ISSN:0975-9646

Cyber Crimes- Challenges & Solutions

Rajarshi Rai Choudhury[1], Somnath Basak[2], Digbijay Guha[3]

[1] Advocate, High Court at Calcutta
Guest Lecturer, BIT Mesra, Kolkata Campus.
132/3, Baruipara Lane, Kolkata- 700035, West Bengal, India

[2]Assistant Professor, MCA Department, Brainware School of IT
173/Z/8, Picnic Garden Road, Kolkata- 700039, West Bengal, India

[3]Lecturer, BCA Department, The Heritage Academy
5/40, Netaji Nagar, Kolkata- 700040, West Bengal, India

Abstract— **Over the past ten years, crime (traditionally based in the world of physical entity) has been increasingly making its way into the world of information. Crime is evolving; since the days when goods were transported by stagecoach, robbery has changed to keep up, even to our modern-day equivalent-credit and debit cards. Internet credit card number theft has become a well-recognized danger. The most common forms of computer crime reported to Inter-GOV include child pornography, fraud, and e-mail abuse. Even more disturbing are new forms of cyber-terrorism made possible by the large amount of the physical machinery now operated by computers. In this article, after attempting to define computer crime, we examine the types that have been committed in the past, and the new types likely to appear in the future. We also examined the difficulty in detecting and measuring computer crime, methods for attempting to prosecute or prevent such crimes, and the effectiveness of these measures. This article evaluates the concepts of computer crimes, detection and the controls. The paper finally exposed us to dangers it poses to organizations, factors that encourage it, and recommending possible controls and preventive measures against computer crimes.**

Keywords— **Challenge, Cyber Law, Global Cyber Law, International Cyber Criminal Court, World Cyber Cop, World Tribunal.**

I. Introduction

Since the beginning of civilization, man has always been motivated by the need to make progress and better the existing technologies. This has led to tremendous development and progress which has been a launching pad for further development of all the significant advances made by mankind from the beginning till date. Probably the most important of them is the development of Internet to put in a common man language. Internet is a global network of computers, all speaking the same language. It is believed that the number of Internet connected devices reached 8.7 billion in 2012 [1].

Internet is believed to be full of anarchy and a system of law and regulation therein seems contradictory. However, Cyberspace is being governed by a system of law called Cyber law. Cyber law is a generic term which refers to all the legal and regulatory aspects of Internet. Publishing a web page is an excellent way for any business to vastly increase its exposure to millions of individuals world-wide. It is that feature of the Internet which is causing much controversy in the legal community. Cyber law is a constantly evolving process. As the Internet grows, numerous legal issues arise. One of the most important issues concerning cyberspace today is that of Cyber crime. Halder and Jaishankar (2011) defines Cyber crimes 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 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)" [2]. Internationally, both governmental and non-state actors engage in cyber crimes, 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. The international legal system is attempting to hold actors accountable for their actions through the International Criminal Court.

II. History Of Cyber Crime

The first recorded cyber crime took place in the year 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This, in broader aspect, is considered as the first recorded cyber crime! [3]

Today computers have come a long way, with neural networks and nano-computing promising to turn every atom in a glass of water into a computer capable of performing a Billion operations per second.

Cyber crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, cyber crime has assumed rather sinister implications. Major Cyber crimes in the recent past include the Citibank rip off. US $ 10 million were fraudulently transferred out of the bank and into a bank account in Switzerland. A Russian hacker group led by Vladimir Kevin, a renowned hacker, perpetrated the attack. The group compromised the bank's security systems. Vladimir was allegedly using his office computer at AO Saturn, a computer firm in St. Petersburg, Russia, to break into Citibank computers. He was finally arrested on Heathrow airport on his way to Switzerland [4].

III. Reasons For Cyber Crime

Hart in his work "The Concept of Law" said that 'human beings are vulnerable so rule of law is required to protect them'. By applying this to the cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them against cyber crime [5]. The reasons for the vulnerability of computers may be said to be:

1. Capacity to store data in comparatively small space:-
   The computer has a unique characteristic of storing data in a very small space. This allows for much easier access or removal of information through either physical or virtual media.
2. Easy to access:-
   The problems encountered in guarding a computer system from unauthorized access are that there is every possibility of unauthorized access not due to human error but due to the complex technology. By secretly implanting a logic bomb or key loggers can steal access codes, advanced voice recorders; retina images etc. that can fool biometric systems and bypass firewalls can be utilized to get passed many security systems.
3. Complex-
   The computers work on operating systems and these operating systems in turn are composed of millions of lines of code. The human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system using often more sophisticated means than originally anticipated by the system engineers.
4. Negligence:-
   Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal to gain access and take control over the computer system. This negligence is usually a property of under resourced IT security provisions and the improvement of security barriers within software packages and network structures could lead to improved security. Negligent behavior of a person can also put a system vulnerable by way of open public telephonic conversation regarding a system’s password, e-mail or security code exchange, personal data sharing etc. Moreover, now a day, this negligence is considered to be the most important aspect for cyber insecurity.
5. Loss of evidence:-
   Loss of evidence is a very common & obvious problem as all the data is routinely destroyed. Further collection of data outside the territorial extent also paralyzes the system of cyber crime investigation.

IV. Profile Of The Problems & Study Of Topics

The threat from cyber crime is multi-dimensional, targeting citizens, businesses, and governments at a rapidly growing rate. Cyber criminal tools pose a direct threat to security and play an increasingly important role in facilitating most forms of organized crime and terrorism.

Challenge 1

There is now a sophisticated and self-sufficient digital underground economy in which data is the illicit commodity. Stolen personal and financial data – used, for example, to gain access to existing bank accounts and credit cards, or to fraudulently establish new lines of credit – has a monetary value. This drives a range of criminal activities, including phishing (the act of attempting to acquire information such as usernames, passwords, and credit card details and sometimes, indirectly, money, by masquerading as a trustworthy entity in an electronic communication), pharming (the fraudulent practice of directing Internet users to a bogus Web site that mimics the appearance of a legitimate one), malware distribution and the hacking of corporate databases, and is supported by a fully fledged infrastructure of malicious code writers, specialist web hosts and individuals able to lease networks of many thousands of compromised computers to carry out automated attacks.

Solutions

- Active targeting of underground fora to disrupt the circulation of powerful and easy to use cyber criminal tools, such as malware kits and botnets.
- Disrupt the infrastructure of malicious code writers and specialist web hosts through the active identification of developer groups and a joint action of law enforcement, governments and the Information & Communication Technology industry to dismantle so-called “bullet proof” hosting companies.
- Active targeting of the proceeds of cyber crime in collaboration with the financial sector. For e.g. money mule (is a person who transfers money acquired illegally (e.g., stolen) in person, through a courier service, or electronically, on behalf of others).
- Continue to develop insight into the behavior of the contemporary cyber criminal by means of intelligence analysis, criminological research and profiling techniques, and based on the combined law enforcement, IT security industry and academic sources, in order to deploy existing resources more effectively.

Challenge 2

In the last decade advances in communications technologies and the "information" of society have converged as never before in human history. This has given rise to the industrialization of a type of crime where the commodity, personal information, moves far too quickly for conventional law enforcement methods to keep pace.

The unprecedented scale of the problem threatens the ability of the authorities to respond with millions of viruses and other types of malicious code are in global circulation, and again innumerable computers are compromised per day.

At the same time, the authorities have more data on criminal activity at their disposal than ever before, and now have an opportunity to harness this information in ways which make intelligence development and investigation more streamlined and cost effective.

Cyber crime rates continue to increase in line with Internet adoption: mobile Internet access and the continuing deployment of broadband Internet infrastructure throughout the world therefore introduces new levels of vulnerability; with potential victims online for longer periods of time and capable of transmitting much more data than before; and the increasing trend for outsourcing data management to third parties presents imminent risks to information security and data protection.

Solutions

- More must be done to harness the intelligence of network and information security stakeholders, not only to provide a more accurate and comprehensive assessment of cyber criminality, but also to ensure that responses are effective and timely. Active partnerships are to be made with ISPs, Internet security organizations and online financial services are keys.
- Collaboration, particularly with the private sector, to proactively identify features of future communications technologies liable to criminal exploitation, and to design vulnerabilities out of technologies and environments which are in development.

Challenge 3

Cyber crime is a truly global criminal phenomenon which blurs the traditional distinction between threats to internal (criminality and terrorist activity) and external (i.e. military) security and does not respond to single jurisdiction approaches to policing. The liability of networks to exploitation for a number of different ends, and the ease with which individuals may move from one type of illegal activity to another suggests that territorialism in all its forms (both of nations and regions, and specific authorities within nations) hinders efforts to successfully combat the misuse of communications technology.

At present, national authorities are overcoming jurisdictional restrictions by coordinating regionally or with agencies with similar levels of capability/capacity to better understand and respond to Internet-facilitated crime.

Solutions

- More centralized coordination at regional and interregional levels, to streamline the fight against cyber crime.
- Global Cyber Law should be implemented.
- The establishment of virtual taskforces to target Internet facilitated organized crime. These should be responsive to the evolving criminal environment – e.g. more permanent groups for information sharing, more ad hoc arrangements for specific operations such as dismantling botnets. In all cases the authorities need to have the flexibility to include a variety of stakeholders (law enforcement, military, and private sector, and academia, user groups) in order to achieve the desired outcome. One of the virtual task force can be World Cyber Cop.
- The World Council for Law Firms and Justice promotes the evaluation and harmonization of the legal systems throughout the world. There are many small and many great steps on the road to fulfilling this vision. This consideration of ideas on the establishment of an International Court for Cyber Crime is intended as the start of an international initiative to mark an important milestone on the long road.

  The establishment of an International Cyber Criminal Court (comprising of highest level of Judicial Authority and Technical Authority) for the prosecution of Internet crimes could wholly or partially reduce the criminals' lead. The realization of this vision requires expertise, commitment and courage – including the courage to ignore borders and to think consistently towards the future.

There should be a World Tribunal which should control all the Country Courts which in turn should have many Regional Tribunals.

Challenge 4

Another most alarming problem in the present day cyber world is the promotion and easy availability of pornography especially Child pornography which refers to images or films (also known as child abuse images) and, in some cases, writings depicting sexually explicit activities involving a child. Abuse of the child occurs during the sexual acts which are recorded in the production of child pornography.

Solutions

- Place the computer in a centrally located area in your home - not in a child's bedroom. This prevents "secret" communications or access and also allows all members of the family to use it. Talk to your children about the Internet. Explain that it is an excellent source of information, but some sites are inappropriate and they are expected to stay away from these sites. Establish time frames for Internet access. This will encourage your children to obtain information in a timely manner and discourage aimless wandering. Keep an open line of communication with your children. Discuss their Internet experiences and guide them to sites that are age-appropriate. Consider using software that can block or filter Internet sites or certain words that may indicate inappropriate sites.
- In a chat room never give out any personal information including: name, address, city, state, school attended, telephone number, family names or other personal family information. Never respond to someone who wants to meet in person or send photographs. Instruct your children to exit the chat room and notify you immediately if this happens. Most importantly, if your child visits a particular chat room, spend at least five or ten minutes monitoring the conversation to see if it is appropriate. Consider purchasing computer software products that can help you monitor and control your child's access to the Internet. Monitor your children's Internet activity by checking all of the sites visited.

V. How To Avoid Cyber Crimes

- **Know How To Recognize Phishing.** Your bank won't send you an email telling you that your account has been compromised and asking you to provide sensitive account and personal information like password, PIN etc. it already has. These are obviously phishing attempts.
- **Recognize that your Smart-phone is really a pocket-size computer** and is prone to the same types of attacks directed at your laptop and desktop. Take steps to protect it, such as keeping your operating system current and creating a strong password.
- **Keep your personal information to yourself.** For instance, don't put your entire birth date, including the year, on Facebook. Think about the security questions normally posed by your bank and other secure locations: "first school you attended," "name of favorite pet" and the like.
- **Know the pitfalls of public Wi-Fi.** CreditCards.com says, "Avoid public wireless Internet connections unless you have beefed-up security protection."
- **Beware of public computers, too.** For instance, Kiplinger says, "Don't access your accounts or personal information on public hotel computers, which could have software that logs keystrokes and records your passwords and account numbers."
- **Use credit cards, rather than debit cards,** when making purchases online. In case of fraud, you'll get much better protection from liability with a credit card.
- **Purchase only from reputable websites** (and look for "https" in the Web address). "It is really easy to create a fake online store or to create a store that sells stuff, but its real purpose is to collect credit card information," former identity thief Dan DeFelippi told CreditCards.com.
- **Check your accounts and your credit reports regularly.** Some experts recommend that you check bank account and credit card activity every day. You can pull a free credit report every four months from AnnualCreditReport.com to verify that fraudulent accounts have not been created in your name.
- **Avoid suspicious E-mails.** Don't click on links in suspicious emails, even those that appear to be from friends. Emailed viruses and malware are the most prevalent cyber threat of identity theft. Just think of how many emails you've gotten in the last year that appeared to be from friends whose email accounts were hijacked.

Acknowledgment

We would take the opportunity to thank ***Professor Radha Tamal Goswami, In-Charge, Birla Institute of Technology, Mesra, Kolkata Campus*** for providing us with all the necessary facilities to make our article work and of worth.

We thank ***Birla Institute of Technology, Mesra, Kolkata Campus*** for paying a pivotal and decisive role during the development of the article.

References

[1] http://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/ (last accessed on 15th September 2013)

[2] http://en.wikipedia.org/wiki/Computer_crime (last accessed on 15th August 2013)

[3] http://cybercrime.planetindia.net/intro.htm (last accessed on 17th August 2013)

[4] http://www.legalservicesindia.com/articles/cyber.htm (last accessed on 15th August 2013)

[5] http://www.naavi.org/pati/pati_cybercrimes_dec03.htm (last accessed on 20th August 2013)