MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

Bridging Gaps in Cybersecurity with Cyber Insurance

Rohit Kumar Sharma

March 21, 2024

Summary

Organisations and businesses are seeking broader risk management tools such as cyber insurance to mitigate the repercussions of cyber threats. India is one of the fastest-growing regions in terms of cyber insurance uptake. Challenges include rapid shifts in the threat landscape which makes it more difficult for both insurers and insured to catch up with emerging threats and exclusion clauses relating to state-sponsored terror attacks and terrorism.

As organisations increasingly digitise their operations, they find themselves vulnerable to cyber attacks resulting in financial losses. IBM Security's 'Cost of a Data Breach Report 2023' noted that the global average cost of the breaches reached an all-time high of US$ 4.45 million, a 2.3 per cent increase from the previous year.[1] The report also highlighted the need for better threat detection, as only one-third of companies discovered the data breach through their own security teams. The remaining were informed either by a third party or by threat actors themselves. The data breach lifecycle, which is defined as the time to identify and contain a data breach, was reported to be 277 days. These figures illustrate the dire situation faced by organisations that are becoming increasingly dependent on data collection, storage and processing to run their operations seamlessly.

Adding to this, the data protection legislations and other regulatory frameworks around the world are tightening the grip around these organisations or 'data controllers'.[2] The cost of a breach in an organisation extends beyond direct expenses like business interruption and data loss. It encompasses hidden costs such as the diminished value of customer relationships, loss of intellectual property (IP), and damage to reputation.[3]

The pertinent question is how organisations can effectively manage these risks, which appear to be growing incessantly. One obvious approach is to enhance cybersecurity preparedness within an organisation to pre-empt these threats. However, these preventive measures do not always yield successful outcomes, given the continuously expanding threat landscape and the evolving tactics, techniques and procedures (TTPs) of threat actors.

Given the inevitable nature of such threats despite the level of cybersecurity preparedness within an organisation, businesses are seeking broader risk management tools to mitigate the repercussions of such threats. To address these issues, organisations are buying cyber insurance policies to spread the risk and save their organisations during times of crisis. Can cyber insurance improve cybersecurity, or is it merely a means of spreading risk? Could insurance companies act as *de facto* cybersecurity regulators within an organisation? This Brief examines the role of cyber insurance while addressing these broader questions.

What is Cyber Insurance?

According to the Insurance Regulatory and Development Authority of India (IRDAI), which is responsible for managing and regulating the insurance and reinsurance

[1] **"Cost of a Data Breach Report 2023"**, IBM Security.

[2] According to the EU's General Data Protection Regulation (GDPR), 'controller' means the natural or legal person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of the processing of personal data. 'Data fiduciary' is used in India to denote the controller.

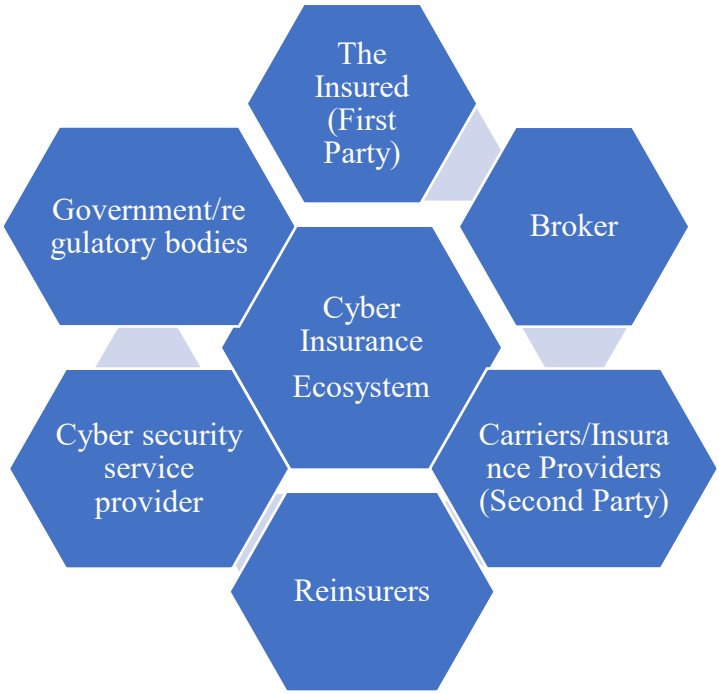
[3] **"Seven Hidden Costs of a Cyberattack"**, Deloitte.

