insuranceday

July 2023

Cyber risk

Building capacity in an evolving market

Predictive Fleet Analytics

Access a new level of reliable and accurate voyage data

Predictive Fleet Analytics saves you time, money and resource by enabling you to accurately track vessels, predict vessel movements, and anticipate port congestion and delays in minutes.

NEW! Market first

Know a vessel's Estimated Time to Berth (ETB)

Understand port congestion and turnaround metrics

See expected vessel arrivals in the next 5 days

Know a vessel's Estimated Time of Arrival (ETA)

Know a vessel's Predicted Destination

Evaluate vessel trading information and timeline

Understand trade lane traffic

NEW! Market first

Know a vessel's Estimated Time of Departure (ETD)

To find out more about Predictive Fleet Analytics click here or contact us on:

UK/Europe: +44 (0)20 8052 0560
Americas: +1 212 600 3460
APAC: +65 6989 6604

Lloyd's List Intelligence

Cyber risk

Cyber is one of the fastest-growing markets, predicted to reach $22.5bn by 2025. But it is also a market beset by issues including the potential for massive accumulative losses, a lack of excess-of-loss capacity and little understanding of what a major cyber catastrophe event could mean for insurers. Insurance Day looks at what the market is doing to address these unknowns and ensure a sustainable future for cyber

Vitalii Gulenok/Alamy Stock Vector

Editor
Michael Faulkner

Production editor
Toby Huntington

Sub-editor
Jessica Sewell

Editorial
Insurance Day,
240 Blackfriars Road,
London SE1 8BF
Email: editorial@lloydslistintelligence.com

Insurers divided over cyber risk modelling challenges

Insurers are split between those that see cyber as an exceptional line of business and those that think it can be modelled like other insurable perils. The industry could be one major systemic loss event from finding out which view is correct

Better data and analytics are heralded by many in the cyber insurance market as the key to solving issues in relation to the line's systemic loss problem, *writes Francis Churchill.*

In many ways, cyber is just like any other peril and a solid understanding of loss exposure is important for any line of business. Stronger models can help insurers take on better risks and encourage investors to provide capacity.

But in many other ways, cyber is very different. Unlike lines such as property, where the industry knows exactly what a large catastrophe event looks like, there has yet to be a major systemic cyber catastrophe event. The Wannacry and NotPetya attacks gave insurers and businesses an idea of what could happen, but many experts have classed these incidents as near-misses.

Recent analysis from Guy Carpenter, which used models from CyberCube, Cyence and Moody's RMS, suggested when it does occur, a one-in-200-year cyber event could cause losses of between $15.6bn and $33.4bn.

$15.6bn to $33.4bn
Possible losses from a one-in-200-year cyber event, according to Guy Carpenter analysis

For businesses in the cyber market, there are largely two camps – those that treat cyber as they would any other peril when it comes to data collection and modelling and those that believe cyber is fundamentally different and needs a new approach.

Specialist re/insurer IQUW argues cyber is not as different from other lines of business as some might argue.

"There's always the argument there might be new cyber threats around the corner and, of course, that's true. But there's a lot we can learn from the losses of the past to help us prepare for losses in the future," Andrew Lewis, the re/insurer's cyber lead underwriter, says.

Privacy liability is a good example of where losses emerging from the Biometric Information Privacy Act in the US and from litigation over the use of tracking pixels have

Igor Sorokin/Alamy Stock Vector

shaped the way insurers view their risks for the future.

And, Lewis says, the data is there to be used. Since 2014, when Lloyd's introduced a dedicated cyber risk code, the market has grown substantially. This, combined with the high loss activity seen through ransomware and other cyber threats over the years, means there is a lot of data on the frequency and severity of losses.

"If you'd have asked [how much data was available] four or five years ago, that was a difficult question to answer because the loss data wasn't vast and it was difficult to get in. That has changed significantly and there is now a much better understanding of where price adequacy needs to be," Lewis says.

Data granularity

The granularity of underwriting data can also be used to assess individual and portfolio risks just like other lines of business, with models helping to diversify portfolios by industry, attachment point and through geographic location.

"This does have an impact from a technological point of view," Lewis says. Cloud vendors, for example, usually host servers in multiple locations to create different "availability zones", making it unlikely an outage will affect all or even several regions at once. This can provide an element of segmentation for insurers.

"We do a lot of work here on portfolio optimisation: where is the best place to deploy our capacity across that portfolio?" Lewis says. "We look to price layers across the programme to determine where IQUW can provide the most value on a tower."

The data is particularly good for modelling attritional risk, Dan Trueman, global head of cyber at Axis Capital, says. He says many of the good cyber hygiene practices that have developed in recent years – including multi-factor authentication, using virtual private networks and keeping offline back-ups of critical data – were all backed up by the loss data.

"I think data is strong in managing attrition risk because we can pick patterns. And when we have enough data and we've consistently gathered it for a long enough period, we are in a better place," he says.

One of the limitations, Trueman continues, is that data and models look backwards. "Yesterday's events and the analysis of yesterday's events doesn't always teach you what's going to happen tomorrow," he says. This is not a problem that is unique to cyber. "We have the same problems with whether we build on floodplains or not or in places where there are forest fires. But there are some things we can do."

He continues: "There's a pernicious myth in cyber that there isn't enough data and that tends to be pointed out when talking about catastrophe modelling. I argue that's not true. I think we're just not collecting it well enough or doing enough with it."

Data such as null results – unsuccessful cyber attacks – have the potential to be just as useful as loss data, Trueman says.

"We have insureds on our books that have billions of attacks a day, that's the level of data we're looking at. And yet those insureds aren't falling over every five minutes. So what are they doing correctly? There is enough granular data to be making some very interesting decisions when we get to that point," Trueman says.

Granularity of data is particularly important for what Trueman describes as the fourth-order complexity of cyber models – meaning they need to go beyond simple action and reaction.

Cyber is essentially a man-made peril and this means human actions need to be taken into account, he argues.

Cyber actors are people, groups or often nation states with objectives and agency, and often cyber attacks succeed because of human error or because an individual in the victim organisation has succumbed to a phishing scam.

Limitations

Because of this, for some, data has its limits. "The problem is – and it's the same problem we have with political violence – as soon as you introduce a human intent it becomes non-probabilistic because it's completely, totally random," Jake Hernandez, chief executive of risk management business Another Day, says. "You can model weather systems fairly accurately [but] as soon as there's that human consciousness element all bets are off."

"There's always the argument there might be new cyber threats around the corner and, of course, that's true. But there's a lot we can learn from the losses of the past to help us prepare for losses in the future"

Andrew Lewis
IQUW

This is echoed by Simon Margetts, a director at consultancy EY. Modelling is an accumulation of the judgments of academics. For natural catastrophes, this is judgments in relation to physical laws, while cyber modelling is about judgments about likely human behaviour.

Margetts also says the data fails to demonstrate the size of the overall risk: "The raw problem with cyber, which does parallel some issues around natural catastrophes, is that it's difficult to assess the overall level of risk."

