IIMC Library Clipping Service | Source: News: Online: Forbes India | Dated: 08-05-2023

How insurance-linked securities can improve cyber-security in India

Indian companies are digitising their workflow and are slowly waking up to the importance of cyber-risk management. But the cyber-insurance market in India is only a small fraction of the total annual cyber-loss incurred by these enterprises. Here's how it can seek more capital and serve better with the help of insurance-linked securities

Why is there a big supply-demand gap despite cyber-insurance being one of the fastest-growing insurance sectors in the country? Image: Shutterstock

The overarching root issue with a big gap in the supply-demand dynamics of current enterprise cyber-insurance markets in India is the lack of enough capital with re-insurers and insurers for them to scale their businesses. In 2018, the Data Security Council of India (DSCI) observed an ₹29,400 crore cyber-insurance market—a 40 percent increase in cyber-insurance purchases by enterprises in India from 2015. However, over the next four years that spanned the Covid-19 pandemic period, the growth in the cyber-insurance market has 'flattened' enough to fall much short of its projected target of ₹1.59 lakh crore by 2024 (when measured by the CAGR since 2018 market valuation). This—despite the total cyber-loss market being on the order of ₹15 lakh crore—implies that the cyber-insurance market in India provides third-party coverage for only a small fraction of the total annual cyber-loss incurred by enterprises.

RSS_Subsequently, this leaves the digital society spanned by the enterprises in India bearing the adverse impacts of billions of US dollars equivalent to unmanaged residual cyber-risk every year. What is most alarming is the fact that these huge supply-demand gap statistics are resulting when insurance experts in companies such as Bajaj Allianz,

ICICI Lombard, Tata AIG, HDFC Ergo, and Lloyds India—major cyber-insurance policy carriers in India—claim that cyber-insurance might be the fastest-growing insurance sector today. This is primarily because companies in nearly every sector—startups, manufacturing, transportation, banks, non-banks, IT service, health, and retail—are steadily digitising their entire workflow for increased ROI and business process efficiency reasons and are waking up to the cyber-risk management importance of such policies, especially post-pandemic.

LACK OF PREMIUM CAPITAL

The big question is: Why is there a big supply-demand gap despite cyber-insurance being one of the fastest-growing insurance sectors in the country? In other words, why is the cyber-insurance sector (in India and elsewhere in the world) starved of premium capital? The answer to this question has four dimensions:

1. High information asymmetry (IA) between the insurer and the insured driven by inter-dependent and correlated cyber-risk among businesses resulting in 'tricky' insurance policy underwriting by the cyber-risk bearing insurers,

2. Aggregate supply-chain cyber-risk,

3. IA-driven unattractive premium/deductible charged to insured businesses, and

4. The rise of ransomware cyber-attacks.

The lack of capital results in large inefficiencies in cyber-risk diversification markets. It hurts the potential of cyber-insurance products to significantly boost the security of enterprises and their ecosystems.

These viewpoints have also been recently echoed by Zurich Insurance chief Mario Greco who feels that enterprise cyber-attacks (especially those on critical infrastructure) might become uninsurable with growing business disruptions due to them. The scarily important lesson from past cyber incidents on critical enterprise infrastructure is not so much what happened as what did not happen. ICS hackers did not push their limits by not poisoning water supplies, not melting down nuclear power plants, and not bringing down the power grid of an entire city—despite them successfully compromising critical infrastructure facilities. Conditioned on the event that malicious actor intentions could only get worse over time, the words of the Zurich chief might be true simply because the post-attack economic damage could be too high for cyber (re)insurance companies around the globe to bear.

A RADICAL WAY TO BOOST CAPITAL

Another big question is: Is there any alternative way to boost capital injection in existing cyber (re-)insurance markets in India and worldwide? Insurance-linked security (ILS) solutions such as catastrophe (CAT) bonds and resilience bonds might provide an answer. The crux behind the potential effectiveness of ILS solutions, such as CAT bonds and resilience bonds, is that their markets rely on trading securities in non-correlated multi-trillion financial markets. Since financial markets can draw on a larger, more liquid, and increasingly diversified pool of capital than the equity of cyber (re-)insurance markets, diversifying (at most) a few hundred billion dollars of cyberrisk in a 30-odd trillion dollar financial market is akin to insuring a drop in an ocean.

