IOSR Journal of Business and Management (IOSR-JBM)
e-ISSN: 2278-487X, p-ISSN: 2319-7668
PP 37-41
www.iosrjournals.org

Cyber Insurance – A Growing Need

Mrs. Sreemathi Raghunandan, Mrs. Kalyani Gorti
Bharatiya Vidya Bhavan Bhavans Vivekananda Collegefor Science, Humanities and Commerce Sainikpuri, Secunderabad.

Abstract: *A nation can move forward economically with overall development when it functions with responsibility and accountability. This can happen with a common vision from management and participant. Management is held responsible for the happening whereas participant is entrusted with honest and diligent accountability. This is possible with high transparency with digital economy. Digitalisation means everything and anything in e-format. This enhances quality and transparency and is vulnerable to risk. The process of digitalization, on the other side, exposes towards the risk of cyber theft with or without the knowledge of a person.*

An action of unauthorized access to digital data is called cyber crime. In order to secure digital data, Information Technology Act has been enacted in the year 2000. Cyber Laws are punitive in nature, which punishes a person who tampers with the digital data. But a victim remains a victim. We need a mechanism which will help the victim to mitigate the cyber loss. A Cyber insurance coverage gives protection to such victim who incurs losses arising from IT Systems and network damages, loss of data etc. The check-in mechanism of digitalization is taken care by the IT Act, 2000(punishment of the criminal) and IRDA (rules for mitigating the loss of the victim is reallocated) for secured digital operation.

This paper enables to understand about cyber insurance and its awareness among the participants of digital economy in twin cities of Hyderabad and Secunderabad of Telangana State. The methodology of study is through the primary and secondary data sources. The study has established that there is a growing need for cyber insurance.

Key Words: *cyber crime, cyber insurance, digital economy, cyber risk, Information Technology Act.*

I. Introduction

The turn of traditional economy into digital economy created numerous concerns like Y2K problem, data security, data management etc. Every step was taken care through a process of innovation and up gradation. Digitalization has also exposed to risk such as data theft, hacking, identity theft etc. This risk has multiplied with demonetization process. The risks have been taken care at multiple levels of operations such as software designing with inbuilt security of operations. But, the risk evolved is equally increasing with the up gradation and innovation. After, all such security levels still the scope of risk is felt and experienced. The number of cyber crimes is increasing rapidly and the statistics says that India is prone to one cyber crime in every ten minutes.

The use of a computer system and a network as a means to achieve illegal or unethical results is called cyber crime. In this age of digitalization, the virtual identities are the order of the day. But they are at a threat as cyber crime aims at attacking information of individuals, organizations, Government etc. This cyber crime may take any of the following forms

1. Hacking: It is an unauthorized access of a computer by a third person. These are normally done by computer programmers who have a sound technical knowledge. The types of hackers may be white hat, black hat, grey hat, green hat depending on their motive varying from greed, power, intellectual curiosity etc. This can be done through SQL injections, theft of passwords, cross-site scripting etc.
2. Virus diffusion: A computer virus is a hostile program that generally replicates itself and infects other files. These are malicious programs developed by hackers. The harm done depend upon the type of virus and the frequency of its strike.
3. Logic bombs: These are similar to virus though not exactly are the same. These are called "slag code", which are incorrect code inserted intentionally into software. It remains inactive until a specific condition is triggered. These may be generally inserted by a dissatisfied employee working with the software.
4. Denial of service attack: This occurs when an authorized user is denied of the service. This can be done by sending more requests which are beyond the capability of the service providers. This results in overload interrupting the services temporarily. The criminals may target banks and various payment gateways using this method.

5. Phishing: This involves a method of obtaining the confidential information like passwords, card details of the user. This is normally done by email spoofing from companies which appear genuine.
6. Web jacking: This involves fraudulent control of website by a hacker. He has the entire control of the website which the actual website holder no longer holds. He may redirect the site to another similar looking site and use for his own interests which may be asking for a ransom, posting some obscene content on the site etc.
7. Cyber Stalking: Unlike physical stalking, a user is followed online through this method. This is depriving the user from his privacy. The information gathered is used to harass the victim on various websites, chat rooms etc.
8. Data Diddling: This is method of unofficial alteration of data before or after entering into the computer. The data can be changed and this cannot be identified even by a computer amateur.
9. Identity theft: This is a method of crime where an individual's identity is stolen. A third person acts as you and access the private data and can use credit cards, bank accounts etc.
10. Salami slicing attack: A cyber criminal steals a small part from large amount of money which cannot be identified. He steals from various users so that he gets a reasonably good amount. This is done with the help of a program inserted into a system which automatically executes the task.

Cyber criminals are taken care by the Cyber Laws whereas the victims are left out. Cyber insurance is a risk rescue device of such victims who are exposed to and experienced the cyber crime. Cyber insurance is a risk reallocation in digital operations. It is also considered as risk management tool. The need was felt way back in 1990's. In spite of improvements in risk protection techniques on hardware, software and cryptographic methodologies, it is really impossible to achieve required perfect cyber security. The reasons are lack of sound technical solutions, non synchronization between security product vendors, regulatory authorities and network users. The more trust vested by network users on service providers,non compatible feature benefits of technical solutions and lack of incentive to release technical solutions among security providers also contribute for the same.

Current Scenario

Let us discuss a small example of a banking transaction. Banks have introduced a system of phone banking. They developed an application for it and transactions can be executed from anywhere and anytime. This can happen through a registered phone number. Such automated transaction solution will generate OTP through which the operations can be successfully completed. Here the banker gives the feeling to the customer that they are executing the task on their own with the confidence of security from the bank. The same bank repeatedly keeps posting messages to the registered phone numbers of the customers stating that "Do not share your OTP/PIN with anyone. Bank or its employees never ask User ID, password, OTP, PIN, ATM-Debit-Credit card number, CVV, Expiry date." This creates an apprehension in the minds of customers/individuals. It is clearly understood with the statement of the bank that if any such PIN/OTP being shared, the bank is not responsible to the customers for their loss of money. The bank is posting such messages because of vulnerability of such risks. If any money is lost, after all caution, the bank will push all the responsibility in the name of the customers. Is it not hinting that there is a dire need for cyber insurance?

II. Literature Review

Shree Krishna Bharadwaj.H (2016), The paper titled above has studied on Cyber liability insurance. This paper also narrated the various risks evolved in technology- involved business activity of tech savvy India. The study explained about inappropriate handling of cyber crimes. The paper also expressed that the regulatory mechanism through Government is very vague in handling the cyber crime cases.

Sasha Romanosky, Lillian Ablon, Andreas Kuehn, Therese Jones, in their work on the paper titled, "Content Analysis of Cyber Insurance Policies: How do carriers write policies and price cyber risk?" have examined about the rising need for cyber insurance. The paper emphasizes on the cyber insurance policy coverage and exclusions, calculation of premiums, insurer's risk etc. on cyber insurance policies for business in United States of America. This paper explained that there is no standardization of policies. This also highlights on the dispute whether the physical damage to the systems is covered under general liability policy or cyber insurance policy.

Robert P Hartwig, Claire Wilkinson (June 2014) in their paper on cyber insurance have emphasized about various cyber risk exposures. The paper also stated that the loss involved in such cyber attacks is unbearable both by the organizations and individuals. This threat has paved way for specialized cyber insurance productsto cover risk involved.

Ranjan Pal USC, Pan Hui T Labs in their research paper have stated about the cyber insurance from an insurer's perspective. The paper has listed about the devising of a policy. It proposed for drawing up of a boundary from the insurer's point of view for indemnifying such risk arising out of cyber crime.

