# Hacking And Cybercrime

Nataliya B. Sukhai
6675 Williamson Drive
Atlanta, Georgia 30328
+1 404-943-1019
nbsukhai@att.net

## ABSTRACT
This paper explores the fast growing Cyberworld and its components. It starts with definitions of who is the hacker, and what is a cybercrime. Types and offenses of cybercrime are addressed as well. The paper concentrates on the possibilities to protect ourselves from the cybercrime, and guard Cyberworld from us. Therefore, it emphasizes the importance of users' education, starting from the early age, creation and enforcement of policies, and awareness training. The paper presents laws, applicable to the computer related crime, highlights the U.S. Department of Homeland Security involvement, and investigates on the fact why businesses do not report hackers' attacks and why is it important.

## CATEGORIES AND SUBJECT DESCRIPTORS
K.6.5 [**Management of Computing and Information Systems**]: Security and Protection- *Unauthorized access (e.g., hacking, phreaking)*

## GENERAL TERMS
Security, Legal Aspects.

## KEYWORDS
Cybercrime, Awareness training.

## INTRODUCTION
Every year privacy and ethical behavior play more and more important role in our lives than the year before. Be ethical is a new requirement on a job market in any field, but it is especially important in the security related areas. Fast speeding process of converting more business data into electronic format creates a constant pressure on the involved businesses due to the liabilities in data protection. Electronic data security is a relatively new growth, which requires everybody's input to make it work. Information technology professionals enhance their skills to use computer mechanisms to secure the data transactions and restrict an unauthorized data access, while achieving the fastest possibly data retrieve. Unfortunately, some of the skilled professionals use their abilities to harm the society, by finding the vulnerabilities in the companies' systems and attacking them, creating and distributing virus-containing codes, finding the ways to avoid payments for the desires services… This is not just wrong and unethical, but also criminal activities, which are prosecuted in accordance to U.S laws.


*InfoSecCD Conference'04*, October 8, 2004, Kennesaw, GA, USA. 

## 1. ARE YOU A HACKER OR CRACKER?
There are hundreds and hundreds definitions of "hackers" on the Web. Combining it all together we get a computer enthusiast, who enjoys learning programming languages and computer systems and can often be considered an expert on the subject, who mastered the art and science of making computers and software do much more than the original designers intended. "Hackers are computer professionals, with skills… Hackers built the Internet. Hackers made the Unix operating system what it is today. Hackers run Usenet. Hackers make the World Wide Web work. If you are part of this culture, if you have contributed to it and other people in it know who you are and call you a hacker, you're a hacker" (Raymond E., 2001).
A person who breaks into other people's computer systems to get a kick out of it or who intent to cause harm is a "cracker".

A hacker is a very talented programmer, respected by his peers. A true hacker can find plenty of useful projects to work on; breaking things is more a characteristic of children of any age. The basic difference is this: hackers build things; crackers break them.

According to Raymond, real hackers consider crackers lazy, irresponsible, and not very bright and want nothing to do with them. Unfortunately, many journalists and writers have been fooled into using the word "hacker" to describe "crackers", which is obviously upsets real hackers (Raymond E., 2001).

Sadly, we have to join the majority and use the term "hacker" in this paper to refer to individuals who cause so much harm in the society.

### 1.1. Why Do They Do It?
Hackers infringe the laws for a number of reasons such in the order from less harmful to more serious (if we can even classify them this way). Hackers do it:

- Because they know how and can, either being smart and figuring out how to, or getting the instructions and tools from friends-hackers

- Because they like the challenge to break into something so secure
- Because they get a trill of doing illegal activities and hoping not to get caught
- Because they seek publicity
- Because they want to take a revenge
- Because they are getting paid (though most hackers are passionate about breaking into the system and do it for free)

## 2. CYBER ETHICS

Internet is not only a tool to use for work, study or pleasure but a very important part of our life in general. It gives that magic feeling to accomplish things and be invisible, but this invisibility may leads to actions, we normally wouldn't do in person or in public - actions that might be wrong. Relatively new terms, "cybercitizenship", "cyber ethics", and "netiquette" refer to responsible cyber social behavior, to what people do online when no one else is looking. Reasonably, we need to educate all Internet users on rules and sequences of being Online in order not to be a victim of our own ignorance as one of the young explorers did not intend to do any damage and did not realize he was doing anything unethical or illegal. But was caught and asked at a Congressional subcommittee hearing at what point he questioned the ethics of his actions, he answered, ``Once the Computer Hacking and Ethics FBI knocked on the door."(Harvey B., 2004).

### 2.1. Cybercrime Offences and Categories

The Department of Justice categorizes computer crime in three ways: Using computer as a target - attacking the computers of others (for example, spreading viruses); Using computer as a tool - using a computer to commit "traditional crime" (for example, credit card fraud); Using computer as an accessory (for example to store illegal or stolen information. (http://www.cybercitizenship.org/crime/crime.html)

The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders as of the year 2000 categorized five offenses as cyber-crime:

1. Unauthorized access,
2. Damage to computer data or programs,
3. Sabotage to hinder the functioning of a computer system or network,
4. Unauthorized interception of data to, from and within a system or network,
5. And computer espionage.

And, emphasize following categories of computer crime: Financial, crimes that disrupt company's ability to conduct e-business. Piracy, crimes of copying copyrighted material without an explicate permission. Hacking, crimes of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this access. Cyber-terrorism can be considered a type of hacking, designed to cause terror, violence against persons or property, or at least cause enough harm to generate fear. Online Pornography, possessing or distributing child pornography is against federal law and distributing pornography of any form to a minor is illegal (http: //www. playitcybersafe. com/cybercrime/hacking.cfm).

## 3. PROTECTION FROM CYBERWORLD

Hacking and its subcategory cyber-terrorism, is a growing problem that must be addressed accordingly. Dr. Les Labuschagne from the California Berkley University suggests two approaches: proactive and reactive. Most organizations adopt a reactive approach to information security. The vulnerability of systems is usually evaluated after an attack takes place, resulting in money spent on fixing the security holes and recovering from the data and business loss. This is the least effective, and more expensive approach. The proactive approach said to demonstrate organizations that try to locate security holes before the hackers do. The proactive approach is sometimes called "ethical hacking" (Labuschagne L., 2000).

Marcia Wilson in her article **"**War, ethics and security" offers to be safe by being aware of what is going outside of company's network. She says, "Awareness isn't about acting unethically in our day-to-day activities by defacing Web sites, promoting unfair discriminatory policies or generally being over reactive and hysterical. Awareness is about applying the necessary access controls and requiring authentication and appropriate authorization to access of information" (Wilson M, 2003).

David Foote in his work "Good Ethics at Work Lie in the Hiring" expresses his opinion on monitoring ethics matters by using following strategies: Making employees sign a code of ethics, hiring an ethics consultant, appointing a chief ethics officer (Foote D., 2002).

Experts say, that for companies to secure their systems it's good to start by searching for hacker programs that might be used in attacks, then distribute formal security policies to employees letting them know how often to change passwords or what to do in case of an attack, and undoubtedly constantly update software with the latest versions and security patches (Khalid A., 2004).

Dr. Michel Whitman from Kennesaw State University, Atlanta recommends continuing awareness training, specific security policies for employees, incident respond plans and visual awareness reminders, such as posters (see attachment for examples of awareness posters) in the computer labs, or other public places (Whitman M., 2004).

One of the easiest yet a very important approach to protect us from unethical data loss is physical data security. While any in use, any confidential information should be securely locked away from unauthorized viewers. Nowadays, the attackers can simply go through the garbage, called "dumpster diving" in search for important pieces of information that can help crack the computers. When no longer needed, should be discharged completely and indivertibly, according to company's policies. Dr. Whitman suggests shredding vertically, then horizontally, then burning the shredded pieces and finally stirring the ashes.

### 3.1. Children and Adults Verses Cyberworld

Now, we know the danger of Cyberworld, its treats and crime. We know how to protect ourselves from Cyberworld hackers, and in most cases we do a good job. Ironically, because we are so well informed and use various tools to interact with Internet and

Cyberspace, the same Cyberworld needs protection from us, who can easily abuse it. Computer ethics call for more education on the subject matter. It is never too early or too late to educate users, regardless of their age.

How can we teach young computer users to be responsible members of the electronic community? We can do it right there where they like to be so much, Online. There are several websites, providing information for children as well as for parents:

•Teach kids to be a good cyber citizen using Cybercitizenship rules at http:// www. cybercitizenship.org

•Let kids take the CyberSpacers' oath and join the Super Cyber Team, from CyberSpacers website at www.cyberspacers.com. The site includes online quizzes, comics, games and contests

•Show kids how to use the Internet safely and responsibly, and let them find out what happened to a young hacker, available from Cyberethics for Kids website at www.cybercrime.gov /rules/

•The FBI site includes links to Internet Law Enforcement Stories and A Parent's Guide to Internet Safety Tips for Kids at http://www.fbi.gov/fbikids.htm

How can we provide a worthwhile culture for young computer enthusiasts to grow into? Brian Harvey from the University of California, Berkeley gives suggestions to set up serious adult models and provide an access to real power. In the computer culture, adults rarely take seriously the idea of belonging to a community, which lacks providing an ethical and hard working idol for our society. Instead, Harvey says “our heroes are the ones who become millionaires by doing a slick marketing job on yet another spreadsheet program” (Harvey B., 2004).

Dr. Michel Whitman recommends several professional IT organizations, worth joining to for becoming a better professional and therefore, serving as a serious adult model. Among them are: Association of Computing Machinery (ACM) strongly supports education, requires members to comply with ethical professionalism in everyday job and to protect the confidentiality of information. International Information Systems Security Certification Consortium, Inc. (ISC) issues IT security certificates and uses the code of ethics to provide guidance to the certified professionals. Information Systems Security Association (ISSA) brings together qualified practitioners for information exchange, promotes Information security awareness and continuing education, enforces the code of ethics (Whitman M., 2004).

According to Brian Harvey, access to real power is an important issue in proper education too. He believes that if adult computer scientists don’t want to put up with CP/M, BASIC, and floppy disks, why should the teens do? Brian Harvey considers the technology available to most young people not a simpler version of what experts use, but rather a fundamentally less powerful medium, which is simply inadequate to challenging intellectual work Adolescents are excluded not only from access to equipment but also from access to ideas. They learn isolated tricks, like how to crack the password, which gives them no real insight into computer science. We should concentrate on providing young kids with powerful ideas that extend to solving other kinds of problems. “The philosophy behind this policy is that most ``malicious'' computer abuse is the result of ignorance, misunderstanding, and thoughtlessness, rather than truly malign intent”, says Harvey. Of course we can’t just open access to the sensitive data for kids, but should try to involve them in relationship with adults; show them trust is a very good start now and powerful investment to our secure future. (Harvey B., 2004).

Another question rises-How do we educate children without defining them as criminals? A safe arena for moral experimentation should be at home and at school. It is a direct responsibility of every parent as well as every teacher to build a set of ethical morals for children. One of the ways to achieve this can be role-playing games where a player can say ``I'm going to be a thief,'' or ``I'm going to be evil,'' trying on these roles without actually harming anyone. (See attachment with sample role-plays). To see the possible punishment without actually getting one is a very strong motivation to choose the “right path” (Harvey B., 2004).
Education should affect not only children and teenagers. To stay on the edge of fast-forwarding Internet growth, computer users, no matter if they are certified professionals or just employees in other fields, should make it a point to be informed of updates on current legal events and its prosecutions, new adapted laws and amendments.

More information about cybercrime is always available from Department of Justice Computer Crime & Intellectual Property Section's website at www.cybercrime.gov. Link to the National Infrastructure Protection Center at the FBI helps to keep up with regularly updated information and descriptions of cyber crimes at www.nipc.gov. The source to develop emergency respond programs for an organization are widely available Online. -The Computer Emergency Response Team (CERT) offers some resources at www.cert.org. All this precautions intent to promote ethical Cyber behavior and illuminate Internet abuse of actions, like by online pornography viewing and distributing and illegal copyrighting.

## 3.2 Law involvement

In addition to the companies’ security mechanism, policies, awareness training, and general public education the law is on the consumers’ side too. Cyber laws vary in the spectrum the cover and issue dates. Most of the laws used in ‘real world’ are applicable to the cybercrime; afterwards these are the same people who commit them by means of technology tools. Online dispute resolutions are available for small disputes and help with settling matters fast and peacefully, instead of battling in court. More serious computer crimes are solved with exercise of United States laws. According to M.Whitman, H.Mattord’s’s classification in their book “Management of Information Security”, the key U.S. laws supporting Information Security and Ethics are:
National Information Infrastructure Protection Act of 1996 (criminal intent)

USA Patriot Act of 2001 (terrorism)

Computer Fraud Abuse Act of 1986 (threats to computers)

Computer Security Act of 1987 (federal agency information security)

Federal Privacy Act of 1974 (privacy)

U.S. Copyright Law (protection of copyrights)

Digital Millennium Copyright Act (protection of technology copyrights)

Georgia Computer Systems Protection Act (protection of information system in GA)

## 3.3. Department of Homeland Security (DHS) involvement

Department of Homeland Security **(**DHS) primary mission is the "capability to anticipate, preempt and deter threats to the homeland whenever possible, and the ability to respond quickly when such threats do materialize" (http://www.dhs.gov/dhspublic/).

DHS is responsible for assessing and evaluating the vulnerabilities of the nation's critical infrastructure as a whole and cyber security threats in particular and for synchronizing its actions with other federal, state, local, and private entities to ensure the most effective response. DHS encourages individuals to report information concerning suspicious or criminal activity and cyber security incidents to Homeland Security. Individuals and Federal Agencies/Departments can report cyber security incidents online at http://www.dhs.gov/ dhspublic/ theme_ home6 .jsp.

Homeland Security Operations Center (HSOC) as heart of the organization is responsible for information sharing and domestic incident management between federal, state, territorial, tribal, local, and private sector partners. The HSOC collects and combine information 24/7 from a variety of sources to help deter, detect, and prevent terrorist acts and is capable of providing a centralized, real-time flow of information between homeland security partners.

The HSOC is home to a variety of agency, state, and local partners that provide constant watch for the safety of our nation. The HSOC receives hundreds of calls; they address about 22 incidents or cases per day. The agencies represented include but certainly not limited to: Federal Bureau of Investigation, United States Coast Guard, Postal Inspection Service, Central Intelligence Agency, United States Secret Service, National Security Agency, Immigration Customs Enforcement, Environmental Protection Agency, Drug Enforcement Agency, and Federal Air Marshal Service.

# 4. WHY COMPANIES ARE SO RESISTANT TO REPORT CRIMES

Even with the knowledge of attacks prevention, technical abilities to protect the systems and laws available, computer crime is still spreading. According to the FBI and the Computer Security Institute annual survey of 520 companies and institutions, more than 60% reported unauthorized use of computer systems over the past 12 months and 57% of all break-ins involved the Internet. Though the numbers look big; as many as 60% of attacks go undetected. Even worse, about only 15% of exposed attacks are reported to law enforcement agencies (http://www. cert.org/about/ ecrime.html).

Why do we see such a low number of attacks reports? Companies just don't want the publicity. When something is going wrong with a company, the last thing they want is for everybody to know about it. A successful attack may challenge other hackers to repeat the crime. Bad publicity can seriously undermine the image and reputation of the company, as well as public trust. When hackers broke into Citibank to steal $10 million, competitors used the news in marketing campaigns against the bank. "Many companies still seem unwilling to report e-crime for fear of damaging their reputation," says Larry Johnson, Special Agent in Charge, Criminal Investigative Division, and United States Secret Service. Some companies want no press attention, which can be very misleading. These reasons make enforcing the law very hard (Sager I, 2000).

Part of the problem also lays in the following motivations: The investigation process can be disruptive to the victim's business, causing harm even as it tried to remedy it, there is a chance of exposure of the confidential information, even if a crime were confirmed, cyber law doesn't promise any compensations for the damage suffered. (Khalid A., 2004).

The chances to actually catch a successful hacker are also very little. With wide broad of Internet, anyone anywhere with computer access can commit a crime. In the example with Aye.Net, a small Jeffersonville (Ind.)-based Internet service provider. In 1998 hackers broke into the ISP, which put the out of business for four days. Steve Hardin, director of systems engineering for the ISP, discovered the hackers and found messages in Russian. He reported it to the FBI, but no one has been able to track down the hackers (Sager I, 2000).

2004 E-Crime Watch Survey shows the impact of cyber crimes on business areas: 56% on operational losses, 25% on financial loss and 12% on other types of losses. Interestingly, 32% of respondents do not track losses due to e-crime or intrusions; among those who do track half say they do not know the total amount of loss. 41% of respondents indicate they do not have a formal plan for reporting and responding to e-crimes. Additionally, respondents indicate a higher degree of familiarity with local and national e-crime laws (39% and 33% respectively), but know little about applicable international laws (8%). (http://www.cert.org/about/ecrime.html)

# 5. CONCLUSION

We all agree that more businesses are converting their data to e-format. Hacking as part of cyber crime is definitely moving forward, with new tools to hack and new viruses to spread coming out every day.

The urgent need of information security, ethical education and awareness programs cannot be emphasize enough in order to achieve the maximum protection from the hackers and also to protect Cyberworld from our own abusive use.

U. S. Government issues information and ethics related laws very frequently, but the problem in applying them is that only a small percentage of attacked companies actually report crimes.

"The result of the "under-reporting" was a lack of reliable information about cyber crimes, which hampered action against cyber criminals, which in turn reinforced the idea that there was little to be gained by reporting them to the authorities", says Amir Khalid in her article "Cyber crime: Business and the law on different pages".

Yes, there is number of reasons why companies are so hesitant to report cybercrime, but they should be more encouraged to do so, in order to fully develop new crime area. By doing so all the computer crimes and sequences will be know to public and

potential hackers, which should lead to less crimes committed; laws will be more accurate in arbitrating cases, which will result in better jurisdictions and more remedies for the injured companies.

As the overall picture, we all live in Cybercrime, therefore it is every cyberspace citizen's obligation to do what it takes to achieve the best security protection now and set ground rules for the new generation.

## 6. REFERENCES


[1] Foote D. (2002, March). Good Ethics at Work Lie in the Hiring. *Computerworld.* Retrieved July23, 2004 from http://www.computerworld .com/printthis/2002/0, 4814,68719,00.html

[2] Harvey B. (2004). Computer hacking and ethics. University of California, Berkeley. Retrieved July23, 2004 from http://www. cs.berkeley.edu/ ~bh/hackers.html

[3] Internet Stuff. (2004, May, 25). 2004 E-Crime Watch Survey. Retrieved July23, 2004 from http://www.cert.org/about/ecrime.html)

[4] Internet Stuff. (2004). Threats and protection by Homeland Security. Retrieved July23, 2004 from http://www.dhs.gov/dhspublic/ display?theme =30&content=3813

[5] Internet stuff. (2004). What is cyber crime. Retrieved July 23, 2004 from http://www. cybercitizenship.org/crime/crime.html

[6] Khalid A. (2004, March 5). Cyber crime: Business and the law on different pages. The Star. Retrieved June 28, 2004 from http://www.niser.org.my/news/2004_03_05_01.html

[7] Labuschagne L. (2000, July). Evaluation criteria. Rand Afrikaans University. Retrieved July23, 2004 from http://csweb.rau.ac.za/staff/labuschagne/ research/articles/eth_hac.pdf

[8] McCullagh D. (2003, August, 1). Hackers get lesson in the law. CnetNews. Retrieved July23, 2004 from http://news.com.com/2100-1009 5058918.html

[9] Raymond, E. (2001). What Is a Hacker? Retrieved July 23 2004 from http://www.catb.org/~esr/faqs/hacker-howto.html

[10] Sager I. (2000, February, 21). Cyber Crime. Businessweek Online. Retrieved July23, 2004 from http://www. businessweek. com/2000/00_ 08/b3669001.htm

[11] Wilson M. (2003, April 09). War, ethics and security. Computerworld. Retrieved July23, 2004 from http://www. computerworld. com/printthis/ 2003/0, 4814,80185,00.html

[12] Whitman, Michael E. and Mattord, Herbert J. *Management of Information Security.* Boston, Massachusetts: Thomson Course Technology, 2004, 363-375.