CYBER RISK INSURANCE – ISSUES AND CHALLENGES

Mrs. Sandhya K. Salve/Wanjare

(Research Scholar) M.B.A.(Finance), M.Com., G.D.C.& A., D.C.M. D.C.S. C.D.J. College Of Commerce, Shrirampur

Keywords: Cyber risk, Insurability, Information security, Data Protection

IntroductionWhereas the 'internet' stands for a global computer network providing a variety of information and communication facilities, the 'cyber space' is the notional environment in which communication over computer networks occurs. The 'World Wide Web, or simply the web or www is a way of accessing information over the medium of the internet. The www, an information- sharing model that is built on top of the internet is further driven by the specification of sharing of information across the network and is guided by an internet protocol (IP). Today, with over 1 billion websites and 6.4 Billions 'things' connected on the internet', the cyberspace has truly become a ubiquitous dimension in itself and a host for all kinds of information services and economic activities. During the last decade the shift from physical space to cyberspace has been so phenomenal that we experienced a bursting of bubble on the financial markets. In the year 2000, the doc-com bubble, had been caused by irrational exuberance regarding the cautions of the internet business by the markets. However, the cyberspace has come a long way and continues to grow in size and significance. In wake of its importance and rate of penetration, the incumbent business, government and other entities have adopted to the internet mode of delivery of services and as such there is exponential growth in opportunities coupled with exposure to new kinds of vulnerabilities known as cyber risks.

The omnipresence of Network Systems and Digital information With raising digital assets, infrastructures and multiplicity of technology platforms, there is also rise in incidences such as hacking and spamming of networks and website with malicious intent. What we observe in the interconnected world is more and more critical information is getting digitized, dematerialized and being stored on to servers. Similarly services are becoming cheap and demonetized in the online world thereby increasing our dependence on network systems and digital information, all such factors are but accentuating the risks. Today the internet has become the absolute tool for all sorts of organizations, governments and business to reach out to people in a cost effective manner. The internet technologies have permeated social, economic, health, financial and political system so much so that there is no turning back from this point. With the power of internet and digital technology and growth of complementary assets, businesses are finding it unusually easy to establish identity, on-board and providing seamless service experience through the internet institutions now simply have to leverage on the computing power and maintain electronic folios or customer ids which form the basis for recording of all transitive information also making their retrieval easy for further treatment . It is therefore pertinent that such organization would actively seek to secure their cyber presence and digital assets through cyber risk insurance.How do firms deal with cyber risks and how do they risk mitigation is of interest . In India, cyber insurance is still in nascent stage, few insurers are providing policies regarding the new form of risks posed by the connected and borderless cyber world. Large firms intending to go for cyber risk insurance generally place their requirement through a request for Proposal, small firms typically go for self insurance . IT Act 2000 gave a further fillip to conducting of transactions in a computerized environment by providing a legal underpinning.

Cyber risk insurance can play fundamental role in developing the digital economy. It is often assumed that the issues of cyber security and cyber insurance are separate- that cyber insurance is no substitute for proper cyber security-but in truth the two are intertwined. The challenge then is to build a smart, well-designed, cyber risk model that is able to analyze potential direct revenue, liability and brand loss scenarios and must quantify how much their future revenues of the firm will fall if a cyber-attack has damaged their brand.

Cyber-Space governance in India The role of the government is immense in developing a system of cyber defense for the entire nation. The Government of India has taken several steps to tackle the menace of cyber attacks and important institutional arrangements made. The Indian Computer Emergence Response Team has been established which monitors Indian Cyberspace and coordinates alerts and warning of imminent attacks and detection of malicious attacks among public and private cyber uses and organizations in the country. Banks Financial Institutions have been identified as critical infrastructure for the purpose . A National Cyber Coordination Centre has also been established. It is mandated by the information Technology Act that periodic IT security assessments are held to determine acceptable level of risks, consistent with the criticality of business/functional requirements, likely impact on business/ functions and the achievement of organization of goals/ objectives. This is also documented in the 'Information Security Policy for protection of critical information of Critical Information infrastructure' of CERT-In. In 2008, the information technology Act 2000 was amended with the introduction of section 70A and 70B. Article 70A mandated the need for a special agency that would look at designated "Critical information Infrastructures."(CIIs) and evolve practices, policies and procedures to protect them from cyber attack. On January 16 2014, the Department of Information Technology (DIT) issued a notification announcing the creation of a specialized body to protect India's CIIs; banking and finance sector being one of these CIIs[9]. The National Critical Information Infrastructures Protection Centre (NCIIPC) was created and placed under the technical intelligence agency, the National Technical Research Organization, to roll out counter-measures in cooperation with other security agencies and private corporate entities that man these critical sectors.

Insurance as a Response to Cyber Risk Faced with the risk of cyber attacks, the prospect of losing data and the potential for large charge fines, the private sector has turned into the insurance industry to protect against losses arising from all manner of Information security incidents. Allianz estimates the total written premium for cyber insurance could reach $20 billion by 2025. In wake of volatile and capricious nature of cyber attacks, the insurance companies that have capacity to respond to multiple incidents simultaneously and have the requisite policies for tackling with the range of potential incidents. According to a PwC report." Worldwide the cyber insurance market will triple in size to 7.5 billion$ in annual premiums by 2020 but the high cost of coverage and restrictive conditions on policies may restrict growth. The report further says that business across all sectors are beginning to recognize the importance of cyber insurance, with 61% of corporate leaders now seeing cyber attacks as a threat to the growth of their business. There was an average of 200000 global cyber security incidents in a day in 2014. The market is still relatively untapped. While some 90% cyber insurance is purchased by U.S. companies, only around a third of U.S. companies have some form of cyber coverage . In the United Kingdom, only 2% of companies have standalone cyber insurance. The much bigger and tougher challenges are the new exposures arising from the technological evolution of risk and how this impacts existing lines of business. The framework for that need to deal with in-house computer systems, cloud storage, industrial control systems and finally the national critical infrastructures, which are the biggest challenge in terms of the physical risks, and business interruption losses. India's ecommerce business is booming. Morgan Stanley Research has revised the estimate of the India's ecommerce market till 2020 from $102 billion to $119 billion, this takes the estimate of the total Indian Internet market size from $137 billion to $159 billion .

Conclusion The cyber insurance market should continue to grow as a result of high profile breaches. Firms can significantly improve their risk practices by adopting common cyber risk management practices. Insurers and reinsurers are actively learning more about these risks and the underwriting process is expected to get better. As the market matures, capital markets may lend a hand in the expansion of capacity for cyber reinsurance as deals become more economically attractive. However, It should be recognized that there are limits to the role that insurance can play for managing the threat of cyber attacks. Sole reliance on insurance as a solution can create moral hazards by reducing incentives to actively manage the threat of cyber attacks.

References:

WWW.gartner .com/newsroom

Philip Rawlings,Queen Mary University of London, School of Law Legal Studies Research Paper No.189/2015

S.S.Mudra: Information Technology and cyber risk in banking sector- the emerging faults.

A report by US Homeland Security, Mar 19 2015,' Examining the Evloving Cyber Insurance Market Place.

The Jounral Of Insurance Institute of India Vol. 5 Dec.2017.