International Journal of Research
Available at https://edupediapublicat ions.org/ journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Cybercrime: A Nightmare for Economics

Ruby

Assistant Professor of Economics, S.G.G.S Khalsa College, Mahilpur, Hoshiarpur, Punjab, India

"We are vulnerable in our military and in our governments, but I think we are most vulnerable to cyber attacks commercially. This challenge is going to significantly increase. It is not going to go away."

-Michael Mullen

Abstract

In the era of artificial intelligence, virtual space occupies a prominent place almost in every walk of life. It is absurd to imagine a life without digital means. However, the ever growing dependence on such facilities has grown the bugbear of cybercrime and cyber terrorism. The impression of cybercrime is getting bigger across the world economies. It is one of the top challenges faced by many eminent organizations around the world. With the changing pattern of the technological attacks, there is augmentation of threats to the different economies of the world. Most of the economies which lack resources, expertise and have low internet penetration rates are prone to these cyber attacks. This paper aims at examining the economic impacts of cybercrimes along with the reasons for its growth at the global level. The volume of cyber crimes is growing by leaps and bounds which have globally made alarming damages to the economic, government, financial and different organizational structures. Combating Cybercrime has been gaining much importance so that it may not go uncontrollable in the upcoming years.

Keywords: Cybercrime, Threat, Organization, Economic, Cyber security, Combat

INTRODUCTION

The most prevalent thing that has been emerged as revolutionary in the 21st century is – The Internet. It has become an opulent tool for the major organizations as well as individuals all around the world. It has integrated the different nations of the world to become a global village. It has been termed as a household commodity as in today's era, it is impossible to imagine a life without internet. Several opportunities have been offered cheaply to the governments, businesses, military, associations and individuals through the internet. However, the internet is a double-edged sword. On one hand, it has contributed enormous in spreading the affirmative values around the world. While on the other hand, it is posing some serious threats to the world which can play havoc in the near future.

Cyber crime is one of the most alarming problems of the world which is unlikely to stop. Everybody has heard something of it, yet is not fully aware about it. Even half of such crimes go unnoticed or unreported which create problems in a cumulative manner. The ever growing economic impacts of cyber crime has been gaining attention of several organizations as well as individuals so as to combat it for the purpose of attaining development without any major disruptions.

International Journal of Research
Available at https://edupediapublicat ions.org/ journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

WHAT IS CYBERCRIME?

The concept of cybercrime is not basically different from the concept of conventional crime. Cyber crime is derived from two words "cyber" and "crime". Cyber refer to any activities either sales or transaction of services in the cyber space while crime are unacceptable activities. When join together, it means all fraudulent, illicit and unacceptable activities related to cyber.[1]

Cyber crime didn't become profound problem overnight. It has been grown and spring up as computing became easier and less expensive. The first recorded cybercrime is said to be in 1820. However, the history of cybercrime is to be found in 1960s when computers were large mainframe systems. At that time, mainframes were not easily accessible which made cybercrime "insider cybercrimes."Actually, in the 1960s and 1970s, the cybercrime, which was "computer crime" in fact, was different from the cybercrime we faced with today, because availability of Internet was restricted within some sections (e.g. US military) in that era. In the following decades, the increasing of computer network and personal computers transformed "computer crime" into real cybercrime. In fact, the former descriptions were "computer crime", "computer-related crime" or "crime by computer". With the pervasion of digital technology, some new terms like "high-technology" or "information-age" crime were added to the definition. Since Internet was invented, other new terms, like "cybercrime" and "net" crime became the order of the day as people began to exchange information based on networks of computers, also keep data in computer rather than paper.[2]

DEFINITIONS

Each organization and the authors of each piece of legislation have their own ideas of what cybercrime is—and isn't. These definitions may vary a little or a lot.[3]

Cybercrime in a broader sense computer-related crime: any illegal behaviour committed by means of, or in relation to, a computer system or network. There was not even an agreed definition of cybercrime. Some of the definitions are listed below:

- The European Commission issued a Communication towards a general policy on the fight against cyber crime. It proposed a threefold definition:

1. Traditional forms of crime such as fraud or forgery, though committed over electronic communication networks and information systems;
2. The publication of illegal content over electronic media (e.g. child sexual abuse material or incitement to racial hatred);
3. Crimes unique to electronic networks e.g. attack against information systems, denial of service and hacking.