Objective Of Study

1. To understand digital economy
2. To understand cyber insurance and its coverage
3. To know about the evolution & awareness of cyber insurance

III. Methodology

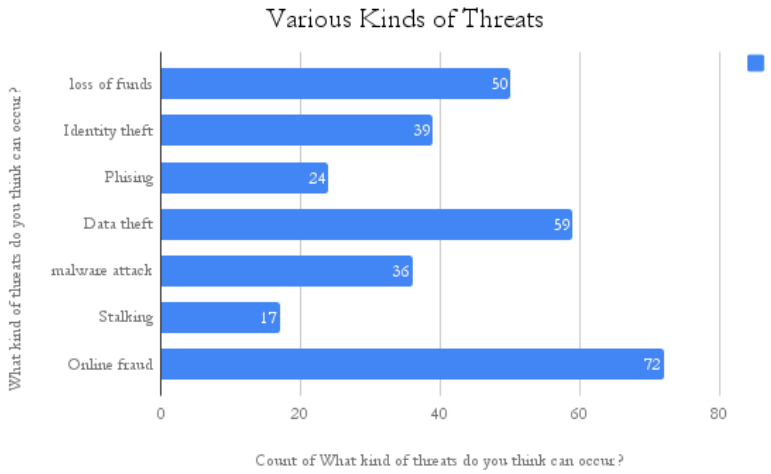
The data was collected through random sampling technique(sample size: 100) by the distribution of questionnaire. The data was also collected through secondary sources like books, journals, trusted websites etc.

Analysisand Interpretation

A questionnaire was circulated randomly to a sample size of 100. The observation is tabulated below as follows

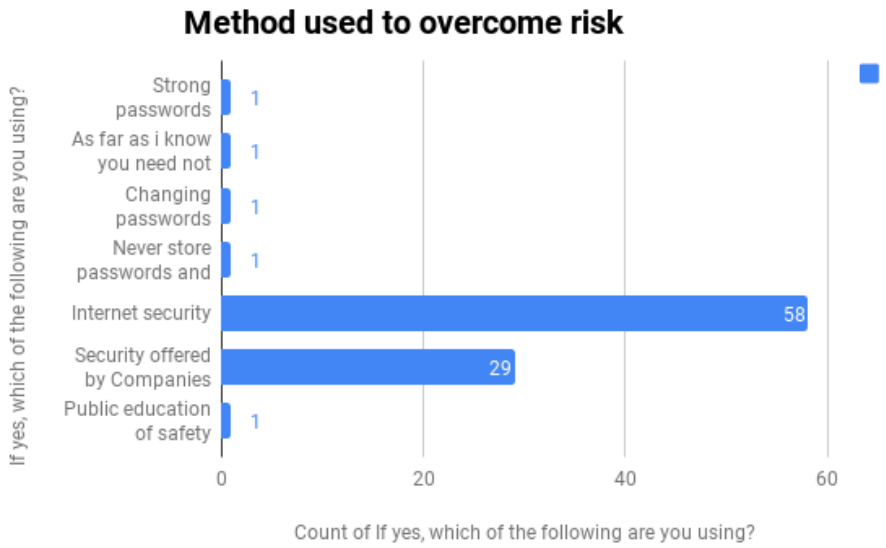
Basis of analysis	Interpretation
Age	It is observed that the age group of 18-25 is falling into a category of 46% and age group above 35 is with 44%. So it can be inferred that youngsters and middle aged are the highest users of digital mode of payments.
Gender	The usage of digital modes is unbiased of gender.
Qualification	It is inferred that 45% of the sample are undergraduates, 38% post graduates & 17% are professionals. They are users of digital modes of payment.
Usage of digital modes	It is observed from the sample that 98% opt for digital mode of payment positively due to demonetization or due to their educational status
Mode of digital payment used	It is clearly noted that all the digital modes are preferred but still debit/credit card mode is used by 65% when compared with 29% on net banking and 6% over phone banking. Whatever be the mode, they are being widely used.
Trained on usage	It is evident that 79% of the sample is trained on the digital mode usage. This indicates that the trained users also have a chance of being victimized.
Frequency of usage	It is understood that the frequency of digital mode of payment is observed to be 43% on weekly basis, 26% on monthly, 18% daily and 12% fortnightly. Perhaps, this scenario is due to demonetization
Risk awareness	The understanding of risk of exposure is felt by 79% positively and 21% are still believed to be secured.
Measures to overcome risk	It has been inferred that the awareness of the threat has secured 62% of the sample with a probable measure of security. The remaining 38% of the sample are clueless about the measures.
Personal risk experience	Among the sample, 82% did not experience any risk of their own whereas 18% have such experience of risk. 63% of the respondents heard about the risk faced by their associates in contrast with 37% who are unheard of.
Awareness of cyber insurance	For the awareness of cyber insurance 25% have responded positively in contrast with 75%.
Method of awareness	Out of the respondents who are aware of cyber insurance, 78% are beneficiaries while 28% are policy holders. This indicates that they have not taken policies by themselves but are provided such benefit by the service providers. Bank providing insurance for credit card may serve as a good example.
Coverage of policy	78% of the sample has opined that the insurance coverage needs to be on the value of loss rather than the point of usage.
Insurer	Majority of the respondents have preferred a Government company to a private company for cyber risk coverage.

