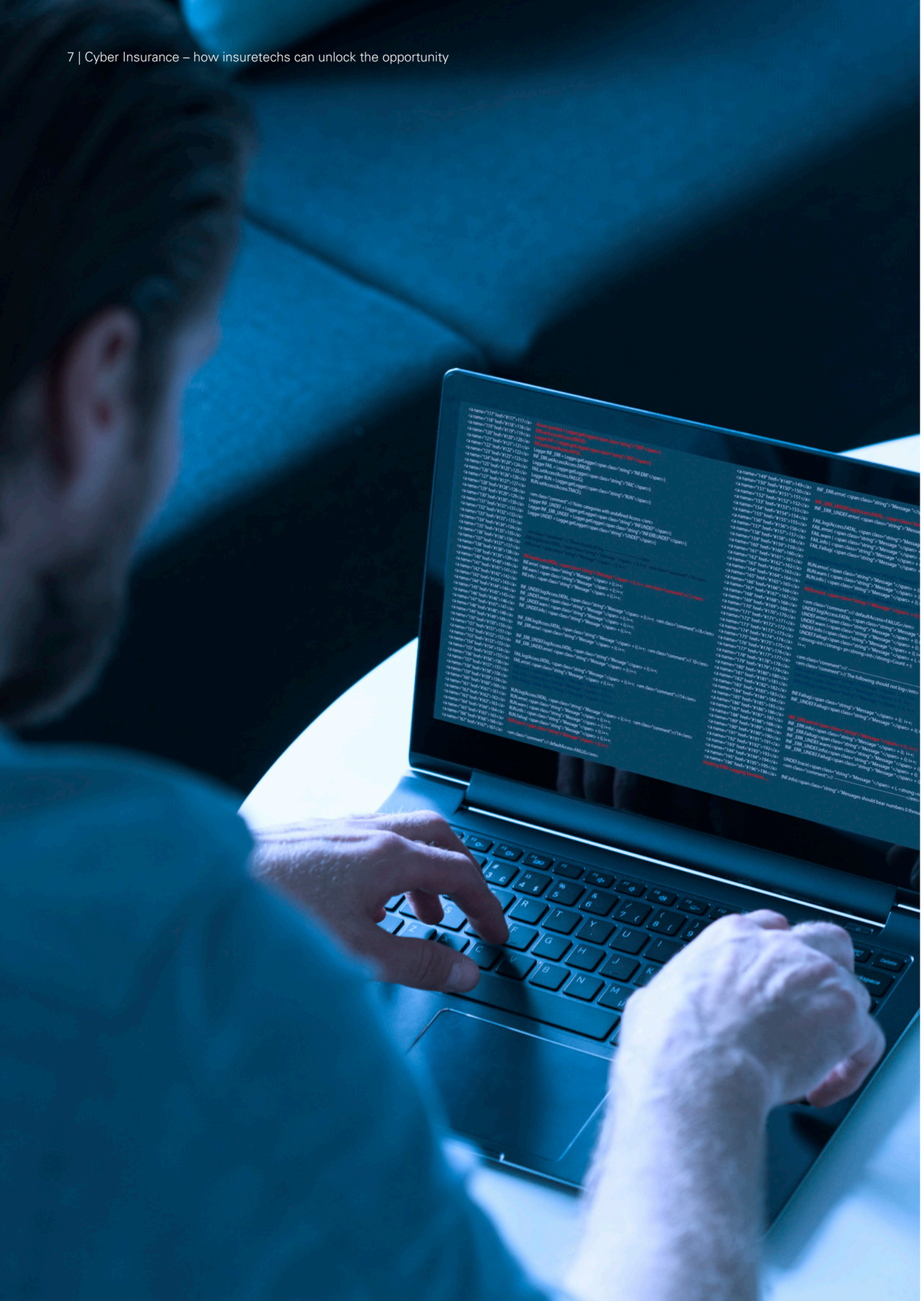
As reporting and aggregation of cyber risk events improve, so will risk modelling capability. However, intangible losses will continue to be a challenge, not least because actuarial and actual quantified losses may be impossible to determine

Reputational damage is another un-modellable risk. However, insured amounts could be heuristic in nature. In some cases it could be the actual costs of mitigating fallout, e.g. costs of engaging PR companies, donations to appropriate NGOs, etc. Alternatively this could cover the costs of cyber-related ransoms.

