MEDIAN

June 2022

J.B.BODA

J.B.BODA

NEWS AT J.B.BODA

Going live with the training session on "**Towards Strengthening Reinsurance Practices**": after a long break, a rendezvous with our Nepal Business Partners at Hilton Hotel, Jaipur on 26th & 27th April 2022

J.B.BODA

PRIME STORY

Why India Must Keep its Cybersecurity Shields Up

A robust intrinsic security framework that operates on the principle of zero trust coupled with security appropriate culture is imperative now and for the future.

On February 24th, 2022, just before Russia launched an all out offensive against Ukraine, there was one of the largest targeted cyberattacks in history against a number of Ukranian entities. March 31st saw yet another cyberattack on a Ukrainian satellite network that affected thousands of users across Europe. Hackers group Anonymous has been in the news since the beginning of the crisis for their attempts to bring down Russian websites. For the first time in history, geo-political conflict have also spilled over into the cyberspace. This prompted the Cybersecurity and Infrastructure Security Agency (CISA) to issue a Shields Up advisory to organizations across the US to prepare them for potential malicious activities. But the fact is that even before this conflict, cyberattacks were on an upward trajectory. 2021 alone saw organizations across the world facing 50 percent more attacks every week compared to the previous year. Evidently, cybersecurity can no longer be an afterthought. Even without a conflict, the time to put those security shields up and keep them up is right now.

The Indian Threat Landscape

Closer home, two thirds of enterprises in India have seen an increase in ransomware attacks over the last year. A recent report even indicated that India is at risk of cyber espionage attempts to collect sensitive geopolitical business and military intelligence. Incidents of malware and even ransomware attacks have been increasing steadily – the ransomware attack on NIMHANS Bangalore and the cyber attack on Indigo Airlines that had hackers swiping their internal documents are two recent ones.

There are several reasons why attacks are on the rise in the country. To begin with, India is on an accelerated digital transformation path. As the number of interconnected devices and networks increase so does the risk of breaches. To complicate matters further, the last two years saw most of India working remotely. The almost overnight shift to remote working resulted in highly distributed enterprise IT that stretched existing security infrastructure to its limits and exposed many unsecured home connections. In fact, India reported a 300 percent increase in cyberattacks in 2020 when the country was working in lockdown. By now its clear that the future of work will be hybrid with most employees choosing whether they want to work in office or remotely. Organizations will have to continue to secure this permanently distributed infrastructure in the years to come. India is also witnessing a boom in cryptocurrencies, and this opens up a plethora of security concerns. The good news is that Indian organizations, both private and govt., are already ramping up their security posture.

Intrinsic, Zero Trust, and AI Powered – The Security Shield India Needs

As India puts its shields up against new threats, it must ensure that security is intrinsic to its infrastructure. Gone are the days when security was an afterthought. For organizations to truly have their shields up at all time security needs to be built into the enterprise architecture. In fact, it must be an inherent and distributed part of the modern enterprise. And it must continuously incorporate all aspects of the technology stack to deliver effective protection through a zero trust approach. This involves building a dynamic and modern security framework that builds trust on a much broader and deeper basis than traditional security approaches. And given the heightened risk landscape, security infrastructure must be capable of continually monitoring for threats and detecting attacks in real time. Automated malware analysis pipelines to detect malware artefacts, and advanced analytics environment to detect attack fingerprints are vital, especially now when bad actors are using increasingly sophisticated technology for their attacks. Artificial Intelligence powered security platforms are particularly effective in always keeping the shields up against even the most sophisticated attacks. Intrinsic security platforms are already in play with most organizations realizing the value they deliver. In fact, for enterprises operating in tightly regulated, sensitive domains like BFSI, intrinsic zero trust security models are inherently tied in with business resilience and growth. The demand for such models will only increase with time.

Ongoing Efforts to Keep the Shields Up

As hybrid work models become the norm all remote access to the network as well as privileged access must mandate multi factor authentication. Software patches to address known exploited vulnerabilities, disabling of ports and protocols not essential for business, data recovery processes are now more critical than ever. Organizations using industrial systems or operational technology must test manual controls and processes regularly to ensure continued availability of critical systems. The human factor in cyber security also needs considerable focus considering 88 percent of data breaches are caused by human error. Security awareness training for all employees is a vital component of the overall security strategy and must be prioritized.

The CISA has issued the Shields Up warning against the backdrop of the situation in Ukraine, but the world must focus on keeping the security shields up long after the physical conflict is resolved. After all, this is the digital era and the world's digitized interconnectedness will only continue to evolve and grow in the future, opening up new vulnerabilities and weaknesses that can be exploited. A robust intrinsic security framework that operates on the principle of zero trust coupled with security appropriate culture is imperative now and for the future.

Source: Economic Times

J.B.BODA

NATIONAL

Insurers barred from advertising additional services unrelated to claims

The IRDAI has said that it is unacceptable for general insurers to advertise services provided by motor workshops that are not related to insurance claims as benefits provided within the motor insurance cover.

The regulator stipulates this in a circular to general insurers concerning the bundling of additional services for motor insurance customers as well as discounts on motor tariffs.

In the circular, the IRDAI notes that general insurers enter into service agreements with motor workshops/garages for the purpose of providing motor insurance claim services for the repair of accident vehicles. It is noticed that the service agreements in addition to claim services, extend certain assistance services not related to insurance claims such as free pick-up and drop-off of vehicles, body wash, interior cleaning, inspection of vehicles, etc.

The circular reads, "While the bundling of the above facilities with insurance is left to the motor service providers, the general insurers issuing advertisements of the said services, projecting them as benefits provided within the insurance cover is unacceptable.

"The main objective of service agreements with motor garages/workshops shall only be providing insurance services for claims of accident vehicles and they cannot arbitrarily expand to include the scope of services which are not relevant for insurance claims."

Discounts

A perusal of advertisements issued by a few general insurers showing discounts up to a certain percentage, savings on the premiums, etc, and the illustrations provided, reveals that the features or benefits are applicable under extreme or exceptional scenarios as defined under IRDAI (Insurance Advertisements and Disclosure) Regulations, 2021 dated 7 April 2021, says the IRDAI. The discounts in certain advertisements are not shown objectively on filed rates but expressed in comparison to rates of erstwhile tariff. "This is not to be done," the IRDAI stressed.

The regulator explained, "Considering that the quoting of motor premium rates is dependent upon multiple factors and a variety of risks, the contents of the said advertisements which may be applicable under extreme or exceptional scenarios would make a large number of prospective customers vulnerable to wrong understanding."

Caution

Insurers are thus advised;

(a) to discontinue the advertisements in respect of the services not related to insurance claims as may be provided by motor garages/workshops.

(b) to stop displaying discounts with reference or comparison to rates of the erstwhile tariff.

(c) to ensure that the discounts and savings on the premium which may be applicable only under extreme or exceptional scenarios shall not be displayed as examples.

Source: Asia Insurance Review

J.B.BODA

GLOBAL

Munich Re develops validation service for artificial intelligence systems

Munich Re has set up a new validation tool for a more responsible use of artificial intelligence (AI)-based solutions.

CertAI, is available via the start-up CertX, in which the German reinsurer has held a stake since 2021.

The new system evaluates AI solutions based on six key factors: fairness, autonomy and control, transparency, robustness, functional and cybersecurity, and data protection.

Source: Munichre.com

Insurance fraud comes at a high cost to Aviva

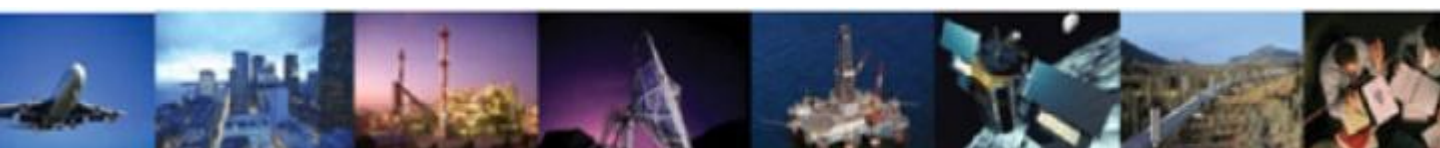
Aviva has identified a 13% increase in fraudulent claims in 2021. The insurer has listed more than 11,000 cases for a total cost of 122 million GBP (164.6 million USD).

The majority of such false claims (60%) relate to motor insurance. Homeowner's and third party liability insurance have also been targeted by fraudsters.

The increase of fraud in 2021 is mainly due to the decrease of income during the closing and lockdown seasons.

The U.K. group continues to strengthen its measures to combat insurance fraud. Aviva is currently investigating another 16,700 suspicious claims.

Source: Atlas Magazine



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 2262 3747 / 2262 5112
E-Mail : jbbmbi@jbbodamail.com * Web : http://www.jbbodagroup.com * Follow us on
For any further enquiry regarding J.B.Boda Group kindly write to jirafe.vinayek@jbbodamail.com