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