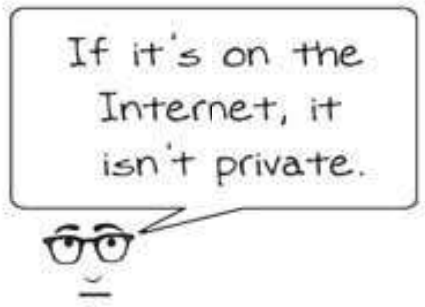
6

Mitigation of Cyber Risk Exposures in Bridging the Insurance Protection Gap - A Way Forward

Mr. P. Umesh



What is Cyber Insurance Protection Gap?

The subject of the Insurance protection gap has rightly become a matter of serious discussion for the insurance industry in recent times. The insurance protection gap means "the difference between the amount of insurance that is economically beneficial and the amount of coverage actually purchased" [1].Put it differently, it is "what is required and what is obtained" in terms of coverage and limits. This could be due to either absence of insurance protection or inadequate insurance in terms of limit or coverage. If there is no insurance protection or inadequate insurance protection, it has many serious consequences for economies; like an enormous financial strain on communities and organisations, wealth erosion, slowdown of economic recovery and weakening economic resilience.

Cyber insurance protection gap is caused by uninsurance or under insurance against cyber risks. While the issue of the insurance protection gap is a matter of concern in respect of all lines of insurance, it is very distinct and more challenging in cyber insurance because of the following reasons:

- Cyber risks are dynamic and continuously evolving risks that can make it difficult for insurance to keep pace with the advances in technology
- An Increasing number of security and data breaches affecting large corporations with sensitive public data.[2]
- Lack of actionable loss or claims data in adequate quantities. Cyber risks can affect various policies / policyholders at the same time. A cyber security incident can trigger losses across many lines of insurance:
    - Property insurance: Property damage and business interruption resulting from computer systems failures or viruses
    - Crime insurance: Siphoning money through phishing
    - Product liability/recall insurance: Product liabilities and product recalls resulting from security vulnerabilities
    - E&O insurance: Breaches of contract or negligence claims under E&O insurance
    - D&O insurance: Managerial failure in cyber security areas

Exposures of the target groups differ widely in different jurisdictions.

As per Dr Kai-Uwe Schanz of The Geneva Association:

"The least researched protection gap is cyber risk. Some studies put the annual global economic cost of cyber incidents at around $400bn, almost 0.5% of global GDP and almost twice the average annual amount of natural disaster losses.

Lloyd's recently attempted to quantify the cyber risk protection gap, based on modelled economic loss scenarios of up to $53bn (i.e., equivalent to losses from a major hurricane) and protection gaps of about 90%."[3]

Causes for Protection Gap

- **Lack of Awareness:** Despite the frequent occurrence of cyber-attacks generating extensive media coverage and the fact that quite a few of them caused losses, awareness about cyber insurance is low, particularly in retail and SME sectors. India ranks low in the cyber literacy index, which measures the population's cybersecurity knowledge as well as the ways that a country can enhance that knowledge through education and training.

- **Perception that Cyber Insurance is Expensive:** As in the case of many other lines of insurance, cyber insurance is perceived as an expensive and avoidable or postponable item since the returns are seen only in the unfortunate event of a claim.

- **Burdensome Buying Process:** Many insureds view the buying process to be long and time-consuming. Cyber insurers seek a lot of information on the risk profile of the insured, including its cyber security practices. Questions relate to many areas like organisational compliance, IT system/network / data security, and access management guidelines. Should the review of the insurance proposal form necessitate further enquiries, they may call for more details or request personal interaction involving, if necessary, outside agencies. While insurer views this as compulsory for proper underwriting, insureds look at it as cumbersome, if not intimidating.

- **Coverage Issues:** Buying any policy is not enough. Whether it is adequate in terms of coverage and limit also matters. While the issue of inadequate limit is easily understood and appreciated, if much thought does not go into coverage aspects, it can many a time cause serious problems, as can be seen from the following:

  As per a study conducted by BlackBerry and Corvus amongst 450 IT and cybersecurity decision makers at businesses across the U.S.

and Canada, about 37 per cent of respondents with cyber insurance don't have coverage for ransomware payment demands, and 43 per cent are not covered for ancillary costs, including court fees or employee downtime.

Coverage issues arise because of a lack of awareness / financial constraints on the part of insureds to purchase or disinclination on the part of insurers to offer.

- **Supply Side Challenges:** Insurance protection gaps are not caused by demand-side issues alone. Equally important are insurance market vulnerabilities and unfavourable loss ratios that impact insurance availability. When insurers/reinsurers look at cyber insurance as a business opportunity, there is nothing wrong about it. But can cyber be equated with other simple products from the point of view of product offering? The answer is in the negative.

