PCI
CONFERENCE NEWS | 2018 ANNUAL MEETING
MONDAY
OCTOBER 29, 2018
BUSINESS INSURANCE®
www.businessinsurance.com

IN BRIEF

AIG scores win in FCA dispute

A New York state appeals court vacated an arbitration award to Allied Capital Corp. in connection with a coverage dispute involving a federal False Claims Act lawsuit stemming from a whistleblower suit alleging New York-based Allied Capital had violated the FCA. Allied Capital settled the case and sought coverage from American International Group Inc. An arbitrator originally ruled for AIG but later awarded Allied Capital $11.9 million. The appeals court ruled the arbitrator exceeded its authority by altering its original award.

Aon reports higher organic growth

Aon PLC reported 6% organic growth for the third quarter of 2018 Friday, including 8% organic growth in its commercial insurance brokerage operations and its reinsurance brokerage unit. The commercial risk solutions unit reported revenue of $1.03 billion, a 12% increase over the prior-year period, and reinsurance solutions reported revenue of $279 million, down 21%, but accounting rule changes reduced revenue by 30% on a comparable basis. The brokerage reported net income of $153 million, down 20.3%.

Hartford benefits from lower catastrophes

Hartford Financial Services Group Inc. on Friday reported 2018 third-quarter net income of $432.0 million, up 84.6% over the catastrophe-hit third quarter of 2017. The insurer reported higher income in commercial lines, personal lines, group benefits and mutual funds, and benefited from a lower U.S. corporate tax rate. The property/casualty combined ratio improved to 97.3% from 107.1%.

Industry faces big changes as politics, technology evolve

BY GAVIN SOUTER
gsouter@businessinsurance.com

Economic growth and technological innovation will present a range of new opportunities for insurers, but they will also have to adapt to regulatory and legislative changes that could result from next week's elections, said David Sampson, president and CEO of the Property Casualty Insurers Association of America.

This year's PCI conference in Miami Beach, with its theme of "Looking Ahead," is designed to help insurance executives make the most of the evolving economic and political environment, he said.

"We really want to focus on the future of the industry and PCI's role in working with our member companies to help them navigate uncharted political, regulatory and legal waters and look at new opportunities that the economy is creating," Mr. Sampson said.

Political and regulatory changes are likely to follow federal and state elections that take place Nov. 6. Several governors are term-limited and won't be running for re-election, which will lead to changes in insurance regulators, which are appointed positions in most states, he said.

At the federal level, there will also be new lawmakers who will likely not be familiar with issues that are of concern to the insurance industry, Mr. Sampson said.

For example, the federal terrorism insurance backstop — usually referred to as TRIA — expires at the end of 2020, and the industry will be leading efforts to reauthorize the legislation.

"With a whole new slate of pol-

See **CHANGE** page 7

Insurers remain frustrated with flood cover impasse

BY MARK A. HOFMANN

It looks like Congress will delay a long-term reauthorization of the National Flood Insurance Program yet again.

The program is slated to expire Nov. 30. Caught in the throes of midterm elections, lawmakers aren't showing any appetite for reforming and reauthorizing the debt-ridden program beyond the minimum needed to keep it in place temporarily. That's despite the impact of hurricanes Florence and Michael, which supporters of greater private insurance participation in the flood market say underscores the need for greater flood insurance takeup.

There are, however, signs that the idea of having private insurers play a bigger role in the flood market may become more attrac-

See **NFIP** page 7

R!SK PERSPECTIVES

Cyber: the hidden risk revealed

Catherine Mulligan | Head of Cyber for Aon's Reinsurance Solutions business

Aon
Empower Results®

Q. | 'Silent cyber' is a buzz word at the moment: how can insurers protect themselves from surprise exposures?

A. | Regulatory attention and high profile attacks — including reports from PRA and EIOPA and the far-reaching ransomware attacks NotPetya and WannaCry — has raised awareness of how cyber incidents can impact multiple lines of business. It's imperative that insurers identify and quantify the exposure in their portfolios. Aon's Reinsurance Solutions cyber practice group works with clients on this process, including running bespoke scenarios. We recommend developing a long term approach to cyber – whether exclusions or additional premiums and express coverage grants – but clash reinsurance capacity is available in the meantime for companies that are in the process of transitioning their books.

