Naavi's Mission- Cyber Insurance

This is a reproduction of an article published on www.naavi.org on July 7, 2015

There is an enthusiasm around India with the declaration of the Digital India project by our Prime Minister. The fact that more than Rs 450,000 crores of funds have been pledged by the Indian industry is an indication that the project will make substantial progress in the coming days.

We wholeheartedly welcome this initiative.

Cyber Security Initiative and Security of the Netizens

At the same time we also welcome the initiative of the Prime Minister in Cyber Security and the call he has made to the industry to make India a significant global player in Cyber Security.

We however believe that while Cyber Security efforts need to continue at the industry level, the common Netizens cannot be used as guniea pigs for introducing technology for the benefit of the industry without proper assessment of the security implications. We are aware that 100% security in Information security domain is impossible since technology is always evolving and even Microsoft does not know the vulnerabilities in its OS before it is exploited by the criminals. Many times vulnerabilities are deliberately allowed to exist to sever state interests. Under these circumstances, Netizens live in the constant fear of Cyber threats to themselves, their financial assets as well as their reputation.

As long as use of ICT was voluntary, it was possible to live with certain risks since those who donot want the risk exposure could have alternate means of living. But gradually,

the scenario is changing. Options to the public to opt out of the use of ICT are shrinking. They are already forced to use technology in Banking. Today Flipkart has announced its desire to turn into completely being “App-Based”. This is a development which indicates that in future all kinds of services starting with commercial services and later the other services will be available only through technology tools even more modern than the computers themselves. There is already an indication that without “Aadhar” certain services of the Government may become difficult to access. Afterall Aadhar it the ultimate form of digital world since it establishes the very identity of a person and if it becomes critical for certain services, its absence in the case of any cyber attack could mean “Digital Death” to the Netizen.

In this scenario of every Citizen of India being forced to adopt to technology, a time has come for them to demand that they should be protected from the technology risks that the Digital India initiative will force upon them.

Just as Mr Modi spoke of “Social Security” through insurance schemes, there is a need for “Digital Security” through “Cyber Insurance for All”.

Naavi.org launches its Mission-Cyber Insurance with the avowed objective of making the public aware of what Cyber Insurance as a concept is and how it needs to be promoted in India.

Scope of Cyber Insurance

As a beginning, let us establish the scope of the term “Cyber Insurance” and later we shall go into its different dimensions.

“Cyber Insurance” is a term which we may use anonymously with “Cyber Crime Insurance”. In effect it means that if an IT asset owner suffers any loss on account of a Cyber Crime he should be compensated. What the public call a “Cyber Crime” is normally attributed by Information Security professionals as

“Security Breach Incidents”. Hence the term Cyber Insurance can be applied to situations where a loss occurs on account of a “Security Breach Incident”.

There are a few instances where a “Security Breach Incident” may not be “Cyber Crime” either because the law has not recognized it as a Crime or because the breach is only a contractual commitment between two entities. We can therefore say that all Cyber Crimes are Security breach Incidents but not all Cyber breach incidents are Cyber Crimes.

Cyber Insurance therefore encompasses Cyber Crime Insurance and we can therefore use it both in relation to security breaches and cyber crimes under law.

Cyber Crime requires an act that is defined as an offence in a law such as Information Technology Act 2000 or any other law. For certain offences to be recognized, there has to be a “malicious intention” in addition to an act. Acts committed without malicious intention though negligently may constitute a lower level of Cyber Crime leading to Civil compensations but not to imprisonment.

From the Cyber Insurance aspect, there is a need for a “Financial Loss” which can be reimbursed by an Insurance policy. Hence Cyber Frauds such as Bank frauds are directly the subject matter of Cyber Insurance as far as the individuals are concerned.

As regards Companies they suffer loss some times because they pay compensation to their clients because of a cyber crime. Typically, when a Bank pays compensation to its customer for a Phishing fraud in which some fraudster has walked away with the money, they are entitled to claim insurance.

We must understand that Insurance is not an incentive for some body to act negligently because there is some body to pick up the claim. The insurance is a concept where the core business entity is not left to chase the cause of the loss at the

expense of its business when it has acted diligently but has faced a criminal attack. The insurer in that case provides him the compensation so that the business entity can carry on its normal business activities where as the Insurance company either pursues its options against the real criminals or absorbs the loss from its profits.

The insurance claims made by the Companies are often an aggregation of the losses suffered by the members of public. This is particularly true of the data breach related insurance claims. In such cases the insurance companies either pay compensation directly to the individuals against their individual policies or the company pays them and recovers the loss through its insurance policy.

Hence Cyber Insurance for individuals and Cyber Insurance for Companies is closely related.

If individuals donot suffer any loss, they can neither recover it from an intermediary company nor the insurance company. If the Intermediary company has not reimbursed its customers any loss, they cannot recover any insurance claim for themselves.

The Challenges

There are many challenges in writing a Cyber Insurance policy and the industry needs to resolve them before Cyber Insurance can be made available to the masses. The Governmental intervention is required for resolving this purpose since there are too many conflicting interests at play.

The Companies would not like to incur the cost of insurance if they could avoid it. But they want information security so that the probability of cyber attacks and resultant loss is reduced. But Information security also has a cost and there has to be a trade off between potential loss if not secured vs reduced loss with good security and insurance coverage.

But today it is not easy to estimate what is the “Potential

Loss” arising out of an operation since threats are dynamic, vulnerabilities are difficult to identify and the business impact of a risk is difficult to be quantified. Hence the industry struggles to identify the number of cyber crimes or data breach incidents that can be forecast during the next say year, what could be loss on the company given a specific security initiative that the company has taken etc. Cyber Crime data therefore becomes a key to this actuarial evaluation of the probability of loss.