Cyber insurance needs to be a complete solution and not just an insurance policy. Take off period for cyber is certainly longer as the market needs to understand and internalise the benefits. Against this premise, when we find that net retentions are low and there is heavy dependence on reinsurance capacity, the outcome is that reinsurers may wield greater influence and seek higher premiums or restrict coverage with a cascading effect. The situation gets worse if reinsurers withdraw their capacity leading to a widening protection gap in the short run and a trust deficit for the industry in the long run. It helps if the insurer and reinsurer relationships are strong and durable, and the reinsurer adds value to loss mitigation education and related processes for the direct insurer.

Remediation

- **Spreading Awareness:** It is imperative to spread awareness amongst insurance buyers about the availability of cyber insurance and the salient features. All entities in the insurance supply chain, and not just insurers, have a role in this endeavour. It is advisable

to talk about case studies and claims settled in India as a part of the education process. The industry can launch awareness campaigns targeted at various sections. Initiatives to spread awareness of cyber risks by various government agencies, including sectoral regulators in India, is praiseworthy. Communication in regional languages also plays an important role.

- **Process Simplification:** It is a fact that cyber insurance cannot be commoditised, and insurers need to underwrite cyber insurance with care and caution. But not all risks are so complex that they call for a deep dive. If as much information as is relevant and necessary is sought at the first instance, with helpful handholding, and when the risk is presented better by the insured and underwritten properly by the insurer, it reduces the purchase process pains. While it is likely that proposal form filling may itself prove to be an educational experience, it will be a good idea to consider a standard proposal form for personal and MSMEs(Micro, Small and Medium Enterprises). A lot of handholding is required for first-time buyers. This is where intermediaries, more particularly brokers, play an important role to demystify the product and handhold the insured through the entire process.

- **Perception on Pricing:** Many insureds think that cyber insurance is expensive and not affordable. This needs to be dispelled by convincing actions and appropriate messaging. Insurers need to make the price engaging and offer explicit incentives for better risk management practices and loss control measures. Once insureds realise that they are obtaining risk management solutions and not just buying a policy, handling objections relating to price becomes easier. Insurers must educate customers about value-added services offered along with cyber insurance policy as a part of the complete solution and communicate this with conviction.

- **Complete Solution:** To make cyber insurance acceptable and popular, and for risk minimisation, it is vital for insurers to offer

various services covering risk analysis, identification and mitigation of risks during the entire policy life cycle. These services may include assessment of cyber security, identification of security vulnerabilities, alerts on compromised credentials, IP & Domain threat blocking services, simulating phishing tests, recognition of false positives, threat vector analysis, cyber security technical audit and cyber security training etc. It is understandable that there are costs attached to build in these services. But it needs to be done in a cost-effective manner so that the idea does not become counterproductive. A graded approach is a good idea.

- **Holistic Approach:** Cyber risk should not be seen only as a technology issue. It is much more. It is for the insurer to present and the insured to understand that cyber risk management, including cyber insurance, ought to be a part of an organization's strategic enterprise risk management culture. Then and only then, the discussion would go beyond Information Technology jargon and touch upon the adverse consequences and likely losses leading to a better understanding of the adequacy of insurance- the central theme of the insurance protection gap. Whilst on this subject, it is critical to pay equal attention to people vulnerabilities besides process and product vulnerabilities.

As per the 2022 Global Cyber Risk and Insurance Survey conducted by Munich Re, many respondents felt that that the main challenges in improving cyber threat defence in their company include low-security awareness among employees, lack of skilled personnel, poor integration/interoperability of security solutions, and a lack of collaboration between individual departments. It is not just systems betterment, maintenance and upgradation that guarantee resilience. It should be fully supported by organisational culture with commitment and employee support.

- **Multi-stakeholder Collaboration:** It is crucial to encourage and tap the entire cyber ecosystem extensively, right from concept seeding to sale fruition and policy life cycle, including claims. At the concept stage, a lot of education is essential, which may require the support of government agencies. Involvement of third-party agencies is necessary preceding and during the cyber risk underwriting and also during the entire policy life cycle for various services like risk scanning and vulnerability alerts. Coopetition, as opposed to competition, is the need of the hour for cyber insurance – be it information sharing on cyber incidents and claims, or threat perception, etc. Insurers can work together in the areas of risk modelling and risk mitigation.