Q. | How are reinsurers reacting to silent cyber — are they prepared? Is capacity available?

A. | Reinsurers are willing to provide clash capacity — Aon has secured $350M to date — for companies that are in the process of actively addressing their exposure. Reinsurers are asking questions about cyber on their traditional treaties so insurers are advised to take a proactive approach.

Q. | The cyber market has huge growth potential but what is driving increased reinsurance buying? What factors do insurers need to bear in mind?

A. | The global regulatory environment and expanding attack vectors continue to motivate new buyers. Insurers understand that being able to provide a cyber solution to their clients is important, but they continue to refine their understanding of the exposures. Analytics and data including bespoke scenarios are helping carriers underwrite and price for cyber exposure. Still, support from the reinsurance market is an essential piece of insurers' overall portfolio management strategies.

Q. | And we also hear from insurers about the threat of aggregation. Can you share an example of the kind of attack that could cause this and how can insurers better understand the exposure in their portfolios?

A. | Public filings have shown financial loss and extra expense estimates from the 2017 malware attack NotPetya are upwards of $2.2B (source: Aon's Cyber Predictions report). This attack and others like it cause widespread disruption and even physical loss or damage. Insurers have not always specifically underwritten or priced for these exposures. We are working with insurers to analyze their so called "silent cyber" exposure across all of their portfolios. Carriers need to develop a long-term plan to address these exposures. Aon has sourced clash capacity to protect these portfolios during the transition.

To further understand silent cyber, Aon and Guidewire's Cyence Risk Analytics team have developed a new scenario where a hacker seeks to create significant disruption in the U.S. by opening the floodgates at a hydroelectric dam. If such a scenario were to occur it would likely cause significant downstream flood damages, resulting in 'silent cyber' losses for insurers. Silent cyber risk is the potential for cyber perils to trigger losses on traditional insurance policies — such as property or casualty — where coverage is unintentional or unpriced.

We analyzed the potential impacts of the scenario at three dams, selected to reflect a small, a medium, and a large exposure respectively. The key findings were that a cyberattack could cause:

- Major impacts not only to dam operations but also to the resilience of local businesses and communities, with the highest economic loss estimated at $56 billion.
- Silent cyber exposure to insurers, with total insured losses of up to $10 billion. By comparison, initial estimates of insured losses resulting from wind and storm surge damage from Hurricane Michael have ranged up to $10 billion.
- A significant protection gap that would impact homeowners and businesses if such an event were to occur, with only 12% insured in one scenario.

Q. | And what is being done to help companies boost their own resilience against cyber attacks?

A. | With growing Internet of Things (IoT) botnets, ransomware that targets backups, and an increasingly complex regulatory environment — cyber risk management must keep up. The goals stay the same: to protect business continuity and your organization's information. But what needs to be done to achieve these goals changes as rapidly as do the threats. Aon's recent Cyber Predictions Report highlights key recommendations of:

- Test the security of Internet of Things (IoT) applications
- Implement multifactor authentication
- Perform cyber-attack simulations and incident response readiness tests

Q. | You're a leading female figure in cyber insurance: how can we encourage more women to develop a career in this space?

A. | The insurance industry is facing a well-documented talent crisis, with increasing turnover and retirements. It's a business imperative that we tap the full scope of human talent for recruiting, retention, and career development. The insurance industry provides a broad platform for people to develop a wide array of skills — including technical, legal, negotiations, people management — making it one of the best kept secrets among those entering the workforce.

The cyber arena is growing and continues to change rapidly, making it an exciting segment in which to grow. But the numbers show room for improvement: according to the US department of labor,[*] about 47% of insurance industry employees are women, but the numbers drop at the SVP level. According to a recent Wall Street Journal article,[**] the number of women at SVP and C-Level positions in the Finance industry is only 23%; this is despite the fact that studies show women leaders outperform their male peers.[**] A thoughtful recruiting strategy and a commitment to mentoring and sponsorship is essential. Grassroots networking efforts such as those by the folks who have organized Women in Cyber Leadership[****] are a supportive initiative for women in this space. Finally, the cyber insurance industry can support the early education and development of girls in STEM careers.

[*] Citation on III website
[**] WSJ, A Corporate Ladder of Attrition for Women, 23 October
[***] https://sp.aonavenue.aon.net/myaon/aonasc/en-us/hr/Documents/Inclusion%20Resources/CEB-Three-Keys-to-Developing-Women-Leaders.pdf
[****] https://www.linkedin.com/groups/13514921/

Organizations should vet their vendors' cyber security

BY JUDY GREENWALD
jgreenwald@businessinsurance.com

Third-party vendors' cyber security is becoming an increasing concern for companies as the popularity of outsourcing data processes and other functions that are not within their basic areas of expertise grows.

