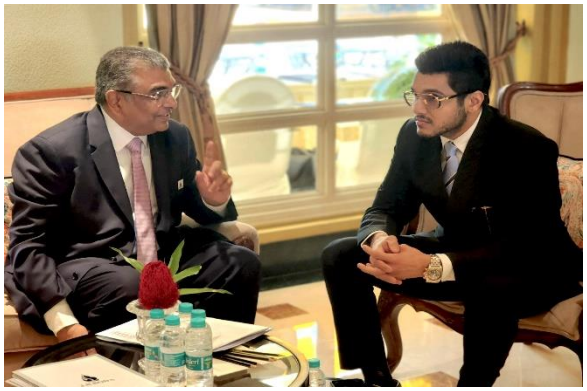
MEDIAN

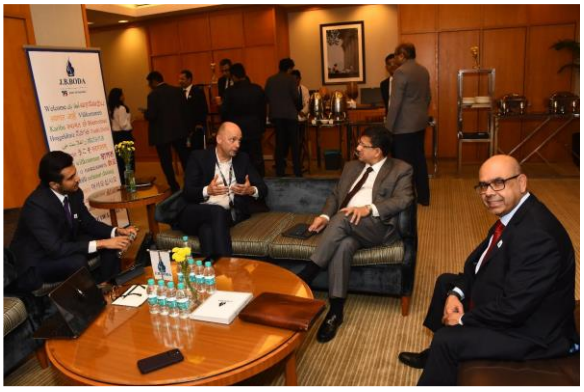
Feb 2023

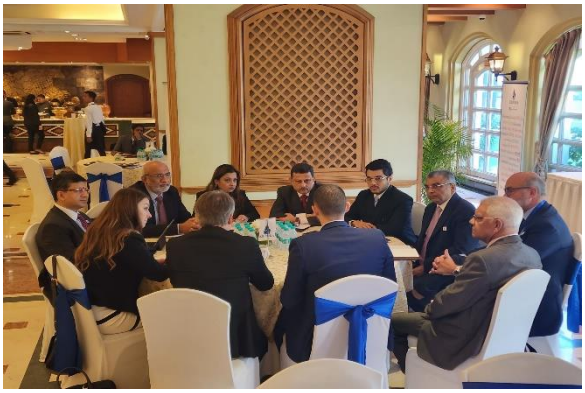
J.B.BODA

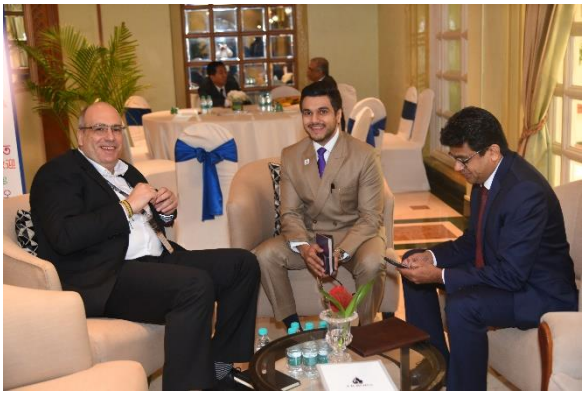
J.B.BODA

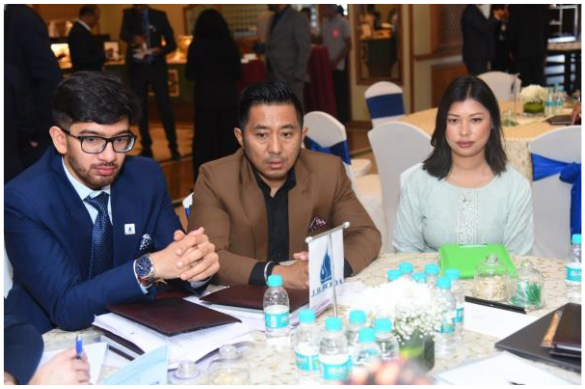
NEWS AT J.B.BODA











India Rendezvous 2023 - A glimpse

J.B.BODA

PRIME STORY

Gallagher Re warns of damaged relationships following renewals

Analysts at Gallagher Re have warned that many of the hard-fought positive outcomes for reinsurers at the recent January 1st renewals may have come at the expense of damaged client relationships.

Negative in its 1st view January reinsurance renewals report, the broker noted that the recent 1/1 period was "very tense" with negotiations running "very late" as reinsurers generally refused to show flexibility.

