Date: 2.6.2017	**Publication:** ET CIO

Cyber insurance – the missing component in enterprise security

Bangalore: A little more than two weeks ago, the massive “WannaCry” ransomware virus hit over 150 countries infecting about 200,000 to 300,000 computer devices and systems globally, as the worst nightmare for cyber security experts unfolded rendering them helpless.

In the wake of this mega attack, cyber-security and IT experts, including CIOs and CISOs across organisations and businesses world over including India have been busy working round the clock to investigate and minimise any sort of impact this virus would have on core applications, systems, and critical data.

Software patches, rigorous info security mechanisms and best practise has helped marginally in controlling the virus and its impact to an extent but the financial losses triggered by it have been estimated to the tune of billions of dollars.

In fact, US based cyber risk modelling firm Cyence have estimated the financial losses triggered by “WannaCry” virus to be around $4 billion, according to CBS News report. Though the actual ransom paid did not account for much, the financial losses in the aftermath of the attack included overall productivity loss, the fees paid for forensic probe, data retrieval services and more.

According to a research report by Allianz released in 2016, cyber incident is the third biggest global business risk and due to cyber crimes the global economy suffers financial losses of whopping $445 billion per year.

Cyber insurance a must

Given the alarming rise in cyber attacks and crimes over the recent years, experts recommend that businesses and enterprises should invest in cyber insurance as a means to reduce and mitigate the overall risks and financial losses.

“Cyber insurance is not openly spoken or discussed in terms of enterprise security and business planning mainly because there’s lack of awareness and education, but it is absolutely necessary,” says Sanchit Vir Gogia, Chief Futurist, Founder & CEO - Greyhound Knowledge Group.

Though the insurance concept is one of the oldest ways to protect and secure assets and lives, but when it comes to cyber attacks, it’s not that simple.

In fact, technology advancement, sophistication and dynamic nature of cyber attacks and crimes have turned cyber insurance into a challenging and complex form of insurance product for the insurance companies to offer in the markets.

For them, it’s a challenge to build a suitable insurance product that can cover and underwrite all the evolving threats, risks and liabilities including third party data protection.

Confusion and complexities around cyber insurance

“There prevails a major confusion between cyber risk insurance or cyber liability insurance coverage (CLIC) and the errors and omissions (E&O) insurance. In fact, our international survey found only 12 percent organisations had clarity on cyber insurance while 68 percent organisations were confused and mixing up CLIC and E&O,” informs Gogia.

According to Mukesh Kumar, HDFC ERGO’s Executive Director, typically IT companies buy E&O insurance policy for IT contracts to insure their IT projects and third party (clients) liabilities.

“However, E&O insurance policy also has some elements of cyber insurance,” says Kumar.

Globally, cyber insurance has been around for more than a decade or so, but in countries like India it is relatively new as not many insurers are offering it today. Bajaj Allianz, TATA AIG, ICICI Lombard and few others are among the general insurance companies that offer cyber insurance products in India.

“Cyber insurance is absolutely new in India. Fundamentally, cyber threats has been steadily increasing and the cost attached to breaches and cyber attacks have also gone up tremendous,” says Sasikumar Adidamu, Bajaj Allianz General Insurance’s Chief Technical Officer –Non Motor.

“Cyber insurance as product globally is just a decade old and in India it’s been around for past 3 -5 years, so it’s relatively new. There are only around 150-200 cyber insurance policies that have been sold so far as per industry estimate and most of them have been bought by the services and IT industry, but now it is expanding to sectors like healthcare as well,” adds Kumar.

Sudden buzz, but not actual buying

Ever since the “WannaCry” attack, Adidamu informs that there has been a sudden interest in cyber insurance and his company has been getting a lot of queries from businesses in India. “But not all of these queries would actually get converted into buying of the cyber insurance covers,” he points out.

“Last year there’s was this massive credit card data breach and even that time, we saw a huge interest among businesses for cyber insurance but gradually it goes down and not many companies are willing to buy or invest in cyber insurance products,” adds Adidamu.

The aftermath of “WannaCry” attack in Kumar’s view has created a buzz around cyber insurance however, there’s no credible information in terms claims and payouts. “But this attack is not a tipping point for cyber insurance,” comments Kumar.