- **Insurance Product Innovation:** Insurance solutions need to keep pace with new and emerging avatars of cyber risks. As regards individuals and MSMEs, the introduction of simple products with process convenience would be ideal. Policy wording must be easy to understand and the claims process transparent and predictable. This enhances the acceptability of cyber insurance. Since many MSMEs are low on knowledge about cyber exposures as also low on financial resources, a broad template with the minimum required coverage based on a common reference framework can be an option.

- **Cyber Event Response Mechanism:** For the insureds, it is critical to initiate immediate action after any cyber incident for loss minimisation and course correction for further loss prevention. The response should be swift and comprehensive. This entails the establishment of a response mechanism consisting of a well-formulated structure with clearly defined protocols to facilitate an immediate and complex commensurate response without the regular layered bureaucratic approach that organisations may normally follow. Insurers need to incentivise insureds in this matter appropriately.

- **Prescriptive Insurance:** Insurers insist that cyber insurance buyers must comply with certain minimum standard requirements. In the Indian context, the minimum standard requirements generally include a sturdy IT infrastructure consisting of secure firewalls, strong passwords, regular training, robust encryption, proper leak detection tools, PCI/DSS certification in case of storage of card information, two-factor authentication, regular scanning for vulnerabilities, frequency for maintaining a data backup and malware protection application etc. Cyber insurance is becoming more prescriptive in that it requires insureds to comply with key cyber security benchmarks in order to qualify for and continuance of coverage. Recently, in the USA, "Travelers and policyholder International Control Services (ICS) jointly filed a stipulation to have a federal court rescind an active cyber insurance policy that the insurer claimed was void due to the insured's misrepresentation of multi-factor authentication use" [4]

  Amongst other things, insurers need to elucidate the importance of security and resiliency measures to their customers that influence outcomes such as pricing, coverages, limits, terms and conditions. It behoves them to set cyber security requirements in a transparent manner. This itself can prove to be both preventive and curative.

  Mitigation of risk exposures prevents and minimises losses of the insured and makes it possible for the insured to obtain appropriate and adequate cyber insurance solutions, thus helping reduce the cyber insurance protection gap.

- **Role of Intermediaries:** Since intermediaries, particularly insurance brokers, are close to the customers, they are likely to have a better understanding of the risk exposures. Some intermediaries have developed preliminary risk assessment tools. Some others are using third-party agencies to assist customers to carry on vulnerability studies. Intermediaries have a major role in

suggesting adequate quantum and appropriate cover, two vital components of the reduction of the protection gap. Generally, the known method of limit selection depends upon peer group comparison and modelling. Peer group comparison alone may not be the ideal way. It needs to be combined with other studies like modelling, estimation of the economic losses from one event, confidential nature of the data stored and operations carried, jurisdictions, a number of employees, likelihood of Business Interruption claims etc. Intermediaries need to develop and continuously update internal expertise in this area. They may also plan to conduct periodical training programs in collaboration with insurers.

Cyber Insurance Protection Gap - Risk Modelling

Risk management, including risk modelling, is dependent, besides other factors, upon the target groups of the customers.

- **Individual Cyber Insurance:** There is always an element of risk involved in all online activities. Exposures here mostly relate to concerns about the management of personal finances like hacking of debit/credit cards, phishing, theft of funds, identity theft, marketplace transactions and banking transactions, cyberstalking, and social media exposures etc.Cyber risks here occur at individual policyholders level – independent of the others.

  In the Indian context, some relief is available to the victims of cybercrimes, like the one offered by RBI to banking customers as provided in the direction on *"Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions"*. However, this protection is not carte blanche. Cyber education and regular alerts are some of the answers for risk mitigation.

  Whilst on the issue of the personal cyber insurance protection

gap, in January 2022, there were over 940 million active debit cards in India. This number was much higher than the number of credit cards, which amounted to around 70 million that same month. Contrast this with the number of individual policies taking into group policies issued in India which are still in 5 digits.

On popularising individual cyber, group propositions are likely to work better. This assists in getting volumes and spreading of risk. Web aggregators, Bancassurance, and affinity programmes are seen as effective media to popularise this insurance. It is also believed that having a bundled cyber policy with other policies like House Holders package policy may work well. The standalone individual cyber policy does not seem to be gaining much traction globally. It is gaining ground when sold as a bundled policy. It is also essential to impart education in the local language. For a better and broaderer spread of cyber culture, all the stakeholders need to reach out to small cities.

- **Corporate Cyber Insurance:** As organisations grow, they get increasingly exposed to a multitude of cyber-attacks like unauthorised access, unauthorised use or transmission of a computer virus which alters copies, misappropriates, corrupts, destroys, disrupts, deletes, or damages the organization's computer system causing losses to the victim organisation and/or may result in failure of security or Denial of Service. These may result in breaches of data, corruption of data, crippling of critical systems leading to business interruption losses and regulatory actions and various adverse consequences. Systemic risks also begin to be a matter of major concern here. Risk modelling gets a lot more challenging because of the dynamic nature of cyber risk and the problems associated with Risk accumulation.

