MONDAY 8 FEBRUARY 2021

insuranceday

MARKET NEWS, DATA AND INSIGHT ALL DAY, EVERY DAY

ISSUE 5,771

Beazley shares soar on improved market outlook

p3

Insurers to face $3.3bn Perdue Pharma lawsuit

p2

Focus: Cyber

Spectre of cyber D&O claims could be nightmare for the market

p4

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

News editor: Marc Jones
+44 (0)7792 483813
marc.jones@informa.com

Reporter: David Freitas
+44 (0)7920 889271
david.freitas@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

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.

Purdue is the manufacturer of opioid painkiller OxyContin
PureRadiancePhoto/Shutterstock.com

Insurers to face $3.3bn Perdue Pharma lawsuit

OxyContin maker files lawsuit in bid to cover mass tort liability

Marc Jones
News editor

Purdue Pharma, the manufacturer of OxyContin, is suing its insurers for $3.3bn in opioid litigation coverage.

Insurers in the suit include AIG Specialty Insurance, Allied World Assurance, Arch Re, Aspen American Insurance, Chubb Bermuda Insurance, Ironshore, Liberty Mutual, Swiss Re and XL Bermuda.

Purdue Pharma was placed into Chapter 11 bankruptcy protection in 2019 as it became involved in litigation over allegations it aggressively marketed prescription opioids, misled consumers and contributed to an opioid addiction crisis that has killed up to 400,000 over the past two decades.

According to the lawsuit filed by Purdue in the US Bankruptcy Court in the Southern District of New York, the company is named in more than 2,760 opioid mass tort claims, including lawsuits, subpoenas and civil investigative demands across the US and its territories. More than 614,000 proofs of claim were filed by a July 2020 deadline.

The lawsuit said: "The debtors' insurance policies provide sweeping coverage for claims against the debtors seeking to hold the debtors liable for injuries for which the debtors are alleged to be responsible. Coverage under the debtors' insurance policies is subject to limits of liability, where applicable, of at least $3.3bn."

Purdue said the aggregate value of the opioid mass tort claims is not precisely known but on information and belief is more than sufficient to exhaust any applicable limits of liability of the debtors' insurance policies. Cumulatively, the proofs of claim assert damages in excess of $140trn.

It added: "The proceeds of the debtors' insurance policies constitute a significant asset of the debtors' estates and are expected to be a valuable asset for purposes of the formulation and implementation of a plan of reorganisation."

Before declaring Chapter 11 bankruptcy in 2019 the company was in negotiations with a wide range of companies to find a solution to its legal issues.

Queensland councils push for national reinsurance pool

The Australian federal government has been urged to create a national reinsurance pool by the Local Government Association of Queensland (LGAQ), *writes David Freitas*.

More than 62,000 properties in Queensland are uninsured and more than 95% of uninsured owners cited costs as a reason, the Australian Competition and Consumer Commission said.

Insurance premiums have gone up 178% in northern Australia over the past decade, which is more than three times as much as other Australian areas.

"We urge the federal government to work with the councils as leaders of their communities to ensure an effective scheme is implemented before the next disaster season," Mark Jamieson, LGAQ president, said. The LGAQ represents Queensland's 77 councils.

A reinsurance pool would help reduce costs for property owners who cannot afford to insure themselves against natural disasters, Jamieson said.

Last week, Zurich-based Perils estimated insurance industry losses from the Queensland Halloween hailstorms at A$1.3bn ($1bn).

The hailstorms battered south-east Queensland, including the surrounding areas of Brisbane, the Gold Coast and the Sunshine Coast, on October 31, 2020.

NEWS

Beazley shares soar on back of improved market outlook

Insurer's strong capital base positions the company for fast growth in 2021, analysts agree

Lorenzo Spoerry
Deputy editor

Beazley's better-than-expected results boosted its share price

Vintage Tone/Shutterstock.com

Beazley's bullish outlook for 2021 and better-than-expected 2020 results sent its share price soaring.

The company's stock rose 15% in early morning trading on February 5 after it booked a loss of $50.4m, less than half analysts' consensus expectations.

The result was supported by a slightly better-than-expected combined ratio at 109% and an investment return of 3%, above consensus expectations of 2.5%.

But the big surprise was the solvency ratio, which reached 123%, close to the top of the company's 115% to 125% range.

This high ratio "bakes in growth for 2021 and should provide some reassurance capital can absorb both rate increases and exposure growth, which was one of the concerns about the company's outlook", Peel Hunt analysts said.

RBC Capital Markets analysts agreed "some of the fears the company does not have sufficient capital should dissipate, leaving the company room to rebuild trust back with investors in the coming months".

Beazley's chief executive, Andrew Horton, said the capital buffer positions the company well for growth in 2021 after a resilient performance in 2020.

Gross written premiums rose 19% to $3.56bn in 2020, supported by accelerating rate increases in many classes. Broken down by division, rates in property rose 15%, reinsurance 13%, specialty lines 15% and marine 16%.

Cyber and executive risk and market facilities were the standout performers, recording rate changes of 18% and 19% respectively.

Political, accident and contingency saw much more muted rate increases of only 4%.

Rate increases on Beazley's renewal portfolio hit 15% (compared to 6% in 2019).

Horton said the new capital entering the market has only had a moderate effect on rate movements and he said the company "has great growth prospects" in 2021 as rates continue to rise.

The so-called "Class of 2020" start-ups that raised capital to deploy into the hardening environment includes Conduit Re, Inigo and Vantage.

Beazley said it is looking to grow market share in marine and property, as well as continue to grow its cyber book.

Across its three main platforms – London market, mainland Europe and North America – the biggest growth in 2021 is expected to take place in the London market, where the biggest rate increases are available.

Beazley's chief underwriting officer, Adrian Cox, said: "It's a good chance for us to rebuild some of the market share we have let go over the last few years as the market softened."

The company is planning to take a much more conservative approach in the employment practices book and parts of the professional indemnity book.

Beazley stuck by its previous estimate for Covid-19 losses of $340m, which assumes restrictions continue throughout the first half of 2021.

The company has reiterated it could be on the hook for a further $50m in event cancellation losses if restrictions continue into the second half of the year.

Shares in Beazley closed up 15% on Friday at 369p.

Aon reports fourth-quarter organic reinsurance growth of 12% in 2020

Aon reported better revenue growth than expected in the fourth quarter of last year, *writes Michael Faulkner*.

The global broking giant's Reinsurance Solutions business booked 12% organic growth in the final quarter of the year to $197m, while the Commercial Risk Solutions division achieved organic growth of 4% in the quarter to $1.38bn.

Wells Fargo had expected 9% growth in Reinsurance Solutions and 1% growth in Commercial Risk Solutions.

Growth in Reinsurance Solutions reflected "double-digit" growth in treaty, supported by growth in facultative placements. However, it was partially offset by a decline in capital markets transactions.

Market conditions had a "modestly positive" impact on the quarter's results, Aon said.

Commercial Risk Solutions saw growth across most major geographies "driven by strong retention and management of the renewal book portfolio".

The division achieved "double-digit growth" in Latin America and "strong growth" in the US, with growth in transaction liability and construction. This was partially offset by a decline in the more discretionary portions of the business, primarily in Europe, the Middle East and Africa, Aon said.

On average globally, exposures and pricing were both "modestly positive".

At group level, Aon's revenues grew 2% to $2.97bn representing a organic growth of 2%. The operating margin rose to 24%, while adjusted earnings per share came to $2.62, beating analysts' forecasts.

Aon chief executive, Greg Case, said the results showed the "resiliency" of the business.

"We enter 2021 in a position of strength, with momentum for Aon and our pending combination with Willis Towers Watson," Case said. The $30bn deal to acquire Willis Towers Watson is set to complete later this year pending regulatory approvals.

Last week Marsh & McLennan Companies reported 3% underlying growth in its risk and insurance division in the fourth quarter of 2020. Marsh's revenue was $2.4bn, up 4% on an underlying basis, while Guy Carpenter's revenue rose 5% on an underlying basis to $164m.

'We enter 2021 in a position of strength, with momentum for Aon and our pending combination with Willis Towers Watson'

Greg Case
Aon

WR Berkley brings in David Brosnan to lead Lloyd's managing agency

WR Berkley has appointed David Brosnan as chief executive of its Lloyd's managing agency, WR Berkley Syndicate Management, *writes John Shutt, Los Angeles*.