Data can help insurers determine how much of a risk an individual company carries relative to its peers, but "the problem we have is we don't know how big that cake is. That's the real money question. How big really is the aggregation that might happen?"

Gianfranco Lot, chief underwriting officer for property/casualty at Swiss Re, agrees. "It's a challenge and requires a lot of investment in getting clarity around what data is needed, what scenarios are thinkable, and can we get a grip on those scenarios?" he says. A good starting point is the challenge of distinguishing acts of warfare from other types of cyber attack.

"We need clarity on what we are covering and which scenarios will then aggregate or not [based on the insured risk] around the world," Lot says. "Currently, the US represents the biggest market in the cyber space, so there's also limited geographic diversification."

Anne Lohbeck, chief underwriting officer for specialty at Swiss Re, says the cyber market will learn from major losses.

When catastrophe modelling was in its infancy in the 1970s and 1980s, there were a number of shock events associated with large natural catastrophes that greatly advanced the models, she says. "Cyber needs to go through what nat cat went through a generation ago.

"Those [aggregation] risks are ever expanding and becoming more vital to the functioning of our industry," she says. "I hope we get to a good advancement on the modelling side first, before we face huge issues."

Wrong dataset

Cyber managing general agent (MGA) Intangic also argues the market is looking at the wrong dataset.

The business, which launched with the backing of Axa XL in March, provides a parametric product that focuses on attritional losses and sees cyber as a high-frequency, low-severity risk.

A small minority of attacks are reported by businesses, Chris Nolan, vice-president of Intangic, says. "70% of the time, companies aren't even detecting ransomware when it occurs in their system, and 53% of the time, attacks infiltrate networks unnoticed," he says.

"The industry is still saying there are limitations in data because they're only looking at a small subset of the actual universe of threat activity," Nolan says. But by looking at other sources – including on the dark web – Nolan claims Intangic can gather a more accurate picture of the threat landscape companies are facing.

The business does not collect any data directly from the companies it insures, relying on its own external assessment of attack frequency on networks to evaluate risk. "We're strictly looking at the outcome: is there a greater volume of attack activity on a [company's] network and volume of attacks being blocked versus another network?" he says.

Nolan argues by focusing on outcomes, not preventative measures, Intangic can bypass the problem of human agency in its modelling. "When we look at the outcome in terms of the amount of malicious traffic on a network, factored into that resulting data is the conclusion of how well or poorly [a company manages its cyber security]".

But for Lewis, cyber is a line of business like any other. Having a cyber expert review a client's security is no different from how property underwriters commission surveys of structures.

"I think because it's a new market and has grown so much, we think we need to be so different in so many ways," he says. "I don't think we need to pretend we're always different. There's a lot we can learn from other lines and that we have learned from other lines."

Margetts' advice is: "Insurers should be doing lots of modelling and trying to collect as much data as possible. But I think there's a limit to how far that will ever take you." ■

"Those [aggregation] risks are ever expanding and becoming more vital to the functioning of our industry. I hope we get to a good advancement on the modelling side first, before we face huge issues"

Anne Lohbeck
Swiss Re

Global insurers wake up to Latin America's fledgling cyber market

incamerastock/Alamy Stock Photo

Cyber capacity from London, Miami and Madrid is being made available to the region, as international companies start to see the segment's growth potential

They took their time, but companies in Latin America are finally waking up to cyber risk, a change of attitude that has translated into strong growth in cyber insurance premiums over the past two years, *writes Rodrigo Amaral.*

It is unfortunate the awakening has taken place on the tails of a three-year hard market, when covers are expensive and underwriters are much more selective than in previous years.

Brokers and insurers have reported ever stronger interest from buyers for cyber covers, a phenomenon reflected in the numbers registered by Susep, the financial regulator in the region's largest economy, Brazil.

The volume of cyber insurance premiums in Brazil's local market grew more than fourfold in the space of two years, moving from Real43m ($8.8m) in 2020 to Real181m last year. The segment is looking quite profitable too, as losses grew at a much slower pace, from Real32m to Real64m in the same period.

At face value the figures do not look all that impressive, considering the size of the Brazilian economy, but the most important factor is the trend, according to market players.

"It won't be long before the Brazilian market reaches Real1bn in premiums. By 2027 it should reach that size," Gustavo Galrão, a partner at cyber insurance start-up Latú Seguros, says.

Brazil is not the only economy with an underdeveloped cyber market. Marsh says it has placed around 500 cyber policies so far across Latin America, which represents a

"The road ahead is a long one. Penetration of cyber insurance remains low. In our portfolio of clients, it reaches only 2%. There is much room for growth"

Paula Ordoñez
Marsh

drop in the region's corporate ocean.

"The road ahead is a long one. Penetration of cyber insurance remains low," Paula Ordoñez, managing director of financial and professional risks in Latin America and the Caribbean at Marsh, says. "In our portfolio of clients, it reaches only 2%. There is much room for growth."

New capacity

The potential for growth is drawing cyber underwriters to the region, with brokers reporting more capacity being made available from hubs such as London, Miami and Madrid.

Liberty Specialty Markets is one insurer that is looking to expand its cyber portfolio in the region. "We want to play a more leading role in cyber," Jelmer Andela, cyber underwriting manager in Europe at Liberty Specialty Markets, says. "We believe we can add value to our relationships in Latin America, although historically we have had more of a following role there.

"Latin America is a large market with companies of all sizes," Andela adds. "The awareness about cyber threats has grown substantially in the region and companies have increased their cyber security maturity levels as a result."

As a consequence, capacity is starting to pick up steam in the region, after a sharp drop in the wake of the pandemic.

"The opening up of cyber capacity in London and Spain for Latin American buyers is recent. There was some capacity available before Covid-19, when it was more or less suspended. But now the appetite is back," Rodrigo Flores, regional cyber manager for Latin America at WTW, says.

Flores adds: "We have placed the largest cyber policy in Latin America, which has a limit of $100m, by raising capacity in local markets, London, Miami and Spain."

Real43m
Volume of cyber insurance premiums in Brazil's local market in 2020

Real181m
Volume of cyber insurance premiums in Brazil's local market in 2022

A programme of such scale requires plenty of participants, as individual lines remain quite limited. "In 2019 we were able to find capacities of up to $10m. Today they reach $5m at most from international insurers that offer cyber capacity in Latin America," Flores says.

But it is not global markets alone that write cyber risks in the region. In countries like Brazil, Mexico and Colombia, local insurers, usually subsidiaries of international groups, are also active in the segment.

AIG and Zurich are the two largest cyber insurers in Brazil, according to Susep. Tokio Marine, which focuses on small and medium-sized enterprises (SMEs), comes third.

Those companies are also strong in other regional markets, as is Fairfax in countries like Chile and Argentina.

New kinds of players are entering the fray as well. Latú Seguros, which operates only in Brazil at present, should soon launch in Colombia and Mexico, Galrão says.

The company, whose name means Latin American technology underwriters, aims to bring international capacity to the region, building on the experience of professionals such as Galrão, a financial lines expert who has worked at the likes of Argos, AIG and XL.

