CYBER CRIMES PREVENTION AND RECOVERY STRATEGIES

Mazhar Hussain Malik*[1], Nuzhat Younis
[1]*Department of Computer Science & IT, Institute of Southern Punjab, 9-KM, Bosan Rd, Multan,Pakistan
*Email: mazhar.hussain@isp.edu.pk (Corresponding Author)

ABSTRACT*—Since In the field of communication, when the whole world becomes a global village, cyber crime becomes a vital issue in the today's modern world. There is no doubt that internet environments have introduced the new levels of the efficiency, productivity and connectivity in businesses.*

In this paper, we discuss, the main types of cyber crimes starting from the individual level to organization and national level and in the next part, we discuss the key consequences of cyber crimes. Based on discussed cyber crimes we propose detection and response mechanism techniques along with the proposed strategies which are needed to handle cyber crimes.

Keywords- Cyber security, prevention and recovery strategies, Intrusion Detection System, Audit and controls

I. INTRODUCTION

Beside the advantages of communication technologies [1, 2, 3] wide ranges of offences are committed through new technologies.

Cyber crimes fall into two major categories. Offences are committed using new technologies, such as offences related to computer systems and data. Network and other supporting devices are used to facilitate the commission of the offence. In the former manner, offences are hacking or breaking computers to alter or steal data [4].

II. TYPES OF CYBER CRIME

There are five [5,6,7,8] types of cyber crimes and each of them are divided into sub heading which are explained in detail as follows;

a. Against Individual

Drug trafficking: - With the usage of communication technologies, drug traders are taking advantages of the internet to sell illegal substances via encrypted emails. They use courier websites to track packages of pills and exchanges the recipes in restricted access chat rooms. Virtual deal allows more security and conformability in purchasing illegal drugs [7,8].

Offensive content & Harassment: - Illegal or offensive material can be found on the internet or in chat rooms or newsgroups. The major source to receive such type of material is through spam emails, which are advertising pornography or illegal products. There is no central body, which monitors and approves the contents, which are required to go online. Pestering via email, illegal computer control, email spoofing, insult, cheating and fraud, offensive exposure and distribution of obscene material are some examples of cyber crimes against individuals [8,9,10].

b. Against Individual Property

Electronic Funds Transfer Fraud: - In the modern era of technology when physical cash is replaced by credit cards and electronic fund transfer. The risk, such as transition lead to hold and diverted are increased and credit card number can be intercepted electronically, as well as physically and digital information, which is stored on credit cards, can be recreated.

A Russian hacker, Vladimir Levin, get access the computers of Citibank's centre wired transfer department and transfer funds from that account to other accounts which were operated by him in the United States [11,14].

Dissemination of Offensive Materials: -There are contents, which can be objectionable for some peoples, and peoples can use such type of contents for harassment. Telecommunications systems some time are used for harassing, threatening or invasive communications. Concept of cyber stalking in which messages are sent to an unwilling recipient [12].

In Denmark, a man allegedly stole nude photographs of his former girlfriend and her new boyfriend and he posted them on the internet along with their name, phone number and email address. Virus transmission, unofficial access over computer system, Internet theft and computer vandalism are some examples of cyber crimes against individual property [13,15].

c. Against Society

Cyber-bullying and Cyber-stalking: - Cyber crimes are affecting society via cyber bullying and cyber stalking. Cyber bullying is the harmful way of the using the internet and the related technologies, which are harmed to other peoples [8].

This becomes more often in the society and especially in the young peoples and awareness campaigns are arisen to combat. Cyber-bullying can be defined as when the internet, cell phones and other devices are used to send messages, post text or image for a particular purpose which can be to hurt or embarrass a person. Cyber-bullying is simple as continuing to send an e-mail to someone who has said that they don't want to contact with the sender, but they can include the treats, pejorative labels and sexual remarks. While cyber-stalking is the using of internet or any other electronic means to stalk an individual or group of peoples, which include false accusation, making threats, damage to equipment and data [9].

Child pornography, trafficking, monetary crimes, sale of illegal articles and online betting and games are some of the society cyber crimes [10].

d. Against Private Organizations

Theft of telecommunications services: - Theft of the telecommunication services is another form of cyber crime in which hackers gain access to an organization's telephone switchboard (PBX) and individual or organization can gain access to dial-in/ dial-out circuits and they make their own calls or sell call time. Another form of theft is capturing calling card and resell them and it is estimated that every year, 5% telecommunication industry renew is lost due to fraud [12].

