International Journal of Management, IT & Engineering
(ISSN: 2249-0558)

CONTENTS

Sr. No.	TITLE & NAME OF THE AUTHOR (S)	Page No.
1	**Role of Ontology in NLP Grammar Construction for Semantic based Search Implementation in Product Data Management Systems.** Zeeshan Ahmed, Thomas Dandekar and Saman Majeed	1-40
2	**Influence of Emotional Intelligence on Academic Self-Efficacy and Achievement.** Armin Mahmoudi	41-52
3	**Role of Online Education in Indian Rural Area.** Prof. Bhavna Kabra, Prof. Swati Sood and Prof. Nilesh Maheshwari	53-64
4	**Partitioning of Special Circuits.** Bichitra Kalita	65-77
5	**Modern Practices For Effective Software Development Process In Project Management.** S. Mohamed Saleem, R. Selvakumar and C. Suresh Kumar	78-109
6	**A Framework for IC-Technology enabled Supply Chains.** Dr. V. Krishna Mohan and G Bhaskar N Rao	110-132
7	**The Problem Of Outliers In Clustering.** Prof. Thatimakula Sudha and Swapna Sree Reddy.Obili	133-160
8	**A Comparative Study Of Different Wavelet Function Based Image Compression Techniques For Artificial And Natural Images.** Nikkoo N. Khalsa and Dr. Vijay T. Ingole	161-176
9	**Accession of Cyber crimes against Our Safety Measures.** Sombir Singh Sheoran	177-191
10	**The Problem Of High Dimensionality With Low Density In Clustering.** Prof. T. Sudha and Swapna Sree Reddy. Obili	192-216
11	**A study on role of transformational leadership behaviors across cultures in effectively solving the issues in Mergers and Acquisitions.** Prabu Christopher and Dr. Bhanu Sree Reddy	217-233
12	**ISDLCM: An Improved Software Development Life Cycle Model.** Sachin Gupta and Chander Pal	234-245
13	**Strategic Analysis of an MFI (Microfinance Institution): A Case Study.** Sunildro l.s. akoijam	246-262
14	**Applying E-Supply Chain Management Using Internal And External Agent System.** Dr. J. Venkatesh and Mr. D. Sathish kumar	263-274
15	**Video Shot Boundary Detection.** P. Swati Sowjanya and Mr. Ravi Mishra	275-295
16	**Key Performance Metrics for IT Projects.** Dr. S. K. Sudarsanam	296-316
17	**“M-Learning” - A Buzzword in Computer Technology.** Pooja Grover, Rekha Garhwal and Ajaydeep	317-341
18	**Survey on Software Process Improvement and Improvement Models.** Sachin Gupta and Ankit Aggarwal	342-357
19	**Integration of Artificial Neural Network and GIS for Environment Management.** Prof. N. S. Goje and Dr. U. A. Lanjewar	358-371

Editorial Board

Editorial Advisory Board

Title

ACCESSION OF CYBER CRIMES AGAINST OUR SAFETY MEASURES

Author(s)

Sombir Singh Sheoran

Research Scholar,

Dravidian University Kuppam

Abstract:

Cyber Crimes, or crimes perpetrated using digital technology and infrastructure, are rapidly growing problem. Yet digital evidence can be tied to more conventional crimes, so helping both police administrations, corporate executives and the public understand cyber complexities is important. Various types of offenses under Computer crimes also reflect the extent to which computers have entered our lives. Our research is about a variety of issues including their levels of experience and training, their job functions, and the problems they experience in their day –to –day work. We find that the largest organization world-wide dedicated to the advancement of training education and information sharing information between law enforcement and corporate cybercrime investigation

Keywords: cybercrime, hacker, intrusions, internet, Security.

1. Introduction:

Cyber technology is like a sword that has double edge which can be used for constructive as well as destructive work .A malicious intention in the form of hacking, data theft, virus attack, etc.can bring only destructive results unless and until these methods have been used for checking the security ,authenticity and safety of the technological device which has been primarily relied upon and trusted for providing the security .It would be better than else if we concentrate on security factors in a separate but coherent and holistic manner. The need of the today is to set priority for a safe and secure electronic environment so that its benefits can be achieved to the maximum possible extent.