industry in India, "cyber insurance is an insurance policy designed to protect the policyholders from cybercrimes".[4] Elaborating further, it describes cyber insurance as

> …a risk management and mitigation strategy having a corollary benefit of improving the adoption of preventive measures (products, services, and best practices), thus, helping improve the cyber security posture of organisations, and thereby the country as well.[5]

Given the nature of cyber threats and ensuing loss to an organisation, cyber insurance, as with other types of insurance, "is intended as a means of risk transfer to eliminate large, unexpected costs and replace them with smaller planned payments charged at regular intervals".[6] Josephine Wolff also writes that unlike traditional insurance policies dealing with automobile, flood or fire-related incidents, cyber insurance does not cover a single, coherent type of risk and damages.[7]

Figure 1. Key Stakeholders in the Cyber Insurance Ecosystem



Source: Data Security Council of India (DSCI).

Cyber insurance not only addresses or mitigates the financial losses resulting directly from a cyber incident, but also provides protection against subsequent third-party

[4] **"Report of the Working Group (WG) to Study Cyber Liability Insurance: Individual Cyber Insurance"**, Insurance Regulatory and Development Authority of India (IRDAI), 23 November 2020, p. 9.

[5] Ibid.

[6] Josephine Wolff, *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks*, The MIT Press, Massachusetts, 2022, p. 13.

[7] Ibid., p. 215.

claims and liabilities stemming from such events. Therefore, coverage for losses due to cyber incidents can be categorised by differentiating between losses incurred as a direct result of the incident (first-party coverage) and losses as a result of litigation by injured parties (third-party coverage).[8]

Elaborating further, the first-party coverage is triggered by a variety of reasons, including data theft, malicious destruction of data, accidental damage to data, cyber extortion, etc.[9] Third-party coverage deals with claims and lawsuits for breach of privacy, misuse of personal data, defamation/slander, legal defence costs, regulatory fines and penalties, etc. Beyond this, cyber insurance also provides coverage for other services, including crisis management cover and consultant services cover.

The coverages mentioned above are not exhaustive and may vary depending on the jurisdictions, reflecting the legal and regulatory norms and frameworks of a particular state. Certainly, cyber insurance can assist an organisation in mitigating financial losses and in swiftly restoring its operations. However, similar to other insurance policies, cyber insurance policies do not provide coverage for every conceivable scenario, particularly due to the systemic risks inherent in cyberspace.

To mitigate certain types of risks from coverage, insurers include exclusion clauses in the contract due to the high level of risk involved. These exclusions are intended, in part, to safeguard the financial stability of insurance companies. However, the exclusion clause restricts the potential coverage for organisations purchasing the policy. Generally, these exclusions clauses are consistent across different jurisdictions, with a minor difference, primarily covering risks stemming from cyberattacks perpetrated by a state or state-linked threat actors.

Why Cyber Insurance?

What motivates organisations to invest in cyber insurance policies, particularly when they are already allocating resources for cybersecurity preparedness? Why would any organisation buy such a policy when they are using the best tech stack available to them? The answer lies in the very nature of cyberspace and the inherent systemic risk associated with digitalisation. Systemic risk refers to the possibility that 'a single event on one part of a digital system could cascade to other interconnected third parties sitting on the same system'.[10]

The rapid growth of such risks is directly correlated to increasing dependence on Software-as-a-Service (SaaS)/third-party vendors. Moreover, these third-party vendors are 'highly concentrated in key areas like cloud services and managed service

[8] **"Report of the Working Group (WG) to Study Cyber Liability Insurance: Individual Cyber Insurance"**, p. 40.

