Global Cyber Insurance Summit 2021
29 January 2021

INDEMNIFICATION TO PROTECTION

KNOWLEDGE PAPER

Contents

Acknowledgements

Gareth Oldale, Head-Data, Privacy and Cybersecurity, TLT Solicitors UK

P. Umesh, Consultant, Liability Insurance

Shay Simkin, Global Head of Cyber, Howden

The New Normal

COVID-19 has profoundly transformed the way we live and work. It has established a 'new normal' in society. With businesses adopting work from home (WFH), the rising dependence on virtual meetings, disrupted supply chains - the pandemic is creating severe systemic changes in consumer and business behaviour and more significantly the kind of 'risk' that is emerging is unprecedented. These changes are causing incidence of new and unanticipated business disruptions.

After the pandemic hit, entire workforces migrated from working in offices, where cyber security was more controlled, to working from home. This presented immediate challenges, as cyber criminals took advantage of new security and human vulnerabilities.

According to the recent City of London Report The Future of Cyber Insurance: Next Steps for the London Market[1], cyber-attacks now stand as one of the greatest risks to the world economy and the 'new normal' of post-pandemic life as more people use digital technologies. In 2020, the world entered a new era of cyberattacks. Major challenges included bandwidth and unsecure connectivity, employee access issues and phishing, social engineering, and other "human" cyber risks.

Last year saw increased bad actor sophistication, a propensity to pay in ransomware cases, and geopolitical uncertainty - conditions that hackers have found favourable.

The World Economic Forum's COVID-19 Risks Outlook[2] found **50%** of enterprises were concerned about increased cyber-attacks due to a shift in work patterns alone:

What do business leaders think are the most worrisome risks to companies due to coronavirus?

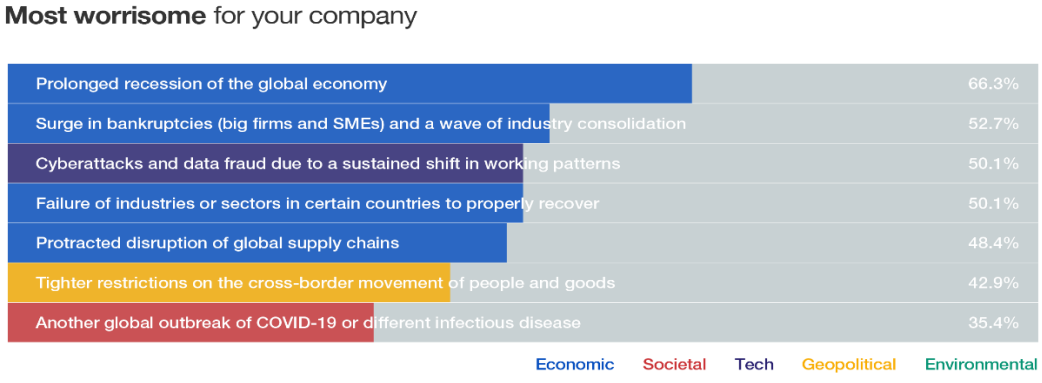

Image: World Economic Forum

[1] https://www.cityoflondon.gov.uk/assets/Business/cyber-insurance-report.pdf

[2] https://www.weforum.org/agenda/2020/05/recovering-from-covid-19-these-are-the-risks-to-anticipate-now/

Ransomware and Data breaches

During the pandemic there has been a sharp increase in Ransomware, where hackers use malware to encrypt a company's data, then demand a cryptocurrency ransom to provide the decryption key.

Insured cyber losses of $1.8 billion in 2019, up an eye-popping 50% YoY

Source: Hiscox Readiness Report 2020

"Whether due to ransomware, human error or a technical fault, the loss of critical systems or data can bring an organization to its knees in today's digitalized economy," says Joerg Ahrens, Global Head of Long-Tail Claims at AGCS. "The inability to access data for an extended period of time can have a significant impact on revenues – for example, if a company is unable to take orders. Similarly, if an online platform is unavailable due to a technical glitch or cyber event, it could bring large losses for companies that rely on it, particularly given today's increasing reliance on online sales or digital supply chains."

Compromised credentials and cloud misconfigurations are tied for second place, in causes of data breaches. Cost of dealing with a large data breach is rising as IT systems and cyber events have become more complex, and with the growth in cloud and third-party services.

Data privacy regulation, which has recently been tightened in many countries, is also a key factor driving cost, as is growing third-party liability and the prospect of class action litigation. So-called mega data breaches (involving more than one million records) are more frequent and expensive, now costing $50mn on average, up 20% over 2019[3].

[3] https://www.agcs.allianz.com/news-and-insights/news/cyber-risk-trends-2020.html#:~:text=Data%20breaches%20and%20state%2Dsponsored%20attacks&text=So%2Dcalled%20mega%20data%20breaches,%2C%20up%2020%25%20over%202019.

India- in the line of fire

According to the Acronis Cyber Readiness Report[4] :

- 31% of companies around the world are attacked at least once a day. India reported almost twice as many attacks per day as any other country;
- 39% of all companies encounter video-conferencing attacks. Canada, UK, Switzerland, and India are among the most affected;
- Since the pandemic, Indian companies have reported more cyberattacks than any other country, with 56% reporting a rise in their IT costs in recent months. This is two times the global average, according to the Acronis Cyber Readiness Report 2020.

31% companies attacked globally, India reported twice as many attacks per day

India, Australia logged the highest number of Ransomware 2.0 incidents[5].
Ransomware 2.0 attacks go beyond kidnapping a company's or an organization's data. According to Kaspersky, at least 61 entities from the region were breached by a targeted ransomware group in 2020. These groups are now utilizing the increasingly valued digital reputation to force organisations to pay hefty ransoms.

Ransomware 2.0: India logged one of the highest incidents

Over 1.17 billion people own a mobile phone in India, which is over 90 percent of the population[6]. Most of the mobile phone users also have a bank account. With a significant portion of the new Internet users emerging from rural India, digital inclusion needs to have security considerations embedded.

According to McKinsey, as businesses struggle to square rising cybersecurity concerns with limited budgets[7], national cyber strategy is becoming increasingly important in protecting business interests – and some countries are doing more than others to develop global cyber power, according to rankings by Harvard Kennedy School's Belfer Center[8]**. The Belfer National Cyber Power Index (NCPI)** measures 30 countries' cyber capabilities in the context of seven national objectives, using 32 intent indicators and 27 capability indicators with evidence collected from publicly available data.

---

[4] https://dl.acronis.com/u/rc/WP_Acronis_Cyber_Readiness_Report_EN-US_200908.pdf

[5] https://www.livemint.com/technology/tech-news/ransomware-2-0-india-australia-logged-the-highest-number-of-incidents-11608807952687.html

[6] https://main.trai.gov.in/sites/default/files/PR_No.101of2019.pdf

[6] https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets

[7] https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets

[8] https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

The US and China lead the pack with the highest intent to pursue national objectives and the necessary capabilities to achieve them. Both countries have invested heavily in cybersecurity. Developments in recent years – such as the establishment of the National Cyber Security Centre and an increased focus in cyber roles across defence and Intelligence services – help explain the UK's overall ranking of 3rd. Perhaps the biggest surprise at the top of the cybersecurity rankings is the Netherlands, which breaks the top five; its digital economy is projected to account for a quarter of its overall economy in 2020 – and expertise in areas like malware. While national cyber power is being pushed to the top of the business agenda, commercial cyber is still one area where most countries lag compared to other objectives like defence and surveillance.

Recently, Ajit Doval, Indian National Security Adviser (NSA) said, "financial frauds have seen exponential increase due to greater dependence on digital payment platforms following the Covid-19 pandemic; there was an increase of 500% in cyber-crimes due to limited awareness and cyber hygiene".

India's upcoming *National Cyber Security Strategy* will deal with cyber insurance, it will include a legislative framework for cyber insurance. The Strategy is in the final stages of approval, and will deal with subjects such as indigenisation of technology and decentralisation of cybersecurity responsibilities. It is also expected to have provisions for funding cybersecurity work. The upcoming policy will also contain frameworks for cyber education - how to process threat intelligence, cyber audits and cryptology.

Global Cyber Insurance Landscape

We are in the digital age, the insurance industry has mobilized to embrace the challenge of providing cyber security insurance to safeguard against the ever-increasing threat of online crime. Part of the challenge is that the economic impact of cyber-crime is both significantly high and extremely difficult to quantify. A study by Cybersecurity Ventures estimates that cyber-crime will cost the world $10.5 trillion annually[9] by 2025.

