IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 7, July 2016

Cyber Crime: A Threat to the Nation and its Awareness

Monalisa Hati

XITE College, Jamshedpur, Jharkhand

Abstract: In the present day world. India has witnessed number of crimes with respect to computer and internet. The users of computer system and internet are increasing worldwide day by day and it is easy to access information easily within a few seconds. Cyber crime which is considered as illegal activity committed on the internet increasing day by day in spite of we are taking precautionary measures. In this paper I have discussed how cyber crime affects to the nation and the awareness and preventive measures by which one can overcome the threat.

Keyword: Cyber crime, precautionary measures

1. INTRODUCTION

The Internet in India is growing rapidly. It has given rise to new opportunities in every field one can think have been it entertainment, business, sports or education. There are two sides to a coin. Internet also has its own disadvantages. One of the major disadvantages is Cyber crime.

Cyber crime is defined as Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS).

Such crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare.

2. LITERATURE REVIEW

Cyber crime which is considered as the illegal activity committed on the Internet is now a big threat to the nation. Now a day's number of internet users is increasing rapidly.

As the use of Internet is increasing by which any information can be accessed easily from anywhere, so various illegal activities basing upon the internet are also increasing.

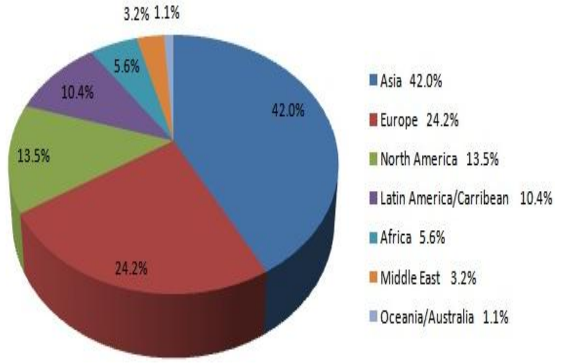

Figure1: World Internet users.

Source: www.google.com

A report McAfee estimates that the annual damage to the global economy is at $445 billion; however, a Microsoft report shows that such survey-based estimates are "hopelessly flawed" and exaggerate the true losses by orders of magnitude. Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud in the US. In 2016, a study by Juniper Research estimated that the costs of cybercrime could be as high as 2.1 trillion by 2019. The majority of cyber crimes are centered on forgery, fraud and phishing. India is the third most targeted country for phishing attack after the US and the UK.

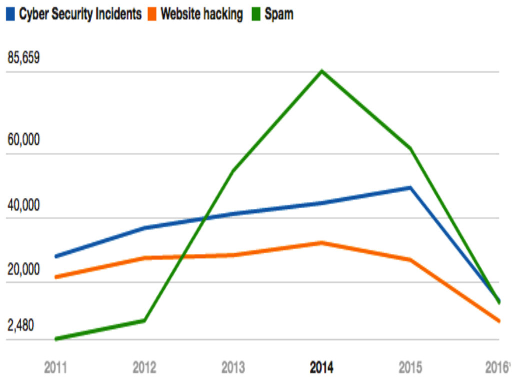

Figure2: Cyber attacks 2011 to 2016.

Source: www.google.com

Social networks as well as e-commerce sites are major targets. India is said to be no.1 country in the world for generating spam. The cyber crime has various categories where technology acts as instrument and target . There are number of cyber crimes those categories into the type where technology acts as instrument. These are as such: Money laundering, mass marketing fraud, child exploitation, cyber bullying, intellectual property infringement, internet based drug trafficking. Some of the crimes where technology acts as target are hacking for criminal purposes, malware threats, distributed denial services.

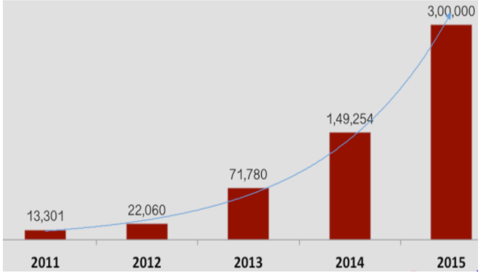

Figure3: Number of cyber crime cases in India

Source: ASSOCHAM-Mahindra SSG report

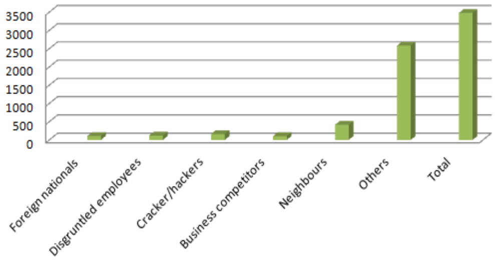

Figure4: Indian cyber crime suspects

Source: www.google.com

3. ANALYSIS AND DISCUSSION

In the technological world Cyberspace can be defined as an intricate environment that involves interactions between people, software, and services. It is maintained by the worldwide distribution of information and communication technology devices and networks. With the benefits carried by the technological advancements, the cyberspace today has become a common pool used by citizens, businesses, critical information infrastructure, military and governments in a fashion that makes it hard to induce clear boundaries among these different groups. The cyberspace is anticipated to become even more complex in the upcoming years, with the increase in networks and devices connected to it. Among the most serious challenges of the 21st century are the prevailing and possible threats in the sphere of cyber security. Threats originate from all kinds of sources, and mark themselves in disruptive activities that target individuals, businesses, national infrastructures, and governments alike. The effects of these threats transmit significant risk for the following –

- public safety
- security of nations
- stability of the globally linked international community

Malicious use of information technology can easily be concealed. It is difficult to determine the origin or the identity of the criminal. Even the motivation for the disruption is not an easy task to find out. Criminals of these activities can only be worked out from the target, the effect, or other circumstantial evidence. Threat actors can operate with considerable freedom from virtually anywhere. The motives for disruption can be anything such as –

- simply demonstrating technical powers
- theft of money or information
- extension of state conflict, etc.

