WannaCry creates awareness of Cyber Insurance

The recent ransom ware attacks with Wanna Cry have woken up the Indian corporate sector to the needs of having Cyber Insurance as a means of recovering the losses arising out of such attacks.

I refer to the **article in Economic Times today** where several industry executives have been quoted with there views on Cyber Insurance.

As readers here are aware, we conducted an all India survey two years back to document the awareness of Cyber Insurance amongst the CISOs and CIOs in India and found that most of them had very little understanding of the nuances of what constitutes Cyber Insurance.

Most CISOs do accept that "Transfer of Risks" is one of the four methods by which risks are managed (Mitigation, avoidance and absorption being the other three). But in most practical situations it is the CFOs who take decision son buying Cyber Insurance policies the risks to be covered, the financial limits to be accepted etc and CISOs are hardly allowed to link the Cyber Insurance needs of a company to the "Risk Mitigation efforts".

Though RBI had mandated that banks should take Cyber Insurance against hacking, denial of service etc ., way back in June 2001, hardly any Bank obtained such insurance until the last few years.

Companies started looking at insurance after their data vendor business partners in USA and EU started getting concerned from the liabilities that could arise by breaches that may occur in outsourced operations and made it part of their business contracts.

Now the ransomware attacks have brought an urgent need for cover as a part of the Corporate Governance policy.

The ransomware attacks create two kinds of liabilities namely

a) Cost of recovery of data and managing the reputation management

b) Actual payment of Ransom

In most cases of WannaCry demands, the actual ransom was upto 3 Bitcoins which was about Rs 4-5 lakhs and it often was less than the minimum self liability in most of the cases. Hence it was not considered as a coverage.

But in principle, ransom payment could be a claim under the policy and we need to understand if this is covered under insurance. We are aware that in another incident of ransom demand on Wipro, there is a demand of ransom upto Rs 500 crores and hence the possibility of ransom demand becoming a real liability is high.

It is understood that some Insurance companies provide specific coverage of ransom payments under an extension of the basic policy.

It is of course debatable if ransom payments should be covered under an “Insurance” since it is an “Illegal payment”. By covering the ransom payment as a genuine business expense, Insurers would be actually providing an incentive for companies to be less vigilant to take security measures and also encourage criminals by making it easier for the victims to pay ransom.

We have also pointed out that there are many challenges in Cyber Insurance including the “Zero day Vulnerabilities”, the “Delay between identification of a vulnerability and its patching up” and the general apathy of companies to subordinate security measures to profitability etc.

The “Uberrimaei Fidei” (utmost faith) nature of Cyber Insurance contracts make it very difficult for the insured to really consider insurance policy as an adequate risk cover since they will be always at the mercy of the insurance companies at the time of a claim settlement.

We have therefore recommended that we need to take a cue from China which has converted the Insurance from a “Contract of Utmost faith” to a “Contract of honest disclosure”.

This is in the hands of IRDA which needs to consider Cyber insurance as a separate category of insurance and not club it with other forms of general insurance and then apply the principle of “Contract of honest disclosure” to these policies.

Today the insurance terms are dictated only by the reinsurance writers and hence IRDA needs to work with re-insurers to structure the Cyber Insurance policies in a manner that it will actually be considered useful to the insurer when the Cyber attack materializes.

The user industry needs to come together and form their own consortium to guide and if necessary lobby with the IRDA for a better structuring of Cyber Insurance plans which is acceptable both to the insurers and the insured.

Naavi