"Our leader will be a London-based underwriter and we are negotiating with Latin American companies to provide capacity too," he says.

Reinsurance reliance

As in other parts of the world, the region's cyber market is reliant on global reinsurance, which means its evolution follows that of North America and Europe, although changes take a little longer to arrive, according to Pablo Jugovic, a lawyer at RAM Consulting in Santiago.

"The trends in lines such as cyber still arrive in Latin America via Lloyd's or the US market, as the region's weight in the reinsurance market continues to be small," Jugovic says.

Following what is happening abroad, cyber insurance forms have become increasingly complex to fill and some underwriters are using forms exclusively about ransomware. Deductibles have gone up significantly and there are also some that apply to ransomware alone.

"The opening up of cyber capacity in London and Spain for Latin American buyers is recent. There was some capacity available before Covid-19, when it was more or less suspended. But now the appetite is back"

Rodrigo Flores
WTW

Co-insurance structures are sometimes demanded by underwriters to participate in the risk.

On the other hand, rate increases have slowed down, from 30% in the fourth quarter of 2022 to 14% in the first three months of the current year, according to Marsh.

"Given the state of the cyber market, it may make more sense to co-insure and work together with other partners to build on the experience acquired over time in the region," Andela says.

Ordoñez says Latin America has traditionally been a market that worries international insurers in terms of legislation and data privacy rules, and, if policies were more flexible some years ago, now they have wordings that are much more restrictive.

That means many buyers struggle to obtain cyber risks, and brokers have had to help them with advisory work.

"Many Latin American companies, unfortunately, still do not have the level of maturity that the market expects. That is why we work with our consultants to improve the quality of the risk," Ordoñez says.

She says cyber security concerns have heightened after the pandemic, and brokers and insurers have strengthened their regional specialist teams. Marsh for instance has around 25 staff in its cyber advisory service.

1,600
Number of cyber attacks Latin American firms are estimated to suffer every second

However, a perception still persists among the region's business community that their companies do not have the heft or financial muscle that could attract the attention of professional hackers.

This is a view that has proved hard to counter, even though surveys show

"The market is offering 44-size shoes for clients who wear 36"

Claudio Macedo Pinto
Bluecyber

Latin American countries, especially Brazil and Mexico, are squarely in the sights of cyber criminals.

Risk management

LatAm CISO, a network of cyber security experts, estimates the region suffers 1,600 cyber attacks every second.

In its 2023 survey of Latin American companies, the organisation found 70% of those companies said they had faced more cyber attacks than in the previous year, despite investments in cyber security.

"There is still a cultural issue with Latin American companies," Jugovic says.

Educating buyers is seen as vital for Latin America's cyber market to achieve its potential, as is offering products that are more suited to the profile of millions of SMEs that contribute to much of the region's GDP, Claudio Macedo Pinto, the co-founder of Bluecyber, a São Paulo-based managing general agent (MGA), says. "The market is offering 44-size shoes for clients who wear 36," Macedo says.

Bluecyber has seen an opportunity in the market and has partnered with Colombia's Sura to offer off-the-shelf packages of cyber insurance covers to families and SMEs. Covers include liability, data privacy liability and breach response.

The MGA also provides a personalised service for small insurance buyers to analyse their cyber exposures and help manage their risk both before and after the purchase of the policy, Macedo says.

Bluecyber is also working with Brazilian brokers to help them better promote the role of cyber insurance covers to their clients.

Pinto says a majority of cyber insurance quotation requests are flatly rejected by insurers because companies have flawed risk management systems.

Another chunk is ignored because Brazilian insurers still do not have teams that are large enough to deal with a large number of submissions for cyber quotes.

Of all quotations put forward, only about 10% result in actual sales, Macedo estimates.

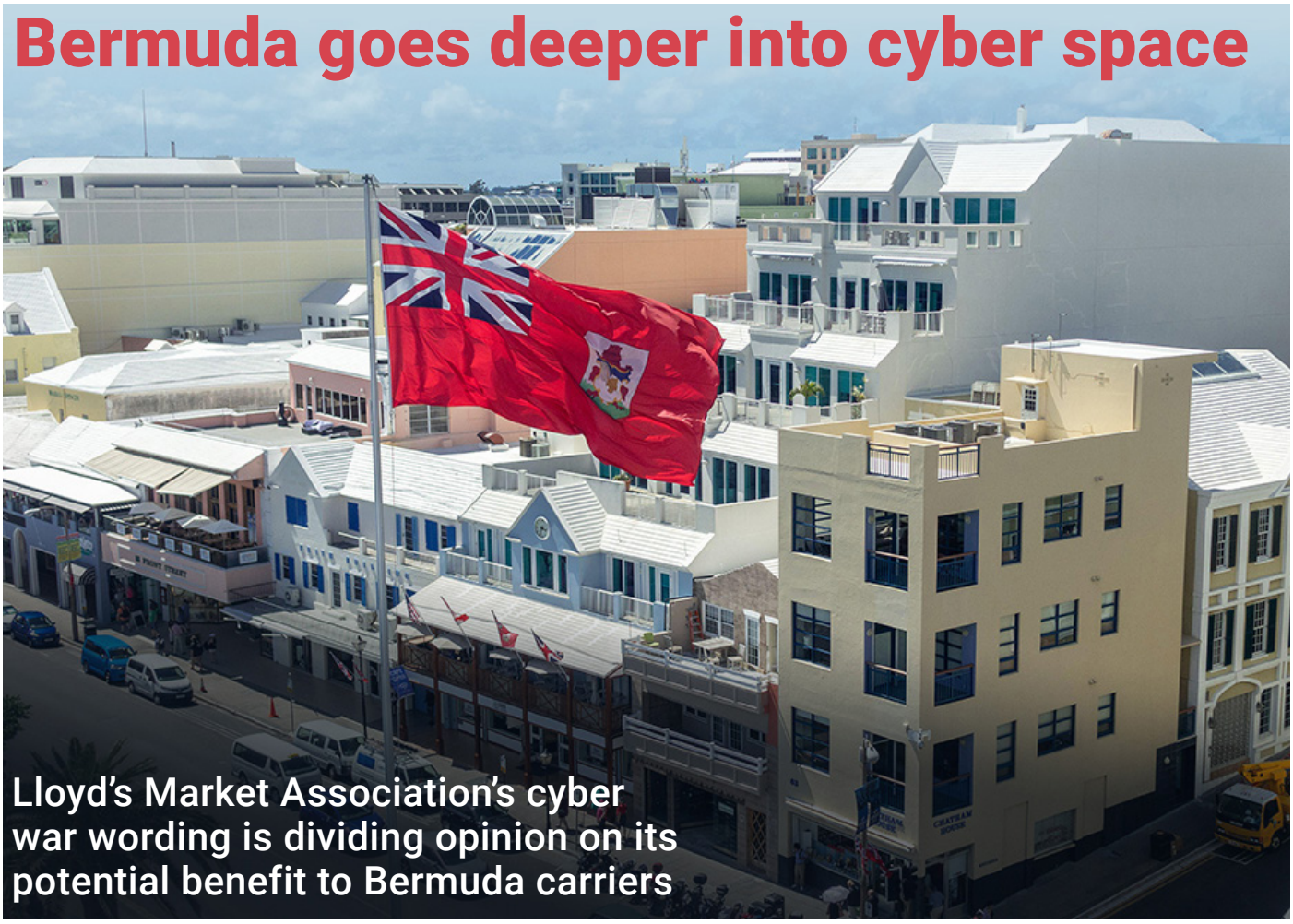
A consequence of this, in his view, is that the smaller, local brokers, which most often deal directly with SMEs, see no point in making a significant investment to understand the technicalities of cyber insurance.