[9] Judy Selby, *A Closer Look at Cyber Insurance: Exploring New Coverages, Including for GDPR and Other Regulations,* 2019, Kindle Edition.

[10] **"Systemic Risk & Cyber Insurance"**, Cyber Insurance Academy, January 2023.

providers'.[11] Major cyber incidents such as NotPetya and WannaCry ransomware attacks or supply chain attacks like SolarWinds illustrate the scope and scale of vulnerabilities in cyberspace.

Organisations choose to procure cyber insurance policies as a safeguard against the fallout stemming from these vulnerabilities. However, cyber insurance serves not only as a mechanism for risk mitigation but can also encompass preventive aspects. The Organisation for Economic Co-operation and Development (OECD) highlighted the role of insurance in improving the management of cyber risk and the need for countries to consider it as an essential component for 'addressing digital security risks'.[12] As data theft grows in both frequency and magnitude, corporate liability is likely to shift to accommodate more third-party concerns.

Risk mitigation to risk prevention

As organisations increasingly rely on digitisation to conduct their operations, they tend to employ various strategies to mitigate the risks emanating from cyberspace. The role of insurance vendors or insurers becomes essential in supplementing these efforts. With the rise in the level of sophisticated cyber threats, organisations are falling behind in implementing cybersecurity measures.

According to the World Economic Forum's Global Cybersecurity Outlook 2024, there are some disturbing trends that need to be addressed. Firstly, there is a widening gap among organisations concerning cyber resilience, wherein certain entities have robust cybersecurity measures while others lack adequate preparedness.[13] Moreover, the Small and Medium Enterprises (SMEs) that make up the majority of many countries' ecosystems are being affected by this disparity. To make conditions worse, cyber-skills and talent shortages make these enterprises more susceptible to threats.

Cyber insurance can play an essential role in addressing these burgeoning issues and can serve as an external gatekeeping mechanism, bridging the oversight gap in the implementation of data security.[14] According to scholars, corporate liability coverage (cyber insurance) has the potential to generate market solutions by 'aligning incentives to implement and maintain robust cybersecurity frameworks'.[15] This means that insurers can assist organisations in implementing a robust cybersecurity framework instead of waiting to pay coverages following a cyber incident. This does not imply that such arrangements do not exist; indeed, they do. However, the role of

[11] Linda A. Lacewell as cited in H. Bryan Cunningham and Shauhin A. Talesh, "Uncle Sam Re: Improving Cyber Hygiene and Increasing Confidence in the Cyber Insurance Ecosystem Via Government Backstopping", *Connecticut Insurance Law Journal,* Vol. 28, No. 1, 2021–22, pp. 1–84.

[12] **"Enhancing the Role of Insurance in Cyber Risk Management"**, Organisation for Economic Co-operation and Development (OECD), 2017.

[13] **"Global Cybersecurity Outlook 2024: Insight Report"**, World Economic Forum (WEF), January 2024.

[14] Lauren Miller, "Cyber Insurance: An Incentive Alignment Solution to Corporate Cyber-Insecurity", *Journal of Law & Cyber Warfare,* Vol. 7, No. 2 (Fall 2019), pp. 147–182.

[15] Ibid.

insurance companies in regulating cybersecurity preparedness within organisations has yet to be thoroughly explored and examined by scholars in the field.

Moving ahead, insurers provide monetary incentives for creating robust cybersecurity systems through adjustments in premiums for cyber insurance. Policy coverage also rests on the adoption of specific security standards or meeting specified industry benchmarks as a prerequisite for coverage. This also involves periodic assessments of the insured as a requirement for the continuation or renewal of cyber insurance coverage. For this purpose, insurers are also partnering or enlisting cyber experts to conduct risk assessments.