Cyber-crime will cost $10.5trn by 2025

- In the first half of 2020, ransomware attacks were found to be the biggest cause of cyber insurance claims in North America[10].
- Some of the largest losses were seen in the UK market, including one UK financial services firm which was hit by total losses of **$87.9 million**[11].
- The largest loss from a single cyber event also was in the UK, costing the professional services company in question **$15.8 million**.
- Data from the Ponemon institute's *Cost of a Data Breach Report*[12] earlier this year also highlighted, that healthcare had the most expensive data breach costs, at $7.13m per incident, with energy in second at $6.39m per breach. This was followed by financial services ($5.85m), pharma ($5.06m) and technology ($5.04m).

[9] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[10] https://www.infosecurity-magazine.com/news/ransomware-biggest-cause-insurance/
[11] Hiscox Readiness report 2020
[12] https://www.infosecurity-magazine.com/news/covi19-push-average-breach-cost-4/

The global cyber insurance market is projected to grow by **21%** next year, reaching $9.5bn in value, according to new research by insurance firm Finaria.it

This is as a result of greater recognition of the increasing cyber-threat landscape, exacerbated by the shift to remote working this year. Finaria.it added that the cyber insurance market is expected to reach $20.4bn by 2025[13], as more organizations look to protect themselves from malicious actors.

Cyber Insurance market expected to reach $20.4bn by 2025

The steady increase in claims has been driven, in part, by the growth of the global cyber insurance market which is currently estimated to be worth $7bn according to Munich Re, and is estimated to exceed $20bn by 2025. At the same time the report also highlights that there has been a 70%+ increase in the average cost of cybercrime to an organization over five years to $13mn and a 60%+ increase in the average number of security breaches.

Also complicating the cyber security insurance landscape is the nature of risk faced by companies - is ever-changing as hacking strategies continue to evolve. As illustrated in the Unites States, by countless high-profile examples of cyber-attacks (Target, Uber, Anthem, Equifax, the FBI and NSA). Though it is unclear how much coverage these companies had against this cyber nightmare, the crippling attack illustrates the phenomenally high stakes involved, especially when the targets are organizations whose operations are interconnected with financial, energy, transportation and communications infrastructure. In this environment, fraught with previously unimaginable risk, cyber security insurance is fast becoming a necessary safeguard against threat actors.

The fact that most general liability policies *do not* cover cyber-related risks has led to the emergence of standalone lines of coverage. However, the market for cyber security insurance is still in its relative infancy as entities like the Department of Homeland Security[14]work to engage key stakeholders (academia, infrastructure owners and operators, insurers, chief information security officers, risk managers) and others to "expand the cybersecurity insurance market's ability to address this emerging cyber risk area."

Data: Increased regulations worldwide

In response to growing cyber risks, data protection requirements are being intensified worldwide. The introduction of the EU General Data Protection Regulation (GDPR) in May 2018 has promoted an awareness of data security, in Europe and globally.

In many cases, it is serving as a foundation for other countries. As a result of increased regulation, which often contains detailed provisions on notifying attacks and data breaches, the extent and cost of cyber-attacks are being made public more often. If a breach occurs, companies must also cope with a potential loss of reputation and significant fines.

[13] https://www.privacyrisksadvisors.com/news/cyber-insurance-market-expected-to-surge-in-2021/

[14] https://www.cisa.gov/cybersecurity-insurance

Governance requirements in the area of data security are complex and binding. They are leading to a process of sensitization within companies and to a growing demand for loss prevention measures and insurance protection.

Most major insurers now offer a range of options for cyber security insurance, policies that are usually customized to the unique needs and risks of the insured.

Role of Cyber Insurance

Cyber insurance policy is a risk transfer mechanism used by organisations to protect themselves from losses and expenses arising due to cyber-attacks.

Cyber insurance policy inclusions invariably include:

- Business interruption costs
- Cyber extortion expenses
- Forensic investigation costs
- Administrative fines
- Legal expenses

Some typical exclusions of a cyber insurance policy are:

- Wilful violations
- Property damage
- Loss of Intellectual Property (IP)
- Bodily injury
- Loss due to cyber terrorism/war

Cyber insurance program > $ 1billion in 2020

Facing the prospect of major financial fallout from an attack, C-suites around the world have turned to cyber insurance. Insurers are issuing more policies, and the amounts of protection available are increasing. In 2020, the global insurance community saw the first cyber insurance program exceed $1 billion.