Computer crime or cyber-Crime is becoming the biggest problem to the modern societies. In the most of Countries the biggest challenge that faces law enforcement is the cyber crimes.

Cyber crime can be divided into two categories:

1. Cyber –Crime in which computer are used as tool to aid Criminal activity such as producing false identification ,reproducing copyright materials, and many other things.

2. Cyber-crimes in which computers are used target, and probably a tool ,to attack organizations in order to steal or damage information, attack banks to make unauthorized money transactions ,steal credit numbers, and many other activities.

According to Computer Security Institute 85% large corporations and government agencies in the US detected computer security breaches during the year 2001.64% of them suffered from financial losses due to computer breaches.95% of these agencies and corporations detected computer viruses. The Same source reported that there were 25000 attempted intrusions into the US defense system during the same year; out of this number 245 attempts were successful.

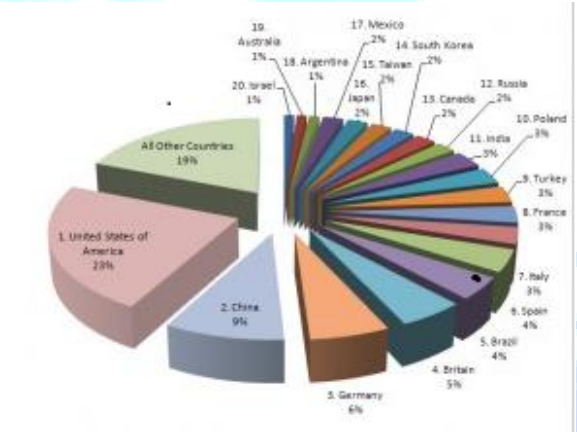


Figure 1 Cyber crime of top 20 countries [29]

2. The Business of Cybercrime:

Globalization with internet offers many benefits to consumers and businesses. Unfortunately, globalization with internet also offers several opportunities for organized crime. Rather than going it alone, many Internet criminals' job organized crime groups or they create new ones. Whether the reasons are technical or economical the motivations behind joining the virtual criminal universe are plentiful. All of the web world, some individuals and many organized mafia or crime groups carry out various illegal acts on the web, often in the hope of becoming rich.

Every day thousands of pieces of information misappropriated, stolen and sometimes even fake credit cards are sold by cyber criminals. Three packages are typically offered:-

To gather personal information of user, cyber criminals are exploiting software vulnerabilities and human psychology to spawn a broad ranged malware and threats including spyware,phising,botnets,adware,rootkits,spam and on safe websites. They no longer deliver threats only via spam and are taking advantages of popular social networking sites to secure personal indentify information. The Cyber World is also using new practices in an effort to sell fake or malicious security software that is either misleading or outright fraudulent.

Many Consumers are shopping online, taking advantage of the discounts or other schemes.They need to be aware of the security risks that exist and protect themselves against spam and malware attacks by using the latest security software with real-time malware updates and be vary of sharing any personal information even if it is a popular website.

3. Crimes in cyber Space:

Security officials and law enforcement know it, and so do insurance professionals. In fact, their expectations of cyber liability to be one of the fastest-growing segments of the internationals property and casualty markets Computer-related illegal criminal activities are a growing problem in the modern marketplace, according to the National Association of Insurance Women. In fact, some cyber security group has listed cyber crime prevention as an industry focus in some last years. Officials modern technologies and the availability of the Internet, they lament its abuse by thieves and scammers .In these days some agencies are writing Combination coverage for theft, property and liability coverage.

4. Attack Access Points:

A networks' known weak spots can help you identify possible access points for attacks (the areas where hackers enter a network).The Following are some common access points for attacks:

1. Hosts that are running unnecessary services(Such as FTP)
2. Networks software that is outdated or unpatched.
3. Firewalls those are full of holes.
4. Passwords that is old, obvious, or weak.

5. Information's that is being leak from services such as and gopher.
6. Security that is not well-defined.
7. Software that are installed on the network without the knowledge of the staff.

Passive and Active Attacks:

Two primary Types of security attacks are Passive attacks and active attacks. Passive attacks typically focus on stealing data. For example ,a hacker can use a sniffer tool or a protocol analyzer to read password,usernames,e-mail messages, and even the data that crosses the wire.

In the Active attacks, attempt to cause harm typically through system faults or brute force Most of the active attack can attempt to overload the victims computer that it either slows to an unusable crawl hangs, or completely crashes.

5. Identifying the Suspicious Behavior:

If we having the right set security tools it will help you identifying specific communication patterns that could be considered suspicious .Port scanner tool is used to find what processes or daemons are running on the device. The device which is performing the scan sends a series of packets on different destinations port numbers.

A hackers uses port scanner tools to find which ports are active on system. Typically ,a hacker will run a port scanner over both UDP and TCP connections .Therefore the hackers knows the ports that are in active state the hackers can begin to exploit there services and look for weakness of system. For example, the echo processes defines that each character sent to the target will be echoed back. An attack uses echo and charge to echo back data.

6. Preparations and Prevention:

You must be prepared to detect network intrusions Preparation includes defining a implementing security procedures, security policy, and activating or developing the tools required to detection of these intrusions. Recommendation of the following four steps plan:

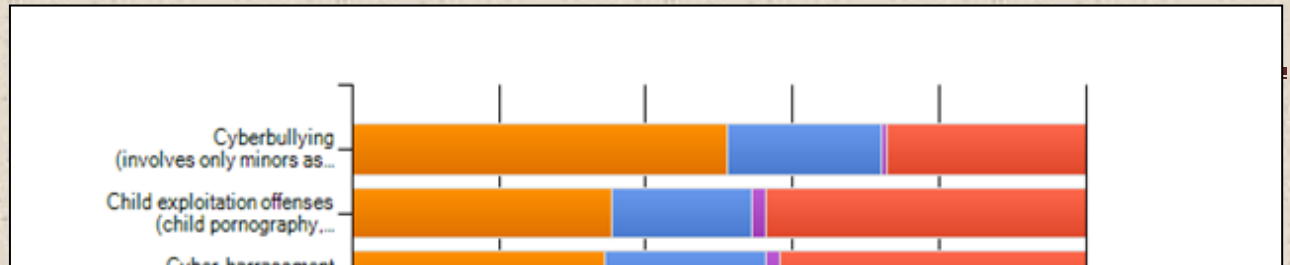
1. Establish a policy for security and procedures that prepare you to detect signs of intrusion.
2. Enable and identify the system and network mechanisms of logging.

3. Detection of intrusions can be done by installations of detection tools.
4. Time to Time verify the integrity of year's system and data.

The tools that you implement on your network should be able to help you detect the following events:

1. Passwords cracking.
2. Execution of unauthorized programs.
3. Installations of tools (network analyzers) that may be used to break into other systems.
4. Internet Relay Chat (IRC).
5. Intruder use of unexpected or unrecognized hosts.
6. Intruder access during non-business hours.
7. Intruder files transfer of tools to be used in launching attacks.
8. Virus infiltration.
9. System or key image files changes.

Most vendors also maintain a security advisory team to announce possibility of security holes and the patches to fix such violations .The most effective methods of securing your system network is to keep software up-to-date.



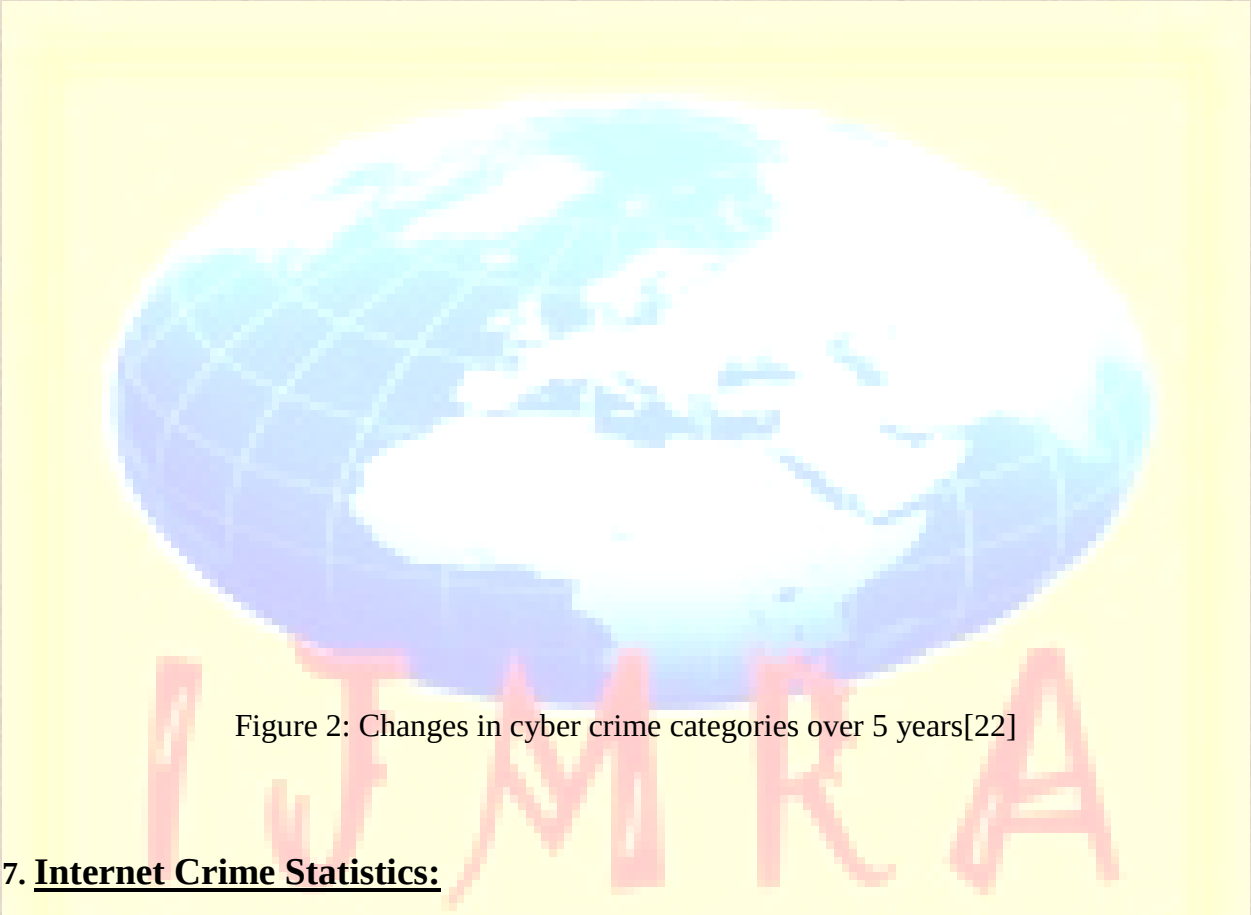


Figure 2: Changes in cyber crime categories over 5 years[22]

7. Internet Crime Statistics:

The latest internet statistics on the various websites indicated that in the year 2001 there were 5700000 intrusions done by hackers.12% of these intrusions caused damage.80% of these intrusions were done by insider hackers and 20% by outsiders hackers. These intrusions cost about 6.5 Billion U.S Dollar in stolen with telephone credit cards. The rate of increase in those crimes is growing very quickly.

The FBI reports that the total U.S.Dollars loss from all cases of Internet Crime Complaints center was $689.7 million in 2010.That,s more than double the previous year:$344.6 million. And the number of Complaints grew substantially as well: 336655-a 22.3 percent jump from 2009's 275284. In 2010 the million dollar loss from these incidents was $675.

Conclusions and Future Work:

The current ways of dealing with cybercrimes are primarily reactive .that is to say ,in spite of the ability to be proactive especially with regard to catching child predators or malicious hackers ----investigators are still in the position of responding to problems rather than seeking them out .

The research clearly shows the need for better support in the following areas:

Public Education:

Public Education is an important activity.However; they lack time and resources to do more of it. The task often fall to detectives or prosecutors, or in the private sector, information technology professionals----who may or may skilled educators.

Dedication of training may instead benefit everyone, breaking down complex topics so that community members and employees can easily understand prevention, while organizational decision-makers can understand resource allocation needs.

Organizational training:

Employee of both corporate organizations and law enforcement must be better trained to handle digital evidence field triage, evidence previews and even rudimentary evidence collection can free investigators and forensic examiners to focus on investigators and analysis

The focus of the training should not just be on forensics. Digital evidence collection across the board comes from basics patrol activity to crime scenes, Internet to network intrusions. Additional organizational training should include multiple levels of educations for all personnel within the organization involved in the investigation or collection of digital evidence.

References:

- Abreu, Elinor Mills: US Firms Announce New Security Technology, www.dailynew.yahoo.com, 2002
- Andamski, A.: Crimes Related to the Computer Network, Threats and Opportunities. A criminological perspective. www.infowar.com/new. 1999.
- CERT Coordination Center, How FBI investigates computer crime, www.cert.org
- Chandler, N.: Profile of a Computer hacker. Florida: infowar. 1996.
- Denning, Dorothy E. and Baugh, William E. Jr. 1999: Hiding crime in Cyber space, Information, Communication and Society: Vol. 2, No.3, Autumn 1999.
- IBM global security analysis lab, York Town Heights, New York.
- International Web Police, Latest internet statistics, www.web-police.org
- Lemos, Robert: Security Confab Call for US Spending, www.news.com, 2002
- Lyman, Jay: In Search of the World's Costliest Computer Virus, www.newsfactor.com, 2002
- Parker, D.: Fighting computer crime: A new frame-work for protecting information. John Wiley & Sons Inc., New York, 1998.
- Rogers, Marc: New hacker taxonomy, University of Manitoba.
- Rogers, Marc: Security threats, University of Manitoba.
- Weisman, Robyn: US Security Holes: Don't Blame Technology, News Factor Network, 2002
- Baturin Y.M., Zodzyshsky A.M., Computer crime and computer protection. 1991. — 158p.
- Collin Barry C. The Future of CyberTerrorism, Proceedings of 11th Annual International Symposium on Criminal Justice Issues. The University of Illinois at Chicago, 1996.
- A Report of the International High Tech Crime Investigation Association, HTCIA, 2010.
- Internet Crimes Website, http://arstechnica.com/web/news/2010/losses-from-internet-crime-more-than-doubled-in-2010.
- Darrel Menthe, Jurisdiction In Cyberspace: A Theory of International Spaces 4 Mich.Tel.Tech.L.Rev.3, 1998.

- Security of computer systems: prevention crime in the field of computer information. /Vertuzaev,Golubev, Kotlyrevsky, Yurchenko/– Zaporozhye.–—Pavel‖.1998.- 316 p. ISBN 66-7340.12-0 /Under common edition Dr., Professor Alexander P. Snigeryev/.
- Vladimir Golubev, Alexander Urchenko Crimes in the field of computer information.– Zaporozhye.–—Pavel‖. – 1998. – 157 p.
- Vladimir Golubev Software-technical means of protection from computer crime. – Zaporozhye.–—Pavel‖. – 1998. – 144 p.
- www.crime-reserch.org
- www.pyramidcyber.com
- www.mcafee.com/us/resources/white-papers/wp-cybercrime-hactivism.pdf
- www.abc.net.au/technology/articles/2010/12/09/30883
- www.provision.ro/threat.../platform.../cybercrime-and-hacktivism
- www.documentsecuritysuites.net/pdfs/CCRC_052808.pdf
- http://www.independent.ie/business/technology/cybercrime-uncovered-1232152.html
- http://blog.knowbe4.com/category/cybercrime-2/
- Kulvinder singh:"Increment in Cyber crime against our securities