CYBER INSURANCE

GLOBAL TRENDS, INSURANCE CAPACITY AND PRICING

GLOBAL
INSURANCE
LAW
CONNECT

CONTENTS

INTRODUCTION

INSURANCE COMPANIES, BROKERS AND GOVERNMENTS NEED TO WORK TOGETHER TO EDUCATE BUSINESSES ON HOW THEY CAN PROTECT THEMSELVES FROM CYBER ATTACKS AND MITIGATE THE RISKS ASSOCIATED WITH THEM.

As the world becomes increasingly more digital, the risks involved are growing on an exponential scale. Prior to the pandemic, cyber risk was already escalating as businesses shifted to online platforms (including medical and critical infrastructure, online shopping and iCloud). However, the pandemic has accelerated cyber risk as we have shifted our professional and private lives online.

Across the globe, there has been a record level rise in catastrophic losses during the last three to four years and the situation has been exacerbated by the war in Ukraine. While the majority of incidents for cyber attacks are through ransomware, there has been an uptick in the number of state-sponsored attacks not witnessed before. It was revealed in September 2022, for example, that Albania had been the target of an Iranian cyber attack which aimed to disable computer systems used by Albanian state police, in advance of Albania hosting a NATO event on its soil. This sort of sophisticated attack presents further additional pressure on the insurance industry as it debates the limits and meaning of cyber war exclusions.

The level of possible impact on businesses from cybercriminals has become increasingly clear in recent years. These include not only threats to infrastructure, but also to the integrity, availability and confidentiality of the information we digitally capture, analyse and exchange.

We expect that the challenges related to cyber risk will only get worse as attacks become more sophisticated and targeted.

This challenge is, of course also impacting cyber insurance pricing and cover globally, and a two-way push-pull situation has developed. Due to increased demand, there is growing capacity in the market but as the severity of attacks grows insurers are also becoming warier about the clients they are willing to insure, and are requiring higher levels of security from client businesses as part of conditions of cover.

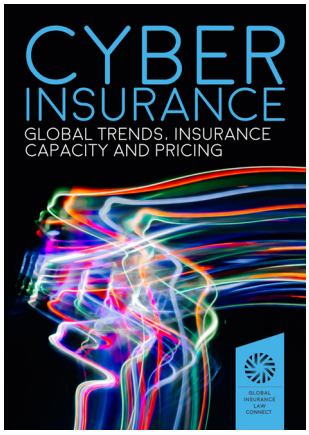
In spite of this, in many countries, there is still a lack of awareness, particularly among the SME community, about the impact cyber attacks could have on their business, how to take basic security precautions, or indeed how a cyber specific policy works with (and is separate to) the other insurance covers that they already buy for their business.

Insurance companies, brokers and governments need to work together to educate businesses on how they can protect themselves from cyber attacks and mitigate the risks associated with them.

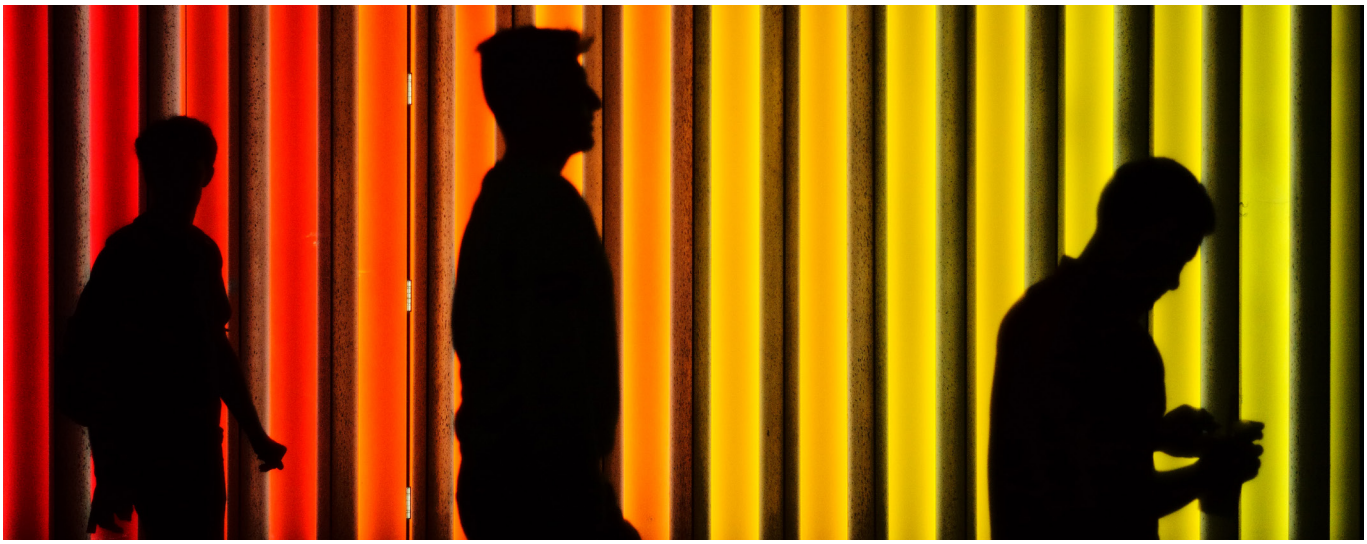
With an eye on the variations of maturity amongst global cyber markets, as well as the different ways that regulators and insurers in different regions have approached the threat, Global Insurance Law Connect has recently asked members in 19 countries around the world to highlight the challenges in their local market, as well as provide analysis of the trends and size of their local cyber market. The results are presented in our first ever global report on the cyber security market, capturing the situation across 19 countries and four continents.