In addition to this, insurance companies can gather data from experience to gain and share more profound insights into the factors shaping the cyber risk environment.[16] The insurance industry can also be a central repository for data related to cyber incidents that can help governments gauge the evolving threats and strategise accordingly. Given the lack of common international standards and norms, the insurance industry can also assist governments in harmonising practices across jurisdictions, as many of these providers have an international presence.

Governments are increasingly recognising the significance of these practices by insurance companies. For example, on 4 February 2021, the New York Department of Financial Services (DFS) introduced the state-wide cyber regulation called Cyber Risk Insurance Framework.[17] The stated goal is to create a framework that 'outlines best practices for managing cyber insurance risk'.[18] Despite the fact that the framework applies to authorised property/casualty insurers that write cyber insurance, it centers around seven practices that are to be employed by the insurers to manage the cyber insurance risk.

One of the practices is the thorough measurement of insured risk, driven by data and information available. The methods for gathering information include conducting surveys and interviews on topics such as corporate governance and control, access control, encryption, endpoint monitoring, and others to evaluate the cybersecurity preparedness of an organisation.[19] According to Asaf Lubin, "the circular helps to codify a certain set of industry practices and general standards" worth mimicking by other state regulators in the US.[20] Clearly, insurers can play an important role as *de facto* regulators of the companies they insure as part of risk prevention and mitigation strategy.

---

[16] Ariel E. Levite, Scott Kannry and Wyatt Hoffman, **"Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance"**, Carnegie Endowment for International Peace, 2018.

[17] **"Insurance Circular Letter No. 2 (2021)"**, The New York State Department of Financial Services, 4 February 2021.

[18] Ibid.

[19] Ibid.

[20] Asaf Lubin, "Insuring Evolving Technology", *Connecticut Insurance Law Journal,* Vol. 28, No. 1, 2021–22, pp. 130–164.

Cyber Insurance Landscape in India

According to the Indian Computer Emergency Response Team (CERT-In), the country witnessed 13,91,457 incidents in the year 2022, which included phishing, DDoS attacks, website defacements, data breaches and ransomware attacks.[21] Further, India saw a rise of 24 per cent in cybercrimes, while nearly 73 per cent of mid and large-sized organisations in the country were impacted by a ransomware attack.[22] Clearly, the situation is concerning, if not alarming, underscoring the increasing necessity for the use of cyber insurance as a risk mitigation strategy.

The first comprehensive report on India's cyber insurance landscape was by the Data Security Council of India (DSCI). The 2019 report titled *Cyber Insurance in India: Mitigating Risks Amid Changing Regulations & Uncertainties* noted that 350 cyber insurance policies were sold in the country till 2018, which was a 40 per cent increase from 2017.[23] The report was an attempt to increase awareness and initiate discussions around this evolving risk mitigation strategy. It was clear from the report that cyber insurance was at a nascent stage in terms of policy uptake and also regulations.

However, the situation changed following the onset of the pandemic. There were rise in cyber incidents and a growing number of high-profile data breaches as companies were encouraging remote working environment. Against this backdrop, in 2020, the IRDAI constituted a working group to study and examine the need for cyber liability insurance.[24] The rationale behind the formulation of the working group was to lay down a 'basic standard product structure to provide insurance cover for individuals and establishments to manage their cyber risks'.[25]

To that end, the working group was given the following tasks:[26]

- To study various statutory provisions on information and cyber security.
- To evaluate critical issues involving legal aspects of transactions in cyber space.
- To examine various types of incidents involving cyber security in the recent past and possible insurance coverage strategies for those.

[21] "Annual Report 2022", CERT-In.

