CYBER CRIME AND ITS IMPACT ON THE GLOBAL ECONOMY

***** *Dr.Saira Siraj Gori*[1]**

Abstract

New technologies create new criminal opportunities and crimes but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Cybercrime ranges across a spectrum of activities. Criminals' activities online can have far-reaching effects. Criminals take advantage of technology in many different ways. The Internet, in particular, is a great tool for scammers and other miscreants, since it allows them to ply their trade while hiding behind a shield of digital anonymity. Cyber crime affects society in a number of different ways, both online and in the offline world. Crime is a common word that we always heard in this globalization era. Crime and criminality have been associated with man since long time ago. There are different strategies practices by different countries to contend with crime. It is depending on their extent and nature. Nation with high index of crime cases cannot grow or develop well. It can contribute to negative impact in term of social and economic development. Cybercrimes are responsible for the interruption of normal computer functions and has been known to cause the downfall of many companies and personal entities and as per the latest report of MacAfee and IC3 the cost of cyber crime for the global economy has been estimated at $445 billion (£266 billion) annually. Hence this research paper aims to discuss various facets of Cybercrimes, its effects on global economy, laws governing them and its prevention procedures.

Introduction

Crime and criminality have been associated with man since long time ago. There are different strategies practices by different countries to contend with crime as it directly affects the development of any nation. Cyber crime is a new type of crime and the outcome of latest Science and Technology. Cybercrime can be defined as any violence action that been

[1] Assistant Professor of Law, Gujarat National Law University,Attalika Avenue,Knowledge Corridor, Koba Gandhinagar- 382007, Gujarat, INDIA

conducted by using computer or other devices with the access of internet. This action can give harmful effects to other. There are many factors that causes the statistic of cyber crime cannot be detected or analyzed i.e. the aggressive development of today's technology, lack of necessary technical expertise to deal with criminal activity and once criminal activity has been detected many businessmen are reluctant to lodge a report because they afraid of adverse publicity, embarrassment, loss of public confidence, investor loss, or economic repercussions. Due to these factors, the actual number of cyber crime cases and the statistic of cyber crime in many countries cannot be recorded accurately. This research paper aims to discuss the various facets of Cybercrimes, global economy and cyber crime prevention procedures.

Cyber Crime and its Classification

There are three major categories of cyber crimes which are crimes against the person, property and the government. The first category of cyber crimes is cyber crime against person. Cyber crime against person is included harassment via email or cyber-stalking. Cyber Stalking means following the moves of an individual's activity over internet. It can be done with the help of many protocols available such at e- mail, chat rooms, user net groups while, harassment can be included sexual, racial, religious, or others. This crime usually happens to women and teenager. Second category of cyber crimes is that of cybercrimes against all forms of property. These crimes include computer vandalism by transmission of harmful programmes to other computer through internet. The other example is cyber criminal can take the contents of individual bank account. One widespread method of getting people's bank account details is the money transfer email scam. People receive emails requesting help with transferring funds from another country. Hacking into company websites is property trespass, and stealing information is property theft. Internet time theft also one of the cyber crime against property. It is done by an authorized person in the usage of the internet hours which is actually paid by another person.

The third category is cyber crimes against governments constitute another level of crime. Cyber terrorism is the most serious type of crime in this category. Hacking into a government website, particularly the military sites, is one manifestation of cyber terrorism. The example of cyber crime against government is web jacking. By web jacking, hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

Cyber crimes are everywhere, can happen to anyone, in any time. Cybercrimes are responsible for the interruption of normal computer functions and has been known to cause the downfall of many companies and personal entities. Cyber crime has been estimated to cost the global economy in excess. The cost of cyber crime for the global economy has been estimated at $445 billion (£266 billion) annually. Cyber espionage and stealing individuals' personal information is believed to have affected more than 800 million people during 2013. Financial losses from cyber theft could cause as many as 150,000 Europeans to lose their jobs, according to a report conducted by internet security company McAfee. Cyber crime damages trade between nations, competitiveness, innovation, and global economic growth, and slows the pace of global innovation. McAfee is calling for governments to begin a serious, systematic effort to collect and publish data on cybercrime to help countries and companies make better choices about risk and policy. Studies estimate that the internet economy annually generates between $2 trillion and $3 trillion, a share of the global economy that is expected to grow rapidly. Based on Center for Strategic and International Studies (CSIS) analysis, cybercrime extracts between 15 per cent and 20 per cent of the value created by the internet. The figures do not come as a surprise to security professionals and big businesses, said Mark Sparshott, EMEA director of security firm Proof Point.