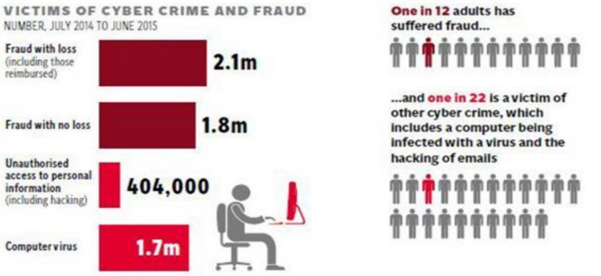

Figure5: Victims of cyber crime and fraud.

Source: www.google.com

Criminals, terrorists, and sometimes the State themselves act as the source of these threats. Criminals and hackers use different kinds of malicious tools and approaches. With the criminal activities taking new shapes every day, the possibility for harmful actions propagates.

Awareness:

The lack of information security awareness among users, who could be a simple school going kid, a system administrator, a developer, or even a CEO of a company, leads to a variety of cyber vulnerabilities. The awareness policy classifies the following actions and initiatives for the purpose of user awareness, education, and training –

- A complete awareness program to be promoted on a national level.
- A comprehensive training program that can cater to the needs of the national information security (Programs on IT security in schools, colleges, and universities).
- Enhance the effectiveness of the prevailing information security training programs. Plan domain-specific training programs (e.g., Law Enforcement, Judiciary, E-Governance, etc.)

DOI 10.17148/IJARCCE.2016.57138

- Endorse private-sector support for professional information security certifications.

Cyber security

Cyber security denotes the technologies and procedures intended to safeguard computers, networks, and data from unlawful admittance, weaknesses, and attacks transported through the Internet by cyber delinquents.

Mission and Vision Cyber security Program

Mission

The following mission caters to cyber security −

- To safeguard information and information infrastructure in cyberspace.
- To build capabilities to prevent and respond to cyber threats.
- To reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.

Vision

To build a secure and resilient cyberspace for citizens, businesses, and Government

Emerging Trends of Cyber Law

Reports reveal that upcoming years will experience more cyber-attacks. So organizations are advised to strengthen their data supply chains with better inspection methods.

Some of the emerging trends of cyber law are listed below

- Stringent regulatory rules are put in place by many countries to prevent unauthorized access to networks. Such acts are declared as penal offences.
- Stakeholders of the mobile companies will call upon the governments of the world to reinforce cyber-legal systems and administrations to regulate the emerging mobile threats and crimes.
- The growing awareness on privacy is another upcoming trend. Google’s chief internet expert Vint Cerf has stated that privacy may actually be an anomaly.
- Cloud computing is another major growing trend. With more advancements in the technology, huge volumes of data will flow into the cloud which is not completely immune to cyber-crimes.
- The growth of Bitcoins and other virtual currency is yet another trend to watch out for. Bitcoin crimes are likely to multiply in the near future.
- The arrival and acceptance of data analytics, which is another major trend to be followed, requires that appropriate attention is given to issues concerning Big Data.

Creating Awareness

While the U.S. government has declared October as the National Cyber security Awareness month, India is following the trend to implement some stringent awareness scheme for the general public. The general public is partially aware of the crimes related to virus transfer. However, they are unaware of the bigger picture of the threats that could affect their cyber-lives. There is a huge lack of knowledge on e-commerce and online banking cyber-crimes among most of the internet users.

Be vigilant and follow the tips given below while you participate in online activities −

- Filter the visibility of personal information in social sites.
- Do not keep the "remember password" button active for any email address and passwords
- Make sure your online banking platform is secure.
- Keep a watchful eye while shopping online.
- Do not save passwords on mobile devices.
- Secure the login details for mobile devices and computers, etc.

4. RECOMMENDATION

There are some grave cyber law related issues that deserve immediate consideration by the government of India. The issues were put forward by the Indian cyber law and Cyber Crimes Investigation Centre of India . Following are some major issues −

- A better cyber law and effective cyber-crimes prevention strategy
- Cyber-crimes investigation training requirements
- Formulation of dedicated encryption laws
- Legal adoption of cloud computing
- Formulation and implementation of e-mail policy
- Legal issues of online payments
- Legality of online gambling and online pharmacies
- Legality of Bitcoins
- Framework for blocking websites
- Regulation of mobile applications

With the formation of cyber-law compulsions, the obligation of banks for cyber-thefts and cyber-crimes would considerably increase in the near future. Indian banks would require to keep a dedicated team of cyber law experts or seek help of external experts in this regard. The transactions of cyber-insurance should be increased by the Indian insurance sector as a consequence of the increasing cyber-attacks and cyber-crimes.

5. CONCLUSION

Indian laws are well drafted and are capable of handling all kinds of challenges as posed by cyber criminals. However the enforcement agencies are required to be well versed with the changing technologies and laws. As internet technology advances so does the threat of cyber crime. In times like these we must protect ourselves from cyber crime.

REFERENCES

1. Steel C.(2006). Windows forensics: The field guide for Corporate computer investigation, Wiley.
2. www.google.com

DOI 10.17148/IJARCCE.2016.57138