The dangerous of computer hacking essay

Business, Industries

Christian Rupe 5/25/09 Research Essay: Final Draft Professor Wilson Hackers and Security Measures A diverse group of people often referred to as “ hackers” have been stereotyped as unethical, irresponsible, and a serious threat to society for their actions of breaching of computer systems in an undesirable manner.

I will attempt to construct a picture of what a computer crime is, as well as a portrait of what a hacker is, their concerns, and how most hacking occurs. I will also cover the best security measures against undesirable hacking. It is my intent to argue that, most hackers are learners and explorers who want to help rather than cause harm. Additionally, my research will suggests that the general principle of hacking is part of larger conflicts in life that we are experiencing at every level of society and business in an information age in which many of us aren’t computer savvy.

These conflicts lie on the issue of whether information should be made publicly available or not (whether we should centralize or decentralize government) and on issues of law enforcement. Hackers have recently raised serious issues about values and practices in an information society. When I first started researching hacking I knew next to nothing about the subject, I was not and am still not an expert on hacking, I was and still am an average person, much like yourself that knows the Internet is a dangerous place. My paper is merely a byproduct of the research that I followed to the most logical explanation of this pandemic. Computers and telecommunication networks have become a substantial aspect of our society and subsequently our lives. This type of technology can be used to carry out unlawful as well as legal activities.

Personal computers and especially the Internet consist of a collection of tools, which attract people from all social classes. People like housewives, workers and chief executives. The Internet cuts all racial, social, gender, and religious divides. Now days criminals are people that are also attracted by today's technology. The Internet can be used for criminal purposes in different ways: from a simple blackmail or white lie to the most perplexed crime like money laundering.

Technology can be applied as easily by the criminal and terrorist as it can by the authorities; and very often the criminal has greater desire to profit from that technology than have the authorities themselves" . Furthermore, companies, institutions and private lives, especially in industrialized nations, are dependent on computers, Internet and similar technologies. Business operations without the support of digital networks would be non-existent. For example, banks distribute funds through computer networks.

Banks and credit card companies are quickly adopting automated payment systems. The computers are the essentially the basis of this cashless society, and not only that, but a society wherein there is less human interaction with each day that passes. Millions of computers are needed to operate these automated payment systems (digital networks). On the other hand, criminals for different reasons can use similar networks also: to hide unlawful software or to distribute illegal material such as child pornography. In these two cases we can see two opposite sides of the use of information technology.

From the hacker's, and the person(s)' who are related with the " digital crime", point of view computers help to carry out ' illegal activities'. From

the business perspective computers are means of accomplishing ‘ legal activities’. But what is really legal and illegal in today’s society? There are certainly some acts like pornography, which is illegal, but sometimes we must ask ourselves about what is legal and what not. As mentioned earlier, the Internet not only attracts individuals from different social backgrounds but commercial organizations as well.

This is a great motivation for criminals whose sole aim is to make profit using unlawful actions. These could be computer hackers, fraudulent traders, or software pirates. In this essay I will discuss about computer crime and hackers and how our society should take measures for the protection of individuals and organizations. This paper is a report of what I discovered about hacking, and subsequently a report about my research. I focused my attention on answering some key questions such as: what is hacking, who are the hackers, what motivates them, why is hacking dangerous, and what is the future of hacking. I also give useful details about computer crime especially its definition and some important categories of it. What is a computer crime? Computer crime is a more serious issue than most realize.

“ According to the FBI, the average profit in a live bank robbery is $4000; the average computer heist exceeds $400. 000. The American society for industrial security calls computer-related crimes a multi-billion dollar annual business”.

Although a lot of people agree that computer crimes are increasing rapidly, there is a disagreement on what a computer crime involves. That is because

the technology and the methods used by criminals are continuously changing. Therefore, there are various definitions.

But if somebody wanted to do a research about the law in different countries he/she will realize that computer is either the medium used to propagate the act or the target of the act. Thus, “ computer crime consist of two kinds of activities: a) The use of a computer to propagate acts of deceit, theft or concealment that are intended to provide financial business-related, property or service advantages and b) Threats to the computer itself, such as theft of hardware or software, sabotage and demands ransom” . Obviously, crime varies so widely between different types of society. For example, conditions and results of crime are different in a small-scale pre-industrial society than to large modernized cities.

A social atmosphere is more restrict and it is difficult to get away from relatives, neighbors and so on. On the contrary, the conditions in big cities are more elastic and people have easy access to targets without encounter social criticism. They can hide behind the anonymity that large cities offer. Who are the victims of the computer crimes? That question is not as difficult to answer. We are living in a capitalistic society, which is dominated by for-profit commercialization. Therefore, it is safe to say that the first target is traditionally large corporations and government agencies. However, every single person who owns a computer that is connected to the Internet is at risk. There are no exceptions in the cyber world.