Best wishes

Giorgio Grasso
Leader of GILC's Cyber Special Interest Group



Designed and produced by Doublelix Ltd.
www.doublelix.com



DANGERS VARY BY REGION BUT INCREASED RISK IS THE NEW NORMAL

There has been a steady increase in cyber attacks for at least a decade, reflecting the ever-accelerating move of people's data and business lives online. While the pandemic certainly rocket-propelled the quantity of cyber attacks, it was noted in every continent that this was only an acceleration of the pre-existing trend.

However, there are differences in different regions and markets. North America and Europe were already experiencing high-volume sophisticated attacks on a regular basis from organised criminal groups, and so large corporates are already aware of the damage that these can do. Huge breaches of network systems, such as the theft of the Xbox live user database, and the hacking of user data held by global card-provider Visa, has raised public awareness. Alongside this heightened public awareness the cyber market – that is already well-established in these regions – has been able to raise the level of risk management that companies undertake, with campaigns to help employees prevent criminals from scamming their way into corporate (and private) data and banking.

Jesper Ravn, partner at Ark Law in Denmark commented: "A worrying trend we are currently seeing in Denmark is the destruction of data without a request for ransom. It is clear that hackers are trying to cause as much disruption as possible even without financial gain." In other regions, cyber crime started from a much lower base, often reflecting smaller or developing economies. However, as cyber crime has become industrialised, it has become cost-effective for crime syndicates to target a wider range of groups, and this has caused exponential growth in some of the faster-growing Latin American and Asian economies.

While many countries are facing similar challenges there are some that are being impacted by geopolitical events. Justus Könkkölä, partner at Socrates Attorneys Ltd in Finland commented: " In the last 12 months we have seen an increase in state sponsored attacks. These may increase depending on Finland's accession to NATO."

In Mexico, Aldo Ocampo, partner at Ocampo 1890 says that "after the pandemic, the volume of cyber attacks in Mexico increased 400 times, making it the first country in Latin America to see this growing number of cyber attacks. Hackers have been using emails infected with malware as one of the main tools for stealing information."

Currently, the most predominant type of cyber attacks are those carried out through remote access connections, representing 48% of the volume of attacks in the last year.

The story is the same in New Zealand. Here Peter Fernando, partner at Duncan Cotterill in New Zealand says: "The intricacy of phishing attempts has become more prominent, with New Zealand individuals and businesses being targeted by schemes that are more "localised", including phishing emails written in te reo Māori, and convincing campaigns impersonating banks, charities, IT firms, and government agencies.

"In addition, in the past few years, CERT NZ has received reports of email phishing attempts designed to prompt a strong emotional response, including, most recently, fake relief efforts for Ukraine."

And while the volume grows, the risks in these economies are also locally directed and ever-evolving. In China, Buren explains that malicious programs recently skyrocketed due to increasing 4G network use, a reduction in mobile phone traffic tariffs and other factors. But this trend has now been contained by joint efforts of the CNCERT/CC and the operating platforms.

As a result the threat has of course, instantly morphed into another form. Recent analysis in China reveals that although the number of DDoS attacks has decreased, attackers are using more high-volume attacks to instantly cripple their targets.