"Systemic risk generally refers to the possibility that distortions in a system may spread across many entities and be augmented due to local or global feedback effects. It is often associated with a

> cascading propagation of losses such that multiple entities in a system are seriously affected within a specific period of time. In the context of cyber risks, the following definition was given by the World Economic Forum (see WEF (2016).”
>
> “Systemic cyber risk is the risk that a cyber event [...] at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component, but consequences also cascade into related ecosystem components [..]” [5]

Focus here would be more on cyber security practices and on the frequency and severity of likely losses.

Role of Insurtech

Because of the paucity of historical data, the extremely dynamic nature of cyber risks, coupled with difficulties in assessing accumulation and loss estimation, pricing cyber risks properly is still a formidable challenge. But as the industry collects and analyses more useful data, it can help at least directionally to minimise cyber threats and resultant losses. It is in this context that one needs to realise the role of Insurtech firms for their ability to significantly contribute to risk detailing, risk exposure reduction, probable maximum loss estimation, and price indication, finally leading to reducing the insurance protection gap.

The use of Artificial Intelligence (AI), Big Data and Data Analytics can identify contributing factors of various types of claims and identify the best means of risk mitigation. Insurtech firms help insurers and their customers to assess their cyber exposures more accurately. They can offer help in risk evaluation, understanding risk triggers and risk accumulation. They can also simulate policy structures to understand how policies perform under different cyberattack scenarios. Insurtech innovations include “Algorithmically derived security ratings and benchmarks from

BitSight and SecurityScorecard; probabilistic cyber models from Risk Management Solutions and AIR Worldwide; modelling and benchmarking tools from CyberCube; technical and behaviour-based loss estimation models on Guidewire's Cyence Risk Analytics platform; and Corax, a cyber risk modelling and prediction platform that leverages proprietary data on the cyber resilience of several million companies to provide insurers with benchmarking, predictions and probabilistic expected loss estimates." [6]

There is a vast space available for Indian Insurtech firms in this area.

Regulatory Actions

When regulatory bodies mandate certain cyber security measures and bring clarity to various concepts and reporting requirements about cyber events, it also helps in mitigating risk exposures. In the Indian context, apart from CERT-In of the Government of India, many regulatory bodies like RBI, IRDAI and SEBI issue directions regarding cyber security aspects.

It is useful to know the role of CERT-In here:

> CERT-In (the Indian Computer Emergency Response Team) is a government-operated information technology (IT) security organisation: the national nodal agency for responding to computer security incidents as and when they occur. The purpose of CERT-In is to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices throughout the country. It also plays a proactive role. The proactive functions include issuing security guidelines and advisories, vulnerability analysis and response, risk analysis, a national repository of cyber intrusions, profiling attackers and conducting training etc. The roles and functions of CERT-In can be read on https://www.cert-in.org.in/.

On 28th April 2022, the Government of India issued directions on compulsory reporting of cyber incidents as given below:

> "Any service provider, intermediary, data centre, body corporate and Government organisation shall mandatorily report cyber incidents as mentioned in Annexure I to CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents.
>
> All service providers, intermediaries, data centres, body corporate and Government organisations shall mandatorily enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days, and the same shall be maintained within the Indian jurisdiction. These should be provided to CERT-In along with reporting of any incident or when ordered/directed by CERT-In."

Details collected in compliance with this mandate would be useful in building the data for quick course corrections and future alerts. For the insurance carriers, they can expect claims to be lodged without much loss of time, which would be helpful for proper forensics and also for prompt settlement of claims. This reporting mandate, while it has met some resistance, places organisations on alert on the need for reporting and may facilitate quick remedial measures.

Considering the all-pervasive nature of cyber risks, continuous and close coordination amongst insurers, insureds, and professional bodies like FICCI, NASSCOM, and other entities associated with cyber security is the need of the hour for both risk prevention and mitigation. With cyber risk being geography, jurisdiction and sector agnostic and global in nature, it is advisable to track the global developments continuously and be in close liaison with all related agencies at the organisation, industry, country and global level.