The main reason that this happened is “ anyone” can do it. Any person who has a personal computer and has some knowledge on computer hardware

and software could easily become a computer criminal. It’s all about simplicity and anonymity. It is believed by most that computer crime started during the1980’s with the first PC and the Internet, that is not true. The first recorded computer crime took place in 1958 and the first prosecution for computer crime came in 1966, “ A few years after the IBM begun marketing its first line of business computers. By the mid-1970s scores of such crimes were being reported every year and yearly losses were estimated to be as high as $300 million. It is useful to cite some past important cases in the history of cyber crime : “ 1964: Robert F.

Hancock attempted to sell $5 million worth of ill-gotten software to the Texaco company. 970: The Fresno state College computers were bombed, with damages exceeding $400. 000.

Also, two employees of a Swedish company sold copies of their firm’s computer tapes to competitors. 1971: An English salary clerk used his company’s computer to embezzle a mere ? 720. In the United States, disgruntled employees of the Honeywell Corporation sabotaged the Metropolitan life computer network and made it inoperable for more than a month. 1986: The American Medical Association filed a lawsuit charging the GTE Telnet communications Corporation with sabotaging its on-line medical information service. A financial analyst changed the district of Columbia treasure’s secret computer code to deny his superiors access to financial codes” . These are small sample of what has happen in a cyber world throughout the years, but the majority of people did not give any attention, at least not until hacking was widely reported by the media around the

world. Computer crimes can be divided into four main categories: Sabotage, Theft of services, Theft of property and Financial crimes (See Appendix A) What is hacker? The term “ hacker” of course has a flurry of meanings. Sometimes it implies a computer programmer who spends a lot of hours working on a personal computer, working on different types of coding and creating technological “ fixes” and “ patches” for existing software.

This kind of activity is not illegal and is encourage by the employers. In a different sense, the term hacking is used to signify criminal activity: the effort of the person to perpetrate through personal computer for the purpose of unlawful activities. In other words, hackers are anyone who brakes into a computer without any for of consent. This type of hacking denotes the necessity for new security systems and legislation to protect people and enterprises from these activities. Hacking really came into existence after 1980s as a result of telecommunication growth as well as high computer literacy.

Hacking include a broad-range of computer-helped activities. Some of them are legal other unlawful and a lot are unethical. Some experts are saying: hacking is a multifarious phenomenon. At this time, it is helpful to state that hacking is totally different and separated from fraud.

Fraud is a human activity which one person has speculative scope or tries to take advantage of others. Finally we can say that all hackers cannot be characterized as benevolent nor nasty or nuisance. We should all bear in mind that it is very risky to connect a computer system to a network, especially the Internet, when there are not all the security systems to protect

from hacking. Motivations for hackers Hacking may be practiced for several reasons. The most important reasons, according to some scientists who have a lot of experience in this subject, are psychological: “ It is this psychological compulsion that can induce some hackers to see every computer system as a challenge, a configuration to be tested, broken or cracked. We have already seen that some hackers strive to access closed computer systems not for pecuniary gain but as intellectual exercise. A stretching of their own programming prowess” .

The majority of hackers when they break into a system, their only objective is to learn and not to cause damage. But we should wonder: is that crime? For example, when a hacker penetrates a system and downloads information from it, in essence he or she copies information. No theft takes place because the information still exists in the system. Moreover, information is not concerned as property. It is also believed that hackers very often come from problematic families. “ Hackers are school dropouts and job changers who turned to computing as a way of outsmarting everyone except the other members of their social group” . Psychologists, sociologist and other scientist view hacking as a computer addiction. Hackers are individuals who use the computers as substitute: computers do not have the perplexity of human relations (antisocial behavior).

Therefore there is a psychology of hacking as there is for every type of human behavior, regardless of criminal behavior or not. Hackers: Criminals or Not? Hackers have a negative public image and identity. The majority of people believe that hackers are immoral and irresponsible individuals. Is that

true? “ We might ask ourselves whether, for the shake of balance, a truly democratic society should possess a core technically gifted but recalcitrant people. Given that more and more information about individuals is now being stored on computers, often without their knowledge or consent, is it not reassuring that some citizens are able to penetrate these database to find out what is going on? Therefore, it is realizable that hackers have an important role in our society and aid to dodge a more centralized government by breaking into their systems and sharing information with other people. On the other hand, absolute decentralization can easily drive humanity to very negative results. Consequently, democracy consists several kinds of people with different cultural, religion and ethnic backgrounds as well as people who have opposing political sights. Every citizen in our society must try to always keep a balance between illegal activities of hackers and activities that are serving the general public’s interest.