For mature lines of business, like property and professional liability, there is often a target amount available in the market, and the amount companies buy may vary a bit, year to year based on price and budget. Assessing cyber risks and pricing cyber insurance products has been a little challenging because of the evolving cyber landscape and lack of historical data for actuaries to work with. Organisations are also facing challenges to quantify the cyber risks and decide on a suitable cyber insurance cover.

Business leaders are now looking for a quantitative approach to assess their cyber risks along with adequate provisioning and close monitoring of key changes in their risk environment. They are looking to gain objective insights into the cyber risk profile posed in the near future, envisaging cost-effective mitigation strategies, procuring tailor-made insurance structures, to best protect against likely attacks and analysing the impact on risk tolerance, accepted risks and retained losses.

Some of the key areas' organisations should keep in mind while deciding their cyber insurance strategy:

- Ensure the cyber insurance policy covers the most recent types of attacks;
- Identify conditions are complied with to ensure cyber insurance coverage applies;
- Awareness and education of employees and clients

Business heads should discuss with insurance providers:

- Cyber security privacy policies and procedures;
- How the business will cope when a cyber-attack has taken place;
- Financial liability;
- Virtual private networks and other secure remote access.

All organisations need to understand the threat levels in this current environment and the risk that they will face with regards to the ever-evolving cyber setting, address key cyber security issues as well and find appropriate approaches towards covering these cyber risks.

Global Cyber Insurance: Demand Vs Supply conundrum

Instead of looking at it as a year-to-year issue, companies need to think about their actual needs. The problem that most companies face is, determining how much cyber insurance they need? It is also difficult for insurers to understand demand, when the buyers themselves are still trying to identify both their exposure, and their buying appetites.

For insurers to respond to this unique threat, they will have to become comfortable allocating capital to the sector, and that comfort will vary over time, until the industry's body of knowledge becomes sufficient to treat cyber like mature classes of business. Until then, companies will need to invest in protection while working with their insurers to increase the types and amounts of insurance available. For C-suites and boards of directors worried about cyber risks and the availability of insurance, the optimal course forward requires longer-term thinking mixed with near-term action.

"Some companies are buying less cover, due to economic strain

On the demand side, despite the spate of cyberattacks, some companies are buying less cyber insurance or not buying any at all, as economic strain from Covid-19 has caused some them to look at cyber insurance as a luxury.

And while more attacks could stimulate demand, they also create a supply problem, making insurers warier of providing cover and reinsurers less interested in backing cyber liabilities.

In addition, the lack of historical loss data (resulting from the sector's short history) adds another layer of unpredictability for all involved.

For companies looking to bring more cyber insurance into their risk management practices - or buy for the first time - planning is necessary.

Evolving Role of Reinsurance

Cyber risks will evolve, and companies will need to manage that risk, including securing insurance protection. Because of the imminent and frequent cyber threat and the lack of historical experience as an industry - the sector is still in its infancy - there is no easy way to fix the market.

One of the most difficult barriers to addressing the structural challenges that the cyber insurance sector faces is that insurers have disproportionately relied on reinsurance. Reinsurance - allows insurers to lay off risk to another capital source. And in the case of cyber, insurers cede an estimated 50% of the premium they collect to the reinsurance market.

According to a recent HBR article[15], the concentration of capital among reinsurers is simply striking. Four reinsurers account for more than 60% of premium - and that cohort's concentration could grow as a result of market volatility in the coming year, as smaller players reassess their commitment to cyber. In fact, more than 75% of the reinsurers writing cyber reinsurance have less than $100 million in premium, and most of them less than $50 million. With the largest reinsurer in the market likely seeing more than $500 million in premium, it's roughly the same size as the collection of companies writing less than $100 million, based on known data.

"4 Reinsurers account for more than 60% of premiums

Based on the insurance and reinsurance market dynamics at hand, there is the potential for increases in demand over the short and medium term to outpace supply.

Meeting a rapid spike in demand on a relatively new risk could result in a significant increase in losses, too. Accepting that sort of risk in a niche market is not the same as doing so more broadly, which ultimately could lead to shortages in capital (and reduced availability in the market) for cyber insurance.

For (re)insurers to respond to this unique threat, the industry has to become comfortable allocating capital to the sector, and that comfort will vary over time, until the industry's body of knowledge becomes sufficient to treat cyber like mature classes of business. Until then, companies will need to invest in protection while working with their insurers to increase the types and amounts of insurance available.