[22] Mahendat Singh Manral and Jignasa Sinha, **"24% Rise in Cybercrime in 2022, 11% Surge in Economic Offences: NCRB Report"**, *The Indian Express,* 4 December 2023; Himanshi Lohchab, **"Nearly 73% of Indian Mid, Large Companies Hit by Ransomware in 2023"**, *The Economic Times,* 27 November 2023.

[23] **"Cyber Insurance in India: Mitigating Risks Amid Changing Regulations & Uncertainties"**, DSCI, 2019.

[24] **"IRDAI Sets Up Panel to Examine Need for Standard Cyber Liability Insurance Product"**, *The Economic Times*, 20 October 2020.

[25] **"**Ref:IRDAI/NL/ORD/MISC/260/10/2020**"**, IRDAI, 19 October 2020.

[26] Ibid.

- To examine the cyber liability insurance covers available in Indian market and in other developed jurisdictions.
- To recommend the scope of the cyber liability insurance covers for the present context and for the medium term.
- To explore possibility of developing standard coverages, exclusions, and optional extensions for various categories.
- Any other matter relevant to the subject.

The working group released a report covering individual cyber insurance along with a model policy wording to standardise policies across India. The report on personal cyber insurance provided the definition of cyber insurance, along with details on the salient features of individual cyber insurance cover. It also identified the gaps in the existing covers, followed by recommendations for improvements. To raise awareness regarding the individual cyber insurance covers, the document advocated for measures including awareness campaigns, easing policy wordings, etc. The model policy wording document consisted of detailed definitions of various kinds of cyber risks along with the duties of the insured.

The other document dealing with the aforementioned terms of references was comprehensive as it gave a brief overview of the legislations and policies around the world. Acknowledging the common underwriting practices by insurers, the report recommended further assessment measures such as:

- Cyber scanning tools and reports that offer a view of potential cyber vulnerabilitites of the insured and cyber risk grading.
- Detailed security risk assessment through in-house or third-party cyber security agencies.
- Tabletop discussion with the insured to get an in-depth view from the insured.[27]

Clearly, these suggestions reflect the changing nature of insurers' practices from mere sharing financial risk to undertaking a more proactive role. Something similar was seen in the 'Cyber Risk Insurance Framework' by New York's DFS, as discussed in the previous section. Moving ahead, the report also highlighted the dire situation in Micro, Small & Medium Enterprises (MSMEs), as they are the most targeted segment because of their less sophisticated IT security infrastructure. It also noted that the lack of awareness, complex policy documents, affordability, and underwriting requirements are vital barriers to increasing cyber insurance penetration in the segment.[28]

[27] **"**Working Group to Study Cyber Liability Insurance on the Various Terms of Reference**"**, IRDAI, 30 December 2020, p. 61.

[28] Ibid., p. 66.

To address the vulnerability in the MSMEs, the working group recommended

> an ecosystem approach involving insurers, cyber risk consultants, solution providers, insure-tech companies, industry bodies, financial institutions, and digital platforms [that] can help accelerate awareness and adoption.[29]

It also advocated for cooperation between the insurance industry and technical bodies like the CERT-In and professional bodies like DSCI and others.

According to a recently published report,[30] it was noted that despite wider adoption of digitisation by Indian organisations, their digital maturity remains at the nascent stage.[31] However, India is one of the fastest-growing regions in terms of cyber insurance uptake.[32] The report also highlighted that despite the majority of respondents showing a willingness to increase spending on securing digital infrastructure, the allocated budget remains smaller in proportion to their turnover. Interestingly, several technology players are entering the cyber insurance business, making ground for partnerships with insurance companies to offer better services to organisations.[33]

The Digital Personal Data Protection Act 2023

The enactment of The Digital Personal Data Protection Act (DPDP) 2023, which aims to regulate how entities process users' personal data, may encourage organisations to purchase cyber insurance to mitigate financial risk arising out of liabilities. A vital part of the act is Section 33, which deals with penalties. It empowers the data protection board to levy penalties on data fiduciaries in case of breaches in adhering to obligations, particularly in implementing reasonable security safeguards. The penalty may extend up to Rs 250 crore.

It is also pertinent to note the additional obligations that may come if the central government notifies any data fiduciary as Significant Data Fiduciary (Section 10). These obligations encompass several requirements such as the appointment of a data protection officer, engaging an independent data auditor, and conducting periodic data protection impact assessments along with other periodic audits. Cyber insurance can help organisations comply with the DPDP's requirements with the kind of services discussed in the previous sections.

---

[29] Ibid., p. 67.

[30] The insights are based on a Deloitte survey in which several CISOs participated to share their perspective on the importance of cybersecurity and cyber insurance as a risk mitigation strategy.

[31] **"Cyber Insurance in India: Navigating Risks and Opportunities in a Digital Economy"**, Deloitte, October 2023.

[32] Ibid.

[33] Ibid., p. 17.

Challenges and Way Forward

Despite the growth of the cyber insurance market and insurers taking proactive measures to ensure the cybersecurity preparedness of their clients, significant challenges still persist. Unlike traditional insurance, cyber risk insurance is a relatively new concept, and data related to cyber incidents are not in abundance, making it challenging for underwriters to model cyber risk. The rapid shifts in the threat landscape makes it more difficult for both insurers and insured to catch up with emerging threats. For instance, in February 2024, it was reported that a financial worker was duped into paying US$ 25 million to fraudsters using deepfake technology.[34] It would be interesting to see how the insurance industry is going to act against these AI-generated threats and what kind of coverage will cover these threats.

Another challenge, as Prof. Wolff notes, is that cyber risk "extends to and interconnects nearly every other type of risk - from crime to liability to property and casualty losses".[35] Elaborating on this further, she states

> …cyber risks will only become increasingly intertwined with the existing classes of risks…autonomous vehicles will require carriers to rethink auto insurance, and buildings furnished with internet-connected heating and cooling systems, fire sprinklers, and security cameras will change property insurance.[36]

The lack of data, coupled with the threats posed by emerging technologies, instills ambiguity among insurers, leading to reluctance to cover risks that appear to be too risky to share. This unwillingness is more profound in the case of state-sponsored cyber attacks and terrorism, often resulting in exclusion clauses that specifically exclude coverage for losses stemming from such acts. Payments for cyber extortion, particularly ransomware, pose a contentious dilemma for organisations. On one hand, paying ransom can facilitate the recovery of data. However, on the other hand, it also effectively contributes to fueling a criminal ecosystem, potential incentivising perpetrators to carry out similar attacks in the future.

Interestingly, according to an assessment, organisations with cyber insurance are more likely to recover encrypted data than those without such policies.[37] Elaborating on the reasons, the report highlighted that cyber insurance policies often mandate organisations to have backup systems and recovery plans as

---

[34] Heather Chen and Kathleen Magramo, **"Finance Worker Pays Out $25 Million After Video Call with Deepfake 'Chief Financial Officer'"**, *CNN,* 4 February 2024.

[35] Josephine Wolff, *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks*, no. 6, p. 217.

[36] Ibid., p. 221.

[37] **"The State of Ransomware 2023"**, Sophos, May 2023.

prerequisites for coverage.[38] Also, insurers assist ransomware victims throughout the recovery process.

Given the high stakes involved for both insurers and insured parties in the rapidly evolving landscape, scholars have advocated for government backstops to cover systemic risks. This approach can help prevent the insurance industry from facing insolvency during a crisis. The backstop can also serve to provide coverage for exclusions within policies, though it should be contingent upon the implementation of sound risk mitigation measures. Data sharing between the agencies and timely notification of a breach can also help the stakeholders respond adequately while also providing a repository of data to make informed choices. It is equally important to examine and explore cyber insurance as a vital element of overall cybersecurity preparedness.

[38] Ibid.

About the Author

Mr. Rohit Kumar Sharma is Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses