Cyber Insurance cover may not be available if there is "Negligence"

In the context of huge regulatory fines envisaged under GDPR, there is a renewed interest in Cyber Insurance among Data Processors everywhere. Since liability under GDPR may arise not only for payment of compensation to data owners but also for making payment of fines that may be imposed by the regulatory authorities, the companies do demand that they should be covered by some Cyber Insurance policy for any liability that comes out of processing of EU citizen's data.

As for as Indian data processors are concerned, their liability will be restricted to what is indicated in the data processing contract. Some of these contracts may be vague and not determine the exact liability or compliance responsibilities. It may make a reference to the liability that may arise on the Data Controller under GDPR and extend the liability in the form of an "Indemnity" to the associate data processor in India. Indian data processors some times assume that they would be liable directly under GDPR and rush to obtain insurance cover for large amounts. This could hurt the profitability of their operations.

If any data is compromised by an Indian data processing company then it would be as a result of a "Cyber Crime". The cause of action lies with the persons who have lost money. Most of the time however, data compromise is recorded but the actual loss may not fructify or fructify only to a small extent not commensurate with the number of data elements lost.

Hence out of the total loss, the loss arising out of "Compliance" requirements which may include sending of notices, arranging identity theft protections for all the

suspected compromised data subjects would be a huge cost even when not a single of the compromised data might result in actual loss. Similarly in such cases the regulator would impose millions of dollars fine depending on the nature of breach, the attitude shown by the data controller before and after the breach to protect the data subjects etc.

When a Cyber Insurance policy is invoked in such cases, an obvious question that would arise is whether the loss occurred more out of the negligence of the Company as a whole in implementing proper policies etc and whether the company should be protected against its own negligence. If Cyber Insurance routinely covers such breaches, then there will be no incentive for companies to improve their security.

Hence it is necessary and natural that the Cyber Insurance Company raises an objection or try to limit its liability citing that the cause of loss was "Not Insurable".

A question has therefore arisen on "Whether Regulatory Fines are Insurable at law". In this context, the article **"GDPR Fines and Cyber Insurance"**

presents some interesting thoughts as may be relevant in the Great Britain. Since India generally follows the English Law and the Insurance law has dependence on the British practices, it is presumed that the English law is also relevant for the Indian Context. Hence the points mentioned in this article are very much relevant to Indian companies both in the GDPR context as well as in other instances of fines arising out of non compliance of HIPAA, Non Compliance of ITA 2008 and even when there is a ransomware attack due to lack of proper security practices in a company.

One of the concepts discussed here is "illegality of defence" which may prevent a claimant from pursuing a civil claim based on the claimant's own illegal acts.

The dividing line however is whether there was "Illegality" on

the part of a company that caused the fine or there was merely “Negligence” in implementing the regulatory precautions.

As long as the negligence is related to “Best practice suggestions” that are made by sectoral regulatory bodies or industry practice, the cause may be contained within the concept of “negligence” unless the level of negligence is “ridiculous”. But if there is a statutory law which has been ignored then such negligence cannot be called anything other than “Illegal”.

To be more specific, if a Bank ignores RBI guideline, it may be “Negligence”. But if it ignores “ITA 2008”, then it would be “Illegal”.

Secondly what distinguishes “Negligence” from “Gross Negligence” or “Recklessness” is the precautions taken by an organization before an event occurs and also its response immediately after the occurrence of an incident.

If an organization has taken reasonable precautions which any other prudent person under similar circumstances would have undertaken but failed in some minor aspects, then the level of negligence is in the lower end. If however, there was no precaution taken or the precaution was ridiculously low, then the breach would be attributed to callous attitude and may be considered as a “Contributory Negligence” or even a “Passive Assistance” to a fraudster.

If we take the recent incident of PNB fraud and another fraud that followed at City Union Bank, it appears that the negligence at City Union Bank which allowed a compromise of its SWIFT system may fall under the category of “Negligence but Not Recklessness”. On the other hand, the PNB negligence which involved allowance of customer’s executives using the passwords of Bank officials to create their own “Sanction letters” and the sharing of passwords between multiple officers of the Bank can be called an abject complicity in the

offence itself.

Even if there was no “Mensrea” at least for some of the executives of the Bank, the “Recklessness” was attributable to all employees of PNB who were aware that SWIFT messaging system was not linked to CBS and passwords were being shared.

The Association of employees in PNB has tried to put the blame on the top management. Similarly, the employees of Mehul Chokshi firm has placed their current loss of jobs to the Mehul Chokshi led Board. But if one is honest, we all know that if a fraud of this magnitude had taken place, then several persons within Mehul Chokshi or Nirav Modi companies as well as PNB, Other lending Banks, RBI, and the Ministry of Finance must have smelt that some thing wrong was going on.

What has collectively failed in the system of “Whistle Blowing” that RBI already has in place but has completely failed to work. The complaint that one franchisee Mr Hari Prasad made to PMO is like many complaints that are forwarded to PMO and are directed to appropriate departments for enquiry.

But each of the Banks had their own Whistle blowing systems and RBI had a Whistle blowing system for the entire Banking system and it appears no body had the courage to report the possibility of such a fraud. The reason could be that the heads of each Bank involved as well as the Governor of RBI themselves were all friend of the then prevalent political system and personally appointed by Mr P.Chidambaram and hence no body trusted them to take action.

If the Whistle blowing system ensures that the whistle blower is protected, then the skeletons would have tumbled as soon as a junior Bank officer acquires a flat costing Rs 3-4 crores or throws up a fancy party in a five star hotel etc.

In all such cases therefore, the negligence is unpardonable and hence there should be no protection from Cyber Insurance.

Cyber Insurance contract being an **uberrimae fidei** contract, the Insurance company is unlikely to discuss these issues with the clients at the time the Insurance policy is bought. But if the liability is huge and the client invokes the insurance, then the legal departments in these insurance companies may certainly raise the "Illegal Defence" clause.

The principle in Insurance is always, "Take as much precautions as you would take as if there was no insurance" and there after, if the loss materializes, it is an "Accident" for which the Insurer should gladly assume liability. If one takes decisions recklessly because there is an insurance to back up, then the insurer would definitely feel cheated and raise objections at the first instance.

Naavi

Bajaj Alliance Launches Cyber Insurance policy for individuals

Bajaj Alliance Insurance has announced the launch of a Cyber Insurance Policy for individuals which could be the first such cover in India.

We have been advocating such a policy for a long time and welcome this development.

As per the **report in Economic Times**

the policy provides for coverage from Rs 1 lakh to Rs 1 crore against the risks of"financial Loss", "Defence cost", "Prosecution Cost", "IT Theft loss" Restoration cost", "loss

due to identitity theft arising out of phishing, , malware attack" etc.

Other then financial loss due to cyber, the policy is said to also provide coverage for expenses incurred on counselling services treatment, claim for damages against third party for privacy breach and data breach and transportation for attending Court summons.

This is an excellent development.

We need to still assess the policy terms in detail and the premium but the introduction of the policy is welcome.

Naavi

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

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

If China can have a PRC law, Can we not too have a similar law?..for Insurance?

Insurance is a vintage industry in India but Cyber Insurance is yet to develop in both its usage and structuring.

One of the most difficult aspects of an Insurance contract is how do we interpret the Uberrimae fedei nature of the contract and determine the limitations of expected disclosure from the proposer.

The “utmost faith” nature of the contract will leave the insured at the complete mercy of the insurer as to whether the disclosures are adequate or not which is done not at the time of accepting the contract but when a claim arises.

The Cyber Security issues are such that no IT user is fully aware of the vulnerabilities that he may be carrying. Some vulnerabilities may be zero day technical vulnerabilities which even the supplier of a hardware or software may not know. Probably some hacker’s conference some where in the world or a torrent post in the underground world could have pointed out the vulnerability and the insurer may find it out

through his post incident research. Then would it be reasonable for the insurer to rescind the contract or raise a dispute that may drag on for years in a Court of law?

Similarly let us say there are some problem employees who have caused the loss and when their background is verified by the insurer on a post incident time, he may extract some adverse observations which might have been overlooked by the insured. How reasonable it would be for the insured to then repudiate his insurance contract?

These are some of the issues that Cyber Insurers need to address. If Cyber Insurance industry need to develop, the Government also may have to take a look at what it can do to make companies more insurable or in other words, how the "Cyber Insurability Index" of a company be enhanced?

In this context, it is interesting to note that China has taken a divergent path to make Insurance contract a "contract of honest disclosure" instead of "contract of utmost faith".

According to the **information available in this article**,

The Supreme Peoples's Court (SPC) in China issued an interpretation in May 2013 on certain provisions of the "People's Republic of China Insurance Law" (PRC insurance Law) focussing mainly on the disclosure obligations of parties entering into insurance contracts and exemption clauses in those contracts.

According to these interpretation, the common law principle of "Utmost good faith" does not apply in China and is over ridden by the provisions of the PRC insurance law tha requires that the policy holder shall make an "Honest disclosure" in response to the insurer's enquiries about the insured and/or the insured subject matter. The insurer's right to rescind is also limited to a period of 30 days from the date on which it learns of the failure to disclose or if the non disclosure was known to the insurer at the time the policy was taken or he

ought to have known it if sufficient due diligence had been exercised.

IRDA needs to give a thought to similar provisions to be adopted in India so as to make Cyber Insurance popular and reach the SMEs and general public.

Naavi

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

India Cyber Insurance Survey Results To be released in

January 2016

The first ever study of the Indian Cyber Insurance Industry-2015 throwing up the perception of the industry on what they want from the Cyber Insurers is ready for being released some time in January 2016.

The study undertaken by the undersigned along with a group of IS professionals collected responses from different professionals from the industry and academia has given a good insight into what the industry perceives about the Cyber Insurance policies.

Since the industry is in a nascent stage and the experience of how the industry functions is yet to mature, the results are more representative as a “Perception” or “Expectation” study and would be available for being expanded in the coming days into a “Status of the industry study.

The survey provides interesting insights into the prospects of the industry and what the Insurance companies need to consider to strengthen their products.

Though only 6% of the respondents indicated that they have actual experience of the products, 72% said that they are willing to consider such products if a suitable product at a proper price is available. There is also an indication that if suitable product under proper price is not available, more than 54% of the respondents were not ready to jump in in the near future.

The study also provides valuable qualitative insights into what would be acceptable to the market in terms of conditionalities, exclusions, liability limitations etc.

The report is being issued in two versions. One will be a free version for public information containing the summary of the findings. The other would be a professional version with

business insights meant for the industry users which may be nominally priced.

Await for more information in due course.

Naavi

P:S: More Information

The mystery land of Cyber Insurance-1: Overcome the “All is Well syndrome”

The mystery land of Cyber Insurance-2: What is Cyber Insurance?

The Mystery Land of Cyber Insurance-3: Who should get Cyber Insurance Cover?

Cyber Insurance-4: The enigma called Cyber Insurance Premium

Data Breach Notification Policy helps Cyber Insurance Industry

Data Breach Notification Policy is a mandatory policy under certain regulations such as HIPAA/HITECH Act and is being increasingly used by different regulatory agencies.

The essence of the policy is that when a potential data breach is discovered in a Company, the data subjects whose interests are adversely affected would be informed. Some times it is required to be notified to the regulatory agency and also to

the media or placed on the website.

Obviously the companies which suffer a data breach are not happy with such a regulation since it adversely affects their reputation and future business flow. Also it will prompt litigation even in cases which would have normally not be escalating beyond a simple dissatisfaction. The Notification would therefore be like “Inviting Trouble”.

If there is a regulation that data breach notifications are mandatory, then there is no choice for the company. Cyber Insurers would look at it as a part of mandatory legal compliance.

When there is a regulation then probably the industry would have clarity on how to define a “Data Breach” for notification purpose and what procedure to be followed. But when there is no regulation, the Companies would most probably try to avoid notification.

In India where we donot have a Privacy law, the only reference to data breach notification is through the rules under Section 79 of ITA 2008 applicable to Intermediaries. Though there is a mandate under this rule, it is doubtful if it has been recognized and followed.

The Cyber Insurance Company is interested in the notification since it is a good practice and has some specific advantages.

One of the main advantages of the policy is that it instills a sense of discipline in a company for information security. Without the need to disclose the data breach, any company would be interested in brushing the problems under the carpet. If there is a policy then there will be a clear definition of how a breach can be recognized and what needs to be done if a breach is suspected.

The second most important advantage is that when smaller breaches get reported, the company would be hardening its

security before anything big hits them. It works as a circuit breaker that defuses the risks instead of allowing risks to accumulate and explode.

For this reason, I advocate that Cyber Insurance Companies need to develop their own Data Breach Notification policies and impose it on the insurers even if there is no law to mandate it.

If a Company already has adopted a Data Beach Notification policy along with a Privacy Policy and Information Security policy, the insurability of the organization actually improves and it should have a positive influence on the insurance proposition.

A Prudent Cyber Insurance Company would be not only interested in imposing a data breach notification policy but also a more comprehensive information security policy of its own to safeguard the interests of itself and the insured organization. Though some companies would prefer to adopt the ISO standards of Information security rather than suggesting anything of its own, it is preferable that the Cyber Insurance companies do suggest some minimum information security standards before considering a proposal. In such a case, the data breach notification policy is one that they should consider.

Naavi's Cyber Law Compliance Center offers a model Data Breach Notification policy that tries to address the concerns of the regulators without unduly humiliating the company reporting the potential data breach incident. The model policy can be adopted by any user industry if necessary with other associated policies.

In due course it would be necessary for regulators to develop requirements of their own which can be incorporated in such polcies. RBI, SEBI, IRDA and CERT IN are some of the regulators who should be considering mandating imposition of

such policies in the larger interest of consumers whose interest they try to protect.

Naavi

Cyber Liability Insurance..What it is?

In US it is stated that 46 of the 50 states have made Data Breach Notification mandatory. As a result when a data breach even occurs the company needs to conduct an in house audit and then send out notifications to all its customers who are likely to have been affected by the breach.

The cost of such notification itself is huge since in most cases the number of data lost runs to millions.

This data breach notification is recognized as one of the key drivers to the Cyber Insurance industry in US since these costs of data breach notification is a clear cash outgo for the company to be incurred almost immediately after a data breach comes to its knowledge.

Related Article in **Computerweekly.com**

In India, many companies are ignorant about whether there is any data breach notification obligation. Presently under Section 79 of ITA 2008, data breach incidents need to be reported to IN-CERT, though this is rarely observed and CERT-IN.

There is still however no specific obligation to notify the customers unless this is introduced as a part of the Section 79 notification on due diligence.

Recently Indian Press reported that **two companies in Mumbai suffered extortion** threats after some hackers threatened to reveal some illegal activities of the companies. This was also an incident of security breach in the company though we donot know if there was any customer information involved in the breach.

But public do not know if this was reported to IN-CERT. In fact the Press have been helping the companies to keep their identity under wraps which also means the crime is kept under wraps.

Sooner or later the situation will change and data breach notification will become mandatory in India. Companies need to be prepared therefore for meeting the liabilities both in terms of costs involved in setting things right, notifying parties and also meet third party liability claims.

It is time they start asking themselves where they stand in this respect since some of these companies are also filing declarations under clause 49 of SEBI rules on listing which is similar to SOX guidelines.

Naavi

Why Cyber Insurance seekers need to do better home work..

Naavi has been advocating that companies need to start using Cyber Insurance in India though the current level of awareness as well as the penetration is low.

In these circumstances, the news that BitPay, a Bitcoin

processor could not recover its claim for a loss of $i.8 million despite having a Cyber Insurance policy since their claim was rejected by the Insurance company is disturbing.

At the same time, the incident highlights how lot of care is required before a Cyber Insurance policy is purchased and the purchaser should be able to analyze the policy terms in detail and avoid the kind of technical interpretations that were used by the Insurance Company in this case to reject the claim.

The details of the incident as reported in networkworld.com indicate as follows.

BTC Media had obtained a "Commercial Crime Insurance Policy" for $ 1 million from MBIC which stated

> "will pay for loss of or damage to 'money,' 'securities' and 'other property' resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the 'premises' or 'banking premises': a. To a person (other than a 'messenger') outside those 'premises'; or b. To a place outside those 'premises,' "

In December 2014, the CFO of the company was spearphished the fraudster managed to get hold of his email credentials. This was used to spoof mails to the CEO and 5000 bitcoins worth $1.8 million were stolen.

The Company filed a claim under the Cyber Insurance policy which was declined for the following reason.

> "The Policy requires that the loss of money be the direct result of the use of any computer to fraudulently cause a transfer of that property from inside the premises to a person or place outside the premises. 'Direct' means without any intervening step i.e. without any intruding or diverting factor. The Computer Fraud Insuring Agreement is only triggered by situations where an unauthorized user hacks into or gains unauthorized access into your computer system

> and uses that access to fraudulently cause a transfer of Money to an outside person or place. The facts as presented do not support a direct loss since there was not a hacking or unauthorized entry into Bitpay's computer system fraudulently causing a transfer of Money. Instead, the computer system of David Bailey, Bitpay's business partner, was compromised resulting in fictitious emails being received by Bitpay. The Policy does not afford coverage for indirect losses caused by a hacking into the computer system of someone other than the insured,"

Bitpay has now sued MBIC for breach of contract, bad faith, failure to pay and statutory damages and seeking $950,000 in damages plus court fees.

The litigation is likely to go for some time and in the mean time the industry will debate whether Cyber Insurance is reliable at all.

MBIC may be technically correct where as BitPay may feel that MBIC has misrepresented and cheated. The argument could be based on the nature of contract and what is implied and what is not.

The incident highlights one of the points I have been highlighting for a long time and that is that a company obtaining Cyber Insurance Contract must be able to decypher the policy terms and map it to the risks against which it needs a coverage. Any ordinary information security professional would list "Phishing" of credentials of any authorized user as one of the threats that can manifest into a risk and result in losses. He would presume that "Cyber Crime Insurance" will cover this. But being a technical person and not able to understand the terminology used in the contract which distinguishes "Direct" and "What is not Direct" as also "What is a loss" etc., he is unable to find out what the policy is really covering or not. While the CFO or even the legal department is able to understand this part, they may not

know the anatomy of all Cyber threats. Thus neither the CFO/Legal team nor the IS team understands the nature of this “Techno Legal Contract” leading to problems of this nature.

Naavi and his group of professionals who are working on the India Cyber Insurance Survey will find out the views of the professionals in this matter and present it to the public shortly. (If you still want to participate and provide your feedback,rush to

https://fs22.formsite.com/SBYrSa/form2/index.html)

CEOs and CFOs should realize that all Cyber Insurance contracts are considered contracts of utmost faith and it is the responsibility of the proposer to disclose what risks he wants to be covered and ensure that the Insurer has not excluded the risks that he requires to be covered in the policy document. This requires the company to take the advise of a suitable consultant on his behalf other than the Insurance Company representatives and also the broker who is more inclined towards the Insurance company than the insured or is not fully conversant with all the legal nuances.

If proper care is taken then the kind of problem that BitPay is now facing should not have arisen.

Naavi

Related Articles:

networkworld.com

ibamag.com