"Many SME brokers are still not prepared to help their clients choose the right protection package," Pinto says.

However, with the global market loosening up a bit, it is likely the Latin American cyber segment will soften a bit in the near future.

"Underwriters remain very cautious, but we see the London market is not asking for sub-limits and is not imposing co-insurance arrangements, and premium rates are more adequate," Flores says. ■

Bermuda goes deeper into cyber space



Norman Pogson/Alamy Stock Photo

Lloyd's Market Association's cyber war wording is dividing opinion on its potential benefit to Bermuda carriers

An undisputed and longstanding hub for property and casualty (P&C) reinsurance business, Bermuda has been attracting attention for its growing expertise in cyber risk, *writes Louise Isted.*

Still regarded as a specialty line in the Bermuda market, cyber accounted for less than 3% of gross written premium (GWP) for all lines in 2021. But the pace of growth is rapid.

According to the Bermuda Monetary Authority, commercial insurers produced total cyber GWP of $4.73bn in 2021, a year-on-year increase of nearly 58%.

Cyber net written premium increased 70% to $3.33bn, the regulator said in its newly published Bermuda Cyber Underwriting Report 2022.

A talking point now is whether Bermuda carriers want to take advantage of the state-backed cyber attack requirements recently introduced by Lloyd's to write more business.

LMA's exclusions

There appears to be a contrast between the traditional and the new carriers in whether they see Lloyd's recently introduced cyber war requirements as a potential shot in the arm for the Bermuda market.

From March 31, syndicates are required to exclude liability for losses arising from any state-backed cyber attack from standalone cyber policies.

Shawn Ram, head of insurance at Coalition, a US-based managing general agent (MGA), says Bermuda has an opportunity to take advantage of the bifurcation in the cyber market between those carriers that adhere to the cyber war requirements introduced by Lloyd's, including the model exclusion drafted by the Lloyd's Market Association (LMA), and those that choose not to.

"For some markets, using a Lloyd's-compliant exclusion is the advantageous option because it's adopted as the language of choice since it's an 'opt-in' selection"

Shawn Ram
Coalition

Coalition has offered excess-of-loss cyber products in the US since 2020 and in Canada since 2021.

In September 2022, it launched in the UK and, the following month, it announced the formation of Ferian Re, an independent Bermuda-based reinsurer that provides capacity across Coalition's cyber programmes.

"The decision to utilise Lloyd's-related language is one that Coalition and Ferian Re can make. We can customise our language based on geography," Ram says.

Capitalised with about $300m from an investor group led by funds managed by BDT Capital Partners, Ferian Re can provide capacity across many product lines, Ram says, while the opportunity in cyber is currently focused on Coalition.

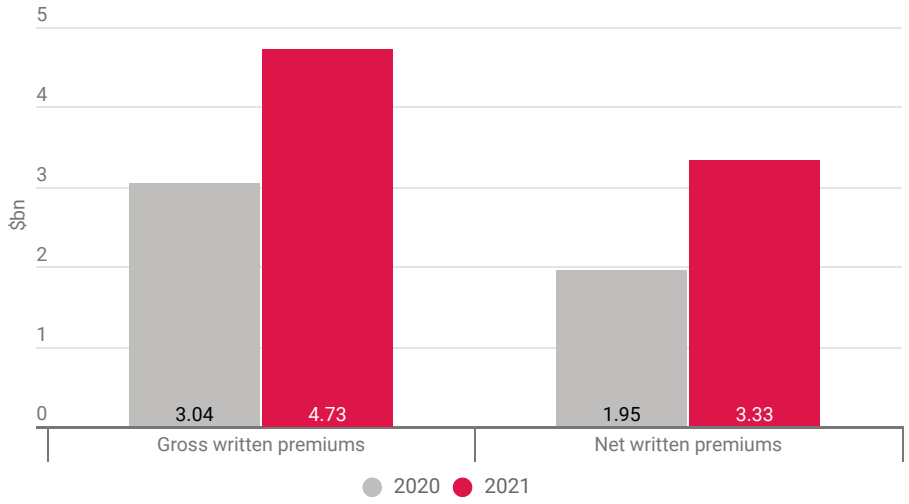
"For some markets, using a Lloyd's compliant exclusion is the advantageous option because it's adopted as the language of choice since it's an 'opt-in' selection, and the excess markets want to follow primary markets that utilise that language," Ram says.

"Coalition spends most of our time in the primary markets. So, you want to have language that excess carriers can follow. Coalition has the flexibility to address the language that is conducive to the market."

Mosaic Insurance, which industry veterans Mitch Blaser and Mark Wheeler launched in Bermuda in early 2021, is looking to grow its cyber portfolio.

Cyber growth in Bermuda is picking up speed

Chart: Gross and net written premiums in the Bermuda cyber market, 2020 v 2021 ($bn)



Source: Bermuda Monetary Authority

Yosha DeLong, global head of cyber at Mosaic, says Bermuda can offer products that cover cyber war risks, adding the new cyber war exclusions are intended to add clarity and contract certainty to the cyber market.

"Implementation and adoption of this exclusion will allow for better understanding of accumulation risk and will open additional re/insurance capacity," DeLong says.

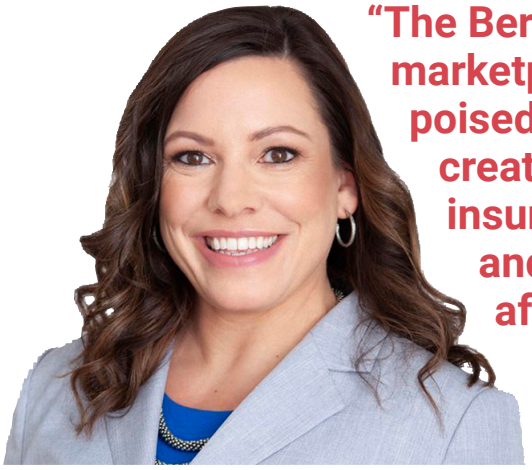
"In addition, the Bermuda cyber marketplace is well-poised to lead in creating innovative insurance solutions and products that affirmatively cover cyber war. Modernisations in underwriting, including inside-out scans and real-time data capture, will allow for comfort around the accumulation exposure presented by cyber war."

Donavan Burgess, senior vice-president and underwriter for digital assets, cyber and professional lines at Relm Insurance, says the industry has adopted an "agile approach" in supporting programmes that employ different types of war wording. Relm is the first regulated crypto insurer to hold Bermuda's Innovative Insurer General Business licence.