He said the attraction of cybercrime to many criminals was due to its relatively low level of risk. "The volumes of attacks are increasing because it is a profitable business model for organised crime," he said. "With cyber crime there is no risky getaway because the attack is routed through hundreds or thousands of PCs in dozens of countries, making it almost impossible to trace. The internet makes most attacks anonymous and untraceable and that is really attractive to cybercriminals.”

Raj Samani, EMEA Chief Technology Officer for McAfee, agreed. “It is clear that cyber crime has a real and detrimental impact on the global economy. Over time, cyber crime has become a growth industry; the returns are great, and the risks are low,” he said.

"As more businesses move online and more consumers connect to the internet, the opportunities for cybercrime will only grow, making it imperative that countries work together now to proactively tackle cyber crime.”

In our modern technology-driven age, keeping our personal information private is becoming more difficult. The truth is, highly classified details are becoming more available to public databases, because we are more interconnected than ever. Our data is available for almost anyone to sift through due to this interconnectivity. This creates a negative stigma that the use of technology is dangerous because practically anyone can access one's private information for a price. Technology continues to promise to ease our daily lives; however, there are dangers of using technology. One of the main dangers of using technology is the threat of cybercrimes.

Common internet users may be unaware of cybercrimes, let alone what to do if they fall victim of cyber attacks. Many innocent individuals fall victim to cybercrimes around the world, especially since technology is evolving at a rapid pace. Cybercrimes are any crimes that cause harm to another individual using a computer and a network. Cybercrimes can occur by issues surrounding penetration of privacy and confidentiality. When privacy and confidential information is lost or interrupted by unlawfully individuals, it gives way to high profile crimes such as hacking, cyber terrorism, espionage, financial theft, copyright infringement, spamming, cyber warfare and many more crimes which occur across borders. Cybercrimes can happen to anyone once their information is breach by an unlawful user.

Cybercrimes create an overwhelming task for law enforcement bureaus since they are extremely technological crimes. Law enforcement organizations must have individuals trained in computer disciplines and computer forensics in order to accurately investigate computer crimes or cybercrimes that have been committed. Additionally, many states must modernize and generate legislation, which disallows cybercrimes and outlines suitable penalties for those crimes. Cybercrimes will likely become more frequent with the arrival of advance technologies. It is important that civilians, law officials, and other associates of the justice system are well-informed about cybercrimes in order to diminish the threat that they cause.

Understanding the threat of cybercrimes is a very pertinent issue because technology holds a great impact on our society as a whole. Cybercrime is growing every day because since technological advancing in computers makes it very easy for anyone to steal without physically harming anyone because of the lack of knowledge to the general public of how cybercrimes are committed and how they can protect themselves against such threats that cybercrimes poses.

Cyber Crime and Global Economy

Recent studies on the evolution of principal cyber threats in the security landscape. They present concerning scenarios, characterized by the constant growth of cyber criminal activities. Even though the level of awareness of cyber threats has increased, and law enforcement acts globally to combat them, illegal profits have reached amazing figures. The impact to society has become unsustainable, considering the global economic crisis. It's necessary to work together to avoid the costs the global community suffers, which we can no longer sustain. The risk of business collapse is concrete, due to the high cost for enterprises in mitigating counter measures, and the damage caused by countless attacks. In this article, we'll quantify the economic impact of cybercrime by highlighting the main trends in the criminal ecosystem that concerns the security community.

Principal security firms which observe and analyze the incidents occurred to their clients has provided estimates of the annual loss suffered by enterprises. Dozens of billion dollars are eroding their profits. If we extend the effects of cybercrime to government circles, public industry and the entire population, it's easy to assume that the amount of damage reaches several hundred billion dollars. In many cases, that estimate can be misleading. That's because there were still too many companies that fail to quantify the losses related to cybercrime. In some cases, they totally ignore that they're victims of attacks. The majority of estimates relied on a survey, and loss estimates are based on raw assumptions about the magnitude and effect of cyber attacks to provide an economic evaluation. Cyber criminal activities are increasing by incidence in a scenario made worse by the economic crisis. We also face tightened spending by the private sector, and reduced financial liquidity. Nearly 80% of cybercrime acts are estimated to originate in some form of organized activity. The diffusion of the model of fraud-as-service and the diversification of the offerings of the underground market is also attracting new actors with modest skills. Cybercrime is becoming a business opportunity open to everybody driven by profit and personal gain. Cybercrime activities are globally diffused, financially-driven acts. Such computer-related fraud is prevalent, and makes up around one third of acts around the world. Another conspicuous portion of cybercrime acts are represented by computer *content*, including child pornography, content related to terrorism offenses, and piracy. Another significant portion of crime relates to acts against confidentiality, integrity and accessibility of computer systems. That includes illegal access to a computer system, which accounts for another one third of all acts. It's clear that cyber crime is influenced by national laws and by the pressure and efficiency of local law enforcement.