Similarly, it is not easy to assign a value to the information security efforts taken by a Company and its potential to reduce the potential loss from say a level of X rupees to Y rupees. Metrics has to be developed for measuring the maturity level of companies in information security implementation.

If we know what is the extent of risk then we can attempt to determine what is the premium to be charged. But to determine the premium there has to be a base of a rate of premium and the value of the asset insured.

Measuring the value of data assets is again a complicated and to some extent arbitrary exercise and it is difficult for the insured and the insurer to come into a common understanding. The same problem persists when there is claim and we need to assess the loss.

Valuation of an asset and premium fixation is therefore areas of concern for the industry where professionals need to step in and provide clarity.

Liability Based Policies

One of the strategies that insurance companies adopt to overcome the uncertainty in valuation of asset insured and the loss probabilities is to define the nature of incidents under which insurance can be claimed subject to certain limits in financial value. One example is that the insurance may cover loss of third party data subject to a total compensation of 25

lakhs per incident and a maximum of 50 lakhs in an year. In this situation, we may not define what was the value of the asset insured. Premium can be fixed based on the number of data elements that could potentially be lost or some other criteria such as a lumpsum based on the turnover of the company.

Asset Replacement Insurance

Compared to Liability insurance, the other type of Cyber Insurance can be providing for replacement of lost asset. This could in a simple case be a theft and general insurance type policy as far as the hardware is concerned. But if a company has a large part of its assets in the form of software and applications, it becomes necessary to assign a value to them for both determining the value of the policy and the claim.

The asset replacement policies have an additional issue about the right valuation of insurable asset. It is a general principle of insurance that an asset which is undervalued for the purpose of insurance is considered to be co-insured by the insured to the extent of the understatement of value. Overvaluation of course can be considered as an attempt t cheat.

Uberrimae Fidei Nature

Yet another related general principle of insurance that the industry should always remember is that all Insurance contracts are considered to be “Contracts of Utmost Faith” (Uberrimae Fedei principle). This means that it is for the insured to declare what all information is relevant to the insurer to write a contract and if any information is held back, it can be a ground for rejection of claim even if premium has been paid.

It is because of this protection that the insurance agents often aggressively promote insurance even with a suggestion that some information need not be provided since the premium

may be increased because of it. Declaring the right value of the asset and whether the company is exposed to extraordinary risks etc are therefore issues that can affect the claims when they arise and there has to be neither misrepresentation nor suppression of facts.

However, threat assessment and risk profiling being fundamentally uncertain, it can always be argued that the insured suppressed facts and the insurance company may reject claims. Hence the insured should always keep appropriate documentation of what is their known risk profile at the time of writing of an insurance contract and get a sign off from the Insurance company.

Role of Legal Compliance

One more fundamental principle of insurance is that once a claim is settled, the Insurance company steps into the shoes of the insured and has the right to pursue recovery from the fraud beneficiaries. To satisfy this need, the insured should protect the legal interest of the insurance company by preserving evidence that they may require to pursue their recovery. Failure to do so may be a ground for rejection of the claim itself. It is therefore necessary for the insured to do whatever is required under law in terms of information security or evidence preservation. Hence legal compliance becomes an essential responsibility of all insured companies. In India this may translate into ITA 2008 compliance as a mandatory requirement for all insured companies.

Role of Certified Information Security Audits

Yet another common insurance principle is that the insured should in protecting the insured asset, act as if there was no insurance. This means that the security measures taken or any omission thereof could be a consideration for acceptance of rejection of a claim. In this context what are best information security practices to be followed, whether

Certified audits such as ISO 27001 will be considered necessary, whether ISO framework is better or COBIT framework is better? are issues that the insured is confronted with. Probably the best way is for the insured and the insurer to agree upon the best practices to be followed in terms of information security rather than adopting any certification formats blindly.

What we Expect the Government to do

Considering the need to implement the Digital India project in the next 3-4 years, Government should immediately set up a Cyber Insurance Advisory Board to assist IRDA in formulating appropriate policies for providing cyber insurance cover both for individuals and companies. Need for a separate advisory board other than IRDA is felt because the Cyber Insurance industry has the potential to influence information security standards and has to coordinate with the Information Security certification bodies, several regulatory agencies such as the RBI, SEBI,In-CERT etc and need a high level of technical expertise besides a knowledge of the insurance industry.

What You Can do

As a part of this Mission-Cyber Insurance, Naavi is undertaking a Cyber Insurance study along with some of his professional friends in the Information Security community and invite all the visitors of this site to participate. The survey would go online in a couple of days through this site. While answering the survey questions, some of the concepts discussed here should be relevant. Findings of the survey will be conveyed directly to the CEO of Digital India namely Prime Minister Modi.

The objective of the Mission-Cyber Insurance is to ensure that Netizens of India are provided adequate Digital Security before being dumped into the Digital India of the future. For this purpose every one of us should be aware of the potential

of Cyber Insurance and we should demand the Government and the regulators to provide us security before forcing us to adopt to new risks.

Just as before a Car is put on road, it should be covered with third party risk insurance, before any digital service is put before us, we should be provided with an option to cover the risks. Cyber Insurance for All should therefore be the motto that we should persuade the Government to work with along with the implementation of the Digital India project.

Let’s us make our voice heard…by participating in the survey and passing on our valuable feedback to the Industry and the Government.

Naavi

(P.S: The Cyber Insurance Survey 2015 referred to here is closing by the end of September 2015. Refer to naavi.org for more information on the survey.)