Conclusion

The insurance industry, including its clients, need to realise that *cyber is not just an IT risk* but a governance issue to cater to data integrity. Additionally, as our world becomes increasingly digital, insurers would need to enhance their cyber capabilities and rethink their organisational structures in their quest to shift insurance from products to solutions.
There is an array of associated disciplines: governance, data privacy, cyber security, risk management, legal, regulatory, underwriting, pricing and effective claims response – all of which require an integrated understanding.

Structural Issues affecting the Global re/insurance industry: The dynamic of low prices and high risk - has negatively influenced cyber insurance market's ability to continue to grow at its previous aggressive rate – and has led to a profound shortage.
Potential causes impacting the size of the cyber insurance market:

1. Market penetration of cyber liability insurance remains relatively low among businesses
2. Poor Cyber Health of organizations
3. Increase in Scale of cyber-attacks
4. Increase in Sophistication of cyber-attacks

One of the most difficult barriers to addressing the structural challenges that the cyber insurance sector faces is that insurers have disproportionately relied on reinsurance. Based on the insurance and reinsurance market dynamics at hand, there is the potential for increases in demand over the short and medium term to outpace supply. Meeting a rapid spike in demand on a relatively new risk could result in a significant increase in losses, too. Accepting that sort of risk in a niche market is not the same as doing so more broadly, which ultimately could lead to shortages in capital (and reduced availability in the market) for cyber insurance.

For (re)insurers to respond to this unique threat, the industry has to become comfortable allocating capital to the sector, and that comfort will vary over time, until the industry's body of knowledge becomes sufficient to treat cyber like mature classes of business. It is hoped, the 'Indian reinsurer', GIC Re would lead the Indian insurance market in establishing an institutional mechanism:

a) *Collaborate* with cyber security agencies whilst also working on a legal and insurance contractual framework;

b) *Liaise* with the insurance regulator to ensure that the business of cyber insurance is seen by the regulator in a different light: For instance, as the cyber insurance policy is a risk transfer mechanism for cyber risks, even the IRDAI working group has opined against standardization of cyber liability insurance as it might impede innovation and hinder adaptation to evolving industry needs, and it may lead to price-based competition instead of developing competencies for agility to design new products suitable to new environments;

c) *Equip* the Indian insurance market to offer appropriate commercial cyber solutions – mitigation and minimum standards across underwriting, claims, emergency responses and segmented market product solutions, and;

d) *Educate* - As of now, the cyber insurance market is lacking in proper cyber education. Insurance professionals are missing the cyber language, and as a result, all roles within the industry are not performing as well as they could, and as well as they should. Insurance is a risk transfer mechanism, and if it has to remain relevant to clients, they must be helped to identify, understand and manage those emerging risks.

According to Shay Simkin, Cyber Policy[16] is a very technical product, and in order to properly manage the risk there is a real need to know technology. Forming the policy requires a deep understanding, both in the constantly changing cyber space, and in insurance. Unlike other insurance policies, the main persona we are interacting with is the CISO/CIO. Therefore, there is a need to know the proper terminology, the "Cyber language".

Integrating People, Processes, Technology and Cyber Insurance: Therefore, organizations need to improve their *Cyber Hygiene* among employees and customers, conduct audits, reduce their risks, and adapt AI to improve their cyber security and data protection to be able to determine the cyber insurance required. After all, the premiums cannot keep chasing claims and/or the anti-selections for the insurers - will not improve the situation as desired.

Developing the Cyber Liability insurance market in India: For businesses, firms and the government concerned about cyber risks and the availability of insurance in India, the optimal course forward requires longer-term thinking mixed with near-term action
The suggestion is for GIC Re to take the lead for the Indian market, from the perspective of raising awareness, cyber insurance penetration, risk improvement, legal/regulatory compliances, bringing the right capacities, and setting minimum standards across all inter-related disciplines of underwriting, claims and service management cannot be over emphasized.

[16] Shay Simkin, Global Cyber Head, Howden

Expert's View

Silence is Golden – Is it?

When cyber insurance was introduced in the 1990s, the focus was on covering data breach exposures in response to regulations framed by authorities in USA and Europe. Later, with business operations getting more digital and owing to spread of all pervasive influence of information technology, insurers started offering wider coverage. But, there was not much foresight about the seepage of silent coverage in other lines of insurance like property, marine and general liability insurance etc. The devastating NotPetya attack and other high-profile cyber security events, in the recent past, have placed the issue high on the agenda for the insurance industry.