Telecommunications Piracy: - Telecommunication piracy is related with the permits perfect reproduction and has dissemination of print, graphics, sound and multimedia which is lead to resell of the metal and cause lost and it is copyright

violation. Distribution of pirated software's, ownership of non permitted information and unauthorized control over the computer networks [16].

e. Against Government

Electronic Vandalism and Extortion: - Cybercrimes activities are also involved in hacking and cracking data of government departments. These crimes are big thread for the nation and government. In 1999 hacker hack a computer system of Sri Lankan government and the North Atlantic treaty organization. In such type of attacks, hacker steals information or block organizations' websites [17].

Cyber Warfare and Terrorism: - As per statistics since 2001, there is a significant rise in the internet problem and server scans. This is a type of cyber terrorism and a cyber terrorist is one who intimidates to an organization or government to gain his political or social objectives. .

III. CONSEQUENCES OF CRIME

a. Loss of Revenue

The biggest cause of cyber crime is wastage of resources, whether those are related to financial or infrastructure. This list may be caused by the person, which acquires sensitive financial information [18].

b. Wasted Time

The key issue caused by the cybercrime is wastage of time as for detection of crime, there is great need of the time to resolve issues which rather than working on creative and productive works and technology staff put a great percentage of their time on the handling of security related issues and other problem which are related with cyber crime [19].

c. Damaged Reputations

When customer records are compromised, the company's reputation can take a major batter as it leads to discontinuity of service and cause bad reputation of the organization [18,19].

d. Reduced Productivity

Keeping in view of security threat, there is great need to implement the security tools and techniques and which lead to extra process and more verification to access systems which cause delay in the system and lead to decrease in the productivity [19].

e. Influence of Cyber Terrorism

Cyber-terrorism can have a great influence on the numbers of peoples and can weaken a country's economy and making it more vulnerable to military attacks [20].

Internet based businesses are greatly affected by the cyber terrorist and can cause downtime for those companies which are managing websites and earning money through advertising and such type of businesses are very good and useful for the country's economy.

IV. PROPOSED CYBER CRIME DETECTION TECHNIQUE

There is great need to define a layout and procedures which are required to handle cyber crimes proactively, we proposed detection techniques for cyber crimes, which are as follows;

a. Reviewing

In first proposed technique, there should be proposing an audit system which should be done on frequently. We proposed a continuous improvement plan that is based on the four steps Plan, Do, Check and ACT is shown in Figure.1

Figure.1. Proposed Review Technique

In the reviewing process, we propose that security within the organization should be done proactively. As per statistics, most of the computer crimes are not drawn from outside the organization, they are done within the organization so there is great need to implement the security techniques and a company or organization can be safe if four propose review steps are implemented.

b. Checking mistakes

The other proposed technique is to make regular checks about mistakes as many authorities claim that cyber crimes are due to carelessness.

c. Email inspection

To control cyber-stalking and cyber defamation, there is need to make regular email inspection, which can be detected and tracked by the email headers along with the Internet Protocol (IP) address of the sender along with the date and time of the message when it was sent. On the basis of this information, the law enforcement agencies can get address and telephone number from the internet service providers.

d. Network Intrusion Detection systems

Every organization should implement the network Intrusion Detection systems as cyber crimes break the computer network for stealing the sensitive data which are more difficult to detect and track. Every incoming and outgoing traffic should be tracked and check whether these are allowed by the networks.

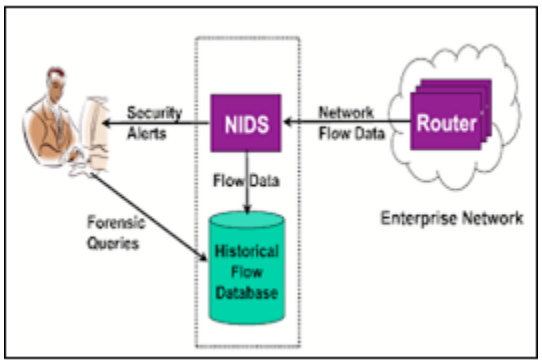

Figure.2. Intrusion Detection System

V. THE RESPONSE TO CYBER CRIMES

Regardless of your efforts to protect yourself, there are high chances that you become a victim of the cybercrime so there was great need of law enforcement agencies which will be able to handle and tackle cyber crimes and the key issues which are associated with such law enforcement agencies is

that the management of such federal law enforcement agencies is not able to understand the issues which are associated with cyber crimes. Things will be better with the passage of time, but still there is a big gap and lack of knowledge to handle cyber crimes issues proactively.

a. Local Law imposition

If you become the victim of the cyber crime and it is your responsibility to report crime to local police and if your local police is unable to handle that are refusing then report the incident to state police. The key issue is that the local police are getting better at reporting the victim information, but due to lack of knowledge, they are unable to process the cases.

b. Necessities in a police report

The following are the key things, which are, need to mention in the police report.

- The first and foremost thing is to mention Date of birth, vehicle number, social security number and ID card number, contact numbers, and e-mail addresses of every victim in the family circle. Financial account numbers which are involved in the theft.
- When, where and how the fraud or theft was happening and under what state of the affairs became the aware of the identity theft.
- The exact locations where counterfeit use of the identity occurred.
- There is need to mention names and addresses (home and work), the contact numbers, and date of birth of each and every individual who is involved in the confrontation.
- The Names of the monetary organizations who are the of the theft, along with names, addresses, and the contact numbers of investigators or customer service department who accepted report, report should contain the date and time.
- Need to include any letter, account statements and other supporting documents which are concerned with the case.

Victims should provide as much as much credentials are possible and they should make sure that each point is listed in the police report and they should obtain a report copy for their own record as well, as banks and other credit card companies ask for your report copy to support your claim.

c. Federal Law Imposition

There is a federal law imposition as in the United States, the cyber crimes are reported to the Federal Trade Commission (FTC) and to the local, state and national authorities.

National, state, local and some International Law enforcement agencies can access the Consumer Sentinel via an encrypted web site to decide whether a reported plot is local, regional, national, or international, and to the help blemish trends for the law enforcement. The web based protected provides the law enforcement a diversity of the tools to facilitate the investigations. Law enforcement whether those are national or state may or may not investigate more about the complaint, depending on amount, type of the crime, and where crime originated from.

VI. CYBER CRIMES PREVENTION STRATEGIES

There is great need to make timely, informed decisions about the effective controls, which can prevent the cyber crimes from the occurred and detect at the earliest stage.

The following are the key recommendations, which are, need to adopt and implement to handle such type of security threats.

a. Security Audit and Controls

Computer Security Institute (CSI) survey recommends that a cyber security audit is the main and the strongest weapon in the prevention and detection of cyber security vulnerabilities.

There should be effective and internal security audits, which should identify the cyber security risks and assessments of each type of risk.

It is recommended that the clients should ask their audit authorities to audit their privacy and security control and policies.

b. Business Insurance

In the era of technology where cyber crimes are motivated to gain financial benefits, each entity of the business should have sufficient business insurance to cover such type of financial losses.

Senior management should take necessary actions and steps and must evaluate the entity's insurance coverage to make sure that could recover estimated losses from the cyber crimes.

Business Insurance should be properly reviewed as per define time interval and leaders should also consider the service providers which offers cleanup and the restore function after the crimes have been committed.

c. Incident Response Plan

There is a need to develop an incident response plan. The employees should have the necessary level of knowledge and serving the key positions within the entities.

To answer the following key questions there are mainly five cyber crimes, which we identify in this paper:-

What type of crimes has potential risks?

Which risk is associated with which type of crime?

How we will respond to each type of crime?

What will be a recovery plan from the crime?

VII. CONCLUSION

Cyber crimes are increasing with the passage of time, as when the internet gaining popularity, the issues of security arises and need great attention.

In this paper, we investigate the key issues, which are needed to attention to prevent cyber crimes, and we discuss the main types of cyber crimes, whether those are related to individual level or on the international or national level.

We discussed the consequence and prevention techniques, which can be, used to handle cyber crimes. We propose three new strategies as well, which are specially designed and suitable for the financial sector as the major reason behind the cyber crimes is financial benefits.

To Sum up, Law enforcement agencies should play an active role and the companies, which are operating within the country, should enforce strictly follow the cyber rule and regulations to ensure cyber security.