Primary insurers based in Bermuda are not restricted by the decisions or choices made by Lloyd's in crafting their war restrictions, Burgess stresses.

"This places us in an advantageous position to continue to provide high-value and tailored cyber risk transfer products to our partnered clients who may, or may not, prefer a Lloyd's-based wording," he says.

"Unlike jurisdictions confined by the mandates of the US or the UK, Bermuda's adaptability and flexibility allow us to fill gaps and meet the needs of clients in a superior manner and set us apart as an advantageous jurisdiction to place insurance," Burgess adds.



"The Bermuda cyber marketplace is well poised to lead in creating innovative insurance solutions and products that affirmatively cover cyber war"

Yosha DeLong
Mosaic

He says: "It is not uncommon to come across programmes that incorporate staggered acceptance of war wording. For instance, a primary insurer may utilise one form of war wording, while one or two layers above may adopt Lloyd's war wording. And then, above this layer and within the Bermuda layer, there is flexibility in choosing whether to follow Lloyd's wording or align with the preferred wording of the primary carrier."

The head of underwriting at a Bermuda-based cyber specialist, who spoke to *Insurance Day* on condition of anonymity, says the island has been able to take advantage of the exclusion.

"New opportunities have surfaced in Bermuda due to the Lloyd's exclusions and we know cedants who have reduced their Lloyd's share to increase [it] in Bermuda," he says.

Noel Pearman, senior vice-president and cyber product line leader at Axa XL, suggests the opportunities for Bermuda to take advantage of cyber war coverage inconsistencies may be limited.

The Lloyd's cyber requirements are designed to address "legitimate and important" issues that can potentially threaten the cyber market's viability, he says.

"In a competitive market, the next questions are how and when do we address the issues. While the Lloyd's market moved first with its clarification language, it is leading to better clarity in the entire market and I suspect that any friction, inconsistency, or dislocation will be short-lived," Pearman says.

He continues: "Cyber risk is a global peril. I work closely with a very smart set of underwriters in our London team, and our global underwriting office ensures consistency across our geographic regions.

"Our teams globally play to our strengths, provide solutions for the varied opportunities that exist in our separate markets and cultivate a 'you win, we all win' mentality. With this model, regional discrepancies around critical issues are eliminated."

Most of Bermuda's clients are Fortune 500/1000 insureds and many of the carriers on the island are part of global re/insurance groups.

However, the cyber market has attracted new types of carriers to Bermuda, including MGAs, cyber specialists and disruptive technology experts.

Diverse carriers

At the company level, it is difficult to ascertain how much cyber business Bermuda is writing each year, says Mosaic Insurance's head of cyber, George Cole.

"On the direct side, we estimate around $120m. Reinsurance premiums are significantly higher, at about $3bn GWP," Cole says, adding that Mosaic is targeting 20% to 25% GWP growth in its own cyber book this year.

Cole continues: "Traditionally, the Bermuda market writes large US and European corporates. However, the hard market during 2021 and 2022 saw a new flow of mid-market accounts to Bermuda, due to clients being unable to obtain favourable terms domestically."

The traditional players are, however, very much the larger part of the increasingly diverse mix of Bermuda's cyber insurers. Their experience means they are less inclined to distraction.

Axa XL's Pearman says although ransomware "doesn't dominate the news cycle" as it once did, it remains a top threat for clients.

"Contrary to popular opinion, ransomware hasn't gone away. This is one of the dangers of 'underwriting by headline'. That said, the cyber liability underwriting around ransomware has matured significantly and our clients' controls and countermeasures have markedly improved. On the other side, threat actors have access to better tools than ever, so vigilance remains the order of the day."

Most of the major reinsurers on the island already participate in the cyber market. They represent close to 50% market share for cyber reinsurance, according to the cyber underwriting source.

There is also new interest from insurance-linked securities markets, "which may constitute new capacity going forward", the source adds.

He continues: "The cyber business Bermuda is underwriting is very well diversified between different reinsurance structures, composition of book and geography. Bermuda is market lead for excess-of-loss business, which constitutes the tail events, while it also has significant share of the proportional market which has SMEs [small and medium-sized enterprises], large cap, international, personal lines, etc."

"While the Lloyd's market moved first with its clarification language, it is leading to better clarity in the entire market and I suspect any friction, inconsistency, or dislocation will be short-lived"

Noel Pearman
Axa XL

Growth prospects

Axa XL's Pearman stresses Bermuda's cyber insurance market has developed "responsibly".

"The market is more diverse than ever, but its bread-and-butter remains large, complex, Fortune 500/1000 insureds. Many of the Bermuda carriers also write cyber out of their US and/or UK offices and, as a result, managing global aggregation on large risks is normal operating procedure," he says.

Bermuda's established underwriting culture "prioritises longevity and consistency" and those carriers who "provide value irrespective of the market cycles".

Coalition's Ram says there are "new capacities from every sector" entering Bermuda's cyber market. "The nuance in Bermuda is that some of that capacity came from reinsurance carriers who brought in their appetite and were able to offer more capacity in reinsurance placements," he says.

One of the "remarkable advantages" of the Bermuda market is its ability to offer capacity across the entire spectrum of risk transfer requirements, encompassing primary, low-excess and high-excess, according to Relm's Burgess.

"Traditionally known as a high-excess go-to market, Bermuda has witnessed a transition in the last two to three years, with the emergence of highly credible primary and low-excess carriers who have made their mark in the industry," he says.

"Bermuda's adaptability and flexibility allow us to fill gaps and meet the needs of clients in a superior manner and set us apart as an advantageous jurisdiction to place insurance"

Donavan Burgess
Relm

On an insurance placement basis, Bermuda has the capability to build excess layers of up to $50m, Burgess says. "On the primary side, we've seen carriers deploy limits of up to $10m. Relm, in particular, can deploy up to $5m lines on a primary basis," he adds.

Bermuda's growth in cyber will, in large part, be thanks to this jurisdiction's reputation for innovation, Burgess says.

For example, Bermuda has played a "pivotal role" in facilitating the trading of the world's first cyber catastrophe bonds, and it is "well-positioned" to provide novel and bespoke cyber insurance for blockchain and artificial intelligence companies.

Pricing outlook

Cyber market cycles have been very short, Pearman says, "bringing surprises when the market was rapidly hardening and as it was stabilising". Such a dynamic makes long-term forecasting a challenge.

He explains: "Large US corporates comprise the bulk of the Bermuda client base, complemented by mid-sized US-based companies and international companies of all sizes, and there is diversification in industry, size and region, but the Bermuda cyber market has been affected by increased competition, especially due to new US-based managing general agents, and increased pressure on higher excess pricing.

"With half of the year still left to go, we've yet to see if the market can add enough new business to fully offset that pricing pressure. It's premature to make predictions at this point, but I remain hopeful."

Mosaic's Cole says cyber risk-adjusted rate change is -20% in 2023 to date, following negative rate movement in the fourth quarter of 2022.