As the range of security vulnerabilities that criminals are exploiting continues to amplify, so does the level of threat across all geographies and industries.

AN EVOLVING MARKET FOR BOTH CLIENTS AND PROVIDERS

As the number of cyber-related incidents exponentially increases, so does demand for cyber risk coverage. The issues are different in different markets, however. In some regions, namely Latin America, the Middle East, China, India and the smaller Asian economies, cyber is a relatively new class of business, and insurers have not yet ramped up to provide high levels of capacity. These markets are finding capacity tightly squeezed as demand grows.

In India, while the number of insurance providers offering cyber cover has grown significantly in recent years, obtaining coverage is still becoming more challenging for clients. Sakate Khaitan, partner at Khaitan Legal Associates in India commented: "The market has hardened in the last few years and due to the complexity of cyber threats, insurers have now shifted towards micro level assessment of organisations."

However, in Europe and North America the issues are different. Companies are used to being able to buy high-quality cyber coverage at a relatively low price, and the product has over a decade of history and usage behind it. The shock for many is that, as claims have risen exponentially, new restrictions are being placed on clients, and this is giving some pause for thought in their buying. Brokers are being forced to work harder to deliver for their clients, and in some cases are having to reduce the quality of the terms.

On the insurer side, the rise in claims is bringing not just changes in wordings but has also seen some insurers pulling out of offering cyber coverage across Europe and the US. Mauro Signorelli, Head of International Cyber & Technology at Aspen, commented: "However, all of these markets are dynamic and have many interested players. This richness of capacity means that new entrants are moving to fill the gaps and the pattern is one of evolution and change rather than shortage of availability. Instead, cyber insurance cover in these markets is evolving at a fast pace as the sophistication and severity of incidents increases." As Marijke Lohman, lawyer at Wij advocaten in the Netherlands, commented: "Reflecting the increase in cyber threats and claims, capacity has decreased and premiums have shown significant jumps, often in combination with changes to coverage (including lower caps, partial self-insurance and higher retentions for example) and a much higher level of scrutiny during the underwriting process."

> "PRIOR TO THE PANDEMIC THERE WAS LOTS OF CAPACITY IN THE MARKET WHICH LED TO RELATIVELY LOW RATES. HOWEVER, IN THE LAST 12 MONTHS RATES HAVE GONE UP BY ALMOST AS MUCH AS 100%. THE CYBER MARKET SIZE IN LLOYDS HAS DOUBLED IN THE LAST THREE YEARS AND IS LIKELY TO DOUBLE AGAIN IN THE NEXT 2 YEARS."
>
> MAURO SIGNORELLI, HEAD OF INTERNATIONAL CYBER AND TECHNOLOGY, ASPEN

According to Mauro Signorelli, Head of International Cyber and Technology at Aspen: "Prior to the pandemic there was lots of capacity in the market which led to relatively low rates. However, in the last 12 months rates have gone up by almost as much as 100%. The Cyber Market Size in Lloyds has doubled in the last three years and is likely to double again in the next 2 years."

Quirin Vergho, partner at Arnecke Sibeth Dabelstein, said: "We expect the market penetration of cyber insurance to continue to increase in Germany over the next few years, although insurers are likely to be more selective in choosing risks. This selectivity should also lead to an improvement in IT security in the medium term, as companies need to improve in order to obtain insurance cover."

> "THE MARKET HAS HARDENED IN THE LAST FEW YEARS AND DUE TO THE COMPLEXITY OF CYBER THREATS, INSURERS HAVE NOW SHIFTED TOWARDS MICRO LEVEL ASSESSMENT OF ORGANISATIONS."
>
> SAKATE KHAITAN, PARTNER, KHAITAN LEGAL ASSOCIATES

BRICS AND DEVELOPING NATIONS HAVE THEIR OWN DYNAMICS

While cyber insurance cover has been available across much of Europe and the United States for some years, it is still a relatively new line in the BRICs (Brazil, Russia, India, China) nations, as well as in developing regions such as Latin America. As elsewhere, the increase in the number of cyber incidents means demand has grown exponentially.

Cyber insurance coverage in most BRICs and developing markets is offered through a combination of local and international insurance companies. Although local providers are growing in number, their experience is necessarily less, and as a result the large multinational insurers tend to provide the broadest appetite for those purchasing cyber coverage.

