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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Cybercrimes, security and challenges

Tahir Hussain Bhat[1], Afaq Alam Khan[2]

Lecturer, Computer Applications, A.S. College, Srinagar, India[1]

Assistant Professor, Information Technology, Central University Kashmir, Srinagar, India [2]

Abstract: Cybercrime is a range of illegal digital activities to target an individual or an organization in order to cause harm. The term cybercrime applies to a wide range of attack methods. It can range from mere web site defacements to grave activities such as service disruptions that impact business revenues.

The cyber-security assures protection of assets which include data, computers and computer networks. The high level of insecurity on the internet is becoming so much troublesome and transaction on the web has become a thing of doubt. Cyber-security is a necessary consideration for individuals, business, government, military, defence and educational institutions.

In this paper, an attempt has been made to provide an overview of cybercrime as a whole and identify different types of crimes. Also we try to find out the casus of these crimes. This paper will focus on exploring who actually is involved in these crimes, how to eradicate cyber crimes and what are the various challenges dealing with cyber crimes. We will also come up with different viewpoints and recommendations in securing the cyber space.

With increasing use of information technology (IT) enabled services such as e-governance, online business and electronic transactions protection of personal and sensitive data have assumed paramount importance. The economic growth of any nation and its security whether internal or external and competiveness depends on how well is its cyberspace secured and protected.

Keywords: Cyber-security; Cyber-crime; Threats; Attacks; Hacking.

I. INTRODUCTION

Information and communication technologies (ICTs) are permeating and transforming every aspect of our lives in the 21st century. Today, the number of global web users, stands at an estimated 2.4 billion, just over one third of the world's total population. Over 60% of all internet users are in developing countries, with 45% of all internet users below the age of 25. It is estimated that by the year 2017, mobile broadband subscriptions will approach 70% of the world's total population. By the year 2020, the number of networked devices (the internet of things) will outnumber people. [l]

As the number of mobile users, digital applications and data networks increases, so do the chances of cybercrimes. Now Cyber security issues are not limited rather they encompass, from electricity and water supply systems to the health service, from public transport to smart cars and from banking and logistics to the emergency services.

Cyber-security is the process of applying security measures to ensure confidentiality, integrity and availability of data. The goal of cyber-security is to protect data both in transit and at rest.

Rising at alarming rate, the number of cyber crimes in India may touch a humungous figure of 3,00,000 in 2015, almost double the level of last year causing havoc in the financial space, security establishment and social fabric, an ASSOCHAM-Mahindra SSG study [10] warned.

II. WHY CYBER SECURITY IS IMPORTANT

Cyber security is an increasingly important requirement for global business and modern society. We exist in a data-centric world, where information technology and associated communication networks and services pervade every aspect of our lives. This makes the protection of our digital assets and activities in cyberspace of critical importance, whether for individual life experience or a prosperous and sustainable society. But the challenge to understand cyber risk and deliver effective and accessible security becomes harder as technology continues to rapidly evolve and our systems become ever more complex. We are increasingly dependent upon such information and communications infrastructures, and the threats we face are organized and evolving the skills to exploit our dependency to further their interests.

Findings from Cyber Crime Survey report 2014 [3] show an upward trend that demonstrates a need for a timely review of existing approaches to fighting this new phenomenon in the information age.

As per the study [10], Andhra Pradesh, Karnataka and Maharashtra have occupied the top 3 positions when it comes to cyber crimes registered under the new IT Act in India. Interestingly, these three states together contribute more than 70 per cent to India's revenue from IT and IT related industries.

III. CLASSIFICATION CYBERCRIMES

Cyber crimes have been classified on the basis of nature and purpose of the offence and have been broadly grouped into three categories depending upon the target of the crime. It may be against person, property or a government. Cyber crimes against person include crimes like hate messages, stalking, defamation and transmission of pornographic material. The cyber crimes involving property include unauthorized computer trespass,

DOI 10.17148/IJARCCE.2015.45108

vandalism and transmission of harmful programs and unauthorized possession of computerized information. Third category of cyber crimes targets the government. This category of cyber crime is more popularly known as cyber terrorism.

The most comprehensive classification of computer crimes has been given by David L. Carter [9] who classifies computer related crimes into three broad categories.

A. *Where Computer Is Target Of The Crime.*

This category of computer crime aims at damaging computer system or stealing valuable information stored on the system.

B. *Where Computer Facilitates The Commission Of Crime.*

The computer crimes falling under this category use computer as a medium for commission of offences. The computer programs are manipulated to defraud others.

C. *Where Computer Is Incidental To The Crime.*

The diverse application of internet made it incidental to the crimes that may be classified into two categories.

○ *Internet crime*

Internet crimes include that group of crimes that make criminal use of the internet infrastructure.

○ *Web based crime*

Web based crimes are those crimes in which a particular web service is being targeted e.g. website, email, Usenet, chat etc.

Credit and debit card fraud cases top the chart of cybercrimes. There has been a six-fold increase in such cases over the past three years. According to the ASSOCAM report [10], around 2277 complaints of online banking/credit/debit card fraud have been reported this year, followed by 191 Facebook-related complaints (morphed pictures/cyber stalking/cyber bullying). Other major cyber complaints were cheating through mobile (61), hacking of e-mail ID (59), abusive/offensive/obscene calls and SMS (55), and others.

IV. CYBER CRIMINALS

The advent of the Internet allows cyber criminals to conduct illegal activity from a computer far removed from where the crime is actually taking place. A criminal can break into a computer network a continent away and steal credit card and banking information without having to be physically present at the scene. Criminals are using computers to conduct narcotics trafficking, child pornography, bank fraud, etc. using a computer and the Internet as a vehicle for illegal activity.

There are many reasons why cyber-criminals commit cyber-crime, chief among them are these three listed below:

Cyber crimes can be committed for the sake of recognition. This is basically committed by youngsters who want to be noticed and feel among the group of the big and tough guys in the society. They do not mean to hurt anyone in particular; they fall into the category of the Idealists; who just want to be in spotlight.

Another cause of cyber-crime is to make quick money. This group is greed motivated and is career criminals, who tamper with data on the net or system especially, e-commerce, e-banking data information with the sole aim of committing fraud and swindling money off unsuspecting customers.

Thirdly, cyber-crime can be committed to fight a cause one thinks he believes in; to cause threat and most often damages that affect the recipients adversely. This is the most dangerous of all the causes of cyber-crime. Those involve believe that they are fighting a just cause and so do not mind who or what they destroy in their quest to get their goals achieved. These are the cyber-terrorists.

According to the National Crime Records Bureau (NCRB), in 2013, 681 cyber crime related cases have been registered in Maharashtra, which has seen a 44.6 per cent rise in cyber crimes when compared to 2012. Andhra Pradesh with 635 cases registered in 2013 has also seen a 48 per cent rise when compared to 2012. Karnataka with 513 cases registered in 2013 has seen a 24.5 per cent rise when compared to 2012. [10]

V. IMPACT OF CYBERCRIME

The effects of a single, successful cyber attack can have far-reaching implications including financial losses, theft of intellectual property, and loss of consumer confidence and trust. The overall monetary impact of cyber crime on society and government is estimated to be billions of dollars a year.

- Financial Impact of Cyber Crime

The overall monetary impact of cyber crime on society and government are unknown. Some estimates are that viruses and worms cause damages into the billions of dollars a year. It is estimated that only 5 - 10% of cyber crime is reported to law enforcement authorities. Reasons why cyber crime is not reported varies from not knowing that a cyber incident has occurred to not wanting the public to know that a company's security data may have been exposed and there may be several other reasons.

- Loss of intellectual property

What the Internet has allowed is the mass production of individual works. Because of the simplicity of posting material to the Internet, for the first time, individuals with relatively little knowledge of publishing are able to present their works to the world. This has resulted in a large increase in the amount of copyrighted material available, which a significant number of people are unaware conforms to copyright law. Many people believe that because they can place work on the Internet without permission from anyone else, they can copy material from the Internet in the same casual manner[17].

- Loss of consumer confidence and trust

The ITRC survey [18] found consumers are increasingly concerned about the security of their personal and financial information when conducting transactions online. Eighty seven percent of respondents expressed significant concern about having their credit card information stolen or having

DOI 10.17148/IJARCCE.2015.45108

merchants lose personal and financial information in a data breach. This shows that consumers are losing confidence and trust on online transactions. [18]

VI. SECTORS PRONE TO CYBER ATTACKS

Today organizations are extensively using information technology and applications for automation of business processes, also, due to the IT revolution, Internet is now the key medium for business transaction, thereby leaving many sectors vulnerable to cyber attacks. The level of vulnerability of sectors depends on the extent of IT pervasiveness in each of these sectors; some of the sectors which are more prone to attacks are given below.

Government: Even as the number of internet users continues to rise and the government increasingly seeks to offer citizen-centric services through the internet. About half the government departments and ministries in India are vulnerable to data theft, hacking and cyber terrorism. [11]

As per the study [10] findings, during 2011, 2012, 2013 and 2014 years, a total number of cyber crimes registered were 13,301; 22,060; 71,780 and 62,189 (till May). Currently, the cyber crimes in India is nearly around 1,49,254 and may likely to cross the 3,00,000 by 2015 growing at compounded annual growth rate (CAGR) of about 107 per cent. As per the findings, every month nearly 12,456 cases registered in India.

Financial Services: Cybercrime continues to remain a tough challenge for financial organizations. "With rise in the cybercrime, businesses are increasingly facing impacts not only on the financial front but also irreversible damage to their brands and market reputations. As a result of this growing threat, there is a significant need for corporate to recognize cyber threats and craft cyber response plans. [12]

Growing internet penetration and rising popularity of online banking have made India a favourite among the cybercriminals, who target online financial transactions using malware and India ranks third after Japan and US in the tally of countries most affected by online banking malware during the year of 2014, highlighted the ASSOCHAM [10] study.

Phishing attacks of online banking accounts or cloning of ATM/Debit cards are common occurrences. The increasing use of mobile/smart-phones/tablets for online banking/financial transactions has also increased the vulnerabilities to a great extent. The maximum offenders came from the 18-30 age group [10].

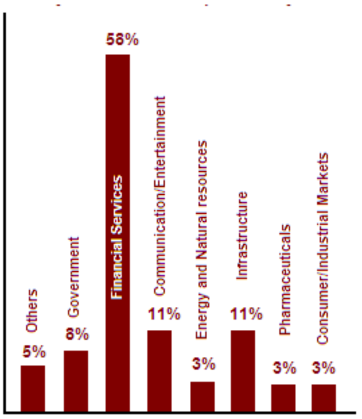
These attacks have been observed to be originating from the cyber space of a number of countries including the US, Europe, Brazil, Turkey, china, Pakistan, Bangladesh, Algeria and the UAE, highlighted the ASSOCHAM-Mahindra SSG joint study.[10]

The ASSOCHAM report [10] further said, mobile frauds are an area of concern for companies as well as 35-40% of financial transactions are done via mobile devices and this is expected and this is expected to grow to 55-60% by 2015.

Communication/Entertainment: Communication and entertainment industries are also facing cyber threats with the advent in internet. Piracy, e-mail threats, spam, social phishing, child pornography are the main threats to communication and entertainment.

There are many ways that sensitive information is hacked as a result of cell phone usage. The most common are due to installation of uncertified applications. The smart-phone users rarely check for security certificates and download apps (games, music and other software) from third party or unsecured sites. Mobile banking apps store data such as PIN, account number on the phone. So, there is a risk that if the phone is hacked or stolen, then the information is compromised, points out the study [10].

Increasing smart-phone sales and usage in India, the number of people falling victim to such crimes is also on the rise. The number of cyber crime victims in India (2012) was 46 million people against the global average of 560 million. [10]



Source: Cybercrime survey report 2014, KPMG in India

Fig. 1. KPMG Survey results – Sectors prone to cyber attacks

VII. LATEST TRENDS AND STATISTICS

Over the past few years, the global cybercrime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security. Until recently, malware, spam emails, intruding into corporate sites and other attacks of this nature were mostly the work of computer 'geniuses' showcasing their talent. These attacks, which were rarely malicious, have gradually evolved into cybercrime syndicates siphoning off money through illegal cyber channels.

During the years 2011, 2012, 2013 and 2014 (till May), a total number of 21,699; 27,605; 28,481; 48,174 Indian websites were hacked by various hacker group spread across worldwide and likely to touch 85,000 by 2015 [10].

