SyberGRC for Cyber Insurance

SYBER GRC

SYBER GRC

What is Cyber Insurance

- Cyber-insurance is a specialty lines insurance product intended to protect businesses, and individuals providing services for such businesses, from Internet-based risks, and more generally from risks relating to information technology infrastructure, information privacy, information governance liability, and activities related thereto.

- Risks of this nature are typically excluded from traditional commercial general liability policies or at least are not specifically defined in traditional insurance products. Coverage provided by cyber-insurance policies may include first-party coverage against losses such as data destruction, extortion, theft, hacking, and denial of service attacks; liability coverage indemnifying companies for losses to others caused, for example, by errors and omissions, failure to safeguard data, or defamation; and other benefits including regular security-audit, post-incident public relations and investigative expenses, and criminal reward funds.

Trends in Cyber Insurance Market:

The estimated losses because of Cyber related events is anywhere between $57B to $109B according to GAO (Government accountability Office)

Rate of coverage in cyber insurance policies annually by 10% - 20% YoY (year on year)

The amount of direct premium return has increased $2.1B to $3.1B

The type of industries that has started participating is: financial, healthcare, education, hospitality, manufacturing, power & utilities, retails, professional services, and communication and media.

The cyber insurance premium has goneup by 10% - 30% in last 2 to 3 yrs.

Reduced coverage and more exclusions because of the cause of events

Problem Statements for Cyber Insurance

Loss ratio of Cyber insurance premium that has gone upto 73% in last year.

- Loss ratio for any cyber insurance company has to be round 40% - 60%
- Based on the current premiums, Insurance companies are facing losses any where $**455M to $1.15B**

Reasons for higher loss ratios:

- Insurance companies model the premium on basis of historical data, which is not available in this case
- Insurance companies model the premium based on number of computers according to society of actuaries
- The above points conclude: The premium that insurance companies are charging is not proportional to the risk that they are taking on.
- Identifying precise access permission for any files in the organization

Problem statements of Cyber Insurance (cont.)

- Insurance companies calculate the premium based of probability of an event, time until a security event, discount rate based on the controls and the amount paid by the insurance companies paid on a breach:

Why Cyber Insurance Payout is more

- **Increasing take-up:** Data from a global insurance broker indicate its clients' take up rate(Proportion of existing clients electing coverage) for cyber insurance rose from 26% in 2016 to 47% in 2020
- **Price Increases**: Industry sources said higher prices have coincided with increased demand and higher insurer costs from more frequent and severe cyberattacks. In a recent survey of insurance brokers, more than half of respondents' client saw prices go up 10-30% in late 2020.
- **Lower coverage limits**: industry representatives told GAO the growing number of cyberattacks led insurers to reduces coverage limits for some industry sectors, such as healthcare and education.

Why Cyber Insurance Payout is more (cont.)

- **Cyber Specific Policies**: Insurers increasingly have offered policies specific to cyber risk, rather than including the risk in packages with other coverage. This shift reflects a desire for more clarity on what is covered and for higher cyber-specific coverage limits.
  - The cyber insurance industry faces multiple challenges; industry stakeholders have proposed options to help address these challenges.
- **Limited historical data on losses**: Without comprehensive, high quality data on cyber losses, it can be difficult to estimate potential losses from cyberattacks and price policies accordingly. Some industry participants said federal and state governments and industry could collaborate to collect and share incident data to assess risk and develop cyber insurance products.

Cyber Insurance Payout is more (Cont.)

- **Cyber Policies lack common definition**: Industry stakeholders noted that differing definition for policy terms, such as “Cyberterrorism” can lead to a lack of clarity on what is covered. They suggested that federal and state governments and the insurance industry could work collaboratively to advance common definitions

    - ***All of above points has be taken from: United States government accountability office; Report to congressional committees***

Cyber Insurance Payout is more (Cont.)

- **Higher Premiums**: After holding relatively steady in 2017 and 2018, cyber insurance premiums increased markedly in 2020. Moreover, more than half of brokers recently surveyed reported that their clients experienced a 10-30% price increase in cyber insurance premiums from the third to the fourth quarter of 2020. Only 15% of these brokers reported no change in premium price during this period.

- **Ransomware Attacks**: According to industry representatives and reports, the continually increasing frequency and severity of cyberattacks, especially ransomware attacks, have led insurers to reduce cyber coverage limits for certain riskier industry sectors, such as health care and education, and for public entities and to add specific limits on ransomware coverage.

Cyber Insurance Payout is more:

- Industry sources have noted that the increase in cyber-specific policies may reflect a desire for coverage of losses related to the confidentiality, integrity, or availability of data and systems and clarity about what is covered, which in turn may help reduce claims disputes and litigation in the event of a cyberattack. Standalone policies also provide policyholders with a greater potential for higher cyber-specific limits.

Solutions from Syber GRC for Cyber Insurance Companies

- Helping in lack of historical data:
  - We quantify the amount of data that a company holds, thereby minimizing the need of historical data to calculate the premium.
  - Instead of nos. of computers we are identifying and associating the riskiest assets and associated file permission in the organization
- We help insurance companies estimate the probability of a security event better
- We can help Cyber insurance companies to decrease their loss ratio

Product features iDPS vs. IRDAI Product Requirements

Sr. Nos.	Section	Description	Syber GRC feature
1	5.b	Identity Theft Cover – Provides protection in terms of Defense cost for claims made against insured by third / affected party due to identity theft fraud, provides expense to prosecute perpetrators and other transportation cost.	* Data scanning * Support for Multiple Indian Languages
2	5.j	Cyber Extortion Cover – Provides protection for extortion loss as a result of Cyber extortion threat and provides expense to prosecute perpetrators.	* Quantified Risk for IT Assets
3	5.k	Data Breach and Privacy Breach Cover – Provides indemnity for defence costs and damages in respect of claims lodged by a Third party against the Insured for Data Breach and or Privacy Breach.	* One Stop Visibility for all private data * Detection of Password Protected & Encrypted Files

**** Please refer IRDAI product structure for Cyber Insurance***

Feature to Feature comparison of SyberGRC Vs. Cyber Insurance according to NAIC (National Association of Insurance Commissioner)

Sr. Nos.	NAIC Requirement	Syber GRC feature
1	Identifty theft coverage	Identify PCI, PHI, and PII Data
2	Risk Based Premium	Quanitification of Risk