Brosnan succeeds Alastair Blades, who will retain his post as WR Berkley syndicate 1967's chief underwriting officer.

With 35 years of industry experience, Brosnan joins from CNA Hardy, where he has served as president of international and chief executive for six years until September 2020. Before CNA, he served with Ace and Chubb.

Berkley president and chief executive, W Robert Berkley, said the decoupling of the two posts "provides each of David and Alastair the opportunity for even greater focus" and will enable the underwriting team to "maximise its capabilities and expansion opportunities in this expanding market".

FOCUS/CYBER

Spectre of cyber D&O claims could be a nightmare for the market

It is critical insurers and reinsurers consider the extent to which a cyber incident exposes carriers to risk covered under D&O and other policies

Siobhan O'Brien
Guy Carpenter

Imagine as a company board member or senior manager being accused of having been "aware of or recklessly disregarded the fact that false and misleading statements were being issued concerning the company; and/or approved or ratified these statements in violation of the federal securities laws".

Such are the allegations against the chief executive and chief financial officer of SolarWinds, a provider of IT infrastructure and management software. SolarWinds was one of the victims of the last major cyber incident of 2020 and has the dubious honour of facing the first security class action lawsuit filed in the US in 2021.

While the SolarWinds breach was big news in the cyber insurance world – and indeed the reinsurance world, as it occurred deep into renewal season for the January 1 treaties – the class action suit made fewer headlines. It will, however, have raised eyebrows among re/insurers as they assess their appetite for the expanding cyber exposures across many lines of insurance.

One of the big winners in the Covid-19 lockdowns has undoubtedly been Zoom, but the surge in usage of its platform was undermined by an influx in privacy issues, with some calls being hacked. Zoom was also the subject of a securities class action claim alleging the company was aware of weaknesses but had not accurately represented them.

Shareholder lawsuits

The shareholder lawsuits against Zoom and SolarWinds came hot on the heels of the cyber breaches – and they are not alone, with firms like Equifax, Google, Target, British Airways, TSB and Marriott having all faced similar situations.

Unsurprisingly, cyber has become a high-priority boardroom issue. Boards need to consider global regulatory regimes, the proliferation of ransomware attacks and the damaging effect the loss or theft of financially sensitive data (especially in relation to mergers and acquisitions and in the run-up to earnings releases) can have on their stock price.

Concern is growing that hacking, accompanied by short-selling, may become a threat to public companies globally. Notably, last month Intel reportedly fell victim to a hacker who stole sensitive financial information from its corporate website, prompting the company to release its earnings statements early.

As cyber risk constantly evolves, it is increasingly a case of when, not if, an organisation will be the subject of an attack.

Boards must therefore consider how to secure their sensitive data, intellectual property, trade secrets, customer information, operational resiliency and business continuity. In addition to cyber security offerings, employee training and the appointment of dedicated technology/cyber executives to the board, cyber insurance can be a valuable additional tool in their armoury.

Cyber cover gives companies access to additional expertise in the form of breach response services, forensic experts and ransom negotiators in the event of a ransom demand. In addition, the business interruption coverage will compensate for lost revenue in the event operations are curtailed by a cyber attack.

Crucially, committing to purchasing cyber coverage and demonstrating adequate coverage is in place through a due diligence decision-making process might be key to defending a securities class action claim if an allegation of failure to maintain or procure insurance is levelled against the directors and officers.

Exclusion

While cyber policies seek to protect the company for the financial losses incurred during and subsequent to the breach event, they typically contain an exclusion for the violation of securities laws. Senior management, directors and officers are protected for their decision-making activities by their directors' and officers' (D&O) liability policy. As an all-risks policy, a typical D&O policy should cover them for all the acts, errors or omissions arising from their activities as directors and officers.

If a cyber attack occurs, the company will be focused on dealing with the incident and recovering the operations of the company, all the while trying to protect its reputation. If a securities class action is subsequently filed that alleges some failing on behalf of the board and/or senior management, they will be scrutinised for their activity not just during the attack but, potentially, in the weeks and months preceding the event. The directors and officers must therefore consider whether their D&O policy protects them for the allegations being made in any securities class action.