"We expect a flattening of pricing as we approach Q4 this year," he says.

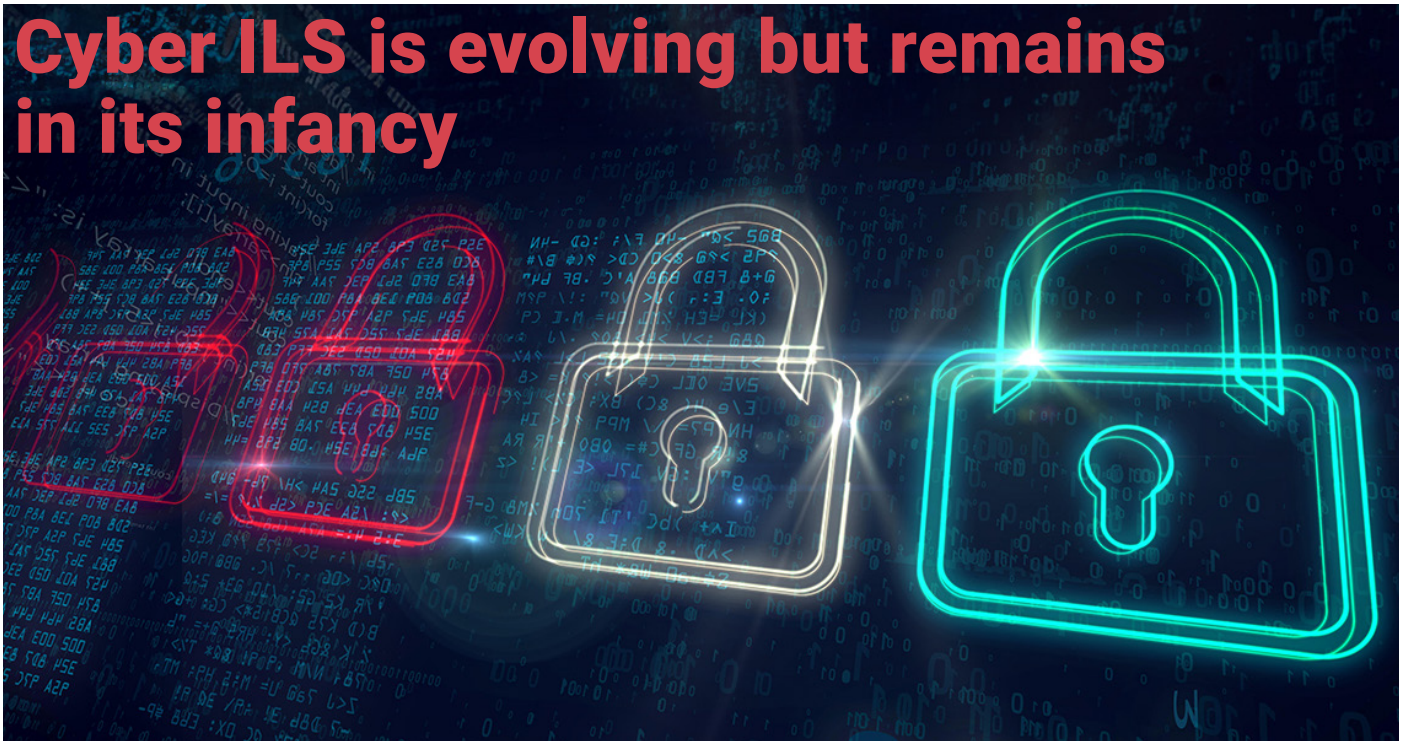
The cyber underwriting source says the cyber reinsurance pricing outlook is around a 10% rate increase in excess-of-loss, while there will be "flat-to-minor increases" in ceding commission in proportional business.

"We are noticing more clients embrace event coverage, which shows the maturity of the market," he says. ■

"The hard market during 2021 and 2022 saw a new flow of mid-market accounts to Bermuda, due to clients being unable to obtain favourable terms domestically"

George Cole
Mosaic Insurance

Cyber ILS is evolving but remains in its infancy



Skorzewiak/Alamy Stock Photo

Investors and carriers are dipping their toes into cyber insurance-linked securities, but the market is still a long way from raising a substantial amount of capital through these structures

This was the year when the cyber insurance-linked securities (ILS) market was meant to take off, *writes Francis Churchill.*

In January, Beazley launched its ground-breaking cyber catastrophe bond, a fully tradable $45m bond to provide cover for catastrophic systemic events.

This was quickly followed by a $100m cyber risk transfer to the capital markets by Hannover Re using a quota-share structure.

Access to capital is often cited as one of the key barriers to the expansion of the cyber market – which broker Howden recently said could reach global premiums of $50bn by 2030 if the right conditions are met.

The use of ILS structures, which provide ways for investors and capital markets to back risks in the insurance sector, has been touted as one of the ways much-needed capacity could be brought into this burgeoning market.

So far, however, the products launched have been modest. "A lot of progress has been made [and] we understand there are a lot of other opportunities in the making. We even expect to hear new deals in the near term. But so far these have been rather modest, so they don't necessarily move the needle," Chris Storer, head of the cyber centre of excellence at Munich Re, says. Companies are only just starting to dip their toes in.

Capacity puzzle

ILS is just one piece of the wider capacity puzzle and the solution lies across the value chain, Storer says.

A recent Munich Re report predicted the market could be as big as $33bn in premiums by 2027, compared with $12bn today.

"If we really want to realise that

"We need reinsurers, which have perhaps been a little bit tentative when it comes to cyber risk, to step up. And we have to build confidence in the retro markets and alternative capital as well. Everyone will need to pull in the same direction"

Chris Storer
Munich Re

opportunity then we all need to be pulling in the same direction and certainly that will require insurers to be more comfortable with risk," he says, pointing out more than half of cyber exposure is ceded to reinsurers, a significant amount and more than in property catastrophe lines.

He continued: "We need reinsurers, which have perhaps been a little bit tentative when it comes to cyber risk, to step up. And we have to build confidence in the retro markets and alternative capital as well.

"You never reach an end point here. You're going to need to be constantly in dialogue with reinsurers, with retrocession and with ILS funds to build confidence. And hopefully, the goal is that at some point you have a more mature product that is comparable to what we see in, particularly, natural catastrophe," Storer says.

Hannover Re argues ILS is indispensable to the growth of the cyber market. "The overall cyber market, I think will not be able to grow as it could grow if we don't get the capital markets involved in the longer term," Henning Ludolphs, managing director of retrocession and capital markets at the reinsurer, says.

While catastrophe bonds are often seen as the poster child for ILS markets, Hannover Re's risk-transfer deal provides an alternative that could side-step some of their issues. Modelling, for example, is not as much of a sticking point for quota-share structured bonds.

Ludolphs says in a quota-share structure, investors do not assess and price every individual risk but instead "follow the fortunes" of the reinsurer. "They more or less underwrite our capabilities to do a good job," he says.