Some markets are restricted by local rules about dealing with international companies. In Brazil, for example, legislation prevents companies from buying cover abroad. This has created an additional incentive for local players in the Brazilian insurance market to offer cyber cover. Without access to the London market, a healthy competitive market has developed here locally, although it should be noted that this is often supported by global companies who have bought and operate local subsidiaries.

João Marcelo Santos, partner at Brazilian law firm Santos Bevilaqua, said: "We expect to see more new players and greater competitiveness and innovation in the market, reflecting the quality of the products developed and the insurance and reinsurance capacity offered."

In China, the history of cyber insurance is shorter, and the market is considerably less developed. In fact, cyber insurance products are generally provided only as add-ons to property insurance policies. This can be tracked back to China's comparatively basic cyber security and data regulatory regime, as well as an underdeveloped network of infrastructure security, which has meant that domestic insurers and brokers have not yet had the confidence to establish separate policies for cyber insurance. When they do, the growth potential – for those with the appetite to survive what could be a wild ride – could be enormous.

It is a similar story in India, where, prior to 2014 cyber-related risks were (in limited form) only covered as endorsements under professional indemnity policies and general liability policies. However, as the nation has encountered growing risk due to rising digitisation, cyber insurance has become more commonly provided as a stand-alone product. After a slow start, currently, many of the largest insurance providers now do offer stand-alone cyber insurance policies in India.

> **"WE EXPECT TO SEE MORE NEW PLAYERS AND GREATER COMPETITIVENESS AND INNOVATION IN THE MARKET, REFLECTING THE QUALITY OF THE PRODUCTS DEVELOPED AND THE INSURANCE AND REINSURANCE CAPACITY OFFERED."**
>
> JOÃO MARCELO SANTOS, PARTNER, SANTOS BEVILAQUA

AN IMMATURE MARKET: CLIENTS, REGULATORS AND MISSING DATA HINDER ASSESSMENTS OF RISK AND PURCHASE OF COVER

One story echoes clearly from every country that we surveyed. Many law firms noted that while there is growing knowledge around cyber security risk, particularly post pandemic, there is still a significant lack of awareness around standalone cyber security insurance coverage and the support it can provide in the event of an incident. It is here that that brokers can play a pivotal role in identifying current trends and educating policy holders.

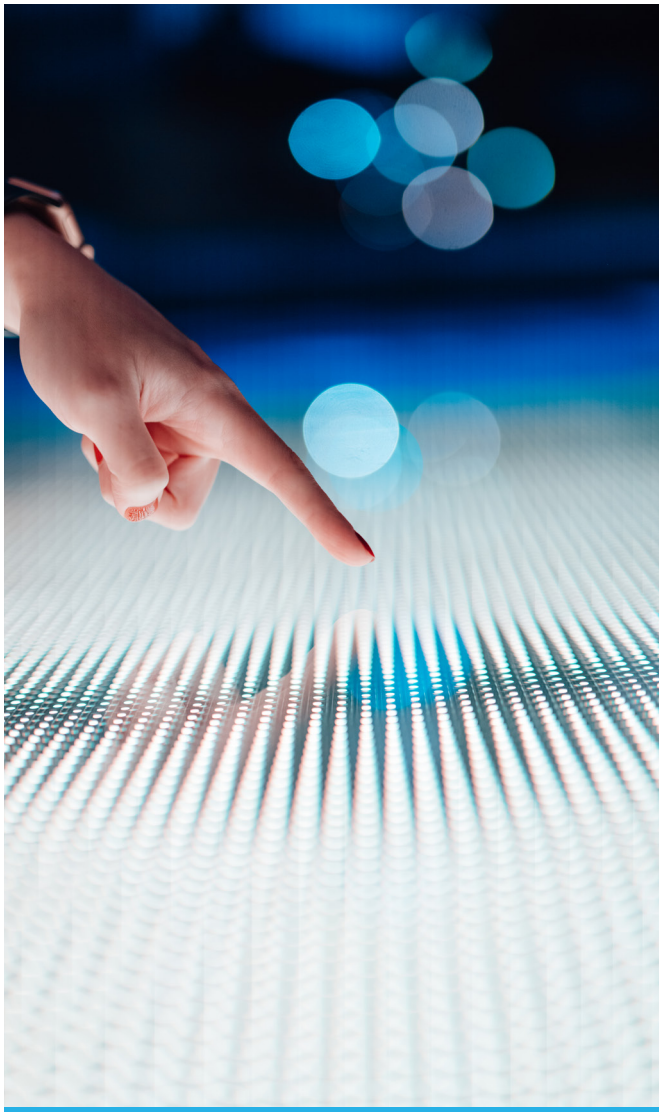
As well as more understanding of the product, insurers are asking for policyholders to take reasonable measures to prevent the risk from occurring or to mitigate it as much as possible. Bastiaan Bruyndonckx, lawyer at Lydian in Belgium commented: "Insurance contracts are characterised by an element of chance, whereas a total lack of security measures would provide almost a certainty that the risk would occur, and a cyber attack will take place. For example, in many cases, it will be required of clients to install anti-virus software and provide a firewall. On the other hand, a number of insurers expect the risk to remain as limited as possible, for example through the requirement to have backups of data.

"However, in some cases, this creates a false perception on the part of the customer when they think they can rely on the cover as they have met the basic requirements to obtain the insurance, but a hack still occurs and they are not covered, which can cause disappointment for the insureds."

Several members, including India, Brazil, China and Mexico, observed that there is a tendency for businesses to look the other way and ignore cyber risk. Many companies see cyber cover as an additional business expense, and in some regions the lack of a data protection law adds to the reluctance within organisations to buy cyber insurance policies. For others, the high levels of cyber cover to comply contractually with their business partners means that getting the appropriate coverage is often unachievable. And in countries such as China, where there is a nascent market for cyber insurance cover, the scope of coverage is not yet comprehensive and detailed enough to cover all practical losses.

Jan Holthuis, partner at Buren in China, said: "There are difficulties in the supervision of cyber security insurance. China's cyber security insurance is still in the early stages of development, and regulators are not equipped with corresponding legal experience. In addition, insurance companies are missing relevant data and information, which are essential to set insurance product rates and design insurance policy."

This was also noted as a challenge in India and Mexico where buyers are reluctant to share data that can help insurers evaluate risks or safely detect the rate of cyber attacks. The lack of actuarial data on cyber attacks in some countries also inhibits robust risk assessment. This often leads to more expensive cyber insurance premiums, which further alienates a potential buyer.



SEVERAL MEMBERS, INCLUDING INDIA, BRAZIL, CHINA AND MEXICO, OBSERVED THAT THERE IS A TENDENCY FOR BUSINESSES TO LOOK THE OTHER WAY AND IGNORE CYBER RISK. MANY COMPANIES SEE CYBER COVER AS AN ADDITIONAL BUSINESS EXPENSE, AND IN SOME REGIONS THE LACK OF A DATA PROTECTION LAW ADDS TO THE RELUCTANCE WITHIN ORGANISATIONS TO BUY CYBER INSURANCE POLICIES.

NEW THREATS ON THE HORIZON

As technology advances and becomes even more intrinsically part of our lives the risks associated with it will only continue to grow.

Jehan Mata, partner at Sparke Helmore in Australia, commented: "As networks grow and organisations become more reliant on IT systems, it will become increasingly difficult to protect and defend individuals/organisations from cyber risks. Cyber criminals will continue to capitalise on people's fatigue and lack of focus. The cyber risks associated with the metaverse (which is unregulated) are yet to be addressed and privacy issues associated with a virtual world are likely to have a substantial impact on the cyber landscape."

Other growing threats include ransomware as it makes use of anonymous digital currency and is rather difficult to target. In addition, as 5G coverage increases globally across industries, it is still unknown what types of attacks will be generated through these networks. Last but not least, in terms of blockchain technology, the security of blockchain-related systems will be subject to frequent attacks from cyber criminals.

In addition, Fernando Blanco Gamella, partner at Blanco y Asociados in Spain commented:"I think the entire tech industry agrees that the future of cyber risk will be concentrated in the cloud. The advantage offered by the cloud of transferring huge amounts of data between many users can at the same time become our worst enemy, as it can pose a huge risk if the data is not encrypted correctly and is easily accessible to cyber attackers. A bigger problem would be if there is already a virus installed in the cloud that gradually diminishes our systems. The costs of cleaning up a virus that infects the cloud can be catastrophic."

LOOKING TO A BRIGHTER FUTURE

The constantly evolving cyber landscape has been a challenge for not only the insureds and insurers but also for regulators and governments. However, it does seem as though the shocks of the last couple of years are forcing a rapid maturing of the market that could, in the future benefit all these parties.

Over the past 24 months the cyber insurance market has undertaken a significant adjustment. A new baseline has been set with regards to premium, deductible levels, coverage availability, capacity, and underwriting rigor. This could bring real benefits in terms of making the cyber market profitable, and opening the doors to much needed global capacity, particularly in developing economies, as well as to more security of relationships between clients and insurers.