Lloyd's silent cyber mandates, YS5258 in July 2019 and YS5277 in January 2020, seek clarity of intent under insurance and reinsurance policies and the Lloyd's Market Association (LMA) has issued a raft of clauses and exclusions addressing many lines of insurance. This includes clarification clauses (LMA 5471, 5472 and 5489 for use on treaties) affirming the intent of D&O policies to cover loss because of a cyber act or cyber incident.

The insurance and reinsurance industry must give consideration to the management of exposure to a cyber incident under many other policies too. In some instances, in addition to the cyber and D&O policies being triggered, kidnap and ransom, crime and financial institutions bond policies may also be affected. This is what is known as a "clash" event, as one incident could result in payment under many policies.

For insurers, this may result in different treaties being triggered and the risk of bearing multiple retentions. Clash reinsurance could reduce the payout by insurers and reduce volatility in their portfolio. Reinsurance brokers such as Guy Carpenter use analytics tools to help clients to identify and quantify these exposures, and are well positioned to support the industry in exploring the impacts of these emerging risk scenarios. ■

It is increasingly becoming a case of when, rather than if, an organisation will fall victim to a cyber attack

Den Rise/Shutterstock.com

Siobhan O'Brien is leader of the Cyber Centre of Excellence, international and global specialties at Guy Carpenter

Personal cyber can be the next growth market


Shutterstock.com

A growing appetite for personal cyber risk among reinsurers provides an opportunity for carriers willing to be pioneers

Amie Watson
Aspen Insurance

If we think about what we do each day, it is easy to see how much more reliant we have become on technology over the past decade. Since the start of the pandemic, this reliance has hugely increased. Retailers are forecasting the adoption rate of new online services is accelerating from years to months and Ofcom's latest study found the number of people who regularly make video calls is doubling in size.

How did we get so dependent so quickly? Usage exploded globally once cheap, internet-enabled mobile phones became easily available to the world's population. We now use the internet for banking, shopping, home learning, health services, teleconferencing and working from home. We also use the internet to run our homes through smart thermostats, fridges, energy meters, security systems, TVs and doorbells.

More people are spending more time on the internet and consuming more online services than ever before to meet their daily needs and the online technology wave is just beginning. According to IoT Analytics, the number of internet of things (IoT) devices that are active is expected to grow to 22 billion by 2025. It is clear we are witnessing the start of a transformation in how we manage our day-to-day activities, both personally and professionally.

Unsurprisingly, criminals are also moving online. UK police statistics show victims of cyber crime lose more than £190,000 ($260,554) a day. In addition, in the UK, the Office for National Statistics found a person is 35 times more likely to become a victim of fraud and computer misuse (for example, hacking, identity theft, viruses and so on) than robbery.

Buying behaviour

It is not common for a homeowner to forgo the purchase of home insurance in the belief that having a burglar alarm is enough to provide the protection they need. Yet a recent study by Verisk shows 72% of US consumers buy antivirus software, but only 20% buy cyber insurance. Why do we buy home insurance and motor insurance to protect against robbery, but not buy cyber insurance to protect against cyber crime? And why is our buying behaviour different when it comes to protecting digital assets compared to our physical assets?

Consumers are not oblivious to the risks. Nearly three-quarters of US consumers make the conscious decision to buy antivirus software and of the people Verisk surveyed, 64% also admitted being concerned about cyber threats or attacks, while nearly one in three people reported they had already been a victim of such attacks or threats.

It is difficult to argue the low take-up rates for personal cyber cover are based on consumers not understanding the risks they face. Campaigns by banks and law enforcement are not new, nor are the frequent media reports of the more extreme and notorious cyber attacks. It is more likely consumers are struggling to find and understand product offerings that are relevant to them. Thus, the insurance industry has some work to do to close this gap.

Personal cyber is a new market for insurers and product offerings are still relatively scarce. The personal lines business is one that depends on economies of scale; insurers need high numbers of policyholders paying low premiums to cover anticipated losses.

However, personal cyber is not conducive to this model, as cyber risks are uniquely exposed to systemic loss that could be catastrophic for a new portfolio. When the potential for a huge aggregate exposure is coupled with a resistance by purchasers to answer too many underwriting questions, the market becomes a challenging space for carriers.

In addition, with hardening market conditions in commercial cyber, it is easy to understand why some insurers may choose to focus their capacity elsewhere.

