Increment of Cyber Crimes against Our Securities

Kulvinder Singh
Assistant Professor, Vaish College of Engineering, Rohtak, India
kulvinderbhum@gmail.com

Abstract
The cybercrimes, or crimes perpetrated using digital technology and infrastructure, are a rapidly growing problem. Yet digital evidence can be tied to more conventional crimes, so helping both police administrators, 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 worldwide dedicated to the advancement of training, education and information sharing information between law enforcement and corporate cybercrime investigators.

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

1. Introduction
The 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 cybercrimes.

Cyber-crime can be divided into two categories:

1. Cyber-crimes in which computers are used as a tool to aid criminal activity such as producing false identifications, reproducing copyright materials, and many other things.

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

According to Computer Security Institute 85% of 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 25,000 attempted intrusions into the US defense system during the same year; out of this number 245 attempts were successful.

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 join 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.

Everyday 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 a user, cybercriminals are exploiting software vulnerabilities and human psychology to spawn a broad range of malware and threats including spyware, phishing, botnets, adware, rootkits, spam, and unsafe websites. They no longer deliver threats only via spam and are taking advantage of popular social networking sites to secure personal identify information. The cyber
underworld 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 increasingly 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 wary 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 international property and casualty market. 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 cybercrime 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 network’s known weak spots can help you identify possible access points for attack (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. Network software that is outdated or unpatched.
3. Firewalls that are full of holes.
4. Passwords that are old, obvious, or weak.
5. Information that is being leak from services such as telnet 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 passwords, 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 attacks can attempt to overload the victim's computer that it either slows to an unusable crawl, hangs, or completely crashes.

5. Identifying the Suspicious Behavior

If we having the right set of security tools it will help you identify specific communications 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 destination port numbers.

A hacker 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 hacker knows the ports that are in active state, the hacker can begin to exploit these 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. Preparation 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 intrusion can be done by installation of detection tools.
4. Time to time verify the integrity of your systems and data.
The tools that you implement on your network should be able to help you detect the following events:

1. Password cracking.
2. Execution of unauthorized programs.
3. Installation 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 system 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.

### 7. Internet Crime Statistics

The latest internet statistics on the various websites indicated that in the year 2001 there were 5,700,000 intrusions done by hackers. 12% of these intrusions caused damage. 80% of these intrusions were done by insider hackers and 20% by outsider hackers. These intrusions cost about 6.5 Billion U.S. Dollars in stolen by software and 1.5 Billion U.S. Dollar in stolen with telephone credit cards. The rate of increase in these crimes is growing very quickly.

The FBI reports that the total U.S. dollar loss from all cases of Internet Crime Complaint 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: 336,655—a 22.3 percent jump from 2009's 275,284. In 2010 the million dollar loss from these incidents was $675.

![Figure 1 - Changes in Cyber Crime Categories Over 5 Years](image-url)
8. 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 falls to detectives or prosecutors, or in the private sector, information technology professionals—who may or may not be 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**
Employees 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 investigative and analysis activities. The focus of the training should not just be on digital forensics. Digital evidence collection across the board comes from basic patrol activity to crime scenes, from the Internet to network intrusions. Additional organizational training should include multiple levels of education for all personnel within the organization involved in the investigation or collection of digital evidence.

**References**


3. CERT Coordination Center, How FBI investigates computer crime, [www.cert.org](http://www.cert.org)


12. Rogers, Marc: Security threats, University of Manitoba.


22. [www.crime-researh.org](http://www.crime-researh.org)

23. [www.pyramidcyber.com](http://www.pyramidcyber.com)


27. [www.documentsecuritysuites.net/pdfs/CCRC_052808.pdf](http://www.documentsecuritysuites.net/pdfs/CCRC_052808.pdf)