MONDAY 3 FEBRUARY 2020

insuranceday

MARKET NEWS, DATA AND INSIGHT ALL DAY, EVERY DAY

ISSUE 5,522

Aon reinsurance growth outpaces Guy Carpenter

p3

Focus: Cyber

'The industry must drive cyber risk into the affirmative market'

p7

Re/insurers wary of the future as Brexit day passes

p3

NEWS

insuranceday

Market news, data and insight all day, every day
Insurance Day is the world's only daily newspaper for the international insurance and reinsurance and risk industries. Its primary focus is on the London market and what affects it, concentrating on the key areas of catastrophe, property and marine, aviation and transportation. It is available in print, PDF, mobile and online versions and is read by more than 10,000 people in more than 70 countries worldwide.

First published in 1995, *Insurance Day* has become the favourite publication for the London market, which relies on its mix of news, analysis and data to keep in touch with this fast-moving and vitally important sector. Its experienced and highly skilled insurance writers are well known and respected in the market and their insight is both compelling and valuable.

Insurance Day also produces a number of must-attend annual events to complement its daily output, including the *Insurance Day* London Market Awards, which recognise and celebrate the very best in the industry.

For more detail on Insurance Day and how to subscribe or attend its events, go to subscribe.insuranceday.com

Insurance Day, Informa, Third Floor, Blue Fin Building, London SE1 0TA

Editor: Michael Faulkner
+44(0)20 7017 7084
michael.faulkner@informa.com

Deputy editor: Lorenzo Spoerry
+44 (0)20 7017 6340
lorenzo.spoerry@informa.com

Editor, news services: Scott Vincent
+44 (0)20 7017 4131
scott.vincent@informa.com

Global markets editor: Rasaad Jamie
+44 (0)20 7017 4103
rasaad.jamie@informa.com

Business development manager: Toby Nunn	+44 (0)20 7017 4997
Key account manager: Luke Perry	+44 (0)20 7551 9796
Advertising and sponsorship: Deborah Fish	+44 (0)20 7017 4702
Classified and legal notices: Maxwell Harvey	+44 (0)20 7017 5754
Head of production: Liz Lewis	+44 (0)20 7017 7389
Production editor: Toby Huntington	+44 (0)20 7017 5705
Subeditor: Jessica Sewell	+44 (0)20 7017 5161
Events manager: Natalia Kay	+44 (0)20 7017 5173
Editorial fax:	+44 (0)20 7017 4554
Display/classified advertising fax:	+44 (0)20 7017 4554
Subscriptions fax:	+44 (0)20 7017 4097

All staff email: firstname.lastname@informa.com

Insurance Day is an editorially independent newspaper and opinions expressed are not necessarily those of Informa UK Ltd. Informa UK Ltd does not guarantee the accuracy of the information contained in *Insurance Day*, nor does it accept responsibility for errors or omissions or their consequences. ISSN 1461-5541. Registered as a newspaper at the Post Office. Published in London by Informa UK Ltd, 5 Howick Place, London, SW1P 1WG.

Printed by Stroma, Unit 17, 142 Johnson Street, Southall, Middlesex UB2 5FD.

Print managed by Paragon Customer Communications.

Steven Beard will leave his post as chief executive of RFIB with immediate effect

RFIB chief Beard exits

Steven Beard's departure follows sale of broking firm to Integro

Scott Vincent
Editor, news services

RFIB's chief executive, Steven Beard, has stepped down with immediate effect.

Beard has led wholesale broking group RFIB and sister company Limehouse Agencies for two years, a period that included the rebranding of the holding company to Risk Transfer Group (RTG) and the sale of the company to Integro.

He is also credited with returning the firm to profit. In June RFIB reported an operating profit of £4.9m ($6.2m) for the year ended December 31, 2018, compared to a £1.9m loss a year earlier.

'Stepping down as CEO and leaving a business is never an easy decision to take, but timing is everything and now feels right'

Steven Beard
RFIB

"Stepping down as CEO and leaving a business is never an easy decision to take, but timing is everything and now feels right," Beard said.

With RFIB set to be integrated with Tysers, Integro's wholesale broking operations, the business will be led by an interim management committee until the integration is complete.

The committee – which comprises Morna Leather, RFIB's finance director, Chris Tansley, the broker's chairman of marine, and Kevin Stratton, managing director of specialty – will lead the day-to-day operation of the business, reporting to the Tysers management committee.

Jason Collins, co-head of Tysers Broking, said: "Steven exercised his position with diligence and focus and we have appreciated his partnership in the acquisition and integration planning."

Integro's acquisition of RTG completed on January 1.