According to a Hannover Re (a global leader in providing re-insurance services) report, the ILS market is approximately worth $100 billion globally. Even though this is not near to being a trilliondollar market (the valuation of cyber-loss annually around the globe), it is high enough to improve the density of current cyber-insurance markets—thereby also improving the ILS market in return. Since the early 1990s, ILS funds have provided retrocession (re-insurance for re-insurers) to the property-catastrophe re-insurance market for hurricanes and earthquakes when their capital is in short supply. ILS funds protect rare events and hence can generate,

1. Enough returns for their investors, and

2. Much required capital for cyber (re-)insurers to manage (catastrophic) cyber-risks more effectively.

In the context of insuring enterprise cyber-risks and especially in the age of rising ransomware demands, cyber-insurers can get enough capital injected into their business (through re-insurers) using ILSs to be able to rapidly proliferate markets with contracts that are not lemons—those that appropriately price exposed enterprise cyber-risk

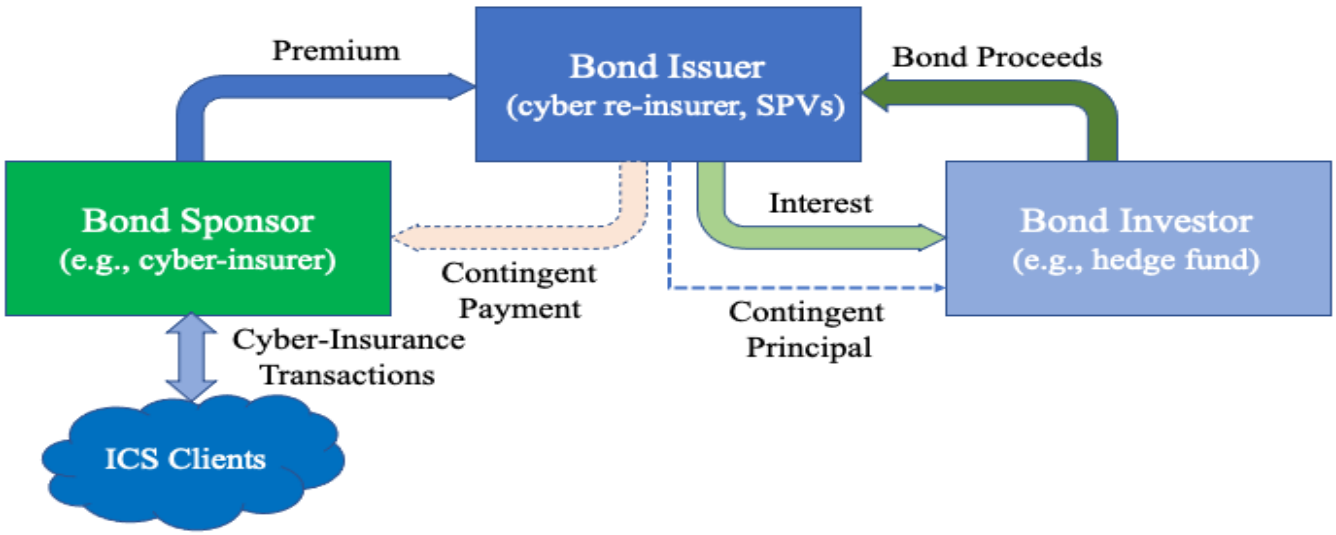
with coverage. This, alongside the fact that IT/ICSoperated smart cities around the globe are growing fast, will densify cyber (re-)insurance markets for the social good.

The International Financial Services Center Authority (IFSCA) committee has recently called for India to develop a framework to enable a captive insurance offering (including cyber-insurance), other alternative risk transfer solutions, insurance-linked securities (ILS), catastrophe bonds, and to specialize in parametric risk transfer as well. The goal here is for India to target being a successful Asian (cyber-) ILS hub, such as Singapore, through effective deregulation and provision of incentives. In other words, the IFSCA of India wants the nation to be another location that encourages global companies to look for an attractive marketplace for the issuance of (cyber-) insurance-linked securities.

HOW DO CYBER ILS SOLUTIONS OPERATE?

CAT bonds, when compared to treasury and municipal bonds, are only triggered in the event of a catastrophe—characterized by a (cyber) loss value above a particularly high threshold (e.g., above ₹10 lakh crores or $400 million in cyber-loss settings)