However, those willing to be pioneers can gain ground. Being an early adopter of a product that embeds cyber coverage within an existing portfolio of personal lines insurance, such as homeowners' cover, can increase market share in a competitive field.

Innovator benefits

Innovators in the space also benefit from the media attention that comes with finding a solution to a problem that can fundamentally can benefit everyone, everywhere. There is also no shortage of support; incident response firms are available to provide the expertise needed to support affected policyholders and insurer's claims teams alike. There is also appetite from the reinsurance market to provide capacity and expertise.

As consumers, we are used to personal lines products that are easy to understand and compare against competing offerings; aggregators do the work of comparing products by highlighting differences that are usually minimal. They also drive a high level of consistency between products through this process, leaving the consumer equipped to make a quick and easy decision about their purchase.

Personal cyber products are still relatively diverse in terms of what is covered and what is excluded, and are filled with nuanced language so that even insurance professionals sometimes struggle to understand the true scope of coverage. As a result, most cyber products are far from being easily digestible for the consumer market. Moving forward, insurers need to focus on developing more standardised, simple policy language with clear loss examples so the consumer can easily understand the value of their purchase.

Insurers are not new to the practice of developing and marketing policies for emerging risks. These same challenges have been faced, and conquered, every time our market has pushed itself to innovate and provide coverage for a "new" risk, and insurers willing to progress personal cyber will benefit by making themselves relevant to a changing consumer base that increasingly demands solutions for the threats they face in the digital world.

Our rapidly increasing dependency on technology is tested daily by criminals with an appetite to compromise that technology and exploit individuals for gain in a host of ways. History teaches us that new risks create opportunity for insurance innovation and growth, and personal cyber risk is no different. If managed correctly, the market presents great potential with growth expected to mirror the recent commercial cyber market boom. ■

Amie Watson is senior underwriter, technology liability and cyber risk at Aspen Insurance

FOCUS/CYBER

The insurance market should not be held to ransom

For carriers to mitigate the increase in the frequency and severity of ransomware attacks, they must introduce IT security solutions into their insurance coverage

Graeme King
Volante Global

Ransomware attacks are becoming one of the most common forms of cyber attack across the majority of business sectors.

Last year saw the figures rise for virtually every sector, from the number of attacks attributable to ransomware and the number of successful breaches through to the costs associated with remediation in the aftermath of an incident and the average length of downtime caused.

Unsurprisingly, the repercussions of this upwards trend have been evident across the cyber insurance market in recent months. Insurers have experienced alarming increases in associated loss ratios as a result of the surge in the frequency and severity of ransomware attacks. In turn, this spike has driven a rise in cyber rates, the introduction of more stringent terms and conditions and a narrowing of the scope of coverage available in an effort to counter losses and reduce exposure.

There is little sign of the threat level reducing. The transition to remote working, initially driven by the Covid-19 pandemic but increasingly being viewed as the new operating norm, has massively expanded the attack surface for cyber criminals, with ransomware attacks continuing to be one of the most effective tools used by cyber criminals.

While cyber insurance is viewed by many market practitioners as a key growth area, there is clearly a disconnect. The threat is expanding and the attack types are evolving; and in such an environment loss ratios will only move in one direction. If the insurance market is to continue to provide a relevant and effective product at a price deemed affordable, the approach to developing a cyber insurance solution must change.

Benefits of endpoint multi-layered cyber security

- The insurance industry benefits from reduced claims activity due to improved security;
- Reduced loss ratios open up greater market potential and enable broader product scope;
- The insured is provided with improved security and reduced exposure to cyber risk; and
- Insurers and insureds operate as a unified force to improve overall cyber security.

Shift in cyber focus

The industry is over-reliant on a cover-based solution to tackle what is fundamentally a technology problem. In such an environment, the only response to increasing exposure levels available to cyber insurers is to adjust the policy levers for rates and terms. A further hindering factor is the focus is often on broad-based risk selection and providing efficient breach response, rather than on the root cause: the attack itself.

A fundamental issue hindering the ability of many organisations to address cyber attacks is they are increasingly resigned to the fact their cyber security will inevitably be breached. There is an assumption that is simply a cost of doing business and cyber insurance is there purely to address those costs when the inevitable happens. That mindset needs to change, particularly as that cost of doing business is likely to increase significantly based on latest trends.

While the threat environment has evolved considerably in recent years, so too has the security environment. The advancements in cyber security now extend far beyond the defensive walls of anti-virus software and firewall technology, which continue to form the cyber security mainstay of many organisations – particularly for small to medium-sized firms.

Multi-layered endpoint protection solutions are becoming mainstream essential cyber security tools for all organisations. Some of these next-generation tools, designed to block all malware before it executes – including malware introduced through zero-day vulnerabilities – are not only available but affordable.

Further, enhanced monitoring capabilities within the organisation's network now enable companies to maintain a hyper-vigilant security domain. Any instances of malware detection result in virtually instant lockdown and automated response processes that block and quarantine the threat before it has a chance to execute and cause damage and well before the company is even aware of the incident.

Fusing technology and insurance

If we are to tackle a technology issue, we must look to make technology part of the solution. To do that effectively, cyber insurance should be tied to specific technology that blocks malware. This requires a shift in mindset from all parties: insurers, brokers and customers.

It is imperative the solution delivered is not simply a "break glass in case of emergency" offering that only adds value after a system has been breached. By integrating malware-preventing security technology into the cyber insurance solution it is possible to create a product that spans the full life cycle of the ransomware attack, from repelling the initial assault to responding effectively in the unlikely event of a successful breach.

Volante Global has been working with cyber security solution specialist GBMS Tech on ways to offer clients endpoint multi-layered security technology as part of its cyber insurance offering. The multi-faceted ransomware proposition is designed to deliver insurance cover at an acceptable premium level through promoting the adoption of the latest technological defences.

Such comprehensive solutions we believe create a win-win situation for all parties to the policy (*see box*). The only party that will not benefit is the cyber attacker.

As an industry, we need to become a cyber security partner to businesses. To do that, we must elevate the insurance solution from being a "patch and repair" service to a fully functioning core component of their cyber prevention strategy. The technology exists to facilitate this – it is up to insurers to grab hold of it. ■

Graeme King is managing director of cyber at Volante Global

Technology can help to tackle the rising risks attributable to ransomware attacks

JMiks/Shutterstock.com

insuranceday

New York regulators release cyber insurance guidance

DFS claims framework is first in US

Marc Jones
News editor

The New York State Department of Financial Services (DFS) has issued a new cyber insurance risk framework.

The framework outlines industry best practices for New York-regulated property/casualty insurers that write cyber insurance to effectively manage their cyber insurance risk.

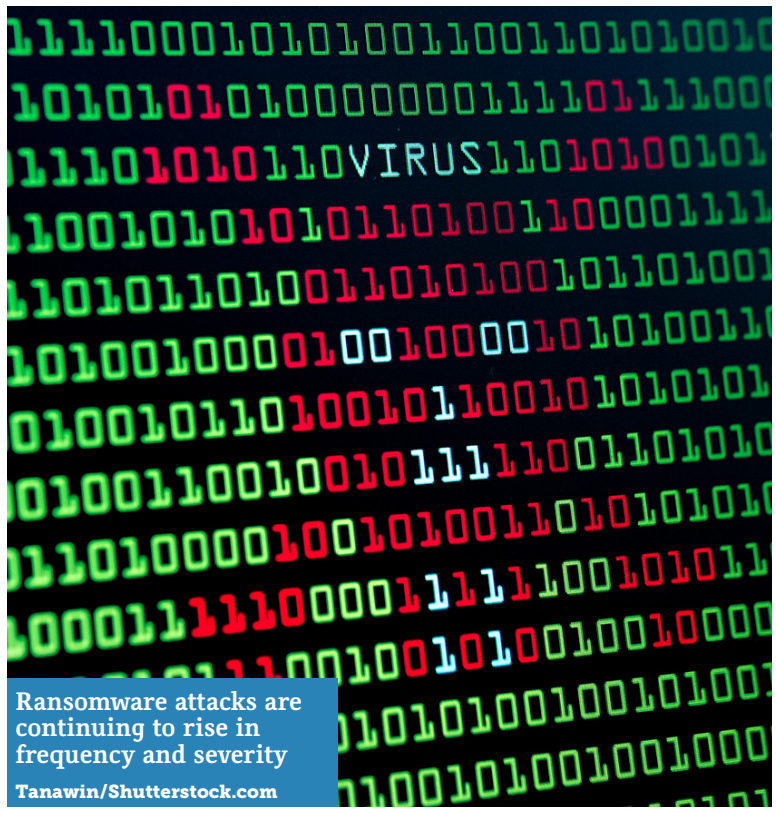
According to the DFS, the framework is the first guidance by a US regulator on cyber insurance. It includes a number of best practices, such as managing and eliminating exposure to "silent" cyber insurance risk, educating insureds and insurance producers and evaluating systemic risk.

"Cyber security is the biggest risk for government and industry bar none. Cyber insurance is critical to managing and reducing the extraordinary risk we face from cyber intrusions," DFS superintendent, Linda Lacewell, said.

"After extensive dialogue with industry and experts, we are issuing guidance to foster the growth of a robust cyber insurance market that can effectively help protect us against the growing cyber threats we face."

The DFS said the risk and cost associated with cyber crime have continued to increase dramatically, driven in large part by the increasing frequency and severity of ransomware attacks. Ransom payments fuel further ransomware attacks, as cyber criminals use ransom to fund ever more frequent and sophisticated ransomware attacks.

The DFS added ransom payments also do not guarantee an organisation will get its data back or that criminals will not use that stolen data in the future. For these reasons, law enforcement authorities, including the Federal Bureau of Investigation, recommend against ransom payments and the DFS concurs.



Ransomware attacks are continuing to rise in frequency and severity

Tanawin/Shutterstock.com

The framework is a result of DFS's ongoing dialogue with the insurance industry and experts on cyber insurance, including meetings with insurers, insurance producers, cyber experts and insurance regulators across the US and Europe.

A full copy of the framework is available on the DFS website.

Eiopa chairman: centralised insurance regulation is needed

Eiopa's chairman, Gabriel Bernardino, has issued a call for more centralised insurance regulation in Europe, *writes Marc Jones*.

Bernardino, who will come to the end of his second five-term as chairman in March of this year, made the call at an online conference marking Eiopa's 10th anniversary.

He said consistency of supervision is an essential element in a single market and it is essential for a level playing field between market participants and for the equal protection of consumers.

Good supervisory outcomes depend heavily on the capacity of supervisors to put in place common proactive and intrusive risk assessments and deliver timely enforcement, Bernardino said.

He said the ability of national supervisors to ensure high-quality and effective supervision is largely influenced by their governance framework, their independence in relation to national political institutions and the industry, and their capacity to recruit and maintain a sufficient number of highly qualified staff. Bernardino said Eiopa continues to have fundamental differences and challenges in these areas throughout Europe.

"While a lot of progress has been achieved over the years due to the common efforts of Eiopa and national supervisors, my personal assessment is that it is impossible to overcome the remaining challenges without a deeper structural reform," Bernardino said.

According to Bernardino, a single supervisory mechanism for insurance is needed and its absence is mostly felt in crises like the Covid-19 pandemic.

He added that in reforming the system, the centralisation of some elements of insurance supervision in the EU is imperative, especially the supervision of the internationally active insurance and reinsurance groups that are present in many member states and worldwide, and the supervision of companies exercising cross-border business under the freedom to provide services.

Sontiq to acquire CyberScout

Specialist cyber service provider CyberScout is to be acquired by Sontiq, part of Wicks Group, *writes Marc Jones*.

Sontiq has signed a definitive agreement to acquire CyberScout, which provides cyber products and services to the insurance industry.

Sontiq, which provides cyber monitoring solutions and breach response services, said the acquisition will see the group expand into the insurance industry with cyber solutions and forensic investigation products and services.

Brian Longe, president and chief executive of Sontiq, said: "By adding CyberScout into our product portfolio we are further strengthening our financial services market position with insurance industry expertise."

Axis Re adds Glass to North America casualty team

The Axis Re division of Bermudian re/insurer Axis Capital has appointed Michelle Glass (*pictured*) as senior underwriter on its North America casualty team, *writes Marc Jones*.

Glass joins from Munich Re, where she served for more than 20 years, most recently as senior vice-president and casualty team leader.

Before Munich Re she worked at AIG, Interstate International Group and Crum & Forster, with a focus on North America casualty.

The company has also named Halina Herc as a senior underwriter for North America casualty. Herc has been with the company since 2002, most recently serving on its regional and multi-line team.