The Future of Hacking Increasing computerization, especially in economic transactions, as well as the emergence of new computer applications such as electronic home banking may lead to an increase in the number of offenses and losses. In addition to this, the growth of the electronic technology associated with cheap modems and personal computers open the possibilities of a computer crime and every kind of hacking: pure or malicious. “ The FBI said that the dangers of cyber crime were rising because of the increased availability of hacking tools on the Internet as well as electronic hardware such as radio frequency jamming equipment. On the other hand, the internet news groups began to make available in public new sophisticated “ smart” programs which have the ability of “ cracking”:

braking the codes of every type of program. These programs are easy to use and are very helpful tools for anyone that wants to break the security of systems' software. Finally, it can be concluded that in the next decade hacking's form will change. It will most likely become a tool used by terrorists and will by utilized more strategically with political motivations. The explosion in the use of the Internet, about how some services may be regulated, has seen an argument all around the world.

Legislation plays an important role of how the humanity can decrease these crimes. Computer crime is now a world-wide pandemic because of the rapid growth of digital technology and especially in the digital network division, which brings hackers and organized crime from all over the world together. A truly sophisticated intrusion leaves no track, no proof of a crime.

On the other hand, how many crimes can be categorized as " perfect crimes? " The computer security industry is well aware that there is a huge number of " perfect crimes". If the crime cannot be perceived, with any evidence, the most likely possibility is likely to be overlooked. Another aspect of the problem is that companies, which are based on customers' confidence, are afraid to declare in public that are targeted by hackers. It is safe to say that these companies feel that they may lose the customers' trust or to be accused of having inadequate security systems. In addition to this, companies have no confidence in the police, because they believe that the police force is inexperienced and unprepared to deal with this type of issue: " In countries like the UK, this might be a fair assumption: the numbers of computer specialist officers and of successful prosecution are very small.

In the USA, it isn’t as fair: the FBI secret service and military investigators have gained experience and capability very rapidly-and willing both to work with and to educate local forces”. Consequently, it is important that the police must have the experience and skills for the detection of computer crime: “ In a survey conducted by the Ontario provincial police: 321 responses received from 648 companies questioned, only 13 companies reported experience of a loss through computer crime; only 5 of these 13 incidents were reported to the police at the time, and it seems that only three prosecutions were pursued. Each of these examples shows us the necessity for international co-operative measures. It should be our top priority to set up security measures to protect ourselves from the evils of computer crime, starting with educating the public and our police force on what computer crime entails, and the best defense against it. I don’t want to have to fear whether or not I am being scammed every time I go to buy a product off the Internet.

Computer security includes the technical and managerial measures, which need to maintain the safety of computer-based systems. According to Mandell S, there are physical menaces to security like fire, physical disaster, environmental problems and sabotage: (See Appendix B) One of the most vital issues in which there is an argument about internet legislation is among the requirements of governments and companies: “ this exemplified by arguments over the use of encryption, with companies saying they should be allowed to protect information-one of the most valuable assets- by encrypting it, and governments arguing that in the fight against crime, they must have the right to control the use of encryption, and to monitor and

decrypt Internet traffic. (Financial Times, 1/04/1998). On the other hand, some governments decided to vote a draft about hacking. The most serious contraventions would carry a maximum five-year penalty. In spite of these difficulties, in some cases, there is perfect conduct between countries and organizations. For instance, Internet Watch Foundation (IWF) is an organization, which is associated with Internet Service Providers (ISPs) and the metropolitan police in the UK. The scope of the IWF is to oversee and hinder the use of Internet to transmit unethical and unlawful material, in the UK.

The initial priority of IWF is to stop the child pornography. In this situation, the advantage is that if IWF in the UK finds illegal material, which comes from a site in France, then it would be possible for the organization to give a relevant report in France. It would be beneficial for the United States to create government organizations similar to this to defend our computer systems and our people. Finally, as you have now seen some of the many aspects of the Internet and the need of an extension of today’s relevant laws concerning hacking and an increase in the need of better information protection. In conclusion, the Internet presents some vicarious challenges in relation to hacking and digital networks or storage devices.

The issues of illegal acts, which are undesirable for companies or other organizations, raise a flurry issues and require immediate action. In my point of view, through the industry’s law enforcement agencies, if special interest groups and government would work together there is the assurance that the reactions would be practical, proportionate, and workable in this new

information age of our society. Hackers say that it is our social responsibility to share information because information hoarding and disinformation cause crimes. However, the ethic of resource and information sharing is different with computer security policies. These are based on authorization and a “ need to know” basis. It is important to look at the differences between the standards of hackers, systems managers, users and the public. These differences may represent a breakdown in current practices, and may present new opportunities to design better policies and mechanisms for making our computer systems more safe, and at the same time making Information more widely available in this Information society.

I began to research hackers with a question in mind: who are they, what motives they have, and why are they dangerous. My research continued past that as part of a larger more social issue question: is it legal to have access and knowledge on information? As I mentioned earlier, the majority of hackers have no malicious intent, so who should care if they access some dirty government secrets, I sure would like to get my hands on some of these government secrets. We are a nosy people plain in simple, there is nothing inherently wrong with that. The answers to these questions are important, the answers tell us whether our policies and practices are serving us well or not.

The issue is not simply concerning hackers and system manager’s security or law enforcement; it is a much larger main-stream issue about the values and practices we hold in high regard in this information society we call home. To sum up my entire paper in once sentence: With release of recent

technologies the world is a dangerous place, and the need to educate ourselves on the dangers we face in this information society is growing every day. Appendix A a) Sabotage is the type of criminal activity, which causes a total devastation or damage in computer hardware. Computers are common targets of sabotage especially at the periods of political commotions. Another kind of sabotage is some self-replicating programs (viruses) that cause damage in the contents of the computer's hard disk (hard drive) or floppy disk drive (removable drives) as well as infects other programs. " Perhaps the most widely reported virus attack occurred in October 1987, when large numbers of microcomputers users began to report problems with their data disk".

A speedy inspection of the volume labels of these disks showed that they all possessed the same volume label "@brain" . These programs have the ability to avoid their detection. New techniques are continuously developed to deal with this problem to keep up with the virus's already roaming digital networks. b) Theft of services is a very common problem. In this kind of computer crime, users can gain illegal access to a computer system and be able to access all kinds of information that was supposed to be strictly confidential.

They could also take advantage of an unauthorized entry to a system by using the facilities and services that the system offers. Unauthorized access to computer systems is primarily committed by juvenile hackers, who have a variety of motives. These are related to their willingness to penetrate successfully a company's security system. They view it as a great challenge.

It is important to mention that for hackers it is easier to gain unauthorized access to a time-sharing system rather than to a closed system. c) The most obvious computer crime that involves crimes of property is the theft of computer equipment itself. By the rapid advance of technology computer equipment and components become smaller and smaller in size.

Thus this increasing miniaturization of computer components and consequently of home computers facilitates the occurrence of more thefts. These types of crime are easily categorized into traditional concepts of crime and are not of unique legal complexity. A more complicated issue is what actually represents property in the context of computer crimes. In different countries different courts have come to conclusions that vary a lot. Computer crimes of property theft very frequently involve merchandise from a company whose orders are processed by computers. Internal personnel that have a thorough knowledge of the company’s operation carry out most crimes.

But this does not mean that these crimes are limited to those within the industry. A computer service having specialized programs but poor security may open itself up to unauthorized access by outsiders. All that an outsiders needs to gain access to the systems is to be in the possession to the proper codes. This could be done in a number of ways, such as, stealthy observation of a legitimate user logging on from a remote terminal or by using remote computers to test for possible access codes. d) Financial computer crimes are, of course, the most serious problem in the information age. With the growing of telecommunication and the diffusion of microcomputers, the

majority of enterprises and banks distribute large amounts of funds through electronic networks.

Therefore, a good opportunity and motivation appears for fraud and hackers. Obviously, these transactions in an economic area tempt criminals for specific reasons. Because the result of the arithmetic operation transferred or processed by computer system are extremely high totals. Electronic money is very easy to be created by the perpetrator. This field of computer area will also be the main area of computer fraud in the future. Appendix B The following is a list of all of the known physical risks that pose a threat to computers and digital storage devices: Fire: Is an important problem for computer security. This happens because most of the computer’s parts consist of flammable materials like papers or magnetic types.

Furthermore, water is impossible to be used as counter measure because it can cause serious damage on hardware. Some kind of extinguisher is very effective, like chemical gas, but is very costly. Natural disaster: Earthquakes floods or hurricanes have impaired a large number of computer centers. The best protection is to choose a location, which is not prone to natural disasters.

Environmental problems: Computers are usually installed in non-specialized buildings for this purpose. This is an aspect, which is not originally planned (accommodate computers) and may cause environmental problems. For example, data on magnetic media can be destroyed by magnetic fields created by electric motors in the vicinity of the computer room. Some other environmental problems could be power failures or external radiation.

Sabotage: sabotage presents the greatest physical risk to computer installations. Saboteurs may cause great damage to computer centers with little risk of apprehension. For example, magnets can be used to mess up coding on tapes, bombs can be planted and communication lines can be cut.