CCAI India Privacy Summit 2017 at Bangalore… and Cyber Insurance

A high profile Privacy Summit had been organized at Taj West End by CCAI (Corporate Counsel Association of India) along with IAPP in which several issues of Privacy were discussed in the emerging technology environment.

The undersigned participating in one of the sessions on presented his views on the relationship between Cyber Security and Cyber Insurance.

A Summary of thoughts presented in this connection are reproduced here:

Cyber Insurance has two parts namely the First Party Coverage and Third party coverage.

The first party coverage refers to the costs incurred by the insured after a breach on invoking DRP/BCP, Payment of Regulatory Fines, Cost of audit and assessment of the breach, forensic investigation of the breach, litigation, ransom payments data breach notification cost etc. These are all costs incurred by the Company for which reimbursement is sought.

The third party coverage refers to the loss suffered by customers (including public) arising out of the breach at the insured facilities. This depends on the claims made by the outsiders. Consequent to the recent Privacy judgement, it is expected that the litigation in this domain may increase and as a result even the cost of cost of cyber insurance may also increase.

Cyber Security Risk Management includes four elements namely

Mitigation, Avoidance, Absorption and Transfer (Insurance). While Mitigation is the responsibility of the IS team, Avoidance is a business decision and Absorption is a management decision. Risk Transfer through Cyber Insurance is a decision in which all the stake holders namely the Information Security, Business and Management should all take together.

In many companies, the decision on Cyber Insurance may be taken at the CFO level as a budgetary provision.

Ideally, Cyber Security personnel should be involved both at the time of taking of a Cyber Insurance policy as well as at the time when Claim is preferred.

When a Claim is preferred the Insurance Company will naturally contest to say

-Breach was caused out of negligence

-Breach was caused by insiders or other reasons not covered under the policy

-Breach occurred long time back and was not detected in time and was not plugged in time to reduce the damage

-At the time of taking the policy, the risk was known and not disclosed.

-Coverage is limited to part of the loss only, because the insured is a co-insurer in part because the assets were undervalued at the time of underwriting

–Policy has sub limits and hence not payable in full, etc.

No Insurance company will be/can be magnanimous as to say…I will ignore all your follies and pay whatever you ask.

At the same time, the Company needs to defend

-It was not negligent

-Root cause of loss is within the risks covered

-Assets are fully valued at the time of the underwriting

-Breach was detected in time and acted upon

-Reasonable action is taken to legally defend the claims against the company and pursue claims against the persons causing the breach, So that Insurance company can step into the shoes of the insurer and pursue its claim against the end beneficiaries of the breach etc.

Company has to all provide evidence that reasonable Security practice is in existence today, yesterday and through out the life of the policy.

All this can be done only by the Information Security team and not by the CFO. It is for this reason that the Information Security team should be at the center of a decision on Cyber Insurance all the time.

There are some challenges in the Cyber Insurance including lack of adequate metrix to measure the security posture of an organization so that a “Risk based Premium” is determined beyond the usual claims of “I am ISO 27001/PCI-DSS compliant” etc.

Challenges are also noticed since normally it takes a time for breaches to be identified and addressed.

It is also not easy for the Information Security professionals to clearly understand the different limitations in the Cyber Insurance contract and since Insurance contracts are contracts of “Utmost Faith” and can be voided by the Insurance company if it can prove that the insured had not shared all relevant information at the time of making his proposal. It is also a challenge to value the assets insured so that the Insurance Company does not limit the claims on the grounds of “Under valuation of Assets”.

As regards the response to a breach when identified, a Company needs to have a clear policy based on the obligations under the Cyber Insurance contract to decide if the breach has to be reported (even when there is no claim preferred) and for all the actions required to be taken such as filing of a Police Complaint, conducting internal forensic assessment, etc.

It is also necessary for the Company to avoid mis-communication to the public and press which can cause more harm to the reputation of the company and increase the losses under claim.

In view of the complications involved in a Cyber Insurance Contract and the high stakes involved, there is therefore a need to obtain appropriate consultation from experts before a Cyber Insurance contract is purchased by an entity.

During the discussions the difficulty of the Insurance companies to assess the Cyber Risk and link it to the Premium was also discussed due to lack of information on cyber crimes in general. The Insurance companies are therefore forced to base their premium fixation on the cost of re-insurance. This has prevented the Cyber Insurance companies from providing appropriate credit to the security measures taken by the insured to reduce the Cyber Risks and more effort is required in this direction so that investments made on Cyber Security should reduce the cost of insurance at least to some extent.

Naavi