Cyber Insurability Index.. to measure how good are you for Cyber Insurance

Cyber Insurability is defined as **" A measure of maturity of an organization for a Cyber Insurance Company to provide a Cyber Insurance Cover".**

The perspective is from the Cyber Insurance Company which has to assess the proposed Insurer, accept an underwriting proposal and quote a premium.

Cyber Insurance proposal normally consists of two key elements. First is a cover for "Own damage" and the second is the cover against "Third Party Liability".

The own damage liability is more controllable than the third party liability which depends on whether the affected third party can successfully make a claim for damages.

If a company does not use or store the personal data of third parties, their exposure to third party liability risk is low. The risk that an Insurance company takes may therefore be dependent on the "Type of Information Asset insured".

We can roughly say for the purpose of understanding that the "Cyber Insurability of an organization which does not use, transmit or store third party liability" is high. The exact amount for which an organization is insurable may however depend on the value of assets possessed by the Company.

In an organization where Cyber Insurance is sought only for its own information assets namely the hardware, software and corporate data residing there in, the insurer's concern is limited to the efficiency of the DRP/BCP and the reputation

loss that the organization may undergo on account of an attack. For example, if there is an E Commerce website which is under DOS attack and closed for say 3 hours, then there is a loss of business for 3 hours besides a marginal reputation loss. If the DRP/BCP System of the organization is efficient, the loss can be reduced further. However, there is some ability to control the loss and contain it within a set of its existing customers.

On the other hand, if the attack involves "Loss of Data" then the question of valuing the loss becomes important. Here the presence or absence of third party data becomes very important to determine the value of the loss. If there is no third party data, the possibility of any claim from third parties is zero.

The loss of corporate data could be the business data or data which constitute "Intellectual Property". Loss of Intellectual Property can be valued and also defended subsequently by litigation. Hence it is also controllable. Loss of corporate business data may lead to reputation loss or weakening of its business competitiveness. There is an element of uncertainty of such damage but an Insurance company may consider such damage as "Discretionary" and "Vague" and reject recognizing an insurable component for "Likely reduction in market share on account of compromise of the Corporate business data".

As compared to the above, if the Insuree possesses third party personal information, any loss arising there of would create a potential litigation from a large section of the customers. The exact loss estimate becomes difficult since each person may make claim for a different amount and the claims may arise at different points of time in the post data breach scenario.

In situations where there is a regulatory authority which can step in on behalf of the data subjects and impose a fine

or collect damages on behalf of the community, it may be possible for the regulatory agency to fix some norms to determine the total liability which becomes a subject matter of Insurance. The individual liabilities also may be limited by the insuree obtaining legally binding contracts from the data subjects limiting the potential damage either to a fixed amount or to a maximum amount. In such cases the losses may be determinable. If no such contractual bindings are there, the potential loss may be open in terms of value as well as time.

The business practices that an Insuree organization follows therefore may have impact on the liabilities that the Insurer has to undertake in the event of a data breach.

This difference is what we may call as the “Cyber Insurability” of an organization.

An organization may be considered Cyber Insurable if its liabilities can be determined with some degree of certainty when a mishap occurs and not so if it is indeterminate.

Obviously, every organization will have a certain “Degree of Certainty and a degree of uncertainty” and hence we cannot measure the Cyber Insurability as a binary property.

We need to therefore develop a “Cyber Insurability Index” that measures the ease with which different organizations may be assessed for its ability to determine the insurance risk.

The Cyber Insurability Index may have two dimensions. One is the index across the other insurance subjects which measures how Company A is more easily insurable than Company B or vice versa. The other dimension is how a given company over the years moving up over a period of time on its own measure of Cyber Insurability.

May be we can call this Inter Company indexing and Intra

Company indexing.

Inter company indexing will depend on the nature of the industry, its potential to be a target for cyber attacks, its location, size, information security culture etc. This can be based on the study of the environment of threats and vulnerabilities affecting a given type of activity. This may be done as an industry level analysis even without a specific study of a company.

For example, from the Cyber Crime studies released by most companies, it emerges that BFSI industry has higher risk in terms of insurance claims and also a high possibility of indeterminable losses that may be claimed by the clients of the company in the even of a data breach.

Intra Company indexing may indicate how the company is improving or declining in its standard of bringing in some kind of control on the potential loss that may occur on account of a breach. This will include information security measures undertaken by the company from year to year, the changes in the industry environment, emergence of new technology in the industry etc. This will be a subject matter to be determined by a "Cyber Insurability Audit" of a company.

When a company is first audited for the Intra Company Cyber Insurance Index, the audit can try to measure the changes that has occurred in the last one year that contributes to making the Insurance liability more determinable and show the current status as an indication of progress or deterioration over a period of one year. This would be a good indicator to be incorporated in the annual report of a company.

For example, if I say the CII-Intra of Company X is 120, it means that there was a 20% improvement in the status (an indication of how much more the company is palatable to an

insurance company) in the last one year. If I say the CC-Intra for Company Y is 70, it may mean that the uncertainties in the company from the point of view of a Cyber Insurance Company has increased.

Each subsequent year the index can be re worked with a reference to the base year.

These are some of my preliminary thoughts that I place before the audience for a feedback and further refinement.

Naavi

Also published at www.naavi.org