Gallagher CEO: Capsicum Re the 'best start-up I have seen'

Arthur J Gallagher chief executive, Patrick Gallagher, has described Capsicum Re as "the best start-up" he has seen in his career, *writes Michael Faulkner*.

The US broking group bought out the remaining stake in boutique reinsurance broker Capsicum Re in January.

Gallagher said the Capsicum Re business had "lots of room to grow" and highlighted the business's strengths in motor, property, facultative and cyber lines. "It is going to be a great acquisition for us," he told analysts.

The chief executive pointed to Capsicums Re's ability to combine broking with analytics as a key reason for its success. "What Grahame [Chilton] and Rupert [Swallow] and their team have found is at the same time as analytics are important, the whole capability to execute as a broker was something that was kind of diminishing in the marketplace," Gallagher said.

"They felt they could take advantage of that by bringing aboard people who really were solid brokers, supported by analytics, as opposed to analytics people trying to broke," he added.

The comments came after the US broking group reported its core broking and risk management segments posted combined revenues of $1.41bn, up 17%, in the final quarter of last year, with organic growth of nearly 6%.

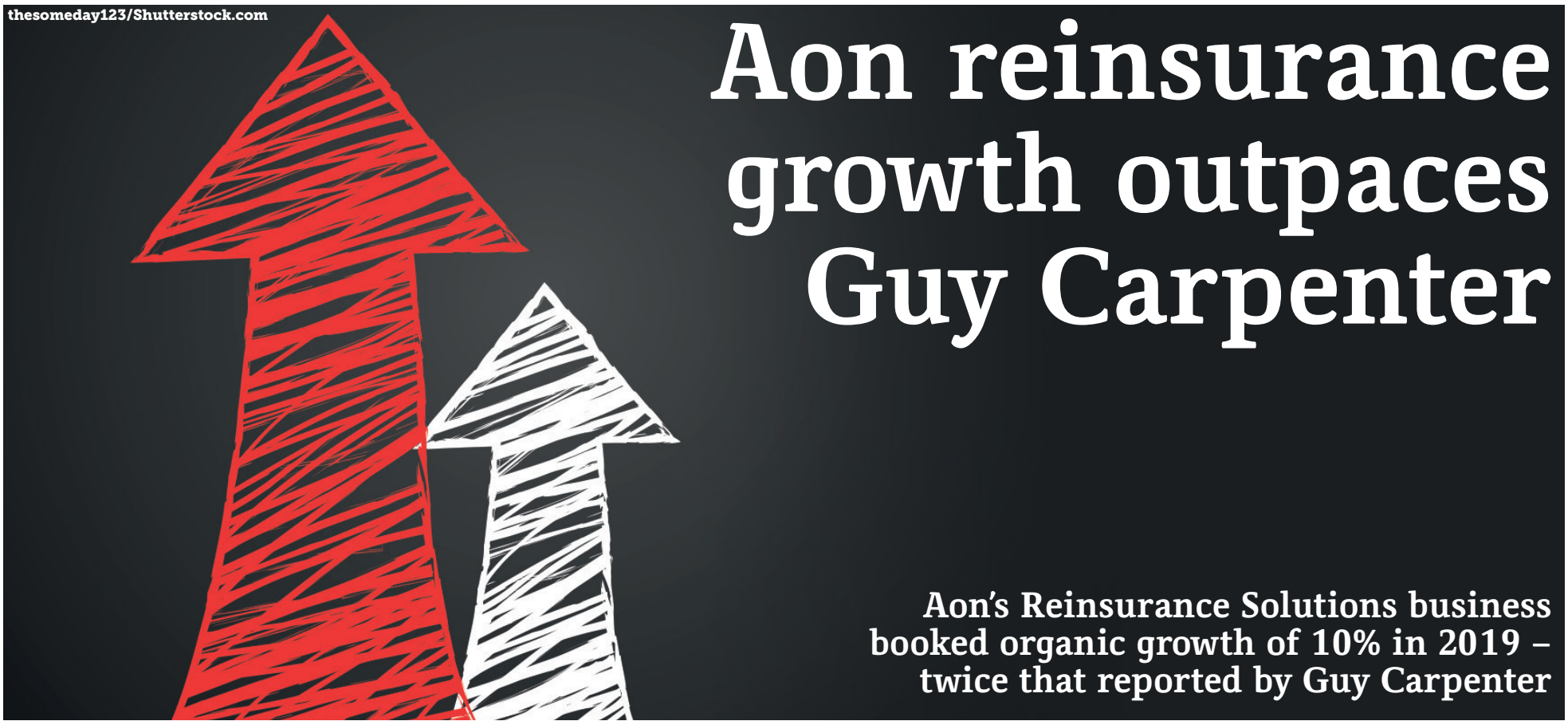
The group's UK operations posted 6% organic growth in the quarter.

Gallagher said rates and exposures continue to be a "tailwind" to the firm's organic growth, with renewal premium change now "comfortably above 5%".

London market specialty rates were up 5% to 10%, the chief executive added.

He said property and casualty pricing had "moved from stable to firm, not hard… but certainly firm".

NEWS



Aon reinsurance growth outpaces Guy Carpenter

Aon's Reinsurance Solutions business booked organic growth of 10% in 2019 – twice that reported by Guy Carpenter

Scott Vincent
Editor, news services

Aon saw double-digit organic growth in its reinsurance business during 2019 as it capitalised on new treaty, facultative and insurance-linked securities business opportunities.

The US broking giant reported 10% organic reinsurance growth in its full-year earnings, double the 5% full-year underlying growth reported at rival Guy Carpenter.

Aon booked fourth-quarter organic growth of 17% in its reinsurance operations, again outpacing its rival Guy Carpenter, which delivered underlying growth of 10% for the quarter.

The company said the quarterly growth was driven by continued net new business generation on a global basis and "strong growth" in catastrophe bonds within capital markets transactions.

17%
Organic fourth-quarter growth booked by Aon in its reinsurance operations

The 2019 performance is significantly above the already strong 7% organic revenue growth Aon Reinsurance Solutions reported for full-year 2018.

During the group's fourth-quarter and full-year earnings call its chief executive, Greg Case, said net new treaty business had accounted for roughly 60% of the full-year reinsurance organic growth.

Aon's reinsurance business generated total revenue of more than $1.68bn in 2019, up from $1.56bn in 2018.

The unit's strong growth in 2019 has ensured it remains larger than rival Guy Carpenter, which booked revenue of $1.48bn in 2018, driven by 5% underlying growth and the acquisition of JLT Re.

At group level, Aon delivered organic growth of 6%, continuing its improving growth trajectory of recent years.

Aon delivered organic growth of 3% in 2014 and 2015. This improved to 4% for 2016 and 2017 before reaching 5% in 2018 and rising again to 6% last year.

Case said the broker was looking to deliver "mid-single-digit or greater" organic growth in the longer term as it continues to reap the benefits of its "Aon United" strategy.

He said the growth profile of the firm is continuing to improve, with its investments helping to create new demand for insurance products, as demonstrated by the creation of a $24bn mortgage reinsurance market since 2012.

Aon also confirmed it has completed its restructuring programme, with all charges related to the programme now incurred.

The restructuring programme delivered savings of $529m in 2019 and is expected to generate savings of $580m in 2020, up from an earlier estimate of $540m.

The programme had cost Aon $1.48bn between 2017 and 2019 and is expected to deliver a return on investment of 39%.

Re/insurers wary of the future as Brexit day passes

The London market is hoping a deal can be done guaranteeing its access to the European market as negotiators prepare to begin hammering out the future trading relationship between the UK and the EU, *writes Lorenzo Spoerry*.

The UK left the EU at 11 pm on January 31, entering into a standstill arrangement that is planned to last until the end of the year, when a trading relationship that has yet to be negotiated comes into force.

For the next 11 months, UK insurers will be able to underwrite European Economic Area (EEA) business via existing passporting rights and EEA insurers will retain access to the UK market.

At the end of the transition period, passporting rights will cease and UK-domiciled insurers will no longer be able to issue insurance contracts in the EEA.

For many UK-based carriers, this will be of little consequence since they have already spent billions of pounds setting up capitalised subsidiaries in the EU to service business even in the case of a no-deal Brexit.

Clare LeBecq, chief executive of the London Market Group (LMG), said: "On a day that is historic by any measure, the London insurance market is as prepared as it can be to ensure continuity of service for clients.

"Longer term, the government must prioritise continued market access for firms providing cover for large commercial risks and ensure we keep attracting the foreign capital that underpins our market," she added.

'On a day that is historic by any measure, the London insurance market is as prepared as it can be to ensure continuity of service for clients'
Clare LeBecq
London Market Group

A key objective for the London market will be to secure an "equivalency" designation from the European Commission, AM Best said. A determination of reinsurance equivalence is necessary to allow UK reinsurers to be treated by EEA supervisors in the same way as EEA reinsurers are treated.

Ivor Edwards, partner at law firm Clyde & Co, said there is hope the equivalence designation can be agreed quickly. However, he pointed to another problem in that there remain questions about whether UK judgments will be enforceable in the EU.