- Cyber crime is committing crime through the internet, it does not necessarily mean it have to happen inside the cyber cafe, you can have your laptop, you have your modern in your house and you commit crime; hack people's mail. That is cyber crime. Cyber crime is any crime committed via the internet, so people watching pornography is committing crime, those people sending fraudulent e-mail that is phishing is also committing crime. And those trying to download academic material, text books or soft ware from the internet without paying for it are also committing crime. So you can see that everybody is involved in this crime.[1]

- Cybercrime can be generally defined as a subcategory of computer crime. The term refers to criminal offenses committed using the Internet or another computer network as a component of the crime. Computers and networks can be involved in crimes in several different ways:
  - The computer or network can be the tool of the crime (used to commit the crime)
  - The computer or network can be the target of the crime (the "victim")
  - The computer or network can be used for incidental purposes related to the crime (for example, to keep records of illegal drug sales)[3]
- At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus:

a. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.[3]

CAUSES OF GROWTH IN CYBERCRIME: - Cyber crime is the order of the day. The amount cybercrime activities like Phishing, piracy, spamming, malwares, pornography has been going out of control. The numbers of such activities are on hike. The FBI estimated there were 4,000 ransomware attacks everyday in 2016.[4]

The following table delineates the growth of cybercrime activities day by day.

Table 1: Estimated daily cybercrime activity[4]

CYBERCRIME	ESTIMATED DAILY ACTIVITY
Malicious Scans	80 billion
New Malware	300,000
Phishing	33,000
Ransomware	4,000
Records lost to hacking	780,000

There are many motivating forces which are responsible for the multiplication of cyber crimes all over the world. Some of them are listed below:

- **Easy accessibility to the Internet: -** The foremost reason for increasing cyber attacks at large scale is the easy access to internet. Today almost everyone in industrialized countries has access to computer technology; children learn to use computers in elementary school, and people who can't afford computers of their own can use PCs in public libraries or on college campuses for free, or they can rent computer time at business centers or Internet cafés. Applications are "point and click" or even voice-activated; it no longer requires a computer science degree to perform once-complex

tasks such as sending e-mail or downloading files from another machine across the Internet[3] , making cyber criminals to do their crimes without any interruption.

- **Unemployment: -** It has been found in most of the studies that the poor economic conditions, lack of financial resources associated with high rate of unemployment leads to cybercrimes in most of the countries.
- **Rich Syndrome:** - In 2014, CSIS estimated that cybercrime costs the world's economy almost $500 billion, or about 0.7% of global income. Currently, it has estimated that cybercrime may now cost the world almost $600 billion or 0.8% of global GDP. That is more than the income of all but a handful of countries, making cybercrime a very lucrative occupation.[4]
- **Quick adoption of new technologies:** - New technologies make people and companies more efficient and effective, cybercriminals included. Cybercriminals adopt new technologies at a fast pace. If we talk about today then Bitcoin and other digital currencies are both targets for theft and a means of payment and money transfers for cybercriminals.[4]
- **Tracing Issues: -** One major reason for the increase in cybercrime is difficulty in tracing the action and the person behind it.The anonymization in this occupation gives a wave this evil as cyber attacks can be conducted easily from any part of the world targeting any number of populations without revealing the identity of the criminal.
- **Poor legislation: -**Lack of law enforcement agencies and inadequate legislation make cybercriminals more powerful in committing the crimes without any disruptions.
- **Defective socialization:** -It has been seen that the framework of the society affects the eruption of crimes in one way or other. If a country has negative role models, corrupt politicians and aimless youth, many evils can be traced in such a place. Nigeria can be taken as the best example for it where the quantum of cybercrimes is increasing because of such activities.

EFFECTS OF CYBERCRIMES ON DIFFERENT ECONOMIES: - The cost of cybercrimes to the economies can be qualitative as well as quantitative. It has the ability to make hundreds of millions of people victims. A statement on cybercrime made by Robert Muller (FBI Director, 2012) shows how widespread the effects of cybercrimes are

"There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category; those that have been hacked and will be again."

