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 CEO of the company was spearphished the company's CFO and 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