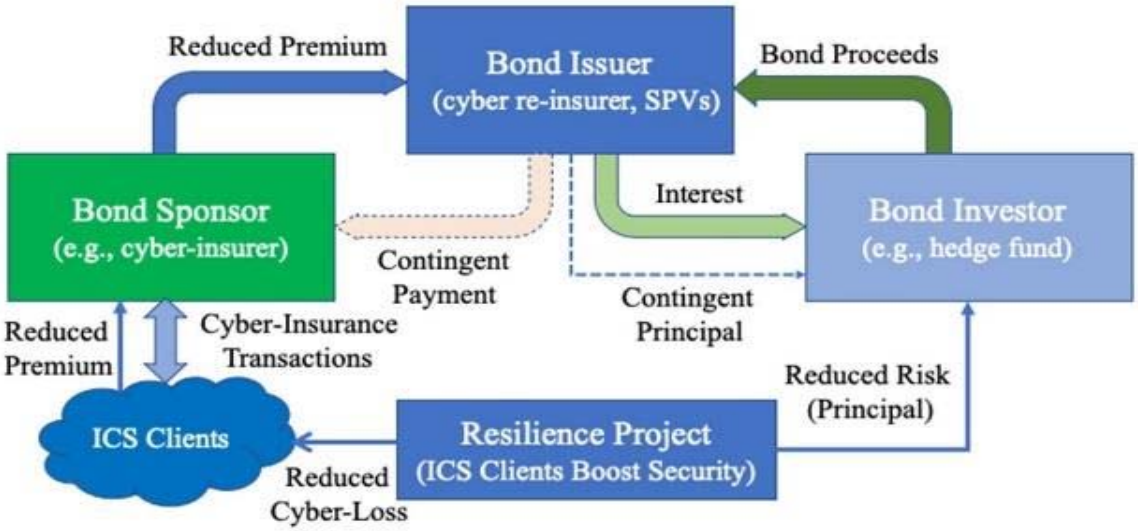
In the context of cyber-space, when a 'rare' catastrophe occurs (e.g., a critical ICS plant like a power plant shuts down for days at a stretch due to a cyber-attack) within a bond term (e.g., two years), the bond sponsor (the cyber-insurer paying premiums to a bond issuer) keeps a portion of the bond value to pay off aggregate first and third-party cyber-losses. The investors (e.g., hedge funds), on the other hand, lose some or all their principal (capital) invested. The bond issuer (e.g., cyber reinsurance firm along with special purpose vehicles and/or investment banks) creates the bond and pays interest to the investors after collecting premiums from the bond sponsor. If the catastrophic cyber event does not occur during the bond term, the investors get their invested capital back at a maturity date. In addition, the return on principal combined with coupon payments acts as the return on investment (ROI) for the investors. Since only catastrophic events trigger cat bonds, the portfolio-diversifying investors are happy to invest significant capital into cyber re-insurance markets (for higher returns) that, in turn, seep through to cyber-insurance markets.



The Basic Structure of a Cyber-Catastrophic Bond

A resilience bond is a new ILS instrument, and quite like a CAT bond in insurance benefits, can be used to inject capital into the cyber re-insurance market apart from protecting cyber re-insurers from cyber-catastrophes. These bonds link insurance coverage with capital investments in cyber resilience projects that reduce expected losses from cyber-catastrophes. To this end, the main difference between resilience bonds and CAT bonds is the former's goal of capturing a portion of insurance value created by cyber-resilience projects governed by critical enterprise infrastructures (e.g., ICSs) in the form of a rebate and transferring them to bond sponsors. This happens in two steps. In the first step, the bond issuer, i.e., a re-insurer and/or a third party (that include independent cyber-risk experts), uses data-driven financial catastrophe models to judge the degree that a cyber-resilience improving effort by an ICS

reduces expected aggregate cyber-losses. This degree contributes to the reduction in coupon, i.e., interest, payments to bond investors. In the second step, the cost savings from coupon rebates are distributed to bond sponsors, i.e., cyber insurers, and subsequently to ICSs in the form of resilience rebates used to finance cyber-risk reduction investments. The difference adds skin to the game of ICSs to boost their security and reduce negative externalities—also paying fewer premiums.



The Basic Structure of a Cyber-Resilience Bond

IMPROVING ENTERPRISE CYBER-SECURITY

We have thus far established that cyber-CAT and cyber-resilience bonds have the potential to densify existing cyber (re-)insurance markets covering (aggregate) enterprise cyber-risk by injecting significantly higher capital. On the other hand, dense cyber (re-)insurance markets have been proved via multiple seminal theory studies (Pal, et.al, IEEE INFOCOM 2014, Pal et.al., ACM SIGMETRICS PER 2018, Lelarge and Bolot, IEEE INFOCOM 2009, Shetty et.al., WEIS 2010) to improve cyber-security in principle. Because cyber-insurance premiums act as a strong control mechanism for enterprises to boost their cyber-hygiene and security culture. These results are conditioned on the fact that cyber-insurance be made compulsory for enterprises—though there will be 'proportional' improvement in cyber-security if a high proportion (if not all) of enterprises invest in cyber-insurance.

About authors

Ranjan Pal *(Massachusetts Institute of Technology, Sloan School of Management, USA)*

Bodhibrata Nag *(Indian Institute of Management Calcutta, India)*

Stuart Madnick *(Massachusetts Institute of Technology, Sloan School of Management, USA)*

Source:https://www.forbesindia.com/article/iim-calcutta/how-insurancelinked-securities-can-improve-cybersecurity-in-india/84811/1