"Will lack of certainty cause disputes or litigation to be delayed or speeded up to try to deal with matters that are in dispute before the transition period ends?" he asked. "Court guidance suggests it may be necessary to commence proceedings suddenly where delay 'might prompt forum shopping in other jurisdictions'."

Edwards said companies should take advantage of these arrangements while they can.

There are also fears the anticipated negative economic consequences of Brexit could affect the UK re/insurance market in a variety of ways.

Potential issues include a weakening of sterling, which could increase claims inflation, and an increasingly challenging investment environment, which would eat into re/insurers' investment income, AM Best said.

In addition, if economic conditions deteriorate, the demand for insurance is likely to reduce as well, depressing premium volumes.

FOCUS/ CYBER

Marine sector should confront the rising cyber threat it faces

The breakneck pace at which the marine industry is digitalising and increasing connectivity means it is critical for the sector to be more open about cyber attacks

Henry Preedy-Naysmith
Standard Club

Ports and terminals are the biggest and most obvious targets in the marine sector for cyber attacks

metamorworks/Shutterstock.com

It is not an overstatement to describe the rise of cyber risk in shipping as one of the most substantial threats to the industry for the coming decade.

Yet when offered ways of transferring some of this risk, why do so many companies instead decide to run the digital gauntlet? Is it to do with the lack of reported incidents, a belief this only happens to others or that the organisation's digital defences are adequate to block any potential breaches?

Given the rise in cyber-related incidents, it would seem imperative to seek solutions to manage the threat. The industry itself acknowledges the issue: according to the report from the Global Maritime Forum on major challenges facing the industry for the coming decade, cyber is in the top five for impact, likelihood and lack of preparedness. Only the existential threats of global economic crisis and failure of climate-change mitigation and adaptation rank higher.

Not only are we underprepared for attacks when they come, but their frequency is increasing. Security breaches have increased 67% since 2014, with the average cost of a data breach being almost $4m, not even accounting for the potential expense and reputational impact of regulatory penalties.

While the threat is not restricted to shipping, the breakneck pace at which the industry is digitalising and increasing connectivity between shore and ship and between parts of a fleet makes it particularly acute for the industry.

The potential financial gain from extorting a port or an entire operation dwarfs the criminal yield from hacking a single ship

Shoreside incidents

By far the greatest surface area for potential attacks is the shoreline. Terminals and ports have increasingly complex and connected systems to deal efficiently with large volumes of transactions and the potential financial gain from extorting a port or an entire operation dwarfs the criminal yield from hacking a single ship.

The drastic impairment suffered by Maersk as a result of the NotPetya malware in 2017 remains the most stark example of this: 17 APM terminals were unable to operate as software crashed under attack, leaving no capability to load vessels or take new bookings. The combined cost to all victims of the attack has been estimated as high as $10bn.

As more operators look to enhancements like electronic bills of lading and blockchain to streamline process and increase efficiency, resilience, redundancy and the ability to continue operating in hostile or exceptional situations are increasingly vital.

Shoreside cyber incidents are increasingly likely as automation increases. Inadvertent contamination of systems by mobile devices infected with malware is a growing trend. Like it or not, the technology is moving faster than many users' awareness of its capability and regular training and education is essential. So-called "spear phishing" accounts for 65% of infections, reliant on unsuspecting employees opening apparently innocent files to provide access to a system.

Best practice

Comprehensive guidelines by the International Maritime Organization (MSC-FAL.1/Circ.3) and Bimco (Guidelines on Cyber Security Onboard Ships) set out accessible best practice to deal with cyber risk but the onus remains on individual companies to train and embed such recommendations.

The Norwegian National Security Authority has also published information and guidance concerning the segmentation of networks between shore and ship, concluding the industry is under increased targeted attack (particularly operations in Marsec level two and higher areas).

The under-reporting of cyber events and near-miss incidents only exacerbates the perception it will happen to somebody else, the reluctance to value the risk appropriately and the lack of appetite for insurance. When Yahoo reported a cyber breach in 2016, $350m was wiped off the value of the deal in its sale to Verizon. Confidence is vital in business and, given the very large sums often involved in shipping transactions, it is particularly critical.

For many businesses, acknowledging the increasingly visceral threat of cyber risk is a challenge. Sharing "war stories" – information about attacks, successful avoidance and incident management – benefits the legitimate operators and the whole industry.

The insurance industry has an important role in providing a comprehensive solution to the growing threat of cyber crime. Carriers and intermediaries may not have been as quick off the block as some commentators would wish in developing solutions but that is no longer the case. As Lloyd's takes steps to clarify the position of its syndicates on cyber in 2020, the argument for the protection cyber cover offers in its various guises has never been stronger.