When assessing the effect of cybercrime, it's necessary to evaluate a series of factors:

- The loss of intellectual property and sensitive data.
- Opportunity costs, including service and employment disruptions.
- Damage to the brand image and company reputation.
- Penalties and compensatory payments to customers (for inconvenience or consequential loss), or contractual compensation (for delays, etc.)
- Cost of countermeasures and insurance.
- Cost of mitigation strategies and recovery from cyber attacks.
- The loss of trade and competitiveness.
- Distortion of trade.
- Job loss.

To better understand the effect of cybercrime on a global scale. The study, titled The 2013 Cost of Cyber Crime Study, provides an estimation of the economic impact of cybercrime. It’s sponsored by HP for the fourth consecutive year. It reveals that the cost of cybercrime in 2013 escalated 78 percent, while the time necessary to resolve problems has increased by nearly 130 percent in four years. Meanwhile, the average cost to resolve a single attack totaled more than $1 million. The frequency and cost of the cyber attacks increased in the last 12 months. The average annualized cost of cybercrime incurred by a benchmark sample of US organizations was $11.56 million. That’s nearly 78% more than the cost estimated in the first analysis conducted four years ago. In spite of improvements in defense mechanisms and the increased level of awareness of cyber threats the cyber crime ecosystem is able to adopt even more sophisticated cyber attack techniques. The cybercrime industry has shown great spirit, and the adaptive capacity to respond quickly to countermeasures has been taken by the police.

Laws of cybercrimes

In this section of this paper the author discusses Laws and legislation that governs cybercrime worldwide. This section will highlight some laws and let people know some of the laws that are out there to protect them and some of the amendments to these laws to keep up with the different advancement in technology**.**

- **United States**

In the United States, the legislation concerning cybercrimes differs from state to states. In other words, each state has their own way of dealing with different types of cybercrimes being committed on a daily basis. This paper discusses a few of the many Acts and legislations available in the United States that govern cybercrimes.

Congress combats cybercrimes by enacting several laws such as The Computer Fraud and Abuse Act of 1984 (CFAA). At the time such it was difficult for federal law enforcers to use such legislation to indict anyone because of the difficulty of writing such an Act.The Act however requires major proof that personnel suspect has or have accessed computers without authorization which in turn can be a major limitation. In 1994, the Act was altered again to meet new complications that arose such as malicious codes which at the time were bugs, viruses, worms and other programs that were intended to harm or modify data on a computer. After applying it was now equipped to prosecute any individuals who broke the law in terms of using programs with the intent to reason harm to the computer or the use of structures without the information of the lawful owners of that computer.

In 1996, The National Information Infrastructure Act (NIIA) was passed and it added onto the CFFA, which include the unlawful access to a threatened computer in excess of the parties' consent, which means that it became illegal to view info on a computer without authorization of any kind. Another Act formed was the Electronic Communication Act which was passed in 1986. It was an alteration to the federal monitor law. The Act made it impossible to take hold of stored or transferred electronic communication without permission. The Electronic Communication Act made it unlawful to access specific forms of communication content even from government bodies which can be provided by the ISP without going through the proper channels to obtain legal procedures to provide such information.

In 1998, The Digital Millennium Copyright Act was passed. This Act basically altered Title 17 of the United States code to WIPO (World Intellectual Property Organization) which was to combat with new technology. This Act excludes the modification of information of inventor, the terms and environments for use of such set work or the purpose of its intent. The act provides a way in which civil preparations can be applied as well as criminal punishments for violation.

In 2002, Cyber Security Enhancement Act was passed. The Act helped law agencies to increase punishments which were set out in the CFFA which in turn means hasher punishments for individuals who willingly committed computer crimes in the end result of even bodily injuries etc. Those punishments can range from 5 to 20 years, or even life imprisonment.

- **India**

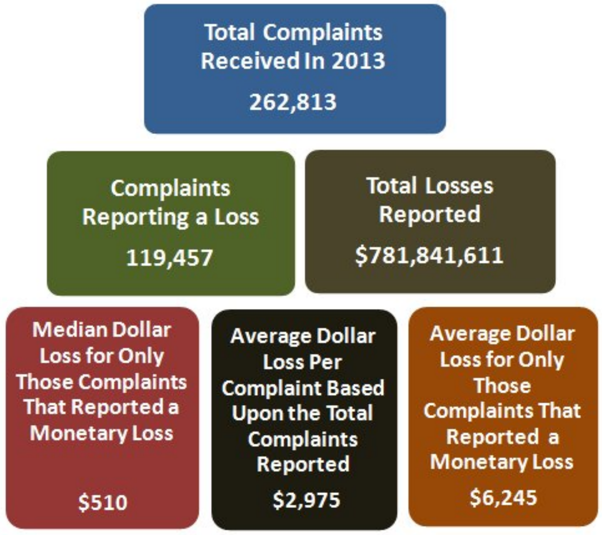
The Information Technology (Amendment) Act 2008 deals with the various cybercrimes. From this Act, the important sections are Ss. 43,43-A,65,66,67. Section 43 which explain and enforce the unlawful access, transferring, virus outbreaks causes harm for example Stuxnet worm, DOA, intrusion with the service availed by anyone. However, other sections combats against source files via workstations being altered which can end result imprisoned up to 3 year or be fined stated by Section 65 whereas in Section 66 it pretends to consent access with systems, crimes that go against criminals can be imprisoned up to 3 years or fine which goes up to 2 lakh rupees or both.

- **Internationally**

All laws aren’t the same in many countries especially when it comes to cybercrimes. For different countries have specific laws governing problems such as cybercrimes. For example, in some countries such as India accepted. The Information Technology Act which was passed and enforce in 2000 on Electronic Commerce by the United Nations Commission on Trade Law. However, the Act states that it will legalize e-commerce and supplementary modify the Indian Penal Code 1860, the Act 1872, the Banker’s Book Evidence Act1891 and the Reserve Bank of India Act 1934**.**

Recent Development: The IC3 report 2013

The IC3 analysts use automated matching systems to identify links and commonalities between numerous complaints and combine the respective complaints into referral groups for law enforcement. Of the 262,813 complaints received in 2013, 45.5 percent (119,457) reported financial loss.



Total Complaints Received In 2013 262,813

Complaints Reporting a Loss 119,457

Total Losses Reported $781,841,611

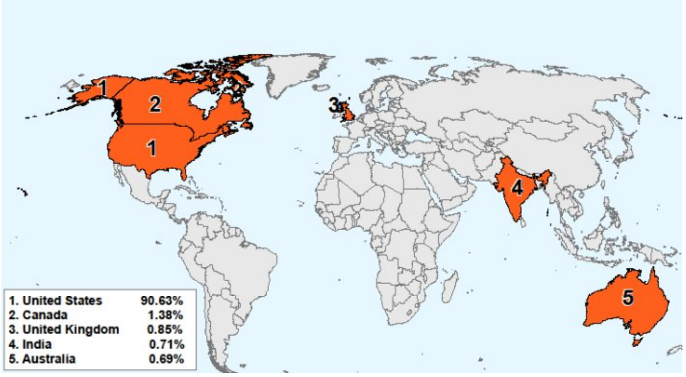
Median Dollar Loss for Only Those Complaints That Reported a Monetary Loss $510

Average Dollar Loss Per Complaint Based Upon the Total Complaints Reported $2,975

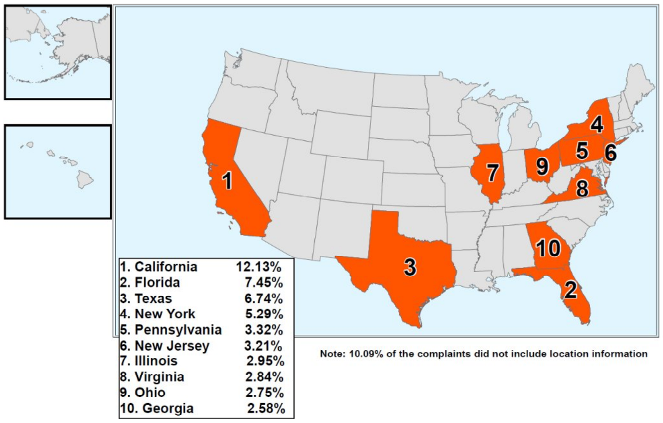
Average Dollar Loss for Only Those Complaints That Reported a Monetary Loss $6,245

The maps on the following page demonstrate the top five countries and the top 10 states ranked by the number of victim complaints reported to the IC3 during 2013.