VIII.REFERENCES

1. Adamski A. (1998) Crimes Related to the Computer Network. Threats and Opportunities: A Criminological Perspective. Helsinki, Finland: European Institute for Crime Prevention and Control, affiliated with the United

Nations (HEUNI). Retrieved on December 15 2006, from http://www.ulapland.fi/home/oiffi/enlist/resources/HeuniWeb.htm

2. Jewkes Yvonne (2006). Comment on the book Cyber crime and Society by Majid Yar, Sage Publications. Retrieved on December 15 2006, from http://www.sagepub.co.uk/booksProdDesc.nav?prodId=Book227351
3. Littlewood, A. (2003) Cyberporn and moral panic: an evaluation of pressreactions to pornography on the internet, Library and Information Research, 27(86), 818.
4. McKenzie, S. (2000). Child Safety on the Internet: An Analysis of Victorian Schools and Households using the Routine Activity Approach. A thesis submitted to the University of Melbourne, February, 2000. Retrieved on November15 2014, from http://www.criminology.unimelb.edu.au/research/internet/childsafety/index.html
5. Mann, David and Sutton, Mike, (1999). NetCrime. More Change in the Organisation of Thieving, British Journal of Criminology, vol. 38, no. 2, Spring 1998.
6. Thomas, D. and Loader, B. (2000) Introduction cyber crime: law enforcement, security and surveillance in the information age.
7. Thomas and B. Loader (Eds.), Cyber crime: Law Enforcement, Security and Surveillance in the Information Age, London: Routledge.
8. Yar, M. (2005) The Novelty of Cyber crime: An Assessment in Light of Routine Activity Theory European Journal of Criminology, Volume 2 (4): 407427:
9. Barton, P and Nissanka, V (2003), Cyber-crime Criminal Offence or Civil Wrong?, 19(5) Computer Law and Security Report, 401.
10. Bazelon, DL, Choi, YJ and Conaty, JF (2006), Computer Crimes, 43 American Criminal Law Review.
11. Bequai, A (2001), Organised Crime Goes Cyber, 20(6) Computers and Security, 475.
12. Brenner, S (2004), Cybercrime Metrics: Old Wine, New Bottles, 9.Virginia Journal of Law and Technology, 6.
13. Burden, K, Palmer, C and Lyde, B (2003), Cyber-Crime: A New Breed of Criminals?, 19(3) Computer Law and Security Report, 222.
14. Hale, C (2002), Cybercrime: Facts & Figures Concerning the Global Dilemma, 18(65) Crime and Justice International, 5.
15. Johnston, DR and Post, DG (1996), Law and Borders The Rise of Law in Cyberspace, 48 Stanford Law Review, 1367.
16. Kshetri, N (2005), Pattern of Global Cyber War and Crime: A Conceptual Framework, 11(4) Journal of International Management, 541-562.
17. Lewis, BC (2004), Prevention of Computer Crime amidst International Anarchy, 41 American Criminal Law Review, 1353.
18. Mazzitelli, AL (2007), Transnational Organised Crime in West Africa: The Additional Challenge 83(6) International Affairs, 1071-1090.
19. Mutume, G (2007), Organised Crime TargetsWeak African States, 21(2) African Renewal, 3.
20. Nykodym, N and Taylor, R (2004), The Worlds Current Legislative Efforts against Cyber Crime, 20(5) Computer Law and Security Report, 390.
21. Sommer, P (2004), The Future for the Policing of Cybercrime, 1Computer Fraud and Security, 8.
22. Ojedokun, AA (2005), The Evolving Sophistication of Internet Abuses in Africa, 37 The International Information and Library Review, 11.
23. Oriola, TA (2005), Advance Fee Fraud on the Internet: Nigerias Regulatory Response, 21 Computer Law and Security Report, 237.
24. Pounder, C (2001a), Cyber crime: the backdrop to the Council of Europe Convention, 20 Computers & Security, 311.
25. Pounder, C (2001b), The Council of Europe Cyber-Crime Convention, 20 Computers & Security, 380.
26. Sussman, MA (1999), The Critical Challenges From the International High-Tech and Computer-Related Crime at the Millennium, 9DukeJournal of Comparative and International Law, 451.
27. Tyson, D (2007),Cyber Crime: A Pervasive Threat, Security Convergence,81.