Cybercrime may shatter any economy to severe extent. Cyber crime is posing some serious problems to all the aspects of a nation's growth. It may slow a country's pace of innovation, create social costs and distort trade. As the economy make progress, its reliance on internet also increases, so as the threat of cyber attacks and cyber espionage. It can be considered as that rounded error in any economy which may prove detrimental for its growth. The several economic effects of cyber crime are discussed as follows:

- **Repudiate National Income: -** Cybercrime may take a huge chunk of the income of different economies. CSIS have found that the richer the country, the greater its loss to cybercrime is likely to be. The relationship of the developing countries to cybercrime is complex. The countries with the greatest loss of their national income are those that are digitalized but not yet fully capable in cyber security. The Table 2 gives us a idea of cybercrime loss of income.

Table2: Regional distribution of Cybercrime 2017[4]

Region (World Bank)	Region GDP(USD Trillions)	Cybercrime Cost(USD billions)	Cybercrime Loss (%of GDP)
North America	20.2	140 to 175	0.69 to 0.87%
Europe and Central Asia	20.3	160 to 180	0.79 to 0.89%
East Asia & the Pacific	22.5	120 to 200	0.53 to 0.89%
South Asia	2.9	7 to 15	0.24 to 0.52%
Latin America and the Caribbean	5.3	15 to 30	0.28 to 0.57%
Sub- Saharan Africa	1.5	1 to 3	0.07 to 0.20%
MENA	3.1	2 to 5	0.06 to 0.16%
World	**$75.8**	**$445 to $608**	**0.59 to 0.80%**

- **Mislead Youth: -** Youths are the mirror of every society. The increasing number of youths in any nation gives that nation a power to utilize them for making economic development in an efficient way. But if the youths of any country are misguided then it can hinder the growth of that nation too. It was found that the majority of the individuals involved in Cyber crimes falls in 18-30 age category which is not less than an evil for any country.
- **Loss of confidential Business Information: -**The most important area for loss of cybercrime is the theft of business-confidential information. It is difficult to accurately estimate the losses. Cyber attacks can take a company's product plans, its research results, and its customer lists today, and the company will still have them tomorrow. The company may not even know that it no longer has control over that information
- **Rattle the Banking system of the country: -** A sound banking system is the pre condition for the development of any economy. Cyber espionage has not left this sector also. Banking system has been remained the target of most of the cybercriminals for many years. Cyber crimes cost many hundreds of millions of dollars every year. One report says that banks spend three times as much on cyber security as non- financial institutions.[4]
- **Drive away Investors: -** Another consequence of cyber crime is that it will drive away investors because most of the things are done electronically and if someone can attack your database, then he has everything about you at his disposal.[1] It may result in slowing down the pace of the development in the concerned nation due to lack of foreign investment.
- **Intellectual property theft: -** Sometimes cybercrime causes theft of intellectual property like patent, copyright trade which causes huge loss to the concerned organization. The stolen information is offered for sale on the dark web which will create problems in near future.
- **Reduced Productivity: -** There is a huge amount of loss through reduced productivity especially when people find themselves spending more time

preventing, protecting themselves from the effects of cyber crime, rather than engaging in more productive activities.

- **Tarnish the reputation of concerned country:** - Cybercrime may worldwide present the nation in a wrong way. That is why the countries with high cybercrime activity are seen in a negative manner.

Besides this cyber crime has also its impact on other activites like cyber terrorism, unemployment and financial growth, lack of organizational competition and time wastage which may not be stimulating for the economic development.

Conclusion

Cyber crime can hamper the economic growth to a great extent. That is why globally it has become the hot topic for the debate. Combating cybercrime has become the top most priority of many nations at the global level because of its grave consequences. It is vital for the governments as well as business organizations to adjust their legal and regulatory framework so as to tackle this menace and put it in to halt.

REFRENCES

1. B. Okeshola, F., & K. Adeta, A. (2013). *The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria*. *Aijcrnet.com*. Retrieved 6 April 2018, from http://www.aijcrnet.com/journals/Vol_3_No_9_September_2013/12.pdf
2. Olusola, M., Samson, O., Semiu, A., & Yinka, A. (2013). Impact of Cyber Crimes on Nigerian Economy. *The International Journal Of Engineering And Science (IJES)*, *2*(4), 45-51.
3. Shinder, D. (2002). *Scene of the Cyber crime: Computer Forensics Handbook*. (1st ed.). USA.: Syngress Publishing, Inc. 800 Hingham Street Rockland, MA 02370
4. McAfee. (2018). *Economic Impact of Cybercrime - No Slowing Down*. CSIS. Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime