Analele Universităţii "Dunărea de Jos", Galaţi - Fascicula XXII
***Drept şi Administraţie Publică* Anul II, Nr. 1 – 2009**
Galati University Press ISSN 1843 -8334

Adriana TUDORACHE

PREVENTING AND COMBATING CYBER CRIMES

Abstract

Recent and anticipated changes in technology arising from the convergence of communications and computing are truly breathtaking, and have already had a significant impact on many aspects of life. Banking, stock exchanges, air traffic control, telephones, electric power, health care, welfare and education are largely dependent on information technology and telecommunications for their operation. We are moving towards the point where it is possible to assert that everything depends on software.

This exponential growth, and the increase in its capacity and accessibility coupled with the decrease in cost, has brought about revolutionary changes in every aspect of human civilization, including crime.The increased capacities of information systems today come at the cost of increased vulnerability. Information technology has begun to produce criminal opportunities of a variety that the brightest criminals of yore couldn't even begin to dream about.

Nowadays, the one place that people thought they were secure could be one of the most dangerous areas in society. Computer use is increasingly spreading, and more and more users are connecting to the Internet. The Internet is a source for almost anybody to access, manipulate and destroy others' information. These "criminal activities directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored on-line data, or sabotage of equipment and data" are defined as computer crimes according to the American heritage dictionary (2000). Even though companies strive hard to prevent these criminal activities, companies are still fighting a losing war against computer invasions ("Experts: Computer Hacking", 1999). Although computer "hacking" has become a growing concern, much is being done to address this problem.

To better understand the situation, users and companies must be aware of the indicators that problems with computer crime do exist. One of these indicators is that many companies are involved in computer crimes. Eighty-five percent of companies reported security breaches in their systems, and 94% detected viruses in their systems in 2001 ("Computer Crime Soaring," 2002). Furthermore, the U. S. Defense Department was also hacked many times. It alone was hit by about 250,000 hacks in 1995 (Allbritton, 1998). These hacks aren't minor, hack damages cost a lot of money. Hacking resulted in a cost of about 377 million dollars ("Computer Crime Soaring," 2002). This problem is also rising and needs to be quelled. Break-ins are rising rapidly and double every year ("Experts: Computer Hacking," 1999).

Companies and users must also be aware of who the hackers are and of their victims. The victims of hacks come in an extensive range. The major targets for most hackers are fortune 500 companies, who are big names and make a lot of money (Allbritton, 1998). "If this [breach of security system] could happen to Microsoft, this can happen to anybody," said Sandra England, president of PGP Security (Markoff, 2000, p. A5). The fact is, though, that every online--computer user is at risk. A hacker can penetrate virtually any computer on the Internet if he has the right tools ("Experts: Computer Hacking," 1999). In addition to knowing the victims, users and companies should know who the hackers really are. The real bad guys are often just mischievous youth trying to steal credit cards or breaking into advanced systems. A hacker going by the pseudonym "Route" says the major hackers are generally "this tiny minority of 13- to 18-year olds who learned to make toll calls for free" (Allbritton, 1998, p. A4). Moreover, some people even hack in online gaming to steal another's virtual items, which can also be sold over the Internet for money (Ward, 2003). Most hackers, though, are actually crackers and don't hack to do real damage but only want to embarrass big-name companies (Ma, n.d.). However, many people are still accessing data with criminal intent. These people can vary from revengeful employees trying to backstab their company to foreign spies wanting to access government files. Some do it simply to steal money, valuable objects or code (Allbritton, 1998). Interestingly enough, half of unauthorized system intrusions involve insiders who actually have legitimate access to the system (Schindler, 2000).

The new breed of crime, which is either perpetrated using computers, or is otherwise related to them, is broadly termed as Cyber Crime.

Methods of Perpetration:

1. **Unauthorized access**
2. **E-mail bombing**
3. **Data diddling**
4. **Salami attack**
5. **Internet time theft**
6. **Logic bomb**
7. **Virus/Worm attack**
8. **Trojan attack**
9. **Denial of service attack**
10. **Distributed denial of service attack**
11. **E-mail spoofing**
12. **Intellectual Property Crime**
13. **Cyber stalking**

Unauthorized access (cracking, not hacking):

Unauthorized access also known as cracking as opposed to hacking, means gaining access to a system without permission of the users or without proper authority. This is generally done either by faking identity, or by cracking access codes.

E-mail bombing:

This means sending a large number of mails to the victim resulting in the victims mail account (in case of individual) or server (in case of corporations) crashing.

Data diddling:

This kind of attack involves altering the raw data before it is processed by a system and re-altering it after processing.

Salami attack:

This is generally used to commit financial crimes. Here the key is to make the alteration so small that in a single case it would go unnoticed. For example, a bank employee deducts five rupees from every customers account. The individual customers are unlikely to notice this small change but the employee will make a significant earning.

Internet time theft:

This connotes the usage by an unauthorized person of Internet time paid for by someone else.

Logic Bomb:

This is an event dependent program. This implies that this program is created to do something only when a certain event occurs (e.g., the Chernobyl virus)

Virus/Worm attack:

A virus is a program, which attaches itself to another file or a system and then circulates to other files and to other computers via a network. They usually affect computers by either altering or deleting data from it. Worms on the other hand do not interfere with data. They simply multiply until they fill all available space on the computer.

Trojan attack:

A Trojan is a program, which appears to be something useful but under the disguise of a useful program causes some damage.

Denial of service attack:

This involves flooding the computer resource with more requests than it can handle. This causes the resource to crash, thereby denying the authorized users of the service.

Distributed denial of service:

This is a denial of service attack in which the perpetrators are more than one in number and geographically displaced. It is very difficult to control such attacks.

E-mail spoofing:

A spoofed email is one, which appears to originate from one source but actually originates from another.

Intellectual property crime:

This is a crime, which involves the unauthorized copying and distributing of copyrighted software. Software piracy is an example.

Cyber stalking:

This involves following a person on the Internet and causing harrassment.

Hackers have many ways of hacking and gaining access to systems. One common way of getting almost anything out of a computer is by utilizing a virus. By accessing the network a hacker can easily put a virus in the source code of big-name programs like Windows and Office, which will damage computers that run or use this software (Markoff, 2000). One of the types of viruses are Trojan horses, which are hidden instructions embedded in software or email that, once opened, may modify, damage or send important data. Another type of virus is the logic bomb, a virus that is placed on a computer to run after a specified amount of time, allowing time to clear up the evidence (Information Systems Unit, n.d.). Other ways that hackers hack are by using program bugs. Examining the original program's instructions can let a vandal find vulnerabilities in programs not known to other people and use them to his benefit (Markoff, 2000). Another problem with these bugs is that even after bugs are found, a company may spend months before releasing a fix for it ("White Paper: Lies," 1999). Furthermore, many hackers utilize vulnerabilities involving computer use. One of these methods is called data diddling. This is when a hacker modifies certain programs to send certain information such as passwords and names back to him when other people use these programs. Many hackers also gain access to systems by guessing passwords. Users often have simple passwords that someone could guess by knowing a few things about the person (Information Systems Unit, n.d.). A hacker may even simply pose as a member of a department to gain access to certain data (Schindler, 2000).

Varieties of Cyber Crime:

1. **Theft of Information Services**
2. **Communications in Furtherance of Criminal Conspiracies**
3. **Telecommunications Piracy Act**
4. **Electronic Money Laundering**
5. **Electronic Vandalism and Terrorism**
6. **Sales and Investment Fraud**

7. Illegal Interception of Telecommunications

Theft of Information Services:

The 'phone phreakers' of three decades ago set a precedent for what has become a major criminal industry. Here the perpetrators gain access to the PBX board of an organization, and make their own calls or sell call time to third parties.

Communications in Furtherance of Criminal Conspiracies:

Just as legitimate organizations use the information networks for record keeping and communication, so too are the activities of criminal organizations enhanced by the advent of information technology.

There is evidence of information systems being used in drug trafficking, gambling, money laundering and weapons trade just to name a few.

Telecommunications Piracy Act:

Digital technology permits perfect reproduction and easy dissemination of print, graphics, sound, and multimedia combinations. This has produced the temptation to reproduce copyrighted material either for personal use or for sale at a lower price.

Electronic Money Laundering:

For some time now, electronic funds transfers have assisted in concealing and moving the proceeds of crime. Emerging technologies make it easier to hide the origin and destination of funds transfer. Thus money laundering comes to the living room.

Electronic Vandalism and Terrorism:

All societies in which computers play a major role in everyday life are vulnerable to attack from people motivated by either curiosity or vindictiveness. These people can cause inconvenience at best and have the potential to inflict massive harm.

Sales and Investment Fraud:

As electronic commerce or e-commerce as it is called becomes more and more popular, the application of digital technology to fraudulent crime will become that much greater.

The use of telephones for fraudulent sales pitches or bogus investment overtures is increasingly common. Cyberspace now abounds with a wide variety of investment opportunities, from traditional securities such as stocks and bonds to more exotic opportunities like coconut farming.

Fraudsters now enjoy access to millions of people around the world, instantaneously and at minimal cost.

Illegal Interception of Information:

Developments in telecommunications as well as data transfer over the net have resulted in greater speed and capacity but also greater vulnerability. It is now easier than ever before for unauthorized people to gain access to sensitive information.

Electromagnetic signals emitted by a computer, themselves can now be intercepted.Cables may act as broadcast antennas.

To add to this no existing laws prevent the monitoring of remote signals from a computer. Under the circumstances information is more and more vulnerable to unauthorized users.

Computer crime can cause many damaging results. For one, computer crime can cause damage involving data. Once inside, a hacker can steal desired items such as credit-card number and passwords ("White Paper: Lies," 1999). He can also manipulate and destroy crucial data such as bank accounts, legal files or personal information (Zikun, n.d.). In addition, hackers can take control of various services, including one time when hackers figured out how to control the phone service nationwide in order to win prizes on phone-related games (Schindler, 2000). Computer crime can also cause business failure. Hacking has caused government sites to temporarily and permanently shutdown, giving users and employees denial-of-service errors when trying to access them ("Experts: Computer

Hacking," 1999). Hacks resulting in losing credit-card numbers or social-security numbers can result in costly lawsuits, threatening bankruptcy for the company (Schindler, 2000). Moreover, after websites are hacked, businesses often lose their credibility, and consumers look elsewhere for the services ("White Paper: Lies," 1999).

Stopping computer crime would raise many problems. For one thing, hacking is very easy to do for almost anyone. With so many free hacking tools available, almost anyone can go around networks and attack machines ("Experts: Computer Hacking," 1999). Furthermore, hackers identify themselves with anonymous names so that tracing a crime back to its source can be difficult (Allbritton, 1998). Even the government has a critical shortage of trained computer scientists for defense. Most go to the private industry, and the current government systems designers haven't been careful with protecting their sites ("Experts: Computer Hacking," 1999). Current anti-virus protection is also another problem with stopping computer crime. Standard anti-virus protection is limited in that it can only find known viruses, leaving new viruses to devastate a user or companies systems (Kabay, 2000). Besides, having bad protection against computer crime, companies have bad detection of computer crimes. A study by the U. S. Department of Defense, where they attacked 38,000 of their own computers and penetrated 65% of them, detected only 4% and only reported 1% of them (Schindler, 2000). Moreover, most hacks are detected only long after the attack took place (Allbritton, 1998). Prosecution of computer crimes is also inadequate. Getting evidence to prove a crime was committed can be hard since data is so easily manipulated before and after a crime takes place (Ward, 2003). In addition, computer crime has an inadequate punishment system. Even if a computer crime is committed, the hacker is given a punishment that doesn't fit the crime, and the victim is required to take most of the action (Zikun, n.d.).

Prevention methods:

1. **Firewalls**
2. **Frequent password changing**
3. **Safe surfing**
4. **Frequent virus checks**
5. **Email filters**

Firewalls:

These are programs, which protect a user from unauthorized access attacks while on a network. They provide access to only known users, or people whom the user permits to.

Frequent password changing:

With the advent of multi-user systems, security has become dependent on passwords. Thus one should always keep passwords and sensitive data secure. Changing them frequently, and keeping them sufficiently complex in the first place can do this.

Safe surfing:

This is a practice, which should be followed by all users on a network. Safe surfing involves keeping one`s e-mail address private, not chatting on open systems, which do not have adequate protection methods, visiting secure sites. Accepting data only from known users, downloading carefully, and then taken from known sites can also minimize the risk.

Frequent virus checks:

One should frequently check one`s computer for viruses and worms. Also any external media such as floppy disks and CD ROMS should always be virus checked before running.

Email filters:

These are programs, which monitor the inflow of mails to the inbox and delete automatically any suspicious or useless mails thus reducing the chances of being bombed or spoofed.

Although users have many problems facing them involving using the Internet, they also have several ways of preventing these problems. For instance, they have many ways to keep their passwords secret. To keep someone from guessing their passwords, they should use special characters, numbers and letters and use at least eight characters. In

addition to keeping their passwords safe, they can use and upgrade certain software to prevent problems with their system. Firewalls allow the user to set policies on his system that will block unwanted data, hidden content or message attachments from his system. The user should also use anti-virus software that can detect logic bombs, Trojan horses and known viruses (Information Systems Unit, n.d.). Users need to upgrade their software whenever it is available to prevent the majority of problems ("White Paper: Lies," 1999). Furthermore, hackers can help prevent problems. Many elite hackers now work to find weak spots in networks and publicly display them so companies will fix them (Allbritton,1998).

In addition to having users prevent such problems, companies have many ways to improve their security systems. Companies need to reevaluate their security systems and respond accordingly. "Companies need to re-evaluate their own security policies and infrastructure," said Sandra England (Markoff, 2000, p. A5). A business should regularly assess its vulnerabilities and respond accordingly with buying firewalls, installing software or upgrading security (Schindler, 2000). Moreover, companies can undertake various actions to improve their security systems. A company should perform regular audits and supervise their employees well. It should also use software to detect for modification of programs (Information Systems Unit, n.d.). Other actions that they should undergo include background and security checks that should be performed on important computer personnel (Schindler, 2000). Companies also need the proper security to handle computer crimes. "Organizations need to properly fund, train, staff and empower those tasked with enterprise-wide information security," said Patrice Rapalus, director of the Computer Security Institute ("Computer Crime Soaring," 2002). Many businesses are also hiring good-guy hackers to prevent bad-guy hackers from breaching their systems (Allbritton, 1998). Reducing networking is another simple solution to improving a company's security system. "Government agencies need to reconsider and probably pull back from their embrace of networking," said James Dempsey, senior staff council for the Center of Democracy and Technology.

Other improvements need to be made by the government to detect criminals better. For one, the government needs to upgrade their systems... Our country and other agency systems are currently using systems that are

at least ten-years old, and they need to upgrade them for better detection (Help Net Security, n.d.). Better employee training and funding should also be done to help catch criminals. Most government agencies have inadequate personnel for catching computer criminals and need to train and fund better and more qualified people (Help Net Security, n.d.). Several agencies have already been set up to help detect criminals and are helping solve this problem. Moreover, many actions are already being taken and need to be taken to punish the hackers. Many new laws are both needed and have been implemented to punish computer criminals. Cyber-criminal laws need to be more severe towards lawbreakers and should establish rules of conduct to clearly define what is illegal (Zikun, n.d.)Most cyber crimes in Romania are currently aimed at the illegal gaining of material benefits,' said Eduard Bisceanu, expert in information security with the Romanian Intelligence Service (SRI), at the opening of a conference dubbed CyberSecurity.

Bisceanu did not disclose the official number of such crimes, but mentioned that the Romanian Police, through its subordinated institutions, can supply such data. Bisceanu specified that not only Romania, but also other EU countries and NATO partners are victims of the cyber crime.

'The danger of cyber terrorism is significant for both Romania and the NATO and EU states. There area several cyber crime cells in Romania and they have the capacity to initiate IT attacks,' Bisceanu explained.

However, he stated that no individuals, groups or organizations able to pose a threat to national security have been found on Romania's territory.

Cyber crime cases in Romania in 2008 targeted mainly the bankcard fraud. According to the General Department for the Combat of Organized Crime (DGCCO), losses of 500 million euro are expected this year.

Conclusion

With the information highway having entered our very home places, we are all at increasing risk of being affected by Cybercrime. Everything about our lives is in some manner affected by computers. Under the circumstances it`s high time we sat up and took notice of the events shaping our destinies on the information highway. Cybercrime is everyone's problem. And it`s time we did something to protect ourselves. Information is the best form of protection.

In short, although computer "hacking" has become a growing concern, much is being done to address this problem. Many problem indicators show that this is a big problem that needs to be solved. The almost limitless number of possible victims for the variety of hackers makes computer crime hard to stop, and hackers have many different ways of hacking, and the results can be catastrophic. The government and companies also have bad protection for preventing the intrusions and many problems with stopping the hackers. However, even though computer crime is a big problem, much can be and has already been done to help fight it. Users and companies have many ways to protect themselves from these invasions, and the government has many ways to help defend the companies and users from the hackers. Also, many actions have already been and need still to be taken to help punish hackers. "While some regard hackers as a threat, others think they are a manageable problem" (Ma, n.d.). If these solutions are undertaken, the world of computer usage will no longer be a dark, dangerous alley for criminals to tamper with and will become a haven for anyone who wants to come.

References

1. Cyber Crime (article), Silicon Times, Vol. 2, Issue 12, December 2002
2. Computer Vulnerabilities, Eric Knight, CISSP, Electronic Edition, March 2000, release 4
3. An Unofficial Guide to Ethical Hacking, Ankit Fadia, Macmillan India Ltd., 2001
4. The Little Black Book of Computer Viruses, Mark Ludwig, Electronic Edition, American Eagle Publications, 1996
5. Allbritton, C. (1998, September 20). Hackers in white hats. The Wichita Eagle, pp. A4, A6.
6. Computer crime. (2000). In „The American heritage dictionary of the English language": Fourth edition. Retrieved March 12, 2004, from http://www.bartleby.com/61/88/C0538800.html
7. Computer crime soaring. (2002, April 8). BBC News. Retrieved March 11, 2004, from http://news.bbc.co.uk/1/low/sci/tech/1916655.stm
8. Experts: Computer hacking is a growing threat to U. S. (1999, August 9). The Wichita Eagle, p. A5.
   Frontline. (n.d.). Computer crime laws. Retrieved April 1, 2004, from http://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html

9. Help Net Security. (n.d.). The FBI fights computer crime. Retrieved March 18, 2004, from http://www.net-security.org/article.php?id=34
10. Information Systems Unit. (n.d.). Computer crime prevention. Retrieved March 18, 2004, from http://www.nrps.com/isu/comprev.eht
11. Kabay, M. E., &Walsh, L. M. (2000, December). The year in computer crime. Information Security Magazine. Retrieved March 11, 2004, from http://infosecuritymag.techtarget.com/articles/december00/features.htm
12. Ma, V. (n.d.). Net virtues become vices in hands of mischief makers (University of Hong Kong Journalism and Media Studies Centre). Retrieved March 11, 2004, from http://jmsc.hku.hk/students/jmscjournal/advance/velentina.htm
13. Markoff, J., &Schwartz, J. (2000, October 28). Hackers hit Microsoft. The Wichita Eagle, pp. A1, A5.
14. Schindler, D. J., &Halpern, T. H. (2000, March 27). WWW.computer.crime: E-crime and what to do about it. Los Angeles Business Journal. Retrieved March 11, 2004, from LookSmart database.
15. Ward, M. (2003, September 29). Does virtual crime need real justice? BBC News. Retrieved March 11, 2004, from http://news.bbc.co.uk/2/hi/technology/3139456.stm
16. White paper: Lies, damned spies and computer crime statistics. (1999, July 22). ComputerWeekly.com. Retrieved March 18, 2004, from http://www.computerweekly.co.uk/Article42001.htm
17. Zikun, N. I., Maksimenko, E. V., &Zharov, A. V. (n.d.). Security of information systems and problem of detecting computer crimes in the practical activities of the operative departments fighting against crimes in the field of intellectual property and high information technologies. Computer Crime Research Center. Retrieved March 18, 2004, from http://www.crime-research.org/eng/library/Zikun28.htm