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.

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