“WannaCry” and other cyber attacks are actually wake-up calls for businesses and their CROs (chief risk officers) but experts believe they are unprepared to take up the risks that come along with those attacks.

Missing piece in the enterprise security

Ironically, most organisations investing in IT including range of cybersecurity technology and services but cyber insurance still remains elusive in the overall cybersecurity and business continuity planning (BCP). And it is not considered from risk mitigation and management perspective.

“Cyber insurance is actually a second line of defence after cybersecurity technology in organisations. Most large corporates today invest heavily in cybersecurity technology because cyber crime has become the prime concern but they lack cyber cover. Unfortunately, cyber insurance is still not seen as means to mitigate business risks and financial losses,” notes Adidamu.

Although the fact remains that organisations are low on cyber insurance, but there are certain factors and contentious issues that actually makes it less popular in the industry.

“Not many insurance companies are offering cyber insurance products due to lack of standardization in terms of underwriting of the types of risks like cyber attacks and threats, data breaches, viruses, etc., as well as third party liability in terms of data protection,” points out Gogia.

Post any cyber attack incidentsks, a comprehensive forensic investigation is required to examine and assess that particular attack, its impact and factors that triggered business losses.

“A forensic probe is an expensive exercise so who will bear its cost remains a question. Even the factors that determine business losses vary and importantly the definition of “business loss’’ remain highly ambiguous,” Gogia explains why cyber insurance is full of complexities.

In the present scenario, Gogia reckons that cyber insurance providers are struggling to come up with products that can cover all the aspect including investigation, liability, cost and insurance cover or claims.

From enterprise security perspective, there’s also a lack of coordination of CIOs / CISOs in organisations with their respective IT, legal, finance and business heads or teams that could handle situations such as cyber attacks in a better way.

Given such complex scenario particularly with the dynamic cyber and security threat landscape, cyber insurance companies need to strengthen their technology background in order keep themselves in pace with the changing time.

Strategic collaboration and partnerships

Cyber insurance providers can cope up with this dynamic scenario by working closely with technology and software security vendors through strategic partnerships and technology collaborations to stay updated with evolving vulnerabilities, viruses, hacking techniques and more.

“Insurance industry at largely has been collaborating with other industries like automobile, healthcare and other; and should collaborate with cyber security and forensic experts that would enable better underwriting of cyber insurance policies and claim processing,” notes HDFC ERGO’s Kumar.

Like in the automobile industry where motor insurance is mandatory, Kumar suggests that government in India should frame new cyber and IT laws that makes cyber insurance mandatory for companies and businesses to mitigate risks and financial losses in case of cyber attacks.

“This would bring some clarity and handshake between security vendors and insurance companies in dealing with cyber crimes,” emphasizes Kumar.

In fact, Symantec and F-Secure have formed partnerships with insurance providers in the area of cybersecurity and insurance. These vendors are offering some security solutions in the US, Europe and Nordic region which has cyber risk underwriting and liabilities addressing buyers’ need of cyber insurance policies.

For instance, Symantec has a dedicated cyber insurance partner program, which helps customers to lower the risks linked with cyber attacks and recover the financial cost of cyber attacks and incidents.

In addition, Symantec Cyber Insurance has collaborated with Guy Carpenter & Company – a global risk and reinsurance specialist; and has developed series of framework that would determine complexities of cyber attacks based on six dimensions including attackers, targets, objectives, vulnerabilities, impact and consequences.

Cyber insurance as a part of cyber security plan

According to Jani Kallio, F-Secure’s Director, Risk & Security Management Consulting, insurance is a recommended part of an organisation’s overall cyber security strategy.

“F-Secure’s Cyber Security Services teams work with companies on many levels to help improve their security posture, and in our work, we see that the eventual breach is inevitable. Companies should do their best to defend their networks, and they should also have insurance to handle the consequences of any mishap,” says Kallio.

Symantec and F-Secure have set a precedent for other vendors to follow and help businesses and organisations to deal with the menace of cyber attacks and crime in more effective way keeping in view the financial risk aspect.

“Partnerships of Symantec and F-Secure with insurance companies show that they are willing to take-up co-liability and co-ownership in event of cyber attacks. So IT firms and tech vendors should also take up some onus and not just point fingers at CIOs or CISOs,” concludes Gogia.