Source: Primary data collected through questionnaire



Source: Primary data collected through questionnaire

The above diagram shows that the fear of online fraud is the highest followed by data theft which includes loss of funds. Every single individual is exposed one or the other risk.



Source: Primary data collected through questionnaire

Most of the respondentsare seeking protection through internet security/ security offered by corporates or other service providers.

IV. Findings

Majority of the digital users are in the age group of 18-25 and 35 above with a minimum qualification of under graduation and there is no gender discrimination.Almost 98% of the sample is the users of digital mode and more than 65% use debit/credit cards followed by net banking and phone banking. 80% of the users are trained and invariably they use more frequently on a weekly basis. Among the users of digital modes, majority of them felt that there is a risk associated with online operations.2/3rd of them are securing their operations through internet security, anti-virus software etc.The study states that a negligible group of people are affected by the exposure of risk and quite a few have heard sharing of such risk from their close associates.To overcome such risk they are expecting Government to design an insurance product than to a private.Most of the respondents preferred risk coverage on value of loss than to point of loss.

V. Suggestions

The growing phase of digitalization urges the need for cyber insurance. The business can afford the insurance coverage against these cyber crimes. The individual users should also benefit from such insurance. The cyber insurance cover prevents the individuals from the fear of vindictive damages. They do not apprehend any insecurity in handling personal data. But the insurance cover should be provided assessing the risk associated. The type and context of the personal information dealt with, education and training of individuals are to be considered while assessing the risk. It should also consider the level of security of mobile devices that carry sensitive information. The Government should initiate awareness about the risk as well as its prevention.

VI. Conclusion

The effect of globalization is very positive in economic growth and development. But it has also given rise to many issues globally. As India is a developing country, the infrastructure and other securing and promising developments are not immediately in the reach, but could be reached. The lead time between, causes anxiety and concern. The primary need is felt in development of hi-tech infrastructure equipped with anti risk. Undoubtedly India is forging ahead with the competitive edge. But it is lagging in preserving such innovations. Currently the cyber insurance concept is felt only in the West whereas in India it is limited only to few business houses. When we are keen in the process of digitalization, and insist on transparency and accountability it is the responsibility of the change to protect the change. Rural India is the worst hit in the process of digitalization. It is truly felt at this juncture, the need for Cyber insurance.

Acknowledgement

We would like to express our sincere gratitude to Prof Y Ashok, Principal, Bhavans Vivekananda College for his consistent support and guidance. Our heartfelt thanks to our Head, Department of Commerce, Dr. K. Sreelatha Reddy for her unconditional support and motivation. We also thank our family and friends for their valuable cooperation but for which this paper would not have been possible.

Bibiliography

[1]. https://en.wikipedia.org/wiki/Cyber-Insurance
[2]. www.aig.com/business/insurance/cyber-insurance
[3]. https://www.onlinejournal.in/IJIRV2I1/004.pdf
[4]. https://www.britannica.com/topic/cybercrime
[5]. https://timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10-minutes/articleshow/59707605.cms
[6]. https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html
[7]. https://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf
[8]. http://www.cyberriskinsuranceforum.com/sites/default/files/CIS%20Cyber%20Insurance_FINAL.pdf
[9]. http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/06/WEIS_2017_paper_28.pdf
[10]. Shree Krishna Bharadwaj.H(2016), "Cyber liability insurance in India: Growing importance", Imperial Journal of Interdisciplinary Research (IJIR) – Volume 2 Issue 1 2016, ISSN: 2454-1362