Whether it is the cost of non-physical damage business interruption, more traditional casualty exposure or specialist incident response, cover is available. Seeking out these solutions offered by the market seems the prudent approach in the face of the growing peril as we continue to advance in the digital age. The risk is not intangible or limited to a minority. Nearly all businesses are exposed and should consider protecting themselves and their reputation against it. ■

Henry Preedy-Naysmith is deputy underwriter for strike and delay at the Standard Club

It is time to dispel apathy about cyber risks in the SME market

Insurers and brokers need to work together and engage with clients throughout the year, not just at renewal time, to increase the uptake of cyber cover

David Legassick and Matt Sumpter
CNA Hardy

As an industry we seem to be missing a trick when it comes to getting clients to see the value of cyber insurance – namely, that the majority of UK businesses are just not buying it. In fact, just 11% of UK companies purchase cyber insurance, despite government figures revealing 43% of businesses in the UK experienced a cyber attack in the past 12 months.

In a world where more is spent on pet insurance than cyber, should the industry be taking a carrot rather than a stick approach, demonstrating the benefits of a cyber policy rather than highlighting the risks?

CNA Hardy's risk and confidence research appears to suggest cyber fatigue is occurring. In May 2018, a quarter of UK business leaders questioned cited cyber as their biggest risk concern. This dropped to 18% in May 2019 and only 10% predicted it will be a significant risk concern by May this year.

Figures from the Department for Digital, Culture, Media and Sport (DDCMS) back this up. In 2018 only 27% of businesses said they had a formal cyber security policy or policies in place, compared to 33% in 2017. The sad fact is, it is estimated only around £80m ($105.2m) of cyber business is written in the UK, according to the Association of British Insurers (ABI), yet the pet insurance market is worth £1.1bn. We know we are a nation of dog lovers, but surely we want to give our businesses the same level of care and protection?

In part, we believe the problem may be business leaders still do not believe cyber attacks will happen to them. Despite the Information Commissioner's Office handing out multimillion-pound fines to the likes of British Airways and Travelex suffering a share price drop of 17% following the ransom attack it suffered over the Christmas holiday, cyber risk is just not resonating with businesses or organisations across the country.

Our theory is small to medium-sized enterprises (SMEs) in particular do not believe they are a target partly because the media narrative is focused so squarely on the multinational companies with deep pockets that can afford to handle the fallout.

But the irony is these smaller businesses are the backbone of the UK economy, accounting for three-fifths of UK employment and around half of turnover in the UK private sector. These are the businesses most in need of the practical, legal and financial assistance offered by a cyber policy if they are to emerge from a cyber attack relatively unscathed.

SMEs are the businesses most in need of the practical, legal and financial assistance offered by a cyber policy if they are to emerge from a cyber attack relatively unscathed

It appears when businesses of this size do experience an attack (and DDCMS stats suggest close to half were attacked last year), such attacks are often swept under the carpet to avoid scaring off customers, suppliers or investors.

Selling the benefits

Our experience is schools, sports clubs, health clubs, solicitors' firms and data-rich businesses in numerous sectors have benefited from insurance when they were hit by a data breach, ransomware or social engineering attack. They were able to draw on the assistance available via their policy – from legal advice, to forensic IT and PR services to name a few, as well as taking advantage of valuable pre-breach services on offer.

Our challenge is how do we use these stories as examples that resonate with their peers?

As an industry, we could, for example, choose to publish our response times, the numbers of firms that have benefitted from cyber policies, the number of claims paid and in what time scale. For example, last year the ABI revealed 99% of its members' cyber policies were paid – one of the highest claims acceptance rates across all insurance products.

We are increasingly making more of our loss data and the intelligence gleaned to inform clients on the latest cyber trends and we publicise key steps they should be taking to try to avoid being a victim of the latest form of attack. So why are these messages not cutting through?

Is this information not reaching the end clients? Is there a danger of broker cyber fatigue? Or is it the case low commissions and a possible fear of not being able to respond to client questions is resulting in some brokers not pushing cyber coverage?

Whatever the reason for cyber apathy there is no doubt there are great swathes of insureds not buying cover that should be.

To change this situation greater insurer, broker and client cooperation and an ongoing conversation throughout the year with insureds, not just at renewal time, is required. There also needs to be greater emphasis on demonstrating where the real value-add is within a cyber policy for SMEs.

The policies, the wording, the capacity and the pre/post-breach response services are there – now together we need to convince insureds of the true value of investing in a cyber policy and demonstrate why they cannot afford to be without one. As a sector, we cannot afford to be the dog that failed to bark. ■

David Legassick is head of segments and Matt Sumpter is European underwriting director, technology and cyber risks at CNA Hardy

Despite the growing threat to SMEs from cyber attacks, take-up of insurance remains low

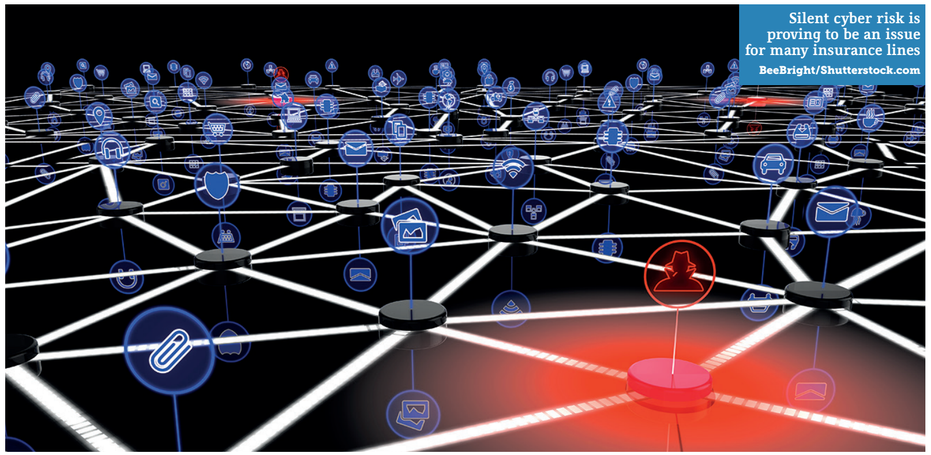
SynthEx/ Shutterstock.com

FOCUS/ CYBER

It is vital to be clear about the script before speaking up about silent cyber

The implications of affirming or excluding cyber risk in policies can be challenging for carriers

Madeleine Shanks
Clyde & Co



Silent cyber risk is proving to be an issue for many insurance lines
BeeBright/Shutterstock.com

Silent cyber is a prominent issue in the insurance market, whereby inadvertent cover is provided by non-cyber policies in response to cyber incidents.

As the cyber class of business grows, there is increasing pressure from the market and regulatory bodies to address silent cyber. This has intensified in recent months following a number of legal disputes focusing on the potential consequences if insurers fail to effectively manage silent cyber risks.

Examples would include an act of so-called "cyber terrorism", which may leave insureds seeking cover under terrorism lines that neither affirm nor exclude cyber-related losses.

Alternatively, insureds that experience a cyber incident that results in physical damage to servers or premises may turn to property policies for cover in the absence of an express exclusion. Silent cyber is revealing itself as an increasingly wide risk across a variety of business lines.

In the US, Mondelez filed a complaint against Zurich American Insurance in response to the insurer's refusal to pay out under a property liability policy for cyber losses of $100m following the NotPetya cyber attack in 2017. Insurers indicated the attack was orchestrated by the Russian government, thereby triggering an act of war exclusion.

Pharmaceutical giant Merck, which sustained reported NotPetya losses of $700m, filed a suit in New Jersey against more than 20 insurers that rejected claims related to NotPetya, including several insurers that cited the war exclusion exemption.

In the UK, DLA Piper is in a legal battle with its insurers following their refusal to pay out on losses following NotPetya, with reports suggesting cover was denied on the basis the policy was not a standalone cyber policy and was not intended to cover cyber losses.

While the specific issues in dispute are nuanced, there is a common theme: why should an insured not expect cover from its non-cyber insurance policy if it is not expressly excluded?

What should insurers do?

Planning and risk mapping are key. The Prudential Regulatory Authority's (PRA) consultation paper from 2016, entitled Cyber insurance underwriting risk, and a subsequent policy statement called for insurers to robustly assess silent cyber risks. The PRA's position was reaffirmed in January last year with an open letter to chief executives of specialist general insurance firms, requiring them to develop an action plan for mitigating silent cyber risks.

Model clauses are a good starting point. The International Underwriting Association (IUA) published two London market model clauses to help underwriters manage cyber losses.

There is the "cyber loss absolute exclusion clause", which broadly excludes any loss arising from the use of a computer system, network or data, and the "cyber loss limited clause" which excludes direct cyber losses only. The Lloyd's Marketing Association (LMA) has also published a series of property and marine cyber clauses for the guidance of its members.

Businesses that follow the mandate can avoid ambiguity. Lloyd's mandated insurers must clarify whether first-party property damage policies written or renewed on or after January 1, 2020 will affirm or exclude cyber cover. Failure to do so will result in an assumption of non-affirmative cover, which could be broad.