Building relationships

With quota-share arrangements, it is all about building relationships with capital providers, Ludolphs says. "I think now is good timing for investors to get a foot into the door. Not necessarily with very large quantities at the beginning, but start a little bit and grow together with your reinsurer and experience the same pros and cons as a reinsurer. Try not to view it on an opportunistic basis year by year but over a longer term."

$33bn
Potential size of the market by premiums by 2027, compared to $12bn today
Source: Munich Re

For Gallagher Re, the ILS market is crucial to growth. "The cyber market is always going to be very capacity-constrained. And it's going to be more challenging for it to be over capitalised in the same way as other classes," Ian Newman, the broker's global head of cyber, says.

This is in part because of the speed the market is growing. Unlike most other lines, Newman argues, the low penetration rates for cyber mean new capital is only likely to drive more demand.

But if the market is to grow to the size many predict then it needs to start thinking about diversifying its capital. "In the same way people do for property catastrophe, having access to different forms of capital has strategic advantages," he says.

For now increases in capacity in the rated market seems sufficient to support growth but Newman says: "As we continue to develop, the larger carriers in particular, are having to look into the future and ask themselves: how do I make sure I have enough capacity to support my growth ambitions? And not only is it about quantum, it's also about diversification."

This could become even more important if a big systemic loss does occur. Such an event could cause a huge spike in demand for cover and reinsurers will need partners that can support their growth ambitions after such a loss.

"To give you an analogy, if there was a significant hurricane that goes through Florida, what happens? Rates would go up very significantly as a result and we would likely see a big hardening in the market," Newman says. "The equivalent in cyber would be like a hurricane

"I think now is good timing for investors to get a foot into the door. Not necessarily with very large quantities at the beginning, but start a little bit and grow together with your reinsurer and experience the same pros and cons as a reinsurer. Try not to view it on an opportunistic basis year by year but over a longer term"

Henning Ludolphs
Hannover Re

going through Florida, except that after the event there would not only be the rate rises as you would anticipate in property cat, there would also be 10 times the number of homes to insure. As penetration rates are so low, a major event would likely significantly increase demand for the product," he says.

At present, investors in the space are looking towards relatively broad, catch-all products, the equivalent of worldwide all-perils catastrophe, because of the uncertainty around what the peak cyber peril could be.

Newman says he expects this to change as the market becomes more comfortable with tail exposure and the impacts of particular types of events. "In the same way as property catastrophe, where someone might buy an extra layer on top for Florida catastrophe because it's where their peak exposure is, we might see the same principle apply to cyber as there is greater comfort," he says.

Investor education

"We are interested in exploring this space in various different formats. A lot of insurers in the market are reviewing whether they should think about doing a catastrophe bond or not. Since the Beazley transaction, there's undoubtedly been a spike in interest," Newman says. "Equally, from the other side, we're hearing from a lot of the conversations we're having within the ILS community there's a lot more interest in deploying capital in cyber and there is a huge amount of work going on there. Education is a big part of what's needed and we are investing huge resources here, but there are other key factors, such as modelling vendor credibility – where a huge amount of work is also being done."

There is consensus more work needs to be done to bring more investors on board. "In my conversations, investors are like: 'Listen, you guys haven't gotten [to the point] where you have of loads of data history and modelling agencies and everything, so I don't know how we can even consider cyber'," Cate Kenworthy, UK head of investor relations at ILS manager Securis Investment Partners, says.

Similarly, Matthew Twilley, head of ceded reinsurance at Ariel Re, says that across the ILS markets there is a certain amount of loss fatigue caused by a string of non-mean loss years in the property catastrophe market.

Evoking the iconic business phrase "Nobody ever got fired for buying IBM", he says: "What we see is something very similar to that in ILS: investment managers won't get fired for going into US equities or investing in all kinds of things they already know. They're mainly worried about investing from their alternatives pot into ILS in case it has another bad year."

Others think there needs to be more government involvement in the cyber ILS space to get the market moving. Ryan Dodd, founder and chief executive of parametric cyber insurer Intangic, argues the market will not take off until states step in as "first risk takers".

"Looking around at the alternatives, why would you put your money in something that's opaque, somewhat new and doesn't provide you returns [you can get from] buying AI stocks or [similar]," he says. "You are competing with venture capital, private equity, crazy Bitcoin nonsense, all sorts of stuff. So, until you have someone step in and say, 'we will guarantee some part of this risk', I don't think you're going to see this thing take."

External impacts are recognised by others in the market. "I know some ILS managers understand the risks but they simply don't have the support to invest," Ludolphs says. "Others have more flexibility... and I assume some of them will put their foot in the door sooner or later."

The fact the first transactions have been done can only help. "People see it's not just talk, which is a big difference," he says, adding these sorts of transactions require protracted negotiations that take time. "I definitely do not expect large volumes of ILS to come into cyber in the very short term, but I'm personally fairly optimistic, over time, there will be more support."

As for Hannover's future, Ludolphs says the company is looking at the "full range" of products. "We are looking at parametric-based covers. We may increase our quota-share support and we take into account cyber catastrophe bond structures, so we already have a fairly big range of concepts to work with." ■

"As we continue to develop, the larger carriers in particular are having to look into the future and ask themselves: how do I make sure I have enough capacity to support my growth ambitions? And not only is it about quantum, it's also about diversification"

Ian Newman
Gallagher Re

Low uptake of cyber cover in maritime sector is a challenge for insurers

Jochen Tack/Alamy Stock Photo

High prices, low limits and inflexible terms, rather than a lack of awareness of the threat, are reasons why maritime businesses are reluctant to buy cyber cover, risk consultants say. Can the insurance industry respond?

The maritime sector has been subject to a number of cyber attacks in recent years, the most notable being the collateral impact of the NotPetya malware attack in 2017 on the Maersk shipping line, which was forced to suspend operations when its computer systems had to be shut down, resulting in business losses to Maersk in excess of $300m, *writes Rasaad Jamie.*

Since then, as highlighted in a *Lloyd's List/Insurance Day* Podcast (The cyber threat to maritime and the insurance industry's response) recorded in April last year, cyber attacks and data theft have featured routinely in industry surveys as among the top three risks perceived by maritime businesses.

But at the same time, those surveys also indicated the maritime sector was lagging behind other industry sectors in its awareness of the cyber threat and its preparedness to tackle the risk.

Indeed, the lack of cyber incident reporting in the sector remains a big concern for the insurance industry.

It was around 2018 that shipping companies started to engage in more detailed discussions with insurers about how to protect against cyber exposures, particularly cyber business interruption losses and physical damage to vessels arising from a cyber attack.

London market insurance broker, Gallagher Specialty, which provides a range of cyber products for the maritime sector, suggests while things have improved over the past year, today there is still less of an understanding of cyber risks in the maritime sector compared with other industries and more work needs

"The difficulty is there is no one authority that cyber attacks could or should be reported to in the sector, so there is no organisation that collates data. It is not necessarily a reluctance on the part of individual companies"

Archie Ghinn
Gallagher Specialty

to be done to help clients better understand their exposure.

Indeed, the need to improve maritime clients' insight into the risks presented by cyber incidents and how these could affect their business has become a particular focus of the co-operation between the cyber and marine teams at Gallagher.