It is a difficult task because of the challenges companies face in ascertaining who their vendors are, determining the extent to which these vendors may be putting their own cyber safety at risk and then addressing the issue.

"It's actually quite a large problem, and one that our insureds and the industry in general is struggling with, and I don't think there's been a perfect solution to date with this," said Yosha DeLong, technical director for Schaumburg, Illinois-based Zurich North America.

"Third-party vendors accounted for more than a quarter of all the claims that we saw" in Willis Towers Watson PLC's proprietary claims data, said Jason Krauss, New York-based cyber/errors and omissions thought and product leader for the brokerage's FINEX North America business.

However, there are steps firms can take to get a handle on this task.

"Any kind of connection to an outside party" brings with it a certain amount of risk, said Bob Wice, Farmington, Connecticut-based head of the U.S. cyber underwriting team for Beazley PLC.

One reason for firms' greater vulnerability is many have embraced the cloud for a wide variety of functions, including payroll, data processing and staffing, experts say.

But companies' success in grappling with this issue has

been mixed. "I think it's fair to say it's something that most companies understand as a risk, but they have a hard time knowing what to do about it, and smaller companies have a much more difficult time managing vendor risk because they simply lack the resources," said William Boeck, senior vice president and insurance and claims counsel at Lockton Cos. LLC in Kansas City, Missouri.

In response, "Many organizations are building a robust set of expectations that are conditions of doing business" with vendors, said Kevin Richards, Chicago-based global head of cyber risk consulting for Marsh Risk Consulting.

"The regulators are forcing this conversation, even more so than the businesses themselves," said Adam Cottini, managing director of insurance and risk management in North America at Arthur J. Gallagher & Co. in New York.

He pointed to the European Union's General Data Protection Regulation, the California equivalent scheduled to take effect in 2020 and the New York State Department of Financial Services Cybersecurity Regulations, with other states considering introducing comparable regulation.

"A lot of people are looking toward regulatory schemes like GDPR or various data protection statutes to provide some guidance and answers" to address the issue, said Tom Sheffield, New York-based head of specialty claims at QBE North America, a unit of Sydney-based QBE Insurance Group Ltd.

Stephanie Snyder, Chicago-based senior vice president and national sales leader for cyber insurance with Aon PLC, said that with other states likely to follow California and the potential for federal regulation around privacy as well, "organizations are much more mindful not only about the data they have, but what they're sharing," and want to protect themselves, both through their contracts and insurance.

Mr. Richards said firms can exercise significant control over third-party vendors in regulated industries, but in other sectors "it gets a little bit harder."

A longer version of this story will appear in the November issue of Business Insurance.

BUSINESS INSURANCE
U.S. INSURANCE AWARDS
Celebrating Today. Creating Tomorrow.

Business Insurance has opened nominations for the 2019 **U.S. Insurance Awards**, which highlight exceptional work by professionals across the commercial insurance industry.

The awards honor teams of professionals working on specific projects. Anyone familiar with a team's work can nominate them for an award. Submissions are due Dec. 18. *BI* editors will select finalists in each category to be reviewed by a panel of risk managers. The winners will be announced at a gala dinner in New York on March 21, 2019.

The categories are:

- **Broker Team of the Year** (firms with less than $500 million in U.S. revenue)
- **Broker Team of the Year** (firms with more than $500 million in U.S. revenue)
- **Community Outreach Project of the Year** – Pro Bono and Volunteer
- **Community Outreach Project of the Year** – Donations
- **Diversity & Inclusion Initiative of the Year**
- **Insurance Consulting Team of the Year**
- **Insurance Underwriting Team of the Year** (all property/casualty)
- **Insurance Underwriting Team of the Year** (management liability/professional liability/cyber liability)
- **Insurtech Initiative of the Year**
- **Legal Team of the Year**
- **Managed Care Provider Team of the Year**
- **Reinsurance Team of the Year**
- **Risk Management Team of the Year**
- **TPA Team of the Year**
- **Wholesale Brokerage Team of the Year**

A fundraising program associated with the awards addresses the industry's talent crisis by funding the *Business Insurance* Scholarship Endowment, which provides scholarships, grants and programming at universities without risk management degree programs.