But while this may have resulted in improved pricing and terms for reinsurers, Gallagher Re says it may also have "reduced confidence from some buyers in the reinsurance product."

European property was viewed as the most strained line of business at the renewal, which was pressured by Hurricane Ian, as well as high inflation and growing demand for catastrophe capacity.

Through negotiations in November and December, Gallagher Re reports that European clients ended up mostly stepping up to reinsurers requests, issuing market led firm order terms, and aiming at full syndication.

Artemis ILS NYC 2023 conference

"Arguably the European property market re-set in two months some ten years of downwards cycle," analysts commented.

European cat and associated placements did eventually come together in a late rush during December after weeks of delays, which Gallagher Re says resulted from a combination of tactical delays by some reinsurers as well as an inability to commit to renewals by others.

Overall, this approach shifted the European market shares of the different global reinsurance markets to a much greater degree than during previous renewals with many traditional European markets gaining from this move.

Despite inflation driven cash increases on programmes that often already represented a double-digit percentage increase, most cat firm order terms – even for loss free covers – were up by at least a further mid +20%s to low +40%s risk-adjusted uplift for contracts covering key perils.

“Accepting to lose existing relationships, reinsurers were determined to force through these changes motivated by their own internal pressures of poor past results and restricted capacity for Euro wind often influenced by limited availability of Retro coverage,” Gallagher Re observed, adding: “other reinsurers were willing to step up but only at a price.”

Reinsurer also challenged low attachment levels and moved on an event basis closer towards the 1 in 10 years for key perils, in some cases achieving slightly lower attachments for combined perils layers.

However, there was little, or no flexibility shown by reinsurers towards these benchmarks with markets holding firm their positions to the end and often ‘forcing’ programme restructurings, analysts say.

Nevertheless, fears of limited capacity for key perils such as European wind and inability of reinsurers to satisfy additional capacity requests didn’t materialise as numerous reinsurers were willing to expand their deployed capacity, but only at the right price for new top layer capacity and often with restricted coverage.

Likewise, an early renewal push by some reinsurers to limit cat coverage to named perils also didn’t materialise but constituted a significant road-block in the early weeks of the renewals process.

Source: Reinsurancene.ws

J.B.BODA

NATIONAL

‘Most Targeted’ Industry In India By Hackers In 2022

Check Point Research (CPR) says that these cyberattacks were driven by smaller, more agile hackers and ransomware gangs. The cybercriminals focused on exploiting collaboration tools used in work-from-home environments and targeted education institutions that shifted to online learning post-Covid-19.

India has seen one of the biggest cyber-attacks last year when the servers of All India Institute of Medical Sciences (AIIMS) were targeted in a ransomware attack, which reportedly originated from China.. Now, a report says that healthcare was the most targeted industry in India even as global cyberattacks increased by 38% in 2022, as compared to 2021.

"Hackers like to target hospitals because they perceive them as short on cyber security resources with smaller hospitals particularly vulnerable, as they are underfunded and understaffed to handle a sophisticated cyberattack," said Omer Dembinsky, Data Group Manager at Check Point Software.

"The healthcare sector is so lucrative to hackers as they aim to retrieve health insurance information, medical records numbers, and sometimes, even social security numbers with direct threats from ransomware gangs to patients, demanding payment under threats of having patient records released," he added.
After the AIIMS attack, authorities feared that the data of crores of patients, including VIPs such as former prime ministers, ministers, bureaucrats and judges had been compromised, however, the data was decrypted, investigating IT authorities announced.

Global Cyberattacks ‘All-Time High’ -
Moreover, the reports revealed that the global volume of cyberattacks reached an all-time high in Q4, with an average of 1168 weekly attacks per organisation. Furthermore, healthcare is followed by education/research and government/military in second and third spots, respectively, in terms of most attacked industries in 2022.

Source: Times of India

GLOBAL

Cyber-attack on ShipManager servers

DNV's ShipManager servers were victim of a ransomware cyber-attack. DNV experts shut down the servers immediately in response to the incident. All vessels can still use the onboard, offline functionalities of the ShipManager software, other systems onboard the vessels are not impacted. The cyber-attack does not affect the vessels' ability to operate.

There are no indications that any other data or servers by DNV are affected. The server outage does not impact any other DNV services. The Ship Manager IT-infrastructure is isolated from the rest of DNV's servers, and the forensic investigation conducted by DNV's global IT security partners has confirmed that no lateral movement to other parts of the DNV IT-infrastructure was detected as part of the attack. Information like DNV user accounts, emails and all other services have not been affected by the incident.

The attack has been reported to the Norwegian Police, who has informed relevant police agencies. It was also reported to the Norwegian National Security Authority, the Norwegian Data Protection Authority (DPA) and the German Cyber Security Authority. All affected customers have been notified about their responsibility to notify relevant Data Protection Authorities in their countries.

As part of the investigation, DNV is working closely with global IT security partners to analyze the incident and ensure secure online operations as soon as possible.

DNV is in regular contact with all ShipManager customers about the situation. About 70 customers, operating around 1000 vessels, are affected. All affected customers have been advised to consider relevant mitigating measures depending on the types of data they have uploaded to the system.

Source: DNV

Japan Units Of Aflac, Zurich See 2 M. Customers' Data Breached

Aflac Life Insurance Japan Ltd. and Zurich Insurance Co., the Japanese unit of Zurich Insurance Group Ltd., said that personal information on a total of around 2 million customers has been stolen.

The information was breached through a hack against a U.S. subcontractor.

The two companies are rushing to conduct a detailed investigation and deal with customer inquiries.

According to Aflac, the breach affected 1,323,468 holders of three cancer insurance policies, covering their last names, ages, genders and insurance information. So far, it has not confirmed any unauthorized use of the stolen information.

At Zurich Insurance, the email addresses, customer IDs and automobile names of up to 757,463 automobile insurance policyholders may have been leaked, but the affected information does not include credit card numbers, bank account details and accident records.

Source: Nippon.com

US says it 'hacked the hackers' to bring down ransomware gang

The FBI revealed it had secretly hacked and disrupted a prolific ransomware gang called Hive, a maneuver that allowed the bureau to thwart the group from collecting more than $130 million in ransomware demands from more than 300 victims.

At a news conference, US Attorney General Merrick Garland, FBI Director Christopher Wray, and Deputy US Attorney General Lisa Monaco said government hackers broke into Hive's network and put the gang under surveillance, surreptitiously stealing the digital keys the group used to unlock victim organizations' data.

They were then able to alert victims in advance so they could take steps to protect their systems before Hive demanded the payments.

"Using lawful means, we hacked the hackers," Monaco told reporters. "We turned the tables on Hive."

Source: India Today

J.B.BODA

J.B.Boda Group of Companies

J.B.Boda & Co. Pvt. Ltd.	• Facilitating Employee Benefit Schemes and Life Actuarial • Valuation & Product Development • Facilitating Non Life Actuarial Services • Wellness Programmes • Risk Inspection • Training & Seminars
J.B.Boda Insurance & Reinsurance Brokers Pvt. Ltd.	• Non Life & Life Broking
J.B.Boda Insurance Surveyors & Loss Assessors Pvt. Ltd.	• Fire, Engineering, Miscellaneous Accident, Marine Hull and Cargo Surveyors & Loss Assessors • Marine Inspection • Superintendent Services • Tank Calibrators, Samplers & Analysts • Asset Valuation
Crowe Boda & Co. Pvt. Ltd.	• Protection & Indemnity Insurance Services Correspondents in India for : - Steamship Mutual Underwriting Association Ltd. (SMUA), London - Shipowners' Mutual Protection & Indemnity Association (SOP), Luxembourg
Atrium Consultancy Services Pvt. Ltd.	• Consultancy Services

Head Office:
Maker Bhavan No. 1, Sir Vithaldas Thackersey Marg, Mumbai 400 020 (INDIA)
Telephone : + 91 22 6631 4949 / 6631 4917 * Telefax : + 91 22 22623747 / 22625112
E-Mail : jbbmbi@jbbodamail.com * Web : http://www.jbboda.net * Follow us on
For any further enquiry regarding J.B.Boda Group kindly write to jirafe.vinayek@jbbodamail.com

DISCLAIMER

- This document is intended for general information purposes only. We do not accept any responsibility or liability for any errors or omissions therein / therefrom.
- We have not verified the contents of this document and we do not vouch for their authenticity. We hereby disclaim any responsibility or liability in these regards.
- Any statements, facts, figures, opinions, beliefs or views contained in this document do not necessarily reflect our sense, opinion or view and we cannot be held responsible or liable for them.
- Nothing herein contained shall constitute or be deemed to constitute a recommendation or an invitation or a solicitation or a suggestion for any party, person, product or service.
- Reproduction or distribution of this document without our permission is strictly prohibited.
- All disputes subject to Mumbai jurisdiction only.