REGULATION WILL HELP IMPROVE SECURITY TOO

The introduction of new regulations will also help in the fight against cyber incidents, according to members in India and Mexico. In India, it is hoped that a new data protection law will be implemented. With the introduction of set standards and penalties for data privacy and cyber security, the dynamics of cyber risk are likely to change. As compliance measures and stricter penalties are imposed by the authorities, cyber insurance policies are likely to move from precautionary measures to an essential business protection decision for organisations.

Governments in some markets, such as Australia and Taiwan, are already passing new legislation relating to cyber insurance. C.T. Chang, partner at Lee and Li in Taiwan, noted: "The government authority has been encouraging enterprises to purchase cyber insurance. For example, the status of cyber insurance coverage is part of the corporate governance evaluation for listed companies."

In Brazil, regulatory changes are being discussed but are yet to be defined. However, in other markets, like Turkey, there is currently no regulation in place for cyber insurance. Mahmut Barlas, partner at Durukan in Turkey, said: "The current lack of legislation brings in uncertainty of cyber cover causing grey areas in the interpretation and implementation."

In New Zealand, going forward there will need to be more focus on directors' responsibilities for cyber risk, in addition to a regulatory focus. That regulatory focus will need to include both domestic and international aspects, as the increase in overseas legislation being imposed on NZ-based entities, such as the GDPR requirements.

CONTRACTIONS IN COVER

While in most countries, increased legislation and regulation around data and cyber crime is only helpful to insurers, there are instances where it is creating barriers to insurers providing cover. Examples of this include:

GDPR

The implementation of GDPR-style regulation in countries such as Brazil, has meant that there is growing momentum for court action contesting the insurability of fines. While none of the member firms are currently seeing such legal activity, it is very definitely a cloud on the horizon. Belgium, Finland, Germany and Italy all have ongoing regulatory and legal debates around the implementation of laws surrounding GDPR. Insurers are already taking action in some jurisdictions. For example, in Belgium, a number of cyber insurers now exclude GDPR fines from coverage, as the risk can be very high. This trend could catch on fast if even one legal challenge comes to court in Europe, where GDPR is an EU-wide piece of legislation.

EXTORTION CLAIMS

Similarly, while there have been no specific legal challenges yet to the payment of extortion claims it remains under discussion in most jurisdictions. Those insurers that do insure payments include significant exclusions within their policies, but it is likely that there will shifts to policy coverage in this space in the next couple of years.

CLIENT KNOWLEDGE/IT GAPS

Finally, and most significantly, as already noted earlier in our report, insurers are becoming increasingly unwilling to carry the can for clients' own gaps in well-documented security precautions.

Jan Holthuis, partner at Buren in China noted: "From the demand side, the general public lacks sufficient willingness to defend against cyber security risks and private information leakage. Their reluctance to invest in relevant insurance hinders the development of cyber security insurance." For larger businesses, one of the key limitations observed is the lack of awareness among board of directors regarding cyber risk. Further, there also seems to be a gap in deciding whether they should address it through a combination of cyber security spending, self-insuring the risk or whether they want to transfer it to an insurer. Clearly there is a gap here waiting to be filled by broker and insurer education programmes to the benefit of all sides.

> "RELUCTANCE TO INVEST IN RELEVANT INSURANCE HINDERS THE DEVELOPMENT OF CYBER SECURITY INSURANCE"
>
> JAN HOLTHUIS, BUREN, CHINA

AREAS OF GROWTH AND PRODUCT DEVELOPMENT

BROADENING THE PRODUCT SCOPE

Insurers face their biggest challenges in creating innovative, cost-effective products that will suit smaller businesses with less-sophisticated IT systems. But there are signs of changes.

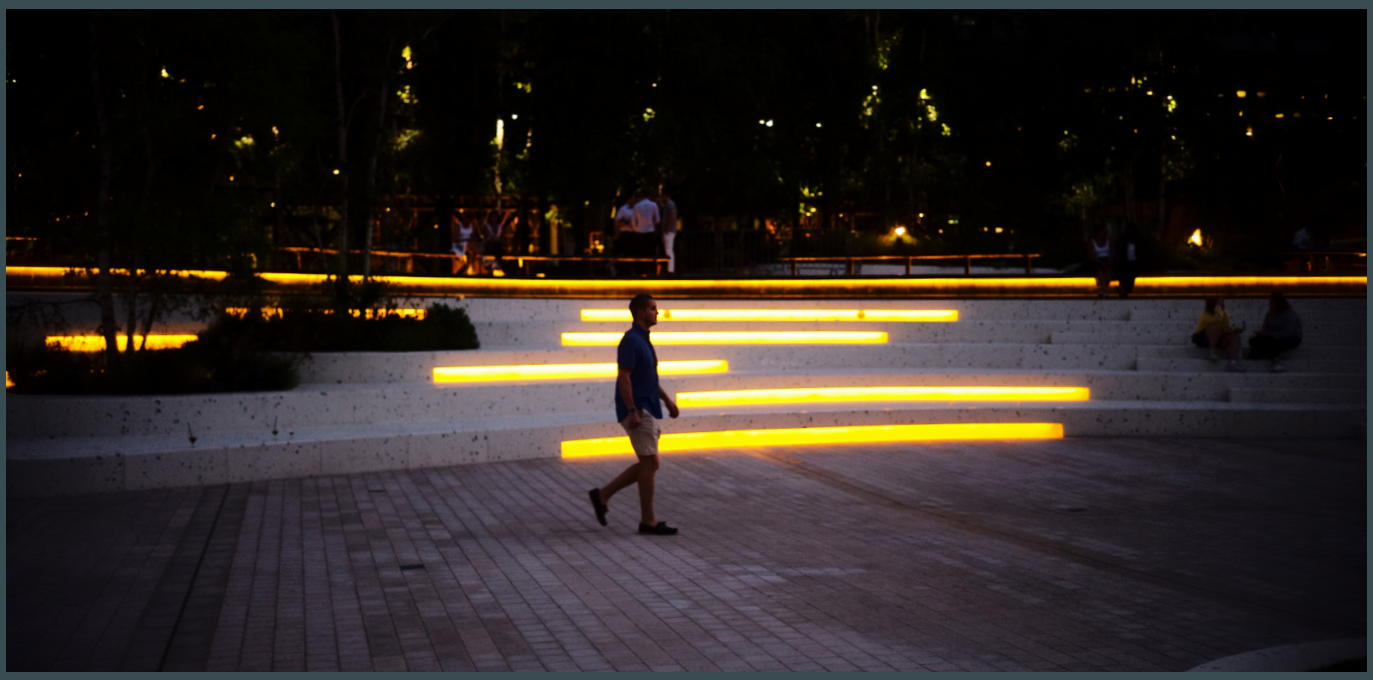
Innovative cyber security technology companies, such as Coalition and Beazley's Lodestone are beginning to emerge, providing instant rapid-reaction response services for companies that experience a breach, alongside initial risk assessments, clean-up programmes, and of course an insurance policy at the core of the offering. These offer a new way forward for cyber clients, giving them access to a suite of services that not only help financially cover losses, but also advise them up front on their own personal risks, help them mitigate them, and finally are there to support in case of a security breach or ransom attack.

PERSONAL LINES

Further growth for cyber insurers could come from the personal lines space. While personal line cyber insurance is offered in most countries, penetration of the product is relatively low but as awareness increases it is likely to be a growth area.

We expect to see a significant uptake of personal cyber insurance as people continue to work from home and rely heavily on technology and their IT systems. Here too new policies are emerging, mainly in Europe and North America for now, but offering a new dimension of cover for solo workers and individuals who rely heavily on their digital network.

Giorgio Grasso, partner at BTG Legal in Italy commented "In the future, insurers should be prepared to offer (i) simple policy wordings and (ii) good services in response to a Data Breach through a tested panel of vendors (legal consultancy, expert forensics, notification players, PR, etc.)."



KEY TAKEAWAYS

For many buyers worldwide, the experience of buying cyber insurance cover for their business is challenging at present. Cyber insurance has become more expensive and sometimes provides limited coverage, particularly outside Europe and North America.

Cyber catastrophes are a new phenomenon and the modelling necessary to accurately predict losses does not yet exist. Jan Holthuis of Buren in China notes that "insurers are missing indispensable tools to design competent insurance plans, such as actionable risk assessment, applicable risk monitoring tools, and plainly, more practical data."

In the short term insurers are likely to include more caveats in policies regarding silent cyber and supply chain attacks and will also adopt more sophisticated pricing techniques. However, the policy review and reset that has already been undertaken by many insurers, plus the global growth in the market does mean that green shoots are beginning to appear. Capacity constraints should soon ease, and product innovation is likely to be shared globally.

