After Cyber Extortion.. What to do?

Here is an interesting article on how a Company should respond after a Cyber Extortion demand.

How to Deal With Cyber Extortion – Before and After It Occurs

Once a company or individual becomes a victim of cyber extortion, the number of good options dwindles quickly. Rather than react after the fact, corporate leaders need to have a response plan in place so mitigating the risk of cyber extortion schemes can be the main focus.

The author of this article suggests a comprehensive plan that should include

- A list of stakeholders to be informed.
- Predetermined and defined lines of communication that will speed information sharing.
- Appropriately trained and informed leaders empowered to make decisions during an incident.
- A process for the continuous updating of information technology systems and security policies (at least quarterly) to keep pace with changes in business and technology.
- Established relationships with law enforcement (local, state and/or federal) to reduce the chance of a slow, confused response.
- **Prevention**Companies can also take a number of steps to lessen the likelihood that they will fall victim to cyber extortion or extortion:
    - Identify all potential internal and external threats by:
        - Monitoring social media.
        - Staying on top of public forums related to

your business.
    - Identifying employees who may want to harm your company.
- Audit computer networks to identify and assess vulnerabilities. Questions include:
    - Are software patches being applied in a timely fashion?
    - Does the network have segmentation so that an attack in one area won't impact others?
    - Are there access controls in place for your data?
    - Are network logs collecting sufficient detail and maintained for a long enough period of time to allow for proper historical investigation?
    - Do you know where all your endpoints are and are network topology maps up to date? This especially is important because networks are dynamic, with companies continually adding and removing servers and distributing new devices to employees.

Refer here for the detailed article: Source Cyber Security Today

---

Cyber Extortion Case.. If the Company had a Cyber Insurance…

*(This debate is related to the case of Cyber Extortion booked in Hyderabad as reported **here by TOI**. In order to*

debate the academic issues involved in a Cyber Insurance contract, we are trying to discuss some of the issues involved, starting with what the Company should do now and how the incident is likely to roll out in different dimensions, assuming that there was a Cyber Insurance cover taken by the company. The discussion is hypothetical and for education purpose only.)

The incident came to light when the MD of the company tried to log in to the Company's data base and was confronted with a message "Pay US$1000 to get your data back and do the payment in Bitcoins".

No information is available on whether a bitcoin wallet number was provided or any communication address was provided.

(P.S: It is possible that the extortionist may send another message in which the details of payment destination may be provided, which will be an opportunity to trace the offender. Now that the issue has got into public knowledge, we anticipate that the offender will simply walk off and will not pursue the extortion. It cannot be ruled out that the extortionist could be an insider and may not risk being identified if the extortion attempt is continued.)

The MD would most likely call the CISO over phone and inform him of his inability to access the account. This then becomes an "Incident" which has to be recorded (Action 1) in the incident management register and tracked to conclusion. This would be a requirement under the Cyber Insurance contract.

Simultaneously, the Cyber Insurer needs to be informed (Action 2) of the incident though the full implications of the incident are not known at present and would be known only after an internal assessment.(Action 3).

Reporting to the Police (Action 4) could be one of the requirements of the Cyber Insurance policy itself. Even otherwise it is a duty of the company since there is an

apparent commission of a cognizable offence under ITA 2008 (section 66) as well as under IPC.

There is one issue however in this case. Once the complaint is filed with the Police, they need to investigate and the investigation has to start with the company's assets only. The internal evaluation also has to be done simultaneously on the same assets. Even the Cyber Insurance Company may poke its nose and say that they will appoint a forensic consultant to give a report. The three agencies all of whom have a stake in the investigation has to therefore come to an agreement on how to proceed with further investigation. This would be the first major task (Action 5) which the CEO need to undertake so that evidence is not lost by negligent handling of the investigation.

Since the issue has become a law enforcement responsibility, any tampering with the evidence from here afterwords could become an offence of its own as "Tampering of Evidence" and hence there has to be a clear understanding between the law enforcement and the company in this regard.

The next task for the CEO is to review (Action 6) the Cyber Insurance policy to find out if the incident is covered under the policy.

Simultaneously the CISO can find out (Action 7) and report (Action 8) if the inability to access the company's data base is restricted to one user or to many and also if there is any data back up from which the data can be restored.

> *(P.S: If a data back up is available, CISO need not rush to back up the data before tying to find out the vulnerability that caused the breach since the data may again be encrypted and if the hacker has gained privileged access to critical data, he may do further damage. How the data back up needs to be done is dependent on the BCP of the Company. If the data only relates to corporate information and not personal*

or sensitive personal information of customers. Since this is an ice cream manufacturing company, possibility of such customer data having been compromised may be less).

The next action point is for the CISO and his Cyber Forensic team and I hope such professionals will start adding their views to this debate on where the investigation has to start…

… To Be continued…

Naavi

Cyber Extortion.. How will Cyber Insurance parties look at it?

