Volume - 5, Issue- 9,September 2017 IC Value : 56.46 e-ISSN : 2347 - 9671| p- ISSN : 2349 - 0187
EPRA International Journal of Economic and Business Review SJIF Impact Factor(2016) : 6.484
ISI Impact Factor (2013): 1.259(Dubai)

Research Paper

www.eprawisdom.com

CYBER CRIME: A NEW ECONOMIC CHALLENGE AND OPPORTUNITY

Baishya, K[1]

[1]*Assistant Professor, Department of Commerce, Karmashree Hiteswar Saikia College, Guwahati, Assam, India*

ABSTRACT

With expansion of information technology, cyber crimes and its costs also take a toll. In 2016 average cost of cyber crime touch 400 billion USD. An analytical discussion is proposed in this study about cost of cyber crime from the point of external consequences and form organisational point of view together with opportunities presented by cyber crime to the economies to enter into cyber security market. As compared to developed nations potent developing economies are targeted more by criminals because of weak cyber security arrangements and lack of user awareness. On the other hand, these economies also have potential to enter into cyber security market supported by low completion. Exploration of market opportunities by developing economies subject to the conditions of improving infrastructure, flow of fund to cyber security industry and identification & polishing of talents.

KEY WORDS: *Analytical discussion, External consequences, Cyber security arrangements, Exploration of market.*

INTRODUCTION

Human history takes a new turn with the conceptualisation of computer by Charles Babbage in 1900 century. What looks like a seed during that time now becomes a giant universe which is even challenging the physical reality of this world. As our world curve into the coded universe of computers, humans seem to lose willingness to spend physical effort in doing day to day activities. It will be an understatement of truth if it is said that use of computers are limited to keeping records and data storage only, they go beyond that and includes data processing trough statistical and qualitative analysis, information sharing through internet and sometimes even decision making when instructed to do so. Irony of human civilization is that no pearl comes without a peril, like a comic book universe these virtual developments are also threaten by villains though not by Thanos (Iron man, volume 55, February1973) or Joker (Batman first issue, April 1940) but defiantly by hackers, viruses, pilferage of storage devices, criminals related to social engineering and so on. According to a report of CNBC cyber crime cost around $ 400 billion US dollars in 2016, worries just not stop at what happened in past but also looming at future as Hiscox Cyber Readiness Report based on 3000 companies (February, 2017) disclose that more than 53% companies are ill-prepared to deal with an cyber attack and just 30% were rated "expert" in their overall cyber readiness. While cyber crime take toll since the last decade another segment raise in the world economy to protect individuals and companies from cyber attacks, this segment although can't be called an avenger (The Avengers, 1963) as it does not run a free show but definitely giving a hope that cost of cyber crime can be reduced and recovered to some extent. This segment includes cyber security agencies, IT companies and cyber security software builders. A report published by MarketsandMarkets states that cyber security market is likely to grow from USD 122.45 in 2016 to 202.36 by 2021. The prime focus of this paper is to discuss about different factors related to cyber crime cost and to identify the drivers of those cost and also review briefly the growth of cyber security market and scope for generating income from this market by potent developing nations.

THE OBJECTIVES OF THE STUDY UNDERTAKEN ARE:-

1. To present a brief overview of cyber crime cost.
2. To analytically discuss about cost of cyber crime from external and organisational point of view.
3. To overview growth of cyber security market, current market constitution and factors to be stressed to rise in this market.

RESEARCH METHODOLOGY

The paper '*Cyber Crime: A new Economic Challenge and Opportunity.*'is an analytical paper seeking to present an overall view of economic cost of cyber crime as well as the opportunities to the developing economies to

derive resources from the cyber security segment of world market. The topic is a global phenomenon, hence, too huge to discuss with the help of primary data. Therefore, the analysis undertaken here is based on secondary data collected from different reports, papers and publications. The cost of cyber crime, in this paper, is analysed from two different points of view that are cost from external consequences point and cost from organisational point of view. Along with cost of cyber crime there is an attempt to briefly discuss about the growth of cyber security market and prospects of certain developing countries to enter into in this market in the light of secondary information. The discussion is undertaken in this paper from economic point of view, therefore, the non economic cost such as social cost, cost of individual reputation due to cybercrime and the legal aspects of cyber crime are ignored to be considered for analysis.

Tools: the mathematical tools applied for data analysis are percentages, conversion of data with the help of assigned weights and conversion of data with the help of factors. The formula for conversion of data are mentioned just below the tables.

Presentation and applications: data are presented with the help of tables; however some of the data are also scripted without tables. Tables, equations (formulas) and diagrams are presented with the help of MS word.

DISCUSSION

As it was already mentioned that cyber crime becomes a threat to the world economy costing around $400 billion per annum. The developed countries feel the heat of cyber crime more than under developed countries. Cyber crime costs incurred by 6 developed economies in 2015 and 2016 are:

Table 1: Cost of Cyber Crime Incurred by Six Developed Economies

	Year 2015	Year 2016
Countries	**Cost (in million USD)**	**Cost (in million USD)**
United States	15.42	17.36
Japan	6.81	8.39
Germany	7.50	7.84
United Kingdom	6.32	7.21
Brazil	3.85	5.27
Australia	3.47	4.30

Source: '2016 Cost of Cyber Crime Study & the Risk of Business Innovation'

Note 1: currency conversion rates were taken from *The Wall Street Journal,* Aug 22, 2016.

From the information of Table 1 rate of increase in the cost of cyber crime in these countries can be calculated, let's take look on percentages of increase in the cost of cyber crime in mentioned countries in 2016 as compared to 2015.

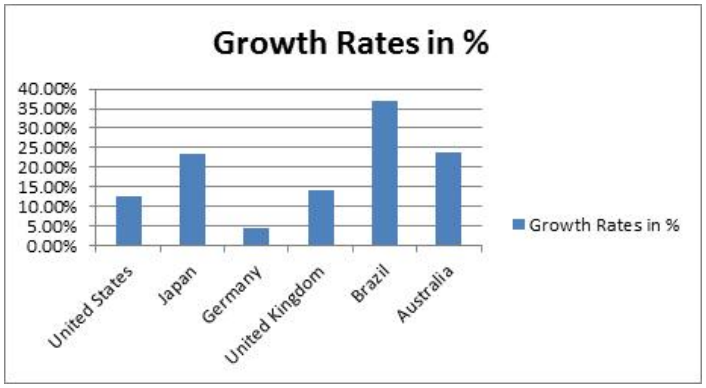
Table 2: Growth rate of Cyber Crime in Develop Economies

Countries	Growth Rates in %
United States	12.58%
Japan	23.20%
Germany	4.53%
United Kingdom	14.08%
Brazil	36.88%
Australia	23.91%

Formula for growth rate: $\frac{Cost\ in\ 2016 - cost\ in\ 2015}{cost\ in\ 2015\ (base)} x100$

From the Table 1and Table 2 it become clear that most of the developed countries observe a growth rate in cyber crime more than 10% in 2016 over 2015. These data can be presented with the help of a graph:

Figure 1: Growth of cyber crime in 6 develop countries in 2016 over 2015



The developed economies are like mirrors of world economy as they are global leader in field of trade, commerce, business innovation and so on, hence, from the data of Table 1 and Table 2 it can assumed that cyber crime causes greater cost in the year 2016 all over the world compared to the year 2015. Apart from above countries there are some other immerging and developing countries like India and China which also feels the heat of cyber crime but the cost of cybercrime in these countries can't be presented due to data constrains.

Cyber crime may take different forms depending on motive of the cybercriminals. The difference in motives of cyber criminals leads to difference in impact, in simple words, it raise different types loss. The most common types of losses identified **by Ponemon Institute (2016), in their study related to 237 companies** with their respective contribution (in %) in total loss in these companies are:

1.	Loss of information	loss in Percentage - 39%
2.	Business disruption	loss in Percentage - 36%
3.	Revenue loss	loss in Percentage - 20%
4.	Equipment damages	loss in Percentage - 04%
5.	Other costs	loss in Percentage - 01%
	Total	100%

To find out the global impact of above losses (external consequences), the aforesaid percentages can be converted into figures by assuming that loss Percentages are nearly same throughout the world. It was already mentioned that average global cost of cyber attacks for the year 2016 was 400 billion USD. Hence, the above loss Percentages can be express in terms of global figures, which are as follows:

Types of losses	Loss in %	Average total Global Cost	Global Loss Figure
Loss of information	39	$ 400 billion	$400 \times \frac{39}{100} =$ $156 billion
Business disruption	36	$ 400 billion	$400 \times \frac{36}{100} =$ $144 billion
Revenue loss	20	$ 400 billion	$400 \times \frac{20}{100} =$ $80 billion
Equipment damages	04	$ 400 billion	$400 \times \frac{04}{100} =$ $16 billion
Other costs	01	$ 400 billion	$400 \times \frac{01}{100} =$ $04 billion

From above calculation a notion can be drawn that loss of information is the most affecting loss in terms financial resources. Why it is so? The answer is that the detection, recovery expenses are very high in case of loss of information as proven by Ponemon Institute's report.

The above figures represent the cost of cyber attacks from the point of view of external consequences, however for deeper understanding of cost of different attacks and cost areas, the global cost figure should also be analysed from organisational point of view. For discussing cost from organisational point of view, first the types of attack faced by the organisations should be mentioned with their resolving period because greater the resolving period more will be the cost. The different types of attack and with their average resolving period are:

Types of attack	**Day's needed for resolving the attack**
Malicious insiders	51.5 or 52 days (approx)
Malicious code	49.6 or 50 days (approx)
Web-based attacks	25.3 or 25 days (approx)
Phishing & Social Engineering	19.8 or 20 days (approx)
Denial of service	17.8 or 18 days (approx)
Stolen devices	13.7 or 14 days (approx)
Malware	5.6 or 06 days (approx)
Botnets	2.0 days

Source: "2016 Cost of Cyber Crime Study & the Risk of Business Innovation" by Ponemon Institute.

It was mentioned that greater the resolving greater will be the cost. Hence, the above attacks can be expressed in global cost figures by assigning the resolving periods as weights and allocating cyber crime cost for 2016 that is $400 billion among these attacks. The table constructed from the above information is as follows:

Table 3: Cost of Different Cyber Attacks in Global Figure

SL NO	Type of Attacks	weights	Global cost figure (in billion USD)
1	Malicious insiders	52	111.23
2	Malicious code	50	106.95
3	Web-based attacks	25	53.47
4	Phishing & Social Engineering	20	42.78
5	Denial of service	18	38.50
6	Stolen devices	14	29.95
7	Malware	06	12.83
8	Botnets	02	04.28
	Total	187	400 (approx)

$$\text{Formula: Total average cost of cyber attacks (\$ 400 billion) x } \frac{\textit{Relative weight of each attack}}{\textit{Total weight}}$$

Table 3 disclose weighted average the cost of different attacks. The costs incurred by an organisation from different attacks are interlinked with resolving period which is further confirmed by Table 3. According to the report of Ponemon Institute there are six different steps involve in resolving the problems/ attacks, companies incurred/ allocate different amount of fund to each steps.

The studies conducted by Ponemon Institute (2016) on 237 companies reveal that funds are allocated to the following steps:

1. Detection- 33% Fund allocation in 2016.
2. Recovery- 22% Fund allocation in 2016
3. Containment- 18% Fund allocation in 2016.
4. Investigation- 13% Fund allocation in 2016.
5. Incident mgmt- 9% Fund allocation in 2016.
6. Ex-post response- 5% Fund allocation in 2016.

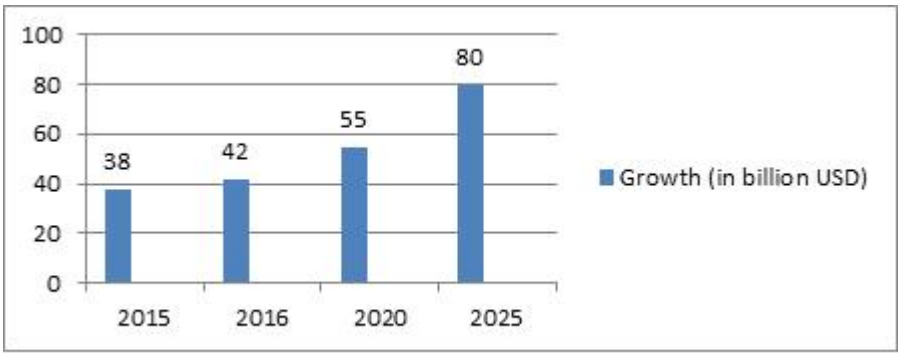
The percentages mentioned above are parts of total funds allotted for resolving cyber attacks.

Different types of attack calls for different steps ranging from any single step to multiple steps or even all the steps together. It become also clear from the percentages that corporate houses spend highest percentages of fund in initial stage of resolving a cyber attack i.e. detection (33%). However, incident management and ex-post response are least costly affairs only claiming 9% and 5% funds respectively out of the total fund allotted for resolving cyber attacks.

The study of cost of cyber attacks from organisational point reveal that actual cost of cyber attacks is constituted by the steps followed for resolving an attack.

After cyber crime cost analysis, a brief study can be helpful to understand the opportunities presented by Cyber Security Industry to the developing nations to increase their revenue bases. At first we can take a look on growth of cyber security market during the years 2015 and 2016 and its expected growth to the year 2020 & 2025.

Figure 2: Growth and Expected Growth in Cyber Security Product Market

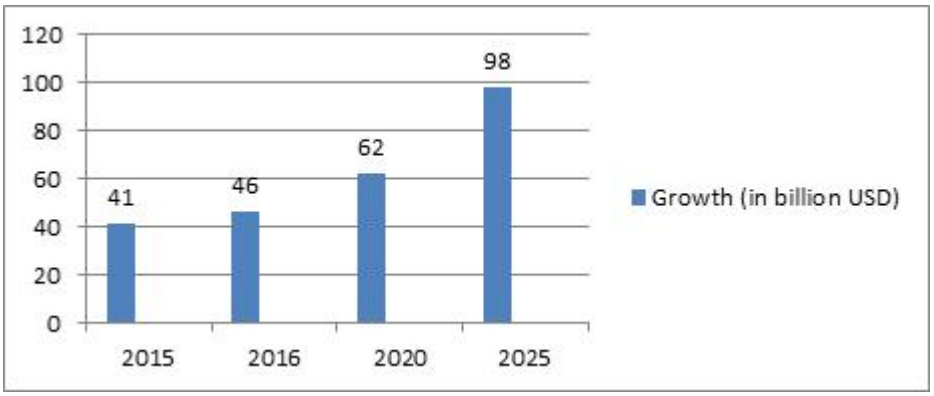


Source: GROWING CYBER SECURITY INDUSTRY Roadmap for India by NASSCOM and DSCI

From Figure 2 it can be said that the growth of demand for cyber security product from 2016 to 2025 will be increase by $ 38 billion ($80 billion-$42 billion) i.e. on an average $ 3.8 or $ 4 billion per year ($ 38÷10 years).

Similarly projected growth for cyber security service market from year 2015 to year 2025 is as follows:

Figure 3: Growth and Expected Growth in Cyber Security Service Market



Source: GROWING CYBER SECURITY INDUSTRY Roadmap for India by NASSCOM and DSCI

The growth of demand for cyber security services seems to will be greater than cyber security product by the year 2025 growing from $ 46 billion in 2016 to expected $ 98 billion in 2025, i.e. at annual average growth of
$ 5.2 billion[($ 98 – $ 46 billion) ÷ 10 years].

The Cyber Security Industry currently constituted by six different clusters as per the report of GROWING CYBER SECURITY INDUSTRY Roadmap for India by NASSCOM and DSCI, containing different numbers of companies (small and large). These clusters either offer cyber security product or cyber security services having different market focus i.e. either focusing domestic market or foreign market. An overlook on these clusters, their offering and focus may give an insight about market competition.

Table 4: Table Disclosing Information about Clusters of Cyber Security Companies

Name of Clusters	Number of Companies	Country of Origin	Product /Service focus	Target market
Greater Baltimore Cluster	More Than 10000	United States	Services	Domestic Market
Hague Security Delta (HSD)	More Than 400	Netherlands	Products	Foreign Market
Beersheva	250	Israel	Products	Foreign Market
Barlin-Brandenburg Cluster	More Than 120	Germany	Products	Domestic Market
Ottawa Security Cluster	More Than 180	Canada	Services	Both domestic & Foreign Market
UK Cyber Security Cluster	More Than 600	United Kingdom	Services	Both domestic & Foreign Market

Source: GROWING CYBER SECURITY INDUSTRY Roadmap for India by NASSCOM and DSCI

Table 4 gives an idea about market completion both in respect of services and products also number companies targeting domestic and foreign markets. It can be seen that most of the company's focus on Cyber security Services (More than 10000). On the other hand product market is targeted only by 800 or more companies. Different clusters focus on different target markets, it should be mentioned that the biggest cluster that is Greater Baltimore Cluster containing more than 10000 companies targets domestic market only.

At the final phase of analysis, a comparative study should be conducted about cyber security capacity assessment between countries with advance cyber security Industry and countries which have potentials to rise in cyber security Industry. The cyber security capacity depends upon five different factors they are Eco-system (Financing, Domestic market, talent), Infrastructure, Enablers (Research and development, incentives and support of government) and Mechanism (process of development of an industry).

For capacity assessment four different countries are chosen, that are United States (Advance country), Netherlands (Advance country), India (developing country) and Brazil (developing country). The factors mentioned above are considered as scale for capacity assessment; each factor scale will have 20 points. The countries having greater capacity will get more points on factor scale. Data available in respect shows that the above mentioned countries have following points on each factor scale:

Table 5: Table of Cyber Security Capacity Assessment

	Factor Scale For capacity Assessment (Max 20 points each)			
Countries	**Eco- system**	**Infrastructure**	**Enablers**	**Mechanism**
United States	17	18	20	18
Netherlands	13	20	15	20
India	07	12	06	12
Brazil	06	13	03	12

Source: GROWING CYBER SECURITY INDUSTRY Roadmap for India by NASSCOM and DSCI

The original Scales only have 4 points but for proving clear picture of the differences between advance countries and developing countries scale points are raised to 20 and accordingly scores are also revised by using formula:

$$: \frac{Original\ score}{orinal\ total\ scale\ point\ (4)} \times 20$$

From the data of Table 5 it becomes clear that the developing countries fall behind almost in every aspect of capacity assessment of Cyber Security Industry but in respect Eco-system along with Enablers mismatch is greater than Infrastructure and Mechanism.

Analysis of cyber crime cost and market for cyber security industry is concluded at this point and in the following section findings of above analysis will be discussed.

FINDINGS

After going through above analysis there are many different facts that are unveiled about cyber crime and its economic impact which are discussed below:

1. The first fact founded about cost of cyber crime is that cyber crime's cost is gradually increasing even in the developed countries, for instance the analysis of Table 1 shows that cost of cyber crime in USA in the year 2015 was 15.42 million USD and in the following year (2016) it was 17.36 million USD. Similarly, in every developed and developing countries there is an increment in cyber crime cost in the year 2016 as compared to the year 2015 as shown by Table 1, increment varies from 0.34 million USD (Germany) to 1.94 USD (America). Lift in cyber crime rate may be due to development of information technology, expansion of internet connectivity which is further confirmed by various reports related to cyber crime.
2. If, Table- 2 (Table Showing Growth Rates in Cost of Cyber Crime) is observed carefully it can be noted that as compared to the developed countries, the growth in the cost cyber crime is fur greater in developing countries. Take the example of USA, Australia and Japan, these developed nations observe high growth rates in cyber crime cost in 2016 as compared to the year 2015 i.e. 12.58%, 23.91% and 23.20%, respectively, on the other hand Brazil which is a developing country observe 36.88% growth in cyber crime cost during 2016 compared to year 2015. The experts in many reports mentioned that developing nations observe high cyber crime cost because of lack of investment in security measures, easy access by cyber criminals due to weak cyber defence, low level of user awareness as they are just introduced to online facilities and so on and it is ensured by the above mentioned differences in growth rates in cyber crime cost.
3. The external consequences of cyber crime are information loss, business disruption, revenue loss, equipment damage and other kinds of losses out of these kinds of losses the loss of information considered to be the greatest lost, when converted into global data almost contribute 40% (156 billion out of 400 billion USD) of total cost of cyber crime in 2016. However, there are many different cost which can't counted properly such as loss of reputation, Intellectual property theft and so on because of lack of proper accounting process.
4. A deeper probe into the cost of cyber crime from organisational point of view gives more clarity about cost of cyber crime. It seems that the external consequences of cyber crime are the results of various cyber attacks that are faced by organisations, these attacks include Malicious insiders, Malicious code, Web-based attacks, Phishing & Social Engineering and so on as mentioned in the analysis, more importantly, each of these attacks have different resolving time. According to the reports greater the resolving period greater will be the cost. From this point of view and analysis it can be said that malicious insiders cost highest i.e. 111.23 billion USD out of 400 billion USD when converted to global data as it has highest resolving period that is 52 days approx.
5. The above finding is also reflected by external consequences as Malicious insiders and Phishing & Social Engineering leads to compromise of information which cost most to an organisation as suggested by the analysis and both have higher resolving periods that are 52 days and 20 days respectively.
6. However, there is a difference in net loss due to cyber attacks and the gross loss, net loss means the volume of information which is actually utilized by cyber criminals and gross loss connotes the volume of data lost or theft by criminals this cost differences are driven by the problem resolving process which include different steps including detection, recovery, containment, investigation, incident management and ex-post response. It can be said from the data presented that most of the companies allocate highest funds for problem detection i.e. 33% of the total funds available for cyber security followed by recovery 22%, containment-18%, investigation-13%, incident management-9% and ex-post response-5%. The fund allocation pattern visualize that diagnosis of cyber crime cost more to the companies then containment and incident management because these steps need services of external cyber experts.
7. The opportunity presented by cyber security problems are also blooming along with the cyber crimes as disclosed by figure 2 and figure 3. Market for cyber security products in 2016 worth 42 billion USD and for cyber security services 46 million USD which are projected grow to 80 billion USD and 98 billion USD respectively by 2025 and together, 178 billion USD.
8. As it can be seen from above discussion that expected demand in future for cyber security services (98 billion by 2025) will surpass the cyber security product market (80 billion by 2025), therefore it is advisable to the economies to target for producing cyber security services. This is further supported by market competition, Table-4 points out that there are more than 11000 companies working under different clusters opted for production of cyber security products or providing cyber security

services. Out of these companies, most of the firms works under Greater Baltimore Cluster containing 10000+ firms originated from USA and its aim is to provide cyber security services but the noticeable thing is that these companies only aims domestic market so rest of the world is open for others to explore. Only two other clusters, currently provide cyber security services in different countries that are Ottawa Security Cluster and UK Cyber Security Cluster but these two clusters contains respectively 180 and 600 companies only.

9. There are hindrances for the potent developing economies in the ways of exploring the cyber security market as indicated by Table 5, according to Cyber Security Capacity Assessment scale (modified) of GROWING CYBER SECURITY INDUSTRY Roadmap for India by NASSCOM and DSCI, developing countries fall fur behind in respect of Eco- system (India 07 out of 20, Brazil 06 out of 20) and Enablers (India 06 out of 20, Brazil 03 out of 20) from developed nations (USA 17 and 20 out of 20 respectively). Eco system includes aspects like Financing, Domestic market, individual talent. Again, Enablers includes Research and development, incentives and support of government, therefore it can be said that main challenge for the potent developing nations like India and Brazil is financing cyber security firms because financing will work as incentive for research and development in cyber security sector and give more scope to the firms to explore domestic market. Apart from financing security firms, investments should also be made in improvement of education system to nurture and identify individual talents.

There is inflation in cost and losses due to cyber crime in recent years which is an undeniable fact. However, at the horizon there is a ray of opportunity for rising economies to gain prosperity from this dark cloud if, plans are formulatedand executed properly as well as educational melioration are introduced, the growing demand for cyber security services and products along with statistics of expected market for these in coming years do not indicated otherwise.

CONCLUSION

Conclusion to this analysis drawn with the hope that cyber crimes will no longer remain threat to this world when the nations join their hands together to restrain it enabled by the corporate houses seeking to protect the nations, economies and individuals from cyber crime. For protecting nations, economies and individuals, the corporations should always remain one step ahead of the cyber criminals. Only time will give answer whether this hope will materialise or not.

REFERENCES

1. *Friedrich, Mike and Starlin, Jim, Iron Man (February 1973), Volume 55, Marvel Comics, USA. http:// en.m.wikipedia.org/wiki/Thanos.*
2. *Finger, B., Kane, B. and Robinson, J., Batman (April 1940), First issue, DC Comics. http://en.m.wikipedia.org/wiki/ joker.*
3. *Lee, Stan and Kirby, Jack, The Avengers (September 1963), Volume 01, Marvel Comics, USA. http:// en.m.wikipedia.org/wiki/Avengers.*
4. *Graham, Luke (2017) 'Cybercrime costs the global economy $ 450 billion: CEO' CNBC (online) 7 February. http://www.cnbc.com/2017/02/07/cybercrime-costs-the-global- economy-$450- billion-CEO. html (Accessed 15 July, 2017)*
5. *Ponemon Institute (2016). 2016 Cost of Cyber Crime Study & the Risk of Business Innovation. Traverse City, USA. Retrieved from http://www.i2.cc-inc.com/Marketing/ Landing.*
6. *Center for Strategic and International Studies (June 2014). Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II, Washington, DC. http:/ /www.mcafee.com/reports.*
7. *NASSC OM and DSCI (2016). GROWING CYBER SECURITY INDUSTRY Roadmap for India, Sector 126 Noida, Uttar Pradesh, India. http://beta.dsci.in/sites/ default/files.*