Uttar Pradesh with 372 cases registered in 2013 is in the fourth place. It has seen a huge rise of 81.5 per cent in just one year. Kerala is in the 5th place with 349 cases registered in 2013. Among the bigger states Tamil Nadu and Bihar have very few cyber crime related cases. Just 54 cases have been registered in Tamil Nadu and just 23 cases have been registered in Bihar in 2013. Gujarat and Odisha have also registered just 61 and 63 cases respectively in 2013. Among the Union Territories, the national capital Delhi has registered 131 cyber crime related cases. It has seen a rise of 72.4 per cent when compared to 2012.[10]

VIII. Technical Countermeasures Against Cyber Crimes

There are a variety of different technical countermeasures that can be deployed to thwart cybercriminals and harden systems against attack. No doubt these countermeasures already exist but the thing is that we need to improve them and make them strong so that they can counter the attacks, as attackers are using latest tools and technology to break them.

Network or host based firewalls are considered the first line of defense in securing a computer network by setting Access Control Lists (ACLs) which determines what services and traffic can pass through the check point. Latest and updated antivirus can be used to prevent propagation of malicious code. Heuristics such as file analysis and file emulation are also used to identify and remove malicious programs. Virus definitions should be regularly updated in addition to applying operating system hot-fixes, service packs, and patches to keep computers on a network secure.

Cryptography techniques can be employed to encrypt information using different algorithms to mask information in storage or transit.

Network vulnerability testing performed by technicians or automated programs can be used to test on a full-scale or targeted specifically to devices, systems, and passwords used on a network to assess their degree of security.

Physical deterrents such as locks, card access keys, or biometric devices can be used to prevent criminals from gaining physical access to a machine on a network. Strong password protection both for access to a computer system and the computer's BIOS are also effective countermeasures against cyber-criminals.

Another deterrent is to use a bootable bastion host that executes a web browser in a known clean and secure operating environment. The host is devoid of any known malware, where data is never stored on the device, and the media cannot be overwritten.

The kernel and programs are guaranteed to be clean at each boot. Some solutions have been used to create secure hardware browsers to protect users while accessing online banking.

IX. Social Countermeasures Against Cyber Crimes

The world's population is large, people are busy, and the processes of society are complex. To date, no society has been able to prevent all criminal acts. Research has shown that no law can be put in place to effectively eradicate the scourge of cyber-crime. Attempts have been made locally and internationally, but these laws still have shot-comings. What constitutes a crime in a country may not in another, so this has always made it easy for cyber criminals to go free after being caught. [12]

These challenges notwithstanding, governments should in the case of the idealists, fight them through education not law. The enforcement of law on them can only trigger trouble, because they would not stop but would want to defy the law. These idealistic should be channelized, they can be hired by private organizations to work against cyber crimes, or even government can hire them which can prove fruitful for nations.

Another means of eradicating cyber-crime is to harmonize international cooperation and law, this goes for the greed motivated and cyber-terrorists. They cannot be fought by education, because they are already established criminals, so they can not behave. The only appropriate way to fight them is by enacting new laws, buildup new foolproof technical security measures, harmonize international legislations and encourage coordination and cooperation between national law enforcement agencies [12].

X. Recommendations

Training and awareness are important steps in mitigating these attacks. All citizens, consumers, and employees should be aware of cyber threats and the actions they can take to protect their own information, as well as the information within their organization.

Cyber Crime Unit Requirements: The impact of cyber crime has been, and will be in the future, felt by all governments and economies that are connected to the Internet. Criminals will use the Internet, computers and other digital devices to facilitate their illegal activities. There should be separate cyber crime cells locally active for controlling such crimes. Prosecutors and cyber police must have resources, training and equipment required to address cyber crime.

Domestic and international law enforcement: It is often difficult to identify the perpetrator of cyber attack as such attack can be made anywhere from globe, and even when a perpetrator is identified, criminal prosecution across national boundaries is problematic. Therefore, legal domestic framework should be inter-operable with international framework.

Education: We need to educate citizens that if they are going to use the internet, they need to continually maintain and update the security on their system so that they cannot be compromised. We also need to educate corporations and organizations in the best practice for effective security

DOI 10.17148/IJARCCE.2015.45108

management. Automated updates are sent to all computers and servers on the internal network, and no new system is allowed online until it conforms to the security policy.

Information security: Information security refers to measures taken to protect or preserve information on a network as well as the network itself. The alarming rise of premeditated attacks with potentially catastrophic effects to interdependent networks and information systems across the globe has demanded that significant attention is paid to critical information infrastructure protection initiatives. Exploiting security flaws appears now to be far easier, less expensive and more anonymous than ever before. This means that governments must adopt an integrated approach to protect these infrastructures from cyber threats. [4]

XI. CONCLUSION

With the advent of hand held computing, cyber criminals are now moving beyond computers, and attacking mobile handheld devices, such as smart-phones and tablet personal computers (PCs). Cyber attackers have now taken advantage of the increasing popularity of mobile phone applications and games by embedding malware into them. Despite the increasing cyber threat risks, many boards fail to ask these questions or attain satisfactory answers.

Government, military, corporations, financial institutions, hospitals and other business establishments collect, process and store a great deal of confidential information on computers and transmit the data across networks to other computers. On the other hand volume and sophistication of cyber attacks is growing day by day.

This paper provides an overview of cybercrime as a whole and identifies different types of crimes. Also we tried to find out the casus of these crimes. This paper has also discussed the recent trends in cyberspace which need to be eradicated and reviewed the latest statistic data on cyber crimes; we also discussed various challenges dealing with cyber crimes. We also came up with different viewpoints and recommendations in securing the cyber space.

REFERENCES

[1] Sumanjit Das and Tapaswini Nayak, Impact Of Cyber Crime: Issues And Challenges, ISSN: 22316604
[2] Azeez Nureni Ayofe, Barry Irwin, Cyber Security: Challenges And The Way Forward, ISSN 1512-1232
[3] KPMG Global Energy Institute , Energy at risk A study of IT security in the Energy and Natural Resources industry, https://www.kpmg.com/IN/en/IssuesAndInsights/ArticlesPublications/Documents/KPMG_Cyber_Crime_survey_report_2014.pdf
[4] Hammond and Allen. The 2001 council of European convention on cybercrime. In an E_cient Tool to Fight Crimes in Cyber-Space?, June, 2001.
[5] http://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity
[6] Cyberterrorism Project – University of Swansea – Executive Summary and Final Report Notes – July 2013
[7] www.mcconnellinternational.com/services.cybercrime.htm
[8] http://www.itu.int/osg/csd/cybersecurity/gca/overview/legal.html
[9] Carter David L. Computer crime categogies – How techno-Criminals Operate, FBI Law enforcement Bulletin, July 1995.
[10] A study by: The Associated Chambers of Commerce & Industry of India [ASSOCHAM] http://www.assocham.org/newsdetail.php?id=4821
[11] http://www.business-standard.com/article/technology/half-the-govt-websites-in-india-are-prone-to-cyber-attacks-113010600025_1.html
[12] http://articles.economictimes.indiatimes.com/2014-07-21/news/51830721_1_cybercrime-survey-cybercrime-threats-51-percent
[13] http://oilpro.com/post/1529/why-the-oil-and-gas-industry-is-prone-to-cyberattacks
[14] http://news.idg.no/cw/art.cfm?id=CE8606BB-1A64-6A71-CEBC0B46E6C21577
[15] http://www.pharmaceutical-technology.com/features/featurecybercrime-pharmaceutical-industry-biotech/
[16] http://cw.com.hk/news/report-18-industries-prone-different-cyberthreats-combo
[17] http://theukwebdesigncompany.com/articles/article.php?article=26
[18] Identity theft resource center [ITRC], 2014 Data Breach Category Summary, http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReportSummary2014.pdf
[19] Abdul Razzaq, Ali Hur, H Farooq Ahmad, Muddassar Masood, Cyber Security: Threats, Reasons, Challenges, Methodologies and State of the Art Solutions for Industrial Applications
[20] N. LEENA, Cyber Crime Effecting E-commerce Technology

BIOGRAPHIES

Tahir Hussain Bhat is MCA (Rank II) with UCG-NET in computer science, he has also qualified GATE 2015 from IIT-Kanpur. He has more than one year of experience in teaching at graduate level. He is also PG diploma in Cyber-law. His area of interest is network and cyber security.

Afaq Alam Kha is B.E., M.Tech (IT) and has more than 7 years of experience in teaching at university level and is currently working as Assistant Professor in central university of Kashmir. His area of interest is computer architecture, network communication, database & data mining.

DOI 10.17148/IJARCCE.2015.45108