Insurers will increase their focus on educating policyholders and providing resources to help them understand and manage cyber risk to facilitate behavioural change. More products are expected to be available (including 24/7 response cover and front-end assistance for policy holders), particularly targeted towards the SME level. The future may be that cyber insurance will be more akin to public liability and/or professional indemnity insurance.

We can be certain that cyber insurance is a market that has the potential to become as globally ubiquitous as car and home insurance, and with that in mind, over the long term, growth is assured on a global basis.

> "INSURERS ARE MISSING INDISPENSABLE TOOLS TO DESIGN COMPETENT INSURANCE PLANS, SUCH AS ACTIONABLE RISK ASSESSMENT, APPLICABLE RISK MONITORING TOOLS, AND PLAINLY, MORE PRACTICAL DATA."
>
> JAN HOLTHUIS, BUREN, CHINA

CONTACTS

Australia
Sparke Helmore Lawyers
Jehan Mata
+61 3 9291 2374
jehan.mata@sparke.com.au

Belgium
Lydian
Sandra Lodewijckx
+32 2 787 90 00
sandra.lodewijckx@lydian.be

Brazil
Santos Bevilaqua Advogados
João Marcelo dos Santos
+11 5643 1066
jmsantos@santosbevilaqua.com.br

China
Buren Legal
Jan Holthuis
+86 21 61730388
j.holthuis@burenlegal.com

Denmark
Ark Law
Jesper Ravn
+45 3333 1000
jra@arklaw.dk

Finland
Socrates Attorneys
Justus Könkkölä
+358 10 322 4360
justus.konkkola@socrates.fi

France
Byrd & Associates
Eloïse Marinos
+33 (0)1 42 61 55 97 eloisemarinos@
byrdassociates.net

Germany
Arnecke Sibeth Dabelstein
Dr. Quirin Vergho
+49 89 388 08 0
q.vergho@asd-law.com

India
Khaitan Legal Associates
Sakate Khaitan
+44 207 034 1430
sakate.khaitan@khaitanlegal.com

Italy
BTG Legal
Giorgio Grasso
+39 02 30322560
g.grasso@btglegal.it

Luxembourg
MOLITOR Avocats à la Cour
Michel Molitor
+352 297 298 1
michel.molitor@molitorlegal.lu

Mexico
Ocampo 1890
Aldo Ocampo
+52 (55) 5339- 5050
aldo.ocampo@ocampo.law

Netherlands
WIJ advocaten
Marijke Lohman
+31(0)20 220 31 91
lohman@wijadvocaten.nl

New Zealand
Duncan Cotterill
Rob Coltman
+64 9 309 1948
rob.coltman@duncancotterill.com

Norway
Riisa & Co
Joachim Dahl Wogstad Skjelsbæk
+47 22 12 15 70
jdws@riisa.no

Spain
B&A Blanco y Asociados Abogados
Adrián Martínez
+34 915 638 407
amartinez@bya.abogado

Switzerland
gbf attorneys-at-law
Marco Novoselac
+41 43 500 48 50
novoselac@gbf-legal.ch

Taiwan
Lee and Li Attorneys-at-law
C.T. Chang
+886-2-2763-8000
ctchang@leeandli.com

UK
Global Insurance Law Connect
Michaela Hickson
+44 (0)7446 954 781
michaela.hickson@globalinsurancelaw.com

US
Global Insurance Law Connect
Michaela Hickson
+44 (0)7446 954 781
michaela.hickson@globalinsurancelaw.com

GLOBAL INSURANCE LAW CONNECT

Global Insurance Law Connect is an alliance of insurance law firms spanning four continents. Inspired by client demand, we have built a formal network that delivers the right advisers in the right places and in the right way for insurance industry clients.

We are:

- Specialist: focusing only on insurance law, advising you on the business of taking risks around the world.
- Commercial: we use the strength and breadth of our formal network to help our clients reduce the time and money they spend on managing risk.
- Creative: whether you are in new or established markets, dealing with familiar or unusual issues, our lawyers have the skills and experience to deliver great outcomes

If you'd like to find out more about Global Insurance Law Connect, contact one of our member firms, or our business manager, Michaela Hickson at michaelahickson@globalinsurancelaw.com

GLOBAL INSURANCE LAW CONNECT

www.globalinsurancelaw.com