"NotPetya, which struck in 2017 and became the most devastating cyber-attack in history, was a virus embedded into a Ukrainian tax-software program. The virus reportedly shut down 10% of the country's computers and vital infrastructure. The contagion then spread to networks worldwide, infecting more than 2,000 companies in 65 countries, among them shipping company Maersk and FedEx, each reporting $300 million in related losses"

While the quantum of losses resulting from the silent cyber losses is not known, there is no doubt that losses have been paid. It is only post NotPetya and Wannacry making news, the issue of silent cyber assumed significance, because of the crippling losses they caused. A few of the cases grabbed attention of public at large because of the enormous damage they inflicted. Mondelez and Merck cases which are in the public domain are noteworthy. Mondelez International filed a claim to the tune of USD 100 million with Zurich Insurance for losses attributed to the NotPetya cyber-attack. This claim was repudiated based on the policy's war exclusion. Merck also filed lawsuits against more than 20 insurers that rejected its claims under the war exclusion.

As regards reference to some Indian insurance policies is concerned, IAR (Industrial All Risks) policy buyers are aware of the fact that there is no reference to cyber coverage under Section I – Material Damage cover whereas under Section II – Business interruption cover, the exclusion relating to cyber risk reads as under.

"Damage resulting from:

a) deliberate erasure loss distortion or corruption of information on computer systems or other records programs or software.

b) other erasure loss distortion or corruption of information on computer systems or other records programs or software unless resulting from fire, lightning, explosion, aircraft, impact by any road vehicle or animals, earthquake, hurricane, windstorm, flood, bursting overflowing discharging or leaking of water tanks apparatus or pipes in so far as it is not otherwise

excluded unless caused by Damage to the machine or apparatus in which the records are mounted."

However, in the recent past some insurers have started incorporating an endorsement for excluding cyber cover for Section I also. Some other insurers are offering add-ons to bridge the gap and provide specific cover for cyber.

Cyber risk permeates all classes of insurance without boundaries of industries. A cyber event can trigger losses across various lines of insurance – property damage and business interruption resulting from computer systems failure / virus under property insurance, siphoning money through phishing under crime insurance, product liability / recalls from security vulnerabilities under product liability / recall insurance, breach of contract / negligence claims under E&O insurance and for managerial negligence under D&O insurance (FedEx case).

P Umesh Consultant - Liability Insurance

Umesh Pratapa - Silence is Golden – Is it? Certainly not in insurance coverage enunciation. This appeared as a Guest Post: Silent Cyber – Is it Deafening? By Kevin LaCroix on December 30, 2019 Posted in Cyber Liability

Cyber insurance is only a few claims away from disaster. This is why it matters

The following article17 by Thomas Johansmeyer, Head, Property Claim Services (PCS), Verisk was published in the World Economic Forum platform, we have reshared parts of it as it brings out a critical element.

"The cyber insurance market has grown rapidly in recent years. Despite this, low premium prices and high risks are combining to stifle further growth, and leaving many firms underinsured against this growing threat. Here are two ways to boost capacity in the cyber insurance sector. Cyber insurance may still be in its infancy, but over the past few years, we have seen rapid growth followed by what we all hope to be a temporary plateau. Insurers are issuing more policies. The amounts of protection are increasing. In fact, our community has finally seen the first cyber insurance programme to exceed $1 billion. Meanwhile, the breadth of coverage continues to expand. Absent the slowing of growth, it would seem that cyber insurance is maturing, and that businesses are adapting to the new and emerging cybersecurity threat.

Unfortunately, cyberattacks have become more frequent and severe. We've seen ransomware perpetrators become emboldened, with ransoms swelling from five and six-figure price tags to a reported $10 million earlier this year. Hiscox Re reports insured cyber losses of $1.8 billion in 2019, up by 50% year over year. Aggregate losses of that amount against estimated premiums of more than $5 billion is certainly not cause for alarm, even with the 50% growth in claims. Caution, perhaps. But not alarm. If you want to worry about cyber insurance, you need to look at the companies that don't have it.

Despite the rapid growth described above, original insureds often don't have enough cyber insurance – if any at all. The "big guys" – insured firms with protection of at least $200 million – account for about 20% of what is believed to be $5.5 billion in global cyber insurance premium, according to internal research conducted by PCS Global Cyber. That's roughly $1.1 billion in premium.

