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