

Effect of Cyber Crime on Economical Development

Dr. Vidhi Khanduja¹ Dr. Roshini Rawal²

^{1,2}Associate Professor

¹Department of Computer Engineering ²Department of Science & Humanity

^{1,2}SALITER, SAL Educational Campus Gujarat, India

Abstract— Internet has become household commodity in India and almost every information and data is running online. Due to this cyber crime has been rapidly increasing its footfall on Indian economy. There are various kind of cyber crimes, creating impact and threat to the economy of a nation and even disturbing peace and the security. This research paper emphasis on how cyber crime is having hazardous effect on Indian economy as it move towards the new investment, digitalization and demonetization. It is increasing the risk factor. Therefore there is need for a holistic approach to combat these crimes and try to find remedies for it. So that we can drag our Indian economy towards developing economy, not the underdeveloped economy and its effects could be more profound. And we can witness the new horizon of cyber crime free Indian economy.

Key words: Cyber Crime, Cyber Espionage, Digitalization, Demonetization, Economic Growth, Risk Factors

I. INTRODUCTION

With Internet becoming household commodity in India, the cyber crime has become major concern today. Any crime committed using computer and Internet is referred as cybercrime. This crime can be against a person, business or non-business organization or government. It has a serious impact on our economy, as well as on our society. According to various surveys and reports, cyber crime is affecting various industries and is increasing the risk factors [1-3]. Political & Governance Instability holds its position at 6th, as per the India Risk Surveys' for 2017 and 2016 respectively. It affects almost every sector in Indian economy like- retail, financial services, health care, banking, stock market, IT sector etc. In this digitalization era, Cyber crime is the biggest risk for the Indian economy. It transforms and impede the business world to give exposure of both opportunities and threats. Thus, we conclude that cybercrime continues to extent – ranking as this year's second most reported economic crime [2].

In India, cyber crime is increasing at the rate of 50% per year [2]. Number of cyber crime incidents are increasing with rapid speed. Earlier, this attack requires experienced computer literate persons, but now a days it is easier for even the layman. The foremost reason for the increase in cyber attacks is difficulty in tracing the action and the person behind it. Further, cyber attacks can be committed remotely from any part of the world targeting any number of population. Due to these reasons, cyber security and Information security has taken centre-stage. "Cybersecurity is going to be a big problem in 2018. I guess there is an outside possibility we may see some devastating attacks in 2018" as per Richard Fenning, CEO, Control Risks [4]. The lot of research is ongoing to protect the data/databases on the web [5-9] and to secure the cyberspace

[10]. In this manuscript we aim to fulfil following objectives:

- 1) To comprehend how cybercrime is affecting economical development in India.
- 2) To study the factors or determinants related to crime that play vital roles in the development of economy of any nation.
- 3) To get acquainted with the above identified factors effecting cyber crime.
- 4) To study and reduce the factors responsible for having effect on Indian economy.

Section 2 discusses various types of cyber crime existing in cyberspace. In section 3, we discuss various risks factors for development in economy followed by the impact of cyber crime on Indian economy in section 4. Section 5 enlist suggestions to combat cyber crime followed by section 6 which concludes our paper.

II. TYPES OF CYBER CRIME IN INDIA

There are many types of cyber crimes, from which we should be aware so as to prevent them. Various types of Cybercrimes identified are as follows [11]:

A. Cyber stalking

This type of cyber crime creates physical threats using technologies such as smart phones, email, messages, websites or videos. Assault by threatening a person or his family members using computer/internet also comes in this category of crime.

B. Child pornography

This crime involves the misuse of advanced communication technology by sexually exploiting underage children. In this case, computer networks are used to create, distribute, or access such objectionable materials.

C. Cyber laundering

This type of cybercrime involves online transfer of currency with an intension to hide its source and destination.

D. Cyber terrorism

This type of crime includes use of technology for destruction or to harm a person or organization. This crime includes hacking and cyber theft. All the activities like DNS cache poisoning, identity theft, fraud, sending spam messages, phishing, plagiarism, and piracy. Other prevailing attacks are:

1) Hardware Hijacking:

This is hijacking of networking equipment. In 2015, CISCO has issued an alert stating attackers are gaining physical access to Cisco IOS devices and replacing them with a malicious ROMMON image.

2) Script kiddies:

Amateur hackers comes under this categories. They attack weakly secured systems.

3) *Insiders:*

Overall percentage of this category of attackers is 20% but it causes 80% of damage. Thus, are at highest risk as they reside within an organization.

E. *Yahoo Attack*

The well known internet service company Yahoo has reported data breaches by hackers. Nearly, 3 billion of Yahoo's user accounts were effected [1].

F. *Salami Slicing*

This attack produces a larger impact through series of smaller one in due course of time. These small attacks normally go unnoticed due to the type of this cyber attack.

III. RISKS FACTORS FOR DEVELOPMENT IN ECONOMY

India is moving towards the steady growth for the development. As per the latest IMF (International Monetary Fund) projection, India's growth rate is expected to be 7.2 per cent in the 2017-18 fiscal and 7.7 per cent in 2018-19 owing to critical structural reforms, favourable equations of trade, foreign direct investment and lower external vulnerability. It is encouraging to note that the change of velocity of structural reforms is bringing a new growth impulse. The Goods and Services Tax (GST) implemented in mid 2017, is helping India in making more of a single market and thus will incite production, job creation and investment in the country. Demonetization has lead to great fluctuations in Indian economy. It encourages online transactions and dragged the Indian economy to the world of digital economy. As we are moving to complete digitalization, the risk factor also increases which is detrimental for the growth of Indian economy. Thus, understanding of the risk factor plays a vital role in Indian economy. According to Secretary general, FICCI, Dr. A Didar Singh, "Risks factor is detrimental to growth and development of any country. The nature of risks globally has changed humongous, and with their occurrences becoming more unexpected and their effects becoming more deeper, risks need to be taken more seriously as it plays crucial role for the growth of any economy. Further, due to rapid digital transformation of businesses, fundamental infrastructure is becoming more complex. Understanding of emerging risks is demand for today's rapid transforming world" [2]. FICCI – Pinkerton India Risk Survey 2017 ranks 'Information & Cyber Insecurity' as the biggest risk in 2017. In the recent past, there has been an increase in incidences of cyber attacks and potential espionage on cyber-security. As the nation is moving towards digitisation of various assets and services being delivered via internet and mobile platforms; and the loopholes that hackers rift upon, cyber security has become more pronounced. The WannaCry malware incident was an example of these kind of risks. Knowledge about future risks can benefit investors, so that they could take appropriate and planned decisions and can move towards a sound economic condition [12]. As it will have a direct and indirect impact on economy. In context of cyber security, it became more essential.

Fig 1. Shows the overall risk ranking in year 2017, 2016 and 2015. Data is taken from [2]. 'Crime' as a risk factor dropped to the 8th rank in 2017, from its third

position in last year's India Risk Survey. According to National Crime Records Bureau (NCRB) data, in 2015, overall crime in India increased by 1.3%. A total of 73, 26,099 crimes were reported, with 29, 49,400 crime registered under the Indian Penal Code (IPC) and 43,76,699 under Special & Local Laws (SLL). Delhi accounted for 25% of all crimes registered in major Indian cities [13].

'Business Espionage' climbed one spot to ninth position in IRS 2017. The inherent problem with business spying is the possible domino-effect which would lead to an extensive collapse within a company [2]. With the help of various risk surveys like Indian risk survey etc. one can understand the intensity of risk of cyber crime for business and the same for economy. The purpose of India Risk Survey 2017, remains to provide a handy guide, drawing attention to potential risks, and providing a base to plan the necessary preventive strategies to protect one's organization and economy from the hazardous effect of these risks on Indian economy [14]. This survey aims to inform about the emerging risks for developing economies like India so that well planned and strategic policy decisions can be made, useful for the growth of Economy [2].

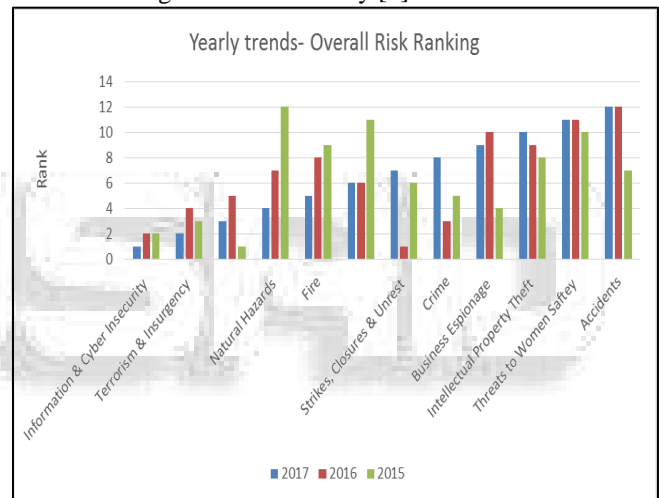


Fig 1. Ranking of various factors for Risk analysis over the year 2017, 2016 and 2015

ASIS the globally renowned industry body of security practitioners, has testified that the threats faced in today's progressive world requires a more holistic strategic approach. Respondents surveyed in year 2017, ranked 'Information & Cyber Security' as the biggest risk to business interests in India, which will remain a significant threat for coming years. Cybercrime climbs to 2nd most reported economic crime affecting 32% of organisations. Most companies are still not adequately prepared for – or even understand the risks faced: Only 37% of organisations have a cyber incident response plan [2]. It will lead to the vigorous development in economy for any country. Especially when we talk about India, risk factor increases and it get affected by various factors as India's economy is changing rapidly. New economical changes will attracts new investments, shows new paths and will lead to the new horizon of economical development of India.

IV. CYBER CRIME: IMPACT ON INDIAN ECONOMY

Cybercrime occurs in the world of computer and the Internet. This kind of crime has a serious and hazardous impact on our economy. Due to the nature of informative society, Indian society is full of information exchange happens in cyberspace. There are various cyber crime like- software piracy, hacking and pornography among others are common crimes in India. It has deep impacts on Indian economy, which can be visualized easily. It is considered as one of the economic crime affecting intensely Indian economy. More than one-third of organisations have experienced economic crime in the last 2 years, as reported by over 6,000 respondents to PwC's Global Economic Crime Survey 2016 [3]. Fig. 2 shows the change in the economic crime over past few years for which data has been taken from [3]. In 2016, for the first time there is decrease in economic crime since the global financial crisis of 2008-09 (albeit marginally by 1%). It seems that it could be the return on the investments (ROI) which organisations have been making over the past few years. But, this decline is actually a worrying trend revealing that there is a significant change in economic crime as the detection and controls programs are not up to the mark. Also, there is increase in the financial cost of each fraud [3].

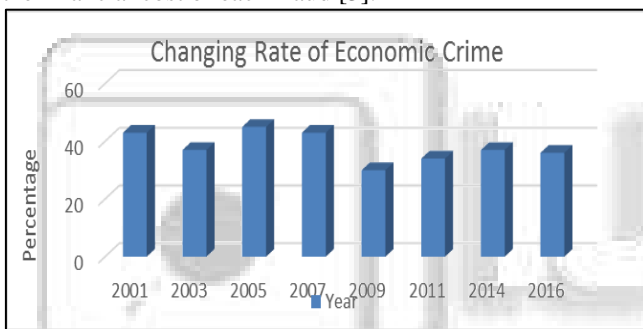


Fig2. Change in the economic crime from 2001 to 2016.

From the last two years, economic crime has increased rapidly having impact on industrial sector and region. A passive approach to detecting and preventing economic crime is a prescription for disaster. We have taken strong steps of preventing, protecting and responding to economic crime. 32% of organisations are affected and 34% think they are likely to be affected in the next two years [3].

Today, all industries in India are at risk for cyber crime – including those which were unlikely previously targeted. According to PwC's Global State of Information Security Survey 2016, "The sector registering the most significant increase in cybercrime activity in 2015 was retail, while financial services – still one of the most attacked sectors – had levelled out, with very little growth in terms of number of attacks over the last three years" [3]. It will have impact on economy directly or indirectly. It affects almost every sector in Indian economy like- retail, financial services, health care, banking, stock market, IT sector etc. That's why it is a crucial issue of Indian economy, needs serious and urgent attention.

V. SUGGESTIONS

In order to provide cyber security, we must implement following measures:

- We should keep keen observation on various sectors having impact on economy. In result to that we can identify problems and then take actions accordingly.
- More profound and extensive research needs to be carried out at local as well as at international level as Indian economy is moving towards Globalization and developing international relations.
- Internet Service Providers, financial institutions and retailers should be convinced to share and be open about their cyber crime experiences.
- Technical security measures that must be followed, includes limited sharing of personal information on social networking sites, using secure and strong password which must be timely changed, installing and updating anti-virus software on regular basis [15].
- Government officials authorities and Banks never ask for Card Number/Expiry detail/CVV/OTP/PIN/Password. We must always be aware and conscious about not to disclose such personal confidential details on phone or emails.

VI. CONCLUSION

Cyber crime has been increasing its footfall on Indian economy. Moving towards the new investments, digitalization and demonetization, will rapidly lead us towards the threat of cyber crime. There are various kind of cyber crimes, creating impact on Indian economy and continuously increasing the risk factor. Direct consequence of this in near future is that the craze of online shopping is slowly declining resulting in increase in physical retailing. There is a need to recognize it and try to find remedies for it. Ideology of using internet need to be spread widely. So that we can drag our Indian economy towards developing economy, not the underdeveloped economy. Hence, cyber crime is a kind of an empirical threat that can be resolved by taking timely security measures so that it could not hamper economical growth.

REFERENCES

- [1] Yerra Shankar Rao, Dr Hemaraj Saini, Dr T.C.Panda, "Effect of Cyber Crime Indian Economy", International Journal for Research in Technological Studies, Vol. 1, Issue 10, September 2014.
- [2] 'Information & Cyber Insecurity' are the biggest risk in business operations: FICCI – Pinkerton India Risk Survey 2017.
- [3] www.pwc.com/crimesurvey accessed on 30/11/2017
- [4] Sanjiv Shankaran, "Cyber security going to be big problem in 2018... lot of the commercial breaches are done through human weakness", TOI Wednesday Dec06 2017.
- [5] Khanduja V., "Watermarking Categorical Data: Robustness and Algorithm Analysis", Defense Science Journal, DRDO, Volume 65(3), pp. 226-232, 2015, <http://dx.doi.org/10.14429/dsj.65>.
- [6] Khanduja V, Verma OP, Chakraverty S. "Watermarking relational databases using bacterial foraging algorithm", Multimedia Tools Appl (Springer), vol. 74(3), pp: 813–39, 2015, doi:10.1007/s11042-013-1700-9.

- [7] Khanduja V, "Dynamic Watermark Injection in NoSQL Databases", *Journal of Computer Science Applications and Information Technology*, Symbiosis, pp. 1-5, 2016.
- [8] Khanduja, V., 2017, "Database watermarking, a technological protective measure: Perspective, security analysis and future directions", *Journal of Information Security and Applications*, 37, pp.38-49.
- [9] Khanduja, V., Chakraverty S, Verma OP, "Enabling Information Recovery with Ownership using Robust Multiple Watermarks", *Journal of Information Security and Applications*, Elsevier, Volume 29, pp.80-92, 2016, DOI: 10.1016/j.jisa.2016.03.005, ISSN:2214-2126.
- [10] Sandlas, Shri Ved Prakash. "Cyber-Space Security.", *USI Journal*, pp-1-9. http://www.usiofindia.org/article_july_sep06_10.htm , 2008
- [11] Hemraj Saini, Y. Shankar R, T.C.Panda," Cyber crime and their impact A review", *IJERA*, March 2012, Vol.2, pp:201-206.
- [12] Syed Munir Khasru, "WannaCry shows that businesses and governments must cooperate", <https://www.weforum.org/agenda/2017/06/wannacry-exposes-need-for-better-public-private-cooperation-in-the-cyber-space/>
- [13] National Crime Records Bureau, 'Crime in India' 2015.
- [14] Maplecroft 2016, Climate change and Environmental Risk Atlas. <https://maplecroft.com/portfolio/new-analysis/2014/10/29/climate-change-and-lack-food-security-multiply-risks-conflict-and-civil-unrest-32-countries-maplecroft/>
- [15] Shweta Kaushik, <http://www.vakilno1.com/legalviews/cyber-crime-child-abuse.html>, Accessed on: 25.11.2017