While the specific issues in dispute are nuanced, there is a common theme: why should an insured not expect cover from its non-cyber insurance policy if it is not expressly excluded?

Practical implications

While the Lloyd's announcement is welcome, the practical and legal implications may be challenging.

For insurers seeking to exclude cover, the IUA model exclusions and LMA marine and property clauses are a good starting point; however, specific tailoring may be required to ensure policies effectively exclude unintended cyber cover. It is likely insurers will need to develop bespoke wordings that are yet to be challenged, potentially resulting in increased market competition.

Contrastingly, affirming cyber cover in general "all-risk" insurance policies (which cover perils in the absence of an express exclusion) may well lead to unintended consequences for insurers, with the cover being broader than anticipated.

In an all-risks policy, for example, perils are covered unless they are expressly excluded. Careful drafting will be required to ensure affirmation of cyber-triggered cover is subject to such exclusions and conditions.

The LMA has pointed out a "logical short-circuit" would be to make it clear cyber events will only be covered if the event "triggers cover that already exists in the policy".

What next?

Now is the time to plan, if this has not been done already.

It is key for insurers to assess their portfolios of risk and analyse where cyber risks may be picked up, whether intentionally or inadvertently.

Starting with first-party property policies, it is likely it will become expected across the insurance market for clarity to be provided to insureds as to whether cyber risks will fall under their policies. Without such clarity, insurers risk widening the scope of cover beyond what was intended. ■

Madeleine Shanks is an associate at Clyde & Co

The industry must drive cyber risk into the affirmative market

Ensuring cyber policy language is frequently reviewed in the face of rapidly changing threats remains a big challenge for insurers

Caspar Stops
Optio

Opinions about the nature of cyber losses are in flux. Historically, data breach was considered the greatest cyber risk, with organisations holding large quantities of sensitive or personal consumer information, such as hospitals and banks, presumed to be most at risk.

But cyber is a broad concept and an evolving peril. Fast-forward to 2020 and with the ever-increasing reliance of organisations on data, technology and third-party providers, the risk of cyber extortion is now arguably a greater threat.

Such attacks are encountered frequently, sometimes even daily, by some organisations. The objective is not to steal data but to hijack control of computer networks to demand a ransom, which is usually exorbitant but on payment returns control and access to their owners.

Getting to grips with and mitigating this threat will remain a battle for insurers, brokers and insureds for some time. With that, privacy will remain high on the agenda.

The notion of the "right to privacy" is a somewhat abstract concept that will continue to challenge regulators, legislators and courts for years to come. This issue lay at the heart of the Cambridge Analytica scandal in 2018 and also Capital One in 2019, when there was a so-called "mega-breach" of millions of personal records.

Despite these infamous examples, data breach claims have begun to plateau.

The proliferation of malware is an entirely different story. With the rise and rise of ransomware causing a multitude of problems and business interruption issues, it has become a far greater risk for many organisations and not just large corporations.

Policy language

Ensuring policy language is frequently reviewed to remain resilient in the face of such fast-evolving threats is a challenge for insurers.

In 2017 the NotPetya malware attack rendered useless 1,700 servers and 24,000 laptops owned by US confectionery manufacturer Mondelez, which claimed for the loss under its property policy. The insurer, Zurich, refused the claim because it regarded the attack as an act of war, which was excluded under the policy.

Under a standalone cyber policy, however, few (if any) claims have ever been denied under a war exclusion. It is an area that still presents complex shades of grey. This also highlights the difficulty of using wordings that were drafted many years ago and may not have adequately considered cyber risks.

Without a clear directive, piecemeal solutions are likely as insurers and brokers search for the path of least resistance

Therefore, we should expect work on policy language in areas such as war exclusions to continue and gather momentum this year. As the threat landscape evolves, policy language can easily lag, meaning frequent reassessment is essential to keep pace. This raises the issue of silent cyber: cyber risks that exist within non-specific cyber policies. UK regulators' increasing intolerance of unmeasured, non-specific cyber cover, is helping to bring clarity to the cyber landscape.

1,700
Number of servers rendered useless at Mondelez by the 2017 NotPetya malware attack

This has and should continue to push cyber risk into the affirmative cyber insurance market and has already prompted the preparation of new London market exclusions. However, much of the regulatory compliance is in its infancy, as insurers continue to work to qualify and quantify where their cyber exposures lie and devise ways to manage them. Consequently, any meaningful transfer into the affirmative cyber insurance market is yet to take place.

Intermediary involvement

While regulatory requirements have been placed on insurers to articulate their exposures and plans, brokers have not been invited to contribute to the effort to eradicate silent cyber. A more co-ordinated effort that involved intermediaries could be hugely beneficial to the London market's market's efforts to provide greater clarity and certainty to insureds.

Regular review of cyber policies will be crucial as the risk landscape evolves quickly
Zenzen/Shutterstock.com

Without a clear directive, piecemeal solutions are likely as insurers and brokers search for the path of least resistance. Insureds will understandably seek the most cost-efficient means of risk transfer – ideally large cyber limits for a low premium – so a demand for coverage buybacks is anticipated, rather than shifting risk to an affirmative cyber-specific solution. Unfortunately, if the response to this emerging risk is the traditional buyback of coverage then I fear a lack of progress will be made.

When a cyber event occurs, crisis management is needed – systems specialists who will rappel from helicopters to get the insured back into business (proverbially, at least). To truly assist insureds, it is imperative we as a market maintain such specialist response mechanisms, which are unlikely to be available with buyback covers.

The UK insurance market should remain free and competitive yet a more co-ordinated effort could lead to greater innovation and a clearer proposition and better solutions for insureds. It is down to all of us in the market to build awareness about the greatly differing levels of provision, but that effort will take time.

Meanwhile, cyber risk will increasingly crystalise on the risk radar of all businesses. With the evolution of the peril, new and forthcoming legislation and regulation could drive litigation and the interdependence of organisations because of increasing interconnectivity will in combination create a very new risk landscape. All of that will drive the growth of the cyber market in the years ahead. Pricing will see positive change, the market will remain robust and is set to continue to thrive as risk maturity quickly increases and cyber risk is mitigated increasingly effectively. ■

Caspar Stops is head of cyber at Optio

insuranceday

A car wedged between two buildings by Typhoon Hagibis's flood waters

Moses.Cao/Shutterstock.com

Everest Re flags $215m in Q4 catastrophe losses

Bermudian re/insurer says Typhoon Hagibis will cost it $190m

John Shutt, Los Angeles
US correspondent

Everest Re said its fourth-quarter results will reflect $215m in catastrophe losses.

The losses, which are net of reinsurance recoveries and reinstatement premiums, included $190m in connection with Typhoon Hagibis in Japan and $25m from tornadoes in Texas.

The results will also reflect higher-than-expected losses in Everest Re's US and Canadian crop reinsurance book, which put a $50m dent in its underwriting income, the Bermudian re/insurer said.

$146m
Everest Re's Q4 investment income

Additionally, net favourable reserve development will amount to $19m and investment income will be $146m.

For the full year, Everest said it expects to post net income of around $1bn.

The group is scheduled to release its quarterly and annual results on February 10.

Blue Capital pays $5m to shareholders

Insurance-linked securities (ILS) fund Blue Capital paid out $5m to shareholders during the fourth quarter as it continued to wind down its operations, *writes Lorenzo Spoerry*.

Partially offsetting the distribution was a benefit of approximately $400,000 related to positive adjustments to premiums and acquisition expenses, coupled with losses that were lower than anticipated.

'We anticipate delisting from the NYSE in March to reduce our operating expenses'
Michael McGuire
Blue Capital

At the end of the period, net assets in liquidation stood at $67.3m, down $4.6m.

"We continue to efficiently manage the run-off of the business and anticipate delisting from the New York Stock Exchange in March to reduce our operating expenses," Michael McGuire, chairman and chief executive, said.

Blue Capital's fully converted book value per common share was $7.65 at December 31, 2019, reflecting a 0.6% increase for the quarter and a 2.8% decrease for full-year 2019. These figures are inclusive of dividends declared in those periods.

IGI receives BMA approval for purchase by Tiberius

International General Insurance Holdings (IGI) has received approval from the Bermuda Monetary Authority (BMA) for its acquisition by investment vehicle Tiberius Acquisition Corp, *writes Lorenzo Spoerry*.

Other regulators, including the UK's Prudential Regulation Authority and the Dubai Financial Services Authority, have yet to approve the deal.

After the transaction completes, IGI will be domiciled in Bermuda and will be listed under the Nasdaq ticker IGIC. Some $120m will be added to IGI's balance sheet, taking its pro forma market capitalisation to more than $550m.

IGI said the deal would provide the financial firepower to support growth and entry into new lines of business at a time of "attractive" worldwide market conditions.

"This transaction will allow IGI to continue to execute its organic growth plan through expanding capacity and relationships in its core Afro-Asian, European and Latin American markets," IGI's president, Waleed Jabsheh, said.

The group said it is also exploring a possible entry into the US excess and surplus markets, as well as entering "niche segments" of the marine hull market.

IGI will be domiciled in Bermuda once its acquisition by Tiberius is completed

Andrew F Kazmierski/Shutterstock.com