Archie Ghinn, an account executive in the cyber team at Gallagher Specialty, says there is a tendency to overstate the unwillingness of companies in the maritime sector to share data. "The difficulty is there is no one authority cyber attacks could or should be reported to in the sector, so there is no organisation that collates data. It is not necessarily a reluctance on the part of individual companies," Ghinn says.

Others such as Rob Smart, chief technical officer at corporate risk consultancy and advisory firm Mactavish, argues the insurance industry has a valuable role to play in aggregating and monitoring incident data, as well as using that knowledge to help its customers be more secure.

"But re/insurers and brokers must do this at a credible and useful level of detail without betraying confidential information or competitive advantage – this can be a challenge but is one they have grasped successfully in other areas of risk, so it should be doable in maritime cyber," Smart says.

Disconnect

There are products available to cover a wide range of risks in the maritime sector and the insurance industry is very innovative in the creation of relevant cover, according to Nick Roblin, a divisional director in the marine team at Gallagher Specialty.

The disconnect, he says, is more in relation to the sector's perception or, more precisely, its underestimation of the scale of risk of a cyber incident. But this, Roblin says, is likely to change as incidents become more prevalent and more costly.

Cyber is a big area of focus for many of Mactavish's clients, including those in the maritime sector, according to Smart. He does not entirely agree the sector is lagging behind other sectors in relation to threat awareness.

"Many industries have had to wake up rapidly to the fact nowadays almost everyone is a cyber crime target, far beyond 'traditional' target areas such as finance. Given the cyber environment is complex, fast-evolving and still relatively untested from an insurance perspective, many companies, not only those in the maritime sector, are still working out what cover is available and how exactly it will respond to their potential loss scenarios," he says.

For Smart, part of the difficulty some maritime businesses have in their "understanding" of cyber risk and the ability of the insurance industry to respond to it is the concern regarding cyber has broadened quite quickly since 2018. "But, critically, it happened at the same time as the hard market made cyber policies much more restrictive, as well as more expensive and underwriting criteria less flexible," he adds.

War exclusions

This includes the move on the part of the insurance market to introduce cyber war exclusions, such as the mandate by Lloyd's requiring syndicates writing standalone cyber to exclude losses arising from state-backed cyber incidents.

From the insurance market's perspective, the threshold for this exclusion to kick in is very high. There needs to be a state attack on another state and the attack must cause a major detrimental impact to an essential service.

Ghinn believes insureds can be confident they will not be denied cover unfairly by the market. "War exclusions are precautionary. They are not relevant while countries are not at war. They don't change the intent of the policies," he says.

"Many industries have had to wake up rapidly to the fact nowadays almost everyone is a cyber crime target, far beyond 'traditional' target areas such as finance"

Rob Smart
Mactavish

For Smart, drawing a distinction between state conflict and "private" cyber malicious actions – and insuring only the latter – is an understandable and reasonable intent from insurers. However, drafting such exclusions precisely is very challenging, he says. "What exactly is 'state conflict'? Where does the burden of proof sit and how in today's increasingly complex cyber environment? Is it possible to definitely identify perpetrators and motives?" Smart says.

The situation is made more challenging for insureds when broadly one side (insurers/the Lloyd's Market Association (LMA)) is doing all the drafting. "Their caution inevitably makes the exclusion broader, capturing things beyond 'state conflict' actions, and making the insured prove otherwise," Smart adds.

For example, there are variants of

the LMA war clauses, with some more definitive than others, he says. The biggest problem, according to Smart, is often at the point of buying a policy the insured is not even made aware which variant of the clauses is being used or that the one used is one of several. "It's just presented as market standard and is non-negotiable," he says.

The cyber insurance market is not really trying in earnest to eliminate grey areas. "It is broadly drafting clauses with safety in mind so it has the right to refuse cover in the event of doubt. The insurer may elect to be more generous, but the policy drafting will invariably support its ability to exclude the grey area," Smart adds.

Comprehensive approach

But, whatever the challenges, Smart believes a comprehensive approach to cyber risk management by shipping companies is vital, no matter how big or small the business. An effective cyber security plan should have many levels: security infrastructure investment, procedural and training measures, internal resourcing and appropriate third-party support, scenario planning and preparedness, and – last but not least – insurance cover, which in many cases can provide practical, as well as financial, support in a cyber incident.

Jochen Tack/Alamy Stock Photo

"It's also essential to not treat cyber security planning as a unique silo unconnected to wider business continuity planning. Cyber security, but in particular incident response, are only partly technical issues. They are also critical for operational planning to minimise disruption," Smart says.

Roblin agrees. It is critically important for companies in the maritime sector to have appropriate cyber insurance, he says. For example, many shipping companies are smaller firms, so full corporate cyber cover is not going to be cost-effective for them, he says. "For many clients the cover they are most interested in is cover for property damage due to a cyber incident, which is excluded on standard hull policies.

"Ships heavily rely on technology. If this is interrupted due to a cyber incident, ships can run aground or get damaged. That's not to say that for larger firms full corporate insurance wouldn't be appropriate, but this is a relatively small segment of the market comparatively," Roblin says.

Nobody doubts demand for cyber cover in the maritime sector will increase. For Roblin, the insurance market is ready and with the appropriate products available. The focus, he says, needs to be on driving awareness of cyber incidents in the sector.

For Smart, in contrast, the supply of cyber cover in the maritime sector is challenging, and the combination of high price, low limits and inflexible terms could continue to turn buyers off insurance and towards other solutions such as investing in cyber security instead of buying insurance, going down the route of self-insurance, captives or mutuals, or lobbying for a Pool Re-type solution to make cyber cover more affordable. "Maritime buyers waiting passively for cyber insurance to be broad, cheap and easy to buy are likely to be disappointed for a good while yet," Smart says. ■

"For many clients the cover they are most interested in is cover for property damage due to a cyber incident, which is excluded on standard hull policies. Ships heavily rely on technology. If this is interrupted due to a cyber incident, ships can run aground or get damaged"

Nick Roblin
Gallagher Specialty

Lloyd's List Intelligence

Seasearcher

Access the new standard in maritime trading risk analysis with Seasearcher Advanced Risk & Compliance

With international sanctions enforcement increasing, it is more vital than ever to find the right maritime risk & compliance solution for your business. With unrivalled data and methodologies, Seasearcher Advanced Risk & Compliance enables you to quickly and efficiently screen and investigate vessels for risk, all in one place.

Reduce your false positives, cut out the manual checks, and confidently identify suspicious activity to stay compliant.

Market-first features include:

- Identify vessels engaged in dark ship-to-ship transfers
- Detect dark port callings
- Screen vessels for risk and escalate investigations all within the same platform

1 trillion data points	60+ analysts researching and validating data
3,000+ reliable and trusted data sources..	500+ agents across 170 countries

Visit **lloydslistintelligence.com/advanced-risk-and-compliance** to request a demo

Call us on **+44 (0)20 8052 0628** to find out more

Access our unparalleled insights via a web platform or API data feeds