Already, we can see how delicate this environment is. With approximately 250 insurance programmes in this cohort, it would take only four insured losses of $300 million to wipe out an entire year's premium - and would likely take decades for insurers to earn back such losses.

Even worse, consider the 40 or so companies with coverage of at least $500 million. Two large losses could wipe out a year's premium and take half a century to recover.

On this basis, it would seem that it's just not worth it to provide protection for cyber-risk. Even for companies occupying the tier directly below the big guys - from $100 million to $199 million in premium – the decision to be in this market is tricky. We believe there are around 500 companies in this cohort, and that they account for another 25% of global insurance premium. Likely more. Again, it would only take a handful of losses to decimate this cohort's $1.4 billion in premium.

So, prices are low and the risk is high. This dynamic has negatively influenced the market's ability to continue to grow at its previous aggressive rate – and has led to a profound shortage of cyber insurance. The easiest way to assess this is to consider the companies in the Fortune 500. With only around 250 insurance programmes of at least $200 million in coverage, you'd have to guess that half the Fortune 500 doesn't have that amount of cover. Nearly 10 of the 50 largest cyber insurance programmes cover private companies - with three of those covers ultimately benefitting one insured (in different ways). There's even less cyber insurance in the Fortune 500 than you may think. Broaden your area of concern, and it doesn't take long to see just how few companies have any cyber insurance protection, let alone enough to make a difference.

In the global re/insurance industry, it's no secret that the cyber insurance market has run into some structural issues. The entire pricing exercise – although sophisticated and effective in getting the market as far as it has come – hasn't been tested by a major loss event. And the lack of cyber insurance penetration would blunt the effectiveness of such a scenario, to be frank. More challenging, though, is the fact that more capital isn't being allocated to the sector. Especially for large risk programmes, insurers need to deploy significant amounts of capital. Historically, they have relied heavily on reinsurance support. (An estimated 40% of cyber insurance premium is ceded to reinsurance). Reinsurers, currently, aren't deploying more capacity to the sector.

There are two ways more capital could flow into cyber insurance. The first is data. In the early days of the cyber insurance market, there was no industrywide view of cyber insurance data. After all, the market was so concentrated that nobody needed such a mechanism. The handful of players in the market pretty much saw everything. Since then, as the market has grown, it has also become increasingly siloed. And while the largest cyber insurance underwriters may still see a lot, there are wide swathes of the market they don't – reinsurers also often do not get the full picture. As you can see from the analysis above, we've begun to find ways to remedy this problem, but the PCS team is still in the early stages of that effort.

The second way to get more capacity into the cyber insurance market (which would benefit from improved and increased data) is retrocession. As insurers purchase protection from reinsurers, reinsurers also purchase protection on their portfolios – in the retro market. To

date, retro has only been available on a limited, tactical basis for cyber reinsurers. There are few players with capital to allocate to the space who don't face unreasonable increases in concentration risk by writing retro. The problem is further exacerbated by an unwillingness of retro buyers to share data, because they are likely buying protection from an existing or future competitor. Developing a consistent, reliable, and robust retro market would help provide increased capacity all the way down to the original insured."

The complete article appeared in the World Economic Forum platform: ***'Cyber insurance is only a few claims away from disaster. This is why it matters'***
by Thomas Johansmeyer, Head, Property Claim Services (PCS), Verisk

Cyber education is the key to development of Cyber insurance

It is to be understood that in order to become a cyber insurance specialist, one needs to be equally knowledgeable on cyber risk management, cybersecurity products, and the changing landscape. The biggest hurdle to the development of Cyber insurance is not the market, product, or the clients. It is the insurance industry where only minimal efforts and resources have been spared to prepare the set of skills needed for underwriters, claims handlers, and brokers.

As of now, the cyber insurance market is lacking in proper cyber education. Insurance professionals are missing the cyber language, and as a result, all roles within the industry are not performing as well as they could, and as well as they should.

Brokers are struggling with selling the policy, and with advising their clients on the right coverages, limits, endorsements, etc. They also lack the confidence to speak to the client's technical figure and to truly understand their needs and challenges. As a result, the broker will most likely shy away from the deal, as they feel that they can't perform as a consultant it is expected to.

Underwriters have already proven that their lacking knowledge can cause great consequences. The inability to understand the magnitude of ransomware attacks has led to huge losses for insurers in the past year. Ransomware attacks reflect the changing nature of the risk and therefore places huge importance on underwriters needing to be up to date to be able to truly understand the challenges an organization is facing.