Need for Alternative Risk Transfer (ART) Solutions

Should the capacity of the traditional insurance market shrink because of continuous huge losses causing the possible withdrawal of market capacity, it becomes unavoidable to seek protection from ART instruments like catastrophe bonds and insurance pools etc. Given the current conditions and claims experience, there does not seem to be to an

immediate need to explore ART options in India. It appears that, as of now, the industry has not suffered many claims in excess of USD 3 million per claim. But the need will be felt when systemic risks operate and result in catastrophic losses. Recent developments such as Lloyd's of London's decision to exclude state-backed attacks from cyber insurance policies makes a case to initiate exploration of ART solutions in cyber insurance, at least in some areas, to ensure that there is no protection vacuum.

Mandatory Insurance

Mandatory insurance is an unpopular opinion. The idea itself is anathema to many and is difficult to enforce. But it certainly is not a bad idea to look at what the Republic of Korea has done.

Under the PERSONAL INFORMATION PROTECTION ACT of the Republic of Korea., Article 39-9 (Indemnity for Losses) (1) Information and communications service providers, etc. shall take necessary measures such as purchasing insurance or deduction plans or accumulating reserves to fulfil its liabilities for compensation pursuant to Articles 39 and 39-2.
(2) Necessary matters, including the scope of personal information controllers subject to the obligation pursuant to paragraph (1) and relevant standards, shall be prescribed by Presidential Decree.

The issue of mandatory insurance may become a serious subject matter of discussion in India after the passage of Personal Data Protection legislation and its effective implementation.

Conclusion

The mission to minimise the insurance protection gap starts with the commitment of insurance providers to bridge the gap of understanding and mutual trust with their customers. Professional and effective response of insurers in the event of a claim in terms of process, speed, and quantum of claim would act as a significant confidence-building measure.

"A common thread in the protection gap discussion is that insurance consumers need to be better informed about their insurance, and if they are better informed, they will buy more insurance and better insurance"[7].

Narrowing the protection gap is not only for the benefit of the insurance industry. It reduces the economic burden on society freeing up resources which has many alternative uses. Bridging the trust gap and reducing information asymmetry with a long-term view of things appropriately accompanied by required actions go a long way to make this mission successful.

Disclaimer: The information contained and ideas expressed in this article represent only a general overview of the subjects covered. It is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. Insurance buyers should consult their insurance and legal advisors regarding specific coverage and/or legal issues.

References :

1. The Geneva Association. (n.d.). *Understanding and Addressing Global Insurance Protection Gaps,* https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/research_brief_-_global_insurance_protection_gaps.pdf

2. Brooks, Chuck. (2022). *Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know*, https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=3f85003a7864

3. Asia Insurance Review. (2018). *Understanding and addressing global insurance protection gaps*,https://www.asiainsurancereview.com/Magazine/ReadMagazineArticle?aid=40849

4. Hemenway, Chad. (2022). *Travellers,* P*olicyholder Agree to Void*

Current Cyber Policy, https://www.insurancejournal.com/news/national/2022/08/30/682564.htm

5. Maochao Xu & Lei Hua (2019). *Cybersecurity Insurance: Modeling and Pricing, North American Actuarial Journal*, 23:2, 220-249, https://www.insurance.uni-hannover.de/fileadmin/house-of-insurance/Publications/2021/Modeling_and_Pricing_Cyber_Insurance.pdf

6. Knutson, Ted. (2019). *The Cyber Insurance Gap is closing,* https://www.garp.org/risk-intelligence/technology/the-cyber-insurance-gap-is-closing

7. Merlin Chip. (2019). *Insurance Coverage Gaps—An Increasing Insurance Crisis Which Needs To Be Addressed and Stopped,* https://www.propertyinsurancecoveragelaw.com/2019/10/articles/insurance/insurance-coverage-gaps-an-increasing-insurance-crisis-which-needs-to-be-addressed-and-stopped/

Bibliography

1. Blackberry Blogs: The Cyber Insurance Gap: What Is It, and How Can We Close It? https://blogs.blackberry.\com/en/2022/08/blackberry-cyber-insurance-study

2. Munich Re Global Cyber Risk and Insurance Survey 2022

3. CERT-In, Government of India https://www.cert-in.org.in/

4. Report of IRDAI Working Group to study Cyber Liability Insurance

5. Statistics on the Number of debit cards in India from November 2019 to January 2022: https://www.statista.com/statistics/1245641/number-of-debit-cards-

india/#:~:text=In%20January%202022%2C%20there%20were,(COVID%2D19)%20pandemic.

6. “Cyence: Cyber insurance risk modelling and analytics. https://www.guidewire.com/products/cyence/

7. A New Approach to Cyber Resilience https://www.insurancethoughtleadership.com/cyber/new-approach-cyber-resilience

8. Personal Information Protection Act (General Law) in South Korea https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=3

9. RBI circular RBI/2017-18/15 dated July 6, 2017, on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions