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