Claims Professionals obviously need to be educated as well. When an attack occurs, fast response, proper notification, and activation of the different roles along the response chain is crucial and can make a huge difference. a contract, therefore, understanding the wording and being able to interpret its meaning is vital.

Clients are still not quite sure what "cyber insurance" actually means and how it can help them in managing their cyber risk. Even though it seems like the cyber product is well-known, clients are still asking 'what exactly can be covered?' 'Are certain things even insurable?': it is not their fault.

As the cyber market toughens coverage and pricing are going to be reflective of the actual underwriting material supplied to the carriers, Underwriters are now asking for more details to better understand the risk they are insuring and they are no longer satisfied with just applications forms with a minimal amount of high-level exposure information. All of them are now looking deeper into the information and the security practices and procedures. In order to add real value to clients in the buying process all above stakeholders must all understand that the businesses that is insured are running on connectivity and computers, and if clients have to be helped to manage their new risks, they must be provide with complementary education needed for the next insurance generation. Insurance is a risk transfer mechanism, and if it has to remain relevant to clients, they must be helped to identify, understand and manage those emerging risks.

Cyber Policy is a very technical product, and in order to properly manage the risk there is a real need to know technology. Forming the policy requires a deep understanding, both in the constantly changing cyber space, and in insurance. Unlike other insurance policies, the main persona we are interacting with as brokers, underwriters, claims and other insurance personals, is the CISO/CIO. Therefore, there is a need to know the proper terminology, the "Cyber language".

Shay Simkin, Global Head of Cyber, Howden

References

https://www.cityoflondon.gov.uk/assets/Business/cyber-insurance-report.pdf

https://www.weforum.org/agenda/2020/05/recovering-from-covid-19-these-are-the-risks-to-anticipate-now/

https://www.agcs.allianz.com/news-and-insights/news/cyber-risk-trends-2020.html#:~:text=Data%20breaches%20and%20state%2Dsponsored%20attacks&text=So%2Dcalled%20mega%20data%20breaches,%2C%20up%2020%25%20over%202019.

https://dl.acronis.com/u/rc/WP_Acronis_Cyber_Readiness_Report_EN-US_200908.pdf

https://www.livemint.com/technology/tech-news/ransomware-2-0-india-australia-logged-the-highest-number-of-incidents-11608807952687.html

Telecom Regulatory Authority of India,
https://main.trai.gov.in/sites/default/files/PR_No.101of2019.pdf

https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets

https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

https://www.infosecurity-magazine.com/news/ransomware-biggest-cause-insurance/

Hiscox Readiness report 2020

https://www.privacyrisksadvisors.com/news/cyber-insurance-market-expected-to-surge-in-2021/

https://www.cisa.gov/cybersecurity-insurance

World Economic Forum https://www.weforum.org/agenda/2020/10/there-s-not-enough-money-in-cyber-insurance/

If you would like a copy of the Knowledge Paper
Email on: marketing.ccoe@dsci.in

Disclaimer: This Knowledge Paper has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this article without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information.

We would like to thank the following organisations for supporting the development of the Knowledge Paper

आपत्काले रक्षिष्यामि
GIC Re

General Insurance Corporation of India Limited abbreviated as GIC Re, is the sole reinsurer in the domestic reinsurance market, GIC Re provides reinsurance to the direct general insurance companies in the Indian market. As a truly world-class reinsurer, GIC Re has its permanent offices in UK, Malaysia, Russia and U.A.E. and is continuously persevering to enter new frontiers. Ranked 11th Among the top 40 global reinsurance groups by S&P Global Ratings.

CYBERSECURITY
CENTRE *of* EXCELLENCE
A joint initiative of DSCI & Government of Telangana

The Cybersecurity Centre of Excellence (CCoE) is a glocal hub based in Hyderabad to catalyse innovation, entrepreneurship and capability building in cybersecurity and privacy. It is a joint initiative of the Government of Telangana and DSCI setup to fulfil DSCI's commitment towards creating a safe, secure and a trusted cyberspace.

CITY OF LONDON

The City of London Corporation manages a dedicated programme of engagement with India. This programme is facilitated through the Corporation's representative office in Mumbai, established in 2007. The India programme aims to promote Indian firms who want to do business in the UK and UK-based financial services firm who have a vested interest in India. Through dialogue and engagement with industry and government the Corporation aims to strengthen business links between the India-UK and boost trade of financial and professional services.