Cyber Insurance trends

Certain industries have arguably led the way in the storage and protection of data, given the nature of their business that generate huge amounts of data daily. However, newer technologies and the digitisation of universal process had led to other industries also becoming vulnerable to cyber threats. Several trends are emerging[6]:

- The growing demand for Cyber Insurance coverage in sectors beyond healthcare, retail, and financial institutions, such as professional services.
- Some shifts in the factors driving sales, especially as more third parties are requiring coverage.
- The importance of first-party coverage is changing as new causes of loss emerge, such as cyber extortion and funds transfer fraud.
- Growing interest in coverage for bodily injury and/or property damage arising from a cyber event.
- Even though large organizations remain targets, they accounted for less than 20% of cyber losses in 2016. Smaller organizations, including those with less than $1m in annual revenue, accounted for larger percentages of the losses.



The best solution for managing cyber risk is prevention

Managing a cyber crisis is becoming an increasingly important part of the management toolset. Insurers now need a wider range of capabilities, not all of which can be developed in house. The drive towards establishing partnerships with external parties with specific skills is a trend that is increasing. The main component in the management of cyber events are:

Understanding risk: assimilating technical know-how to gain a deeper understanding of the drivers and symptoms of risk events to identify and quantify risk factors to adequately price and structure Cyber Insurance products.

Preventing risk: Increase awareness and implementation of solutions that could prevent risks – these range from simple incentives to clients (premium discounts), e.g. downloading anti-virus software all the way to a fully governed programme of risk prevention encompassing : cyber risk assessment, advisory services, security software, hardware solutions, training of personnel and compliance. Encouragingly, global information security spending increased by 7.9% to reach $81.6bn in 2016, a significant increase compared to the 4.7% additional spending observed in 2015[4].

"If you turn on CloudFlare or a solution we've approved, we will lower the business interruption waiting period from 8 hours or 12 hours to 1 hour". CEO of cyber security insuretech

Responding to incidents: Incident response offerings have been integrated with insurance cover although this is not often used in many cases. A well prepared cyber incident management response system is required to mitigate additional fallout, e.g. including access to a breach coach, forensic support to identify and remediate the cause of the event, customer notification services, credit and ID monitoring and legal support. The main objective of these services is to minimize the potential loss arising from a cyber incident by rapidly coordinating and managing the various aspects of the response from communication and notification of the event to forensic and legal support.

Fight cyber with cyber

It is quite clear that cyber risk will dominate the list of emerging risks as companies grapple with understanding and mitigating these. A singular feature is that these risks can emanate from one person working alone with a computer in a foreign country and could cripple an entire organisation's operations worldwide.

Most Cyber Insurance has been offered by the large traditional insurers. Other insurers are starting to recognise the opportunity and are also starting to focus on niches that they are comfortable with while others are more cautious.

In addition, cyber risk is as applicable to small business as to larger ones – the difference is that the impact on a small business could be devastating yet it is estimated that only 15% of small businesses have Cyber Insurance.

AIG is the largest writer by direct premiums of standalone Cyber Insurance in 2016 and announced that it would add cyber coverage to its commercial casualty insurance in 2018, i.e. move away from issuing policies that do not specify whether cyber losses are covered.

"When you buy affirmative cyber coverage, you should be paying for it." AIG, 2017

"Most of the in-force policies that we have are for small businesses, and I suspect that will continue in the near term. And I say that because I don't think that cyber is adequately priced for larger risks." Argo Group

"I think there's a greater sense of the need for the (Cyber Insurance) product and we think that's a healthy thing and we think to a degree that we'll be there to help solve that problem." Travelers

"The more you talk to specialists the more you come to the conclusion that it's more likely that it's probably not insurable. I think it's clear the risk is accumulating. But the more intelligence we gather from the different countries, and the more places we go, the clearer it is that very significant damage can be created by some parties to other countries." Swiss Re

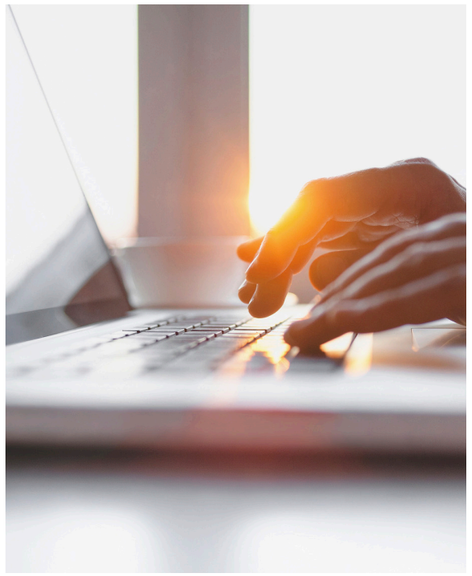
"Every policy that you'll read - and I've read probably a hundred of them now - is different. There are no standards. It's a Wild West out there", Chief of security strategy at SentinelOne Inc.,

Tech startups are starting to emerge in Cyber Insurance with new technologies and value propositions, partly due to the opportunity to exploit a niche as well as solutions to address cyber risks.

Companies and insurers alike need to tap into the rapidly increasing insuretech universe which offers an array of highly sophisticated tools exploiting multiple emerging technologies to prevent and mitigate cyber risks.

Insuretechs that play in the cyber risk space include:

- Cyber risk monitoring
- Cyber risk modelling
- Security readiness
- Cyber Insurance providers



A. Data monitoring on cybersecurity

A key preventative measure is the continuous monitoring of cyber attacks. Several insuretechs have developed solutions which analyse data or hone in on behaviours that are indicative of potential attacks.

BITSIGHT TECHNOLOGIES - offers a security rating platform that continuously analyses data on cybersecurity behaviours in order to help organizations manage third party risk, benchmark performance, and assess and negotiate Cyber Insurance premiums.

B. Cyber risk modelling

The actuarial models of risk based premiums provide challenges to cyber events that are not well documented or transparent. Some startups have utilised cutting edge probability based models to help develop adequate pricing models for Cyber Insurance.

CYENCE - offers an economic cyber risk modelling platform specifically for the insurance industry to understand the impact of cyber risk in the context of dollars and probabilities. For insurers, cyber offers plenty of potential growth but also lots of uncertainty. How likely is it that any given client will be hacked — and, if they are, how much damage could there be? San Francisco-based Cyence is developing a system that can model these risks in financial and economic terms. It has already won its first customers, including Brit Insurance, AM Best and Marsh.

C. Security readiness

Both insurers and companies have to determine their cybersecurity posture, which is essentially the level of trust they have in their ability to address cyber risks. Tech companies are developing quantitative measures of readiness to assist insurers in managing their portfolio of cyber risks for their clients, as well as clients determining their own readiness.

SECURITYSCORECARD - offers a product specifically for insurance companies to assess the security risk posture of potential and existing clients, as well as determining policy premiums.

UPGUARD - offers CSTAR, a cybersecurity preparedness score for enterprises to understand the risk of breaches and unplanned outages and to procure cybersecurity insurance.

D. Cyber Insurance providers

Inevitably, innovators will recognise the niche in an industry and attempt to fill these with focused products and services. Cybersecurity is one such opportunity and several startups are developing products that offer this type of product, competing directly with established insurers.

AT-BAY provides Cyber Insurance for the digital age that empowers clients to embrace technology. The company was founded with the intent to provide insurance products and services that enable companies to innovate despite the recurrent threat of cyber risk. They continuously analyse, model and predict cyber risk, to create the best coverage for clients, and partner with brokers to deliver a comprehensive risk management program.

Sources

1 Seizing The Cyber Insurance Opportunity – KPMG, 2017

2 Cyber Insurance: Recent Advances, Good Practices and Challenges, ENISA, Nov 2016

3 Actuaries Institute – General Insurance Seminar, Melbourne, Dec 2016

4 Global Cyber Market Overview, Uncovering the hidden opportunities, AON, Jul 2017

5 http://searchsecurity.techtarget.com/feature Grossman-Cyberinsurance-market-is-like-the-Wild-West, Oct 2017

6 2016 SURVEY OF Cyber Insurance MARKET TRENDS, Advisen/PartnerRe, 2016