Patrick Schmid

THE INSTITUTES RISKBLOCK ALLIANCE

Patrick Schmid is vice president of The Institutes' RiskBlock Alliance in Malvern, Pennsylvania. RiskBlock was formed last year to establish a blockchain network for the Institutes' member companies to allow them to work on insurance industry issues, such as sharing information and improving efficiency in insurance underwriting and claims. Recently, he spoke with *Business Insurance* Editor Gavin Souter about the progress insurers have made with blockchain and the potential for the technology in insurance. Edited excerpts follow.

Q How would you explain blockchain in a couple of sentences?

A Blockchain is defined as a distributed shared ledger that maintains a continuously growing list of chronologically added records in the form of blocks. These blocks contain data — it could be a transaction, it could be a smart contract — and this information is confirmed and verified through a decentralized consensus process that removes the need for intermediaries to be involved in validation and therefore establishes trust within the network without the use of a centralized authority.

Q Why do you think there is so much interest in this type of technology?

A I think it's the next logical step in technological innovation. You had advancements in a variety of different areas – computing, databases, networks, e-commerce – and this is the next step where you are fusing them all together. Businesses need to trust one another to interact and trade information, but trust is paid for. Businesses and governments store data themselves, they pay intermediaries to store data, or both, and that comes with a cost. What if every untrusting competitor within an industry trusted a secure blockchain to deliver that necessary information or what they deem appropriate on a permission basis? If that was the case, you'd see costs falling and a lot of universal problems being worked on together. The key reason for the interest is that it can really reduce reconciliation issues.

Q What efficiencies does it bring to insurance transactions?

A Consumers want a seamless personalized solution and that's challenging for insurers to provide without additional information on the individual. They also want lower prices, but it's challenging for insurers to do that. In emerging markets, folks want insurance, but it's not necessarily being provided because it's too costly for insurers. Blockchain could really help with the operational efficiency of an organization and therefore allow for more streamlined access to information to improve the customer experience. It could also make the process more operationally efficient, and cost savings could be passed on to consumers. It could lower the cost of entry in emerging markets because you can put parametric insurance on a blockchain and reduce claims costs.

On the insurer side, it can help with the administrative costs — record-keeping, verification of identities, contract validity — it could help with streamlining the flow of information and provide a single source of truth. And you can automate manual processes using smart contracts. Maybe it's also possible to set up a regulator node within a consortia setting that grants permissioned access to certain information so it eases the burden on regulators to retrieve the information and for insurers to supply the information.

Q How do you see blockchain's use in the insurance industry advancing in the next couple of years?

A I anticipate that there will be a movement to a common framework for the industry. If you end up with a multitude of networks, it will be a challenge for the industry. You are also going to see real production-ready use cases starting to emerge. As that starts to take place, I anticipate that members of various consortia, including ours, will start to recognize the (return on investment) and then you'll see it go a little exponential.

Q What about 10 years out from now?

A I can imagine all the areas along the insurance value chain being affected. In underwriting and risk management, for example, you'll have data sharing capabilities, risk registries may start to emerge, new customer data will be confirmed at origin, repeat entries will have gone away. Claims management will probably be extremely simplified by smart contracts, but also, by tying it to the "internet of things," you can imagine how sensors on automobiles will ignite the claims process. Finance, accounting and payments will change.

There will be more of a move to risk management.

Blockchain is defined as a distributed shared ledger that maintains a continuously growing list of chronologically added records in the form of blocks.

What the Hack!

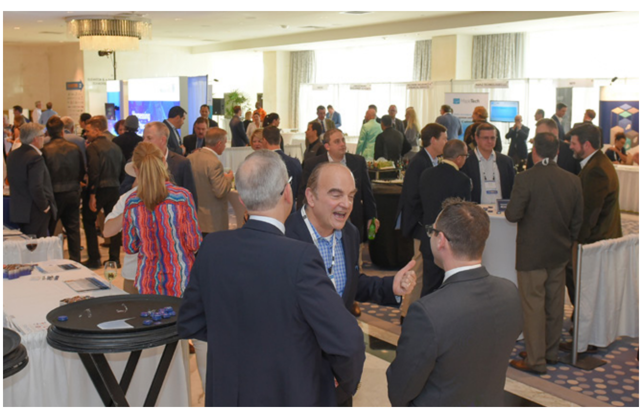
Who's hacking into your system right now? Your business could be next.

Learn more at munichreus.ly/PCIcyber

Products and services provided by Munich Reinsurance America, Inc. (Princeton, NJ)

NOT IF, BUT HOW

Munich RE



PCI SCENE

MIAMI

BUSINESS INSURANCE®

PHOTOS BY JASEN DELGADO

CHANGE

Continued from page 1

icymakers, there will be quite an educational effort that will need to be underway," Mr. Sampson said.

In addition, efforts to reform the National Flood Insurance Program is an ongoing effort (see related story).

The PCI conference has been structured to help insurance executives better position their companies in the changing environment, Mr. Sampson said.

The opening keynote speaker, Mohamed El-Erian, chief economic adviser at Allianz SE, will start the conference with an overview of the economic environment and how it will affect the industry.

Following the keynote, a panel of experts will address issues in the Florida insurance market. While PCI does not routinely discuss the market where the conference is held each year, "Florida is a unique and problematic state, so that's why we are taking the opportunity to do that this year," Mr. Sampson said.


Mr. Sampson

The regulatory panel that follows will focus on technological changes and how insurance regulation can keep pace with innovation in the sector, he said.

On Tuesday, retired Navy Adm. William H. McRaven, who headed the U.S. Special Operations Command, will focus on how to build cohesive, agile leadership teams in a rapidly changing environment.

And Robert Kagan, senior fellow at the Brookings Institution, will explore the U.S. role in the geopolitical environment, Mr. Sampson said.

"It's all about helping to position our members to look out over the horizon and anticipate where the broader trajectories of the economy and geopolitics are taking us, and then be able to take business decisions in their own companies to adapt and take advantage of those trends," he said.

NFIP

Continued from page 1

tive. Private reinsurers have been involved in the market for a few years. And the Federal Emergency Management Agency — which oversees the NFIP — is changing provisions that prevented private insurers that sell NFIP policies from also offering their own products, and prevented buyers from canceling NFIP policies in favor of potentially more cost-effective private policies.

"A lot of the real work of reform is accomplished by executive branch personnel carrying out subtle policy changes while looking at the legislative branch for signals," said John Rollins, an actuary with Milliman Inc. in Tampa, Florida. Mr. Rollins told a Capitol Hill policy briefing hosted by the Property Casualty Insurers Association of America in mid-October that recent Milliman research demonstrated that allowing private insurers to enter the market alongside the NFIP would increase the number of households with flood insurance.

"We think the bottom line is that public and private flood insurance can coexist in the regions we studied," he said in an interview before the presentation.

"I think that hurricanes Florence and Michael highlight the need for a more robust public and private flood insurance market," said Frank Nutter, president of the Reinsurance Association of America in Washington. "The number of uninsured properties is significant, and the need again for significant disaster assistance to help people demonstrates the need for the private and public sectors to do a better job of demonstrating the value of insurance. If you look at Hurricane Harvey, FEMA reported that the average household grant was $4,300 and the average NFIP claim paid was $115,000. It highlights the value of having insurance when recovery is financed."

"I think there's a good opportunity for our industry," said Don Griffin, Chicago-based PCI's department vice president of policy, research and international. Like Mr. Nutter, he pointed out the aftermath of every hurricane underscores how many people don't have flood insurance.

Mr. Griffin also noted that even before tallying all the claims from hurricanes Florence and Michael, the NFIP was $20.53 billion in debt at the end of last year.

Yet Mr. Griffin doesn't anticipate that Congress will move swiftly on a long-term reauthorization of the program.

"We're getting into the last push to the elections," he said. No matter which party wins control of Congress, "you've essentially got a lame-duck Congress, and I don't see them being in a hurry to address this other than to kick the can down the road into next year sometime."

He said he would like the program extended to Sept. 30, 2019, to align with the beginning of the next fiscal year and to give the new Congress a chance to settle in.

"It'll definitely be kick-the-can time again because of the calendar," agreed Blaire Bartlett, director of government affairs at the Washington-based Council of Insurance Agents & Brokers. She added that "unfortunately, nobody is thinking after Nov. 7, and Nov. 30 comes quickly after that. You don't have members and staff thinking about how to reform flood insurance right now."

"The federal government can't keep doing flood insurance on its own," said Ms. Bartlett. "The industry needs to figure out a way where you have the federal government and you have private industry — it's the same game."