Today, Times of India has reported a Cyber Extortion attack on the Managing Director of a Company in Hyderabad. Typically in such cases, the data of the Company is hacked and encrypted. The authorized persons who try to access would be confronted with a message to pay a ransom for getting the decryption password. In this particular case, the ransom amount demanded is $1000/-

Refer TOI report here

Let us pick up this case as a hypothetical case study by assuming that this Company had obtained Cyber Crime Insurance. We shall then discuss some of the possible developments.

I request readers to send their views on "If you are the MD who is the victim of the Hyderabad incident, and your company

has a Cyber Insurance policy, what would you do now”

(…To Be continued)

Naavi

“Why am I not in this business still?”

Cyber Insurance is a term which is not found in the The Insurance Act 1938 which governs the Insurance industry in India. The Act defines besides “Life Insurance”, “General Insurance” services such as “Fire Insurance”, “Marine Insurance” and “Miscellaneous Insurance” .

Cyber Insurance is a business which comes under “Miscellaneous Insurance” which also covers “Motor Insurance”, “Burglary Insurance”, “Employee Fraud Insurance”, “Fidelity Insurance” etc.

While Life Insurance, Marine Insurance, Fire Insurance and also Motor Insurance are well developed parts of Insurance business where there is a huge actuarial data, Cyber Insurance is a relatively new form of Insurance in which there is little experience available in the industry. Out of the 28 licensed Insurance companies operating in India, hardly 5 or 6 companies offer Cyber Insurance.

At a time when the business systems in the country are adopting e-commerce in a big way and companies are building

data assets with huge investments, there is a general feeling that there must be a good demand for insuring such assets from losses. Hence the business prospect for Cyber Insurance should be very attractive.

However, when we try to quantify the business prospects for Cyber Insurance, there is lot of uncertainty. First of all the demand for Cyber Insurance comes from the fear of loss which is related to

a) Loss of data through technological failures in a Company

b) Loss of data through frauds and cyber crimes in a Company

c) Loss arising due to third party claims following a data loss from an intermediary company.

The Cyber Insurance policy will have to be structured either for these specific losses or as a comprehensive policy including all causes.

The second factor that impacts the Cyber Insurance business is the value of assets building up in the hands of the users. If we ignore the asset build up in the form of hardware which can be covered under other conventional policies we need to look at the value of “Data” as an “Asset”.

Any technology person will vouch for the fact that the quantity of data building up in the society has increased many folds during the last two years. The “Big Data” industry says that between 2009 to 2020, the quantity of data being produced would grow by around 44 times.

The growth is so large that in order to measure data, we are trying to familiarize ourselves with new units of measurement beyond Gigabytes, to Terra bytes, Peta Bytes, exa bytes, Zetta bytes and so on.

Whatever be the value of data, the sheer volume presents a growth picture that is mouth watering for any businessman.

The value of a unit of data itself is not remaining static. Perhaps it is also increasing. Nearly 70% of the data is being created by individuals and most of it is handed over to companies for use, value addition and safe custody.

With laws such as HIPAA, GLBA, Data Protection Act, ITA 2008 etc, the intermediaries are required to protect the data and ensure protection of privacy rights of individuals. With increasing awareness of such laws and better enforcement, the liability that a company has to bear on account of third party data loss is also exponentially increasing.

Of course the cost of data produced within the company is also growing with increased cost of production due to increasing manpower costs and real estate cost.

With such developments, the value of data as an asset representing "Prospective Insurable Assets" is growing at an unimaginable rate. We can therefore expect that the gross market for insurance business will grow at 200% to 300% per annum for the next several years.

The last factor that determines the market for Cyber Insurance is the rate of premium. This is one area where we can see a reduction as the market matures and competition grows. However increasing levels of Cyber Crimes may tend to keep the rate from falling alarmingly and any way the crazy growth in the volume of data assets will ensure that the gross premium potential will be growing in tandem with the data volume growth.

In this background, any shrewd business entity would consider that Cyber Insurance is a gold mine ready to be harnessed. There is no need to look for quantification of the demand which is much more than any individual company can handle.

For records sake however, we may recall a recent study released by PWC titled "Insurance 2020 and beyond-Reaping the dividends of Cyber Resilience" which puts the Cyber Insurance

market based on premium at around $ 2.5 billion today and set to grow to around $.7.5 billion by 2020.

It is difficult to cull out the statistics for India separately, but considering that the nation is looking at "Digital India" project with Smart cities, increased e-Governance, etc, the growth prospect in India could be higher than the average global figure represented by the PWC study.

According to the PWC study,

> "some 90% of cyber insurance is purchased by US companies, underlining the size of the opportunities for further market expansion worldwide.
>
> In the UK, for example, only 2% of companies have standalone cyber insurance.
>
> Even in the more penetrated US market, only around a third of companies have some form of cyber coverage.
>
> There is also a wide variation in take-up by industry, with only 5% of manufacturing companies in the US holding standalone cyber insurance, compared to around 50% in the healthcare, technology and retail sectors"

It is difficult to see many other business opportunities where the growth prospect is of this order.

So, if you are already in Insurance business but not in Cyber Insurance it is time to ask yourself "Why am I not in this business still?"

If you are little more adventurist, but not in the Insurance industry at present, it is time to think of entering this specialized field where competition is low but prospects are mind boggling.

Let's explore more on this in subsequent articles..

Naavi

Open Letter To Mr Modi on Cyber Insurance

18th September 2015

To

Sri Narendra Modi , Honourable Prime Minister, Government of India

Sub: "Cyber Insurance For All Netizens of India

Dear Sir,

One of the distinguishing features of the Governance model adopted by your Government is its reliance on technology. **"Smart Governance through E-Governance"** is the recognizable face of this Government.

In pursuance of this policy, you have adopted the "Aadhar" as the core citizen identity and linking every welfare programs of the Government to this e-identity of the Citizens. In a way you are converting every Citizen to a Netizen. With the ambitious projects such as "Smart Cities" and "Digital India" in the anvil, the dependence of the society on technology is only going to increase.

I am fully in support of this push for using of technology for development and have been advocating such a policy for a long

time as documented at www.naavi.org. I had also advocated a "Charter of Demand for Netizens" which included several initiatives including "Digital ID for all Citizens of India" and "E Consumer Protection". I request you to kindly take some time to look into these suggestions.

I firmly believe that success or failure of your Government will be hugely influenced by the success or failure of the E-Governance model which you are adopting and hence no stones should be left unturned to make it a success.

However, I always keep recalling how Mr Chandrababu Naidu lost an election despite his many good E-Governance measures in Andhra Pradesh and this should be remembered as a lesson for people like you who want to do good things but the society may not be fully ready for absorbing the long term thoughts.

Cyber space has its fair share of risks and any society dependent on Cyber technology is open to the adverse effects of cyber attacks from cyber criminals, cyber terrorists and Cyber war capable nations.

It is therefore a certainty that such cyber attacks will have to be faced by the society from time to time. Measures to prevent an adverse fall out therefore should be considered as inevitable.

We know that Cyber risks are an essential evil that has to be endured with, but politicians in the opposition will easily use any adverse attack as a consequence of "Anti People Policies" of the Government.

For example, in case there is a Cyber attack on the Indian Banking system and 10000 customers lose their money in their JanDhan accounts, opposition will say that it is a scam and all the money has been misused by BJP politicians. In a charged atmosphere that may follow, the perception battle is more likely to be won by the opposition than the Government.

If therefore your Government needs to insulate itself from the risks of being blamed for Cyber risks, you need to go an extra mile to ensure that citizens don't lose out of cyber attacks.

In this context, I suggest that there is a need for a policy of **"Cyber Insurance for All"** as a means of protecting the Netizens from the vagaries of Cyber risks.

"Cyber Insurance" is a protection against financial losses arising out of cyber crimes such as "Phishing", "Identity Theft", "Denial of Services", "Hacking" etc. It includes frauds involving cloning of credit cards, debit cards, ATM cards, Aadhar data, etc. It includes mobile related frauds which will be one of the biggest threats of the future where a large number of victims will each lose a small amount making it impossible for them to invoke any traditional legal remedy such as approaching the Courts.

Just as "Drip Irrigation" is essential to fight the vagaries of failure of rains in the agricultural sector, "Cyber Insurance" is essential to fight the risks of cyber attacks in the Digital environment.

In the Motor Insurance area there is already a concept of Mandatory Third Party insurance. A similar policy is required in the E Commerce and E Banking area.

Of late, RBI has issued many licenses for Payment Banks and Small Banks as well as new generation Banks. These will all be heavily technology dependent and the customers will hold all the risks. Hence RBI should be persuaded to mandate that all new Banking licensees introduce mandatory Cyber Insurance for its customers.

Kindly don't be swayed by any argument that Cyber risks are not "insurable" since it is too huge a risk to be covered or that no insurance company may be interested etc. Presently, insurance companies are doing a profitable cyber insurance business but are restricting it to companies and not extending

it to individuals. They are milching the higher end of the market and are avoiding the lower end because they feel it is expensive to manage. They need to be persuaded and incentivized to provide the retail cyber insurance policies.

If the Rs 12 per year accident insurance policy for a cover of Rs 2 lakhs against accidents is commercially feasible, the individual cyber crime insurance policy that protects the individuals against any loss say to the extent of say Rs 10000/- to Rs 25000/- per incident must be also feasible.

I therefore suggest and also urge you to adopt the **"Cyber Insurance for ALL"** as a new policy of the Government to support its Digital India initiative.

Regards

Yours faithfully

Na.Vijayashankar (Naavi)

Founder: www.naavi.org

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.)

Welcome to Cyber Insurance Information Center for India

Welcome to the Cyber Insurance website meant for Indian Cyber Insurance users.

This site is maintained by Na.Vijayashankar, popularly known as Naavi, the founder of www.naavi.org.

The objective of this site is to provide information on the emerging Cyber Insurance industry in India.

In due course it is expected that Cyber Insurance seekers and Cyber Insurance providers will converge on this website for exchange of information.

Additionally, this site should be of interest to professionals who would provide different services in the domain.

Looking forward to your active cooperation.

Naavi