Top Five Countries Ranked by the Total Number of Complaints Received by IC3 in 2013



Top Ten States Ranked by the Total Number of Complaints Received by IC3 in 2013



Note: 10.09% of the complaints did not include location information

Conclusion

Cyber crimes will always be an ongoing challenge despite the advancements being made by numerous countries. Most countries have their own laws to combat cybercrimes, but some doesn’t have any new laws but solely relies on standard terrestrial law to prosecute these crimes. Along with outdated laws to combat cybercrime, there are still feeble penalties set in place to punish criminals, thus doing no major prevention of cybercrimes’ which affect the economy and people’s social lives on a large scale by those criminals. Consequently, there is a desperate need for countries on a global scale to come together and decide on what constitute a cybercrime, and develop ways in which to persecute criminals across different countries. It is recommend that until sufficient legal actions can be put in place where individual countries and global ways of persecution criminals, self-protection remains the first line of defense. The everyday individuals and businesses need to make sure they are educated on what to do in terms of prevent in becoming the next victim of cybercrimes. This basic awareness can help prevent potential cybercrimes against them. It is almost impossible to reduce cybercrime from the cyber-space. Looking back on the many different acts passed, history can be witness that no legislation has thrived in total elimination of cybercrime from the world. The only possible step is to make people aware of their rights and duties and further making more punishable laws which is more stringent to check them. Undoubtedly, the different Acts were and still are historical steps in the virtual world as we know it. This further suggests that there is a need to convey modifications in the Information Technology Act so it can be more effective to fight cybercrimes. Caution should be employed for the pro-legislation educational institutions that the requirements of the cyber laws are not prepared so rigorous that it may delay the growth of the commerce and demonstrate to be counter-productive to many. Remember, cybercriminals are evolving as well in terms of computer knowledge per technological advancement made.

Nevertheless, business should employ practices where their employees follow proper safety practices to ensure that integrity and confidentially of stored information is kept at all times to combat cybercrimes. Safety practices like ensuring that staying off game sites on company time where viruses can be downloaded, forwarding chain emails, leaving workstation unattended or password sharing over virtual mediums should be prohibited. With all these safety practices implemented, it can be said that the safety of many clients stored information is optimal.

References

1.http://resources.infosecinstitute.com/cybercrime-and-the-underground-market/

2.http://securityaffairs.co/wordpress/18206/cyber-crime/f-secure-threat-report-h3-2013.html

3.http://securityaffairs.co/wordpress/18517/cyber-crime/ponemon-2013-cost-of-cyber-crime.html

4.http://securityaffairs.co/wordpress/18475/cyber-crime/2013-norton-report.html

5.http://www.cybersec.kent.ac.uk/Survey1.pdf

6.http://www.emc.com/collateral/fraud-report/current-state-cybercrime-2013.pdf

7.https://www.icspa.org/uploads/media/ICSPA_Project_2020_%E2%80%93_Scenarios_for_the_Future_of_Cybercrime.pdf

8.http://www.theguardian.com/technology/2013/aug/23/cybercrime-hits-nine-million-uk-web-users

9.http://www.unodc.org/documents/organized-Crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

10.http://www8.hp.com/us/en/hp-news/press-release.html?id=1501128#.Ullf0VC-0uv

11.http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

12.http://securityaffairs.co/wordpress/17945/cyber-crime/enisa-threat-landscape-mid-year-2013.html#!

13. Center, Finjan Malicious Code Research. "Web Security Trends Report." Securing your web (1996-2008): 1-20.

14.Justice, Bureau of Justice Assistance U.S. Department of. "Internet Crime Complaint Center." 2009 Internet Crime Report (2008): 1-26.

15. Denning, D., *"Cyberterrorism"*, Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, 23 May 2000. (http://www.cs.georgetown.edu/~denning/infosec/cyberter ror.html)

16.National White Collar Crime Center. "IC3 2008 Internet Fraud Report." from Scribd: http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf

17.http://www.telegraph.co.uk/technology/internet-security/10886640/Cyber-crime-costs-global-economy-445-bn-annually.html

18. http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf