Issues in cybersecurity: understanding the potential risks associated with hackers/crackers

Alan D. Smith
Department of Management and Marketing, Robert Morris University, Pittsburgh, Pennsylvania, USA
William T. Rupp
Department of Management and Marketing, Robert Morris University, Pittsburgh, Pennsylvania, USA

Keywords
Internet, Computer security, Information technology

Abstract
It is commonplace to say that the 11 September attacks have changed everything. A global revolution is changing business, and business is changing the world. With unsettling speed, two forces are converging: a new generation of business leaders is rewriting the rules of business, and a new breed of fast companies is challenging the corporate status quo. The Internet is an information superhighway, touching almost every aspect of the economy from government agencies, financial institutions, businesses, and professional organizations. With the year 2002 and its increasing number of court cases on Internet-related issues, the courts are obviously still struggling with the question of intellectual property rights in an open source code environment supporting e-commerce. By modeling and classifying the risks associated with cybersecurity issues, firms and specific individuals should not become a casualty of this cyberwar, nor become paranoid about the risks – be informed and follow common business sense practices, policies, and procedures.

Introduction to the need for cybersecurity

Internet security overview

The Internet is not a single network, but a worldwide collection of loosely connected networks that are accessible by individual computer hosts in a variety of ways, including gateways, routers, dial-up connections, and Internet service providers. The Internet is all about speed, change, convenience, sharing, and communications innovation. The Internet has made everything move farther and faster than ever before. It is easily accessible to anyone with a computer and a network connection. Individuals and organizations worldwide can reach any place at any time on the network without regard to international, geopolitical, or geographic boundaries or time of day. According to McDonald *et al.* (1996), the existence and popularity of the Internet makes utility patents for software desirable for two main reasons:

1. the Internet has made it easier to copy and distribute software; and
2. the Internet has opened up a new, lucrative market for software development – much of the software being developed includes interactive functions that can only be protected under patent law.

McDonald *et al.* have suggested that early court cases and legislative efforts point to the trend that courts facing Internet issues will attempt to apply traditional principles of intellectual property law to this new form of communication. With 2002 and its increasing number of court cases on Internet-related issues, the courts are obviously still struggling with the question of intellectual property rights in an open source code environment supporting e-commerce.

Traditionally, and especially after the 11 September 2001 tragedy, a well-prepared IT security policy should focus on implementing the following:

- A secure remote access – an interactive tool that allows you to be proactive in securing your system.
- Address internal security gaps – if left unaddressed, this could provide an easy way for hackers to penetrate IT systems.
- Secure your password and change it often.
- Install a virus protection tool and keep it current – such as Black Ice.
- Hire or outsource for security expertise.

Although these are only some of the many IT security issues, the major thrust on this paper is to explore the fairly recent but well socially established criminal phenomena of computer crime – hacking/cracking.

The phenomena of computer crime: hacker versus cracker

This paper will provide the reader with an overview of the criminal offender of information technology (IT) security as compiled from current literature, previous case studies and surveys related to the various types of offenders of Internet security issues. It is not within the scope of this paper to detail every security exposure or characteristic of every perpetrator of Internet security or control. In addition, it should be remembered that the bulk of the reported incidents and complaints are problems that can be prevented, based on research by the Center for Democracy and Technology (http://www.cdt.org/), a group that promotes civil liberties on the Internet. According to Dunn (2001), of the 538 businesses surveyed by the Computer Security Institute, 64 per cent say they experienced financial losses from computer breaches. In addition, only about 70 per cent

Information Management & Computer Security
10/4 [2002] 178–183

[ISSN 0968-5227]
[DOI 10.1108/09685220210436976]

of the respondents report their Internet connections are a frequent target of cybercriminals, rather than their internal systems.

However, despite the increasing numbers, many do agree that tougher cybercrime laws are not the answer, since the government has a bad track record in online security (Dunn, 2001). Since the Internet has been referred to as the information superhighway, the Internet phenomenon touches almost every aspect of life and has become the backbone for telecommunications, finance, governments, health care, and education (Garfinkel and Spafford, 1996). However, the growth of this information technology has introduced a new category of criminal offender, the computer criminal (Denning, 1998). There has been little empirical research on these offenders because the crime is non-replicable, poorly designed and anecdotal. However, the most studied group is the criminal "outsider", but the most costly and least caught is the criminal "insider". Even today, there is still one main hurdle for anyone trying to study these offenders, and that is definition. Although the term "hacker" is used quite often, there is no agreed upon definition for what this word actually means (Chantler, 1996). An interesting definition of the term hacker was suggested on a hacker's Website (Raymond, 2002) as the hacker mind-set, which is not confined to the software-hacker culture. There are people who apply the "hacker attitude" to other endeavors, such as electronics or music and it is found at the highest levels of science or art. Software hackers recognize these "kindred spirits" and may call them hackers too – and some claim that the hacker nature is really independent of the particular medium the hacker works in. Interestingly, there is a sense of positive purpose that the hacker has that the cracker does not – hackers build things and crackers break them. In fact, many hackers pride themselves on becoming the first serious security attack in a benevolent manner, thus providing an invaluable service to software vendors and firms alike. For example, on one Website (Neonsurge and the Rhino9 Team, 2000), it outlines that the initial step an NT hacker or intruder would take is to port scan the target machine or network. As suggested on the Website, it is surprising how methodical an attack can become based on the open ports of a target machine. You should understand that it is the norm for an NT machine to display different open ports than a Unix machine. Intruders learn to view a port scan and tell whether it is an NT or Unix machine with fairly accurate results. Obviously there are some exceptions to this, but generally it can be done. Recently, several tools have been released to fingerprint a machine remotely, but this functionality has not been made available for NT.

The psychological and criminological studies traditionally have been hampered by other factors as well the skills and attitudes of software hackers, and the traditions of the shared culture that originated the term hacker. Several studies relied on the subject's own classification as a hacker with no corroborating evidence – arrest record. Other studies were conducted via the Internet, which can cause a negative impact on the validity of the study (Rogers, 2001). Information technology is unique in that it is without borders and there is no clear delineation of jurisdiction (Hutchinson, 1997). With the many patches and backdoor access points and improvements that have been generated since the Y2K problem, many firms have opened the doors to information and the sharing of ideas/software/groupware without giving much thought to cybersecurity issues. It is evident that it is the ease of this computer-Internet usage that leads to security violations. Of course, there have been documented attacks against emergency 911 systems, banks, the military, air traffic control systems and private businesses (Denning, 1998). There have been some studies that have defined the term into more useful subcategories. Many of these studies have used data from the popular media, self report surveys, or personal observations (Chantler, 1996).

An examination of hacker/cracker profiles

The Landreth study

Landreth (1985) was one of the first to attempt to define the hacker community. He constructed a system based on what the hacker was involved in. In order to properly classify hacker/cracker behavioral patterns, he developed five categories:

1 novice;
2 student;
3 tourist;
4 crasher; and
5 thief.

The novice was considered the least experienced and their activities were viewed as petty mischief making (Landreth, 1985). The student was just that, a student. He found homework boring and unchallenging and preferred to explore others' systems instead of doing homework. The tourist was

Information Management & Computer Security
10/4 [2002] 178–183

"hacking" for the thrill of being there. It was a sense of adventure. The crasher was destructive. He intentionally damaged systems. The thief was believed to be the most rare. Thieves profited from their activities (Landreth, 1985).

The Hollinger study

Hollinger (1988), a criminologist, interviewed a number of university students who had been convicted of gaining unauthorized access to the University of Florida's computer system and damaging files. He also interviewed eight randomly chosen computer science students. This study was limited to two hours in duration and involved completing a questionnaire regarding any illegal computer activity in which they had been involved. His study concluded that individuals fit into three categories:

1 pirates;
2 browsers; and
3 crackers.

The pirates were least technical and confined their activities to copyright activities – pirating software. The browsers had moderate technical ability and used this ability to gain unauthorized access to other people's files. The crackers were the most technical and were the most serious abusers.

The Chantler study

Chantler (1996b) conducted a more in-depth investigation. This study attempted to more fully understand the profiles of hackers. The study concentrated on describing the hacker's environment and characteristics and then developing a hypothesis on the genesis of hackers (Chantler, 1996b). This study was fairly qualitative and relied on interviews, both in-person and through e-mail. The interviews focused on a hacker's educational background, the genesis of a hacker (his home and life environment), knowledge, motivation, information, information processing, threats to systems, levels of threat, and category of hackers. Chantler believed that qualitative based research was an appropriate approach when attempting to discover intricate details of phenomena that are difficult to convey with qualitative methods.

This study concluded that individuals fit into three categories:

1 the élite group;
2 neophytes; and
3 losers and lamers.

The élite group displayed a high level of knowledge and was motivated by a desire to achieve, self-discovery, and by the excitement and challenge. The neophytes displayed a sound level of knowledge, but most were still learning. They were followers and usually went where the élite group had been. The losers and lamers displayed little evidence of complex intellectual ability. In general, as a group they were motivated by a desire for profit, vengeance, theft, and espionage. Chantler discovered that only 30 per cent of the hacker community fell into the élite group, 60 per cent were neophytes, and 10 per cent were losers/lamers.

The study concluded that no one had forced the hackers into hacking (Rogers, 2001). Chantler (1996b) warned that hackers posed a potential threat because of their intense interest in systems and curiosity about what they contained. The intensity of the level of intervention for all three of these studies can be seen via the scale displayed in Figure 1.

Understanding and dealing with the profile of a potential hacker/cracker

From the literature reviewed it is apparent that the research to date has focused on participants who have either been caught, come to the attention of officials, or who were eager to volunteer to be interviewed (Denning, 1998). There are two basic types of hackers that this paper will look at:

1 outsiders or external hackers; and
2 the insiders or internal hackers.

The profile of an outsider is predominantly male, 12-30 years old, Caucasian, single and has a 12-level, pre-college education. He performs poorly in school but has an aptitude for computers and technology. The outsider generally is characterized with demonstrating limited social skills and is classified as being a loner in terms of behavior patterns, yet displays a strong need to belong to a larger social group. Their families are often dysfunctional, single parent, abusive – both physically and emotionally – and in some cases sexually abusive. They often display compulsive traits, such as staying online for days on end without sleep (Feldman, 1993).

The profile of an insider is someone who commits illegal activity against their own organizations (Post, 1996). They are predominately introverts. They generally experience social and personal frustrations. They often display loose ethical boundaries and disregard the notion of the word private. They have a lack of empathy. They believe they are owed special recognition by their organizations and would seek revenge if they did not receive it. Hence, a general category or profile of these types of hackers/crackers

can be easily constructed and identified by the grid displayed in Table I.

General conclusions and implementations

As individuals and businesses increase information sharing, and communication via the Internet, vulnerability to attack or intrusion rises. Despite the attention being focused on criminal hackers, we still know very little about them. The computer and the Internet provide a cloak of anonymity for these offenders. The computer is their safe haven. There is no face-to-face interaction on the Internet. This allows the offender to portray whomever they wish to portray. This is their escape from reality or a means to create a false sense of a safe-haven. Chantler (1996b) warned that hackers posed a potential threat because of their intense interest in systems and the curiosity about what they contained.

A survey by Post (1996) indicated that hackers claimed they were motivated by the challenge, the excitement to succeed, and to learn for the pure intellectual satisfaction. However, some of the respondents did include vengeance, sabotage and fraud as motivating factors. The most common documented attack is directed at defacing Web pages and is a type of virtual vandalism or virtual graffiti as opposed to any real learning exercise (Denning, 1998; Swanson, 2001a, b).

Although cybercrime and hacking have been around for over 30 years, research in the area has been sparse (Chantler, 1996b). The finding that 60 per cent of the participants admitted to engaging in criminal computer activities illustrates the extent of this criminal behavior. The prevalence may be due in part to the unique morality surrounding this type of criminal activity. As Denning (1998) indicated, the ethical boundaries of technology seem to be at odds with ethical standards found in the real physical world. Many people feel that because they are not dealing with tangible items – virtual files as opposed to real property – the ethical considerations relating to personal property and privacy in the "real" world do not apply in the "cyber" world. This flexible morality allows people to engage in behaviors in the "cyber" world that they probably would avoid in the real world – invasion of privacy and theft (Rogers, 2001).

Ethics, or an apparent lack of them, has become such a concern that there have been several heated debates surrounding this issue in the IT sector. Criminal behavior is maintained through a complex schedule of reinforcement and punishment throughout the life of the individual (Feldman, 1993). Since the computer is the superhighway and hacking is a criminal activity that relies on the dependence of computers and the Internet, there is reason to believe that the hacker will be around for quite a while, so competitive firms and e-businesses need to prepare themselves.

According to the social learning theory, criminal behavior is acquired through observational learning. The learning takes place in three contexts, the family, subculture, and social environment (Ewen, 1980). The reinforcement for criminal behavior comes from both the internal and external sources. Hence, criminal behavior is maintained through a complex schedule of reinforcement and punishment throughout the life of the individual (Feldman, 1993). The differential reinforcement concept states how these factors influence criminal behavior. According to the theory, if a criminal's behavior was reinforced in the past, there is an expectancy that such behavior will be reinforced in the future (Hollin, 1989).

In addition, there are numerous studies that were not represented in this paper that may be reviewed in the future in connection with cybercrime, such as control theories. These theories, for example, include, but are not limited to:

- Kohlberg's (Kohlberg, 1994; Kohlberg and Puka, 1994) moral development theory;
- Eysenck's (2000) theory of crime and work on personality;
- Bandura's (2001) social learning theory; and
- Skinner's behavior theory (Skinner and Fream, 1997).

Figure 1
Level of intervention as illustrated in relevant studies of hackers/crackers

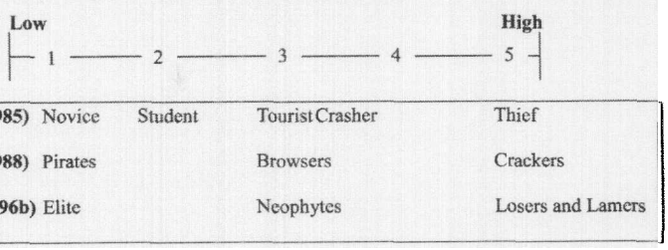

Table I
There are two basic types of hackers/crackers: outsiders or external hackers and the insiders or internal hackers

	General types of hackers/crackers	
Type of hacker/cracker crimes	**Internal (insiders)**	**External (outsiders)**
Computer crimes	Disgruntled employees	Organized crime
Computer assisted crimes	Fraud	Child pornography

Information Management & Computer Security
10/4 [2002] 178–183

In Kohlberg's theory on moral development, one of the pre-morality stages is hedonism or the lack of concern by hackers over the systems they have attacked, while control theory (Eysenck and Eysenck, 1977) is a mix on personality, crime and the extraversion scale. These theories may also offer some insight into the behavioral pros and cons in the profile of a hacker/cracker.

There does not appear to be any one theory that accounts for all types of criminal behavior (Blackburn, 1993). Although the world of hacking/cracking has limited empirical research into criminal behavior, there are indications that there are various sub-groups in this classification, from novices to professional criminals (Post, 1996). The psychoanalytic theories concentrate mainly on unconscious factors and the child-parent interactions (Blackburn, 1993). Although some hackers have come from dysfunctional families, this alone is not sufficient to explain their choice of the criminal activity to engage in (Goodell, 1996). Hacking is an activity that requires a specific skill set, familiarity with computers, networks, and a relative technological understanding.

The lack of behavioral theories dealing specifically with hacking behaviors makes this activity somewhat unique and dependent. The current method of categorizing all persons involved into one generic group called "hacker" is not meaningful. More subgroups need to be developed and defined before a better understanding of this criminal activity and behavior can be defined. In the meantime, in this world of technological evolution, everyone is a target of electronic crime and needs to be concerned about security. Threats are not decreasing. E-commerce has brought with it many new avenues: it is an attractive target for cybercrime, research has indicated that there is an increase in organized criminal activity because e-commerce is an attractive target for cybercrime. As suggested by McDonald *et al.* (1996), few effective laws exist domestically and internationally that specifically deal with technological crimes and there has been too much focus on technological controls. Generally speaking, many firms are paralyzed by an inability to separate government infrastructures from business infrastructure. In addition, it is extremely difficult separating technological problems from social and behavior problems with organizational structure. A review of the current research on IT and IS security issues has indicated that cybercrime and attacks are on the rise. Hence, firms and specific individuals should not become a casualty of this cyberwar, nor become paranoid about the risks – be informed and follow common business sense practices, policies, and procedures. In essence, become proactive – do not reduce the bar of standards to the next weakest link.

References

Bandura, A. (2001), "Social cognitive theory of mass communication", *Media Psychology*, Vol. 3 No. 3, pp. 265-99.

Blackburn, R. (1993), *The Psychology of Criminal Conduct: Theory, Research and Practice*, John Wiley & Sons, Toronto.

Chantler, A. (1996a), "The changing definition and image of hackers in popular discourse", *International Journal of the Sociology of Law*, Vol. 24, pp. 229-51.

Chantler, N. (1996b), *Profile of a Computer Hacker*, Infowar.

Denning, D. (1998), *Information Warfare and Security*, Addison-Wesley, Reading, MA.

Dunn, L. (2001), "Cybercrime skyrockets, say security reports: incidents double in 2000 and are still climbing, but who's playing cybercop?", *Medill News Service*, 6 July, available at: www.idg.net/go.cgi?id=506588.

Ewen, R. (1980), *An Introduction to Theories of Personality*, Academic Press, New York, NY.

Eysenck, M.W. (2000), "A cognitive approach to trait anxiety", *European Journal of Personality*, Vol. 14 No. 5, special issue, pp. 463-76.

Eysenck, S. and Eysenck, H. (1977), "Personality differences between prisoners and controls", *Psychological Reports*, Vol. 40.

Feldman, P. (1993), *The Psychology of Crime – A Social Science Textbook*, Cambridge University Press, Cambridge, MA.

Garfinkel, S. and Spafford, G. (1996), *Practical UNIX and Internet Security*, 2d ed., O'Reilly and Associates, Sebastopol, CA.

Goodell, J. (1996), *The Cyber Thief and the Samurai*, Dell Publishing, New York, NY.

Hollin, C. (1989), *Psychology and Crime: An Introduction to Criminological Psychology*, Routledge, New York, NY.

Hollinger, R. (1988), "Computer hackers follow a guttman-like progression", *Social Sciences Review*, Vol. 72, pp. 199-200, available at: www.fcc.gov/Bureaus/Mass_Media/News_Releases/2001 and http://public.iastate.edu

Hutchinson, S. (1997), "Computer crime in Canada", unpublished manuscript from Marc Rogers, University of Manitoba, Winnipeg.

Kohlberg, L. (1994), "Stage and sequence: the cognitive-developmental approach to socialization", in Puka, B. (Ed.), *Defining Perspectives in Moral Development*, Garland Publishing, New York, NY, pp. 1-134.

Kohlberg, L. and Puka, B. (Eds) (1994), "Kohlberg's original study of moral development", in *Moral Development: A*

Information Management & Computer Security
10/4 [2002] 178–183

Compendium, Vol. 3, Garland Publishing, New York, NY.

Landreth, B. (1985), *Out of the Inner Circle*, Microsoft Press, Bellevue, WA.

McDonald, D.W., Reich, J.C. and Bain, S.E. (1996), "Intellectual property and privacy issues on the Internet", *South Dakota Business Review*, Vol. 55 No. 2, pp. 1, 4.

Neonsurge and the Rhino9 Team (2000), "The Windows NT wardoc: a study in remote NT penetration", available at: http://rhino9.ml.org

Post, J. (1996), "The dangerous information systems insider: psychological perspectives", available at: www.gocsi.com/preleas2

Raymond, E.S. (2001), "How to become a hacker", available at: www.tuxedo.org/~esr/faqs/hacker-howto.html

Rogers, M. (2001), "A social leaning theory and moral disengagement analysis of criminal computer behavior: an exploratory study", University of Manitoba, Winnipeg.

Skinner, W. and Fream, A. (1997), "A social learning theory analysis of computer crime among college students", *Journal of Research in Crime and Delinquency*, Vol. 34, pp. 495-518.

Swanson, S. (2001a), "Business culture is obstacle to cybersecurity", *Informationweek.com*

Swanson, S. (2001b), "Internet too unsafe for Feds", *Informationweek.com*

Further reading

Albanese, J. (1984), "Corporate criminology: explaining deviance of business and political organizations", *Journal of Criminal Justice*, Vol. 12, pp. 11-19.

Atanasov, M. (2001), "The truth about Internet fraud", *Smart Business*.

Babcock, C. (2001), "I-deluge of security threats overwhelms I-managers", *Interactive iWeek*.

Beaucar Vlahos, K. (2001), "FBI seeking to wiretap Internet", *FOXNews.com*

Campbell, D. (2000), "The spy in your server", *Guardian Unlimited*.

Deloitte Consulting (2001), *Deloitte Consulting Launches e-Outlooks for the Year Ahead*, press release.

Deloitte Consulting (2001), "Deloitte Consulting monthly reports on insights into emerging issues that will affect businesses – the new economy", *e-Views*.

Fisher, D. (2001), "Aiming at security", *eWeek*, available at: http://eWeek.com

Gibson, S. (2001), "Reporter's notebook: disaster recovery", *eWeek*.

Guardian Unlimited (2000), "Internet monitoring 'time bomb' for e-commerce".

Jesdanun, A. (2001), "Online ads becoming intrusive", *Canton Repository*, 23 December, p. D-13, available at: www.cantonrep.com/cantonrep01/menus.php?external=repsearch_detail.php2ID=23918

Kaufman, C., Perlman, R. and Spencer, M. (1995), *Network Security: Private Communication in a Public World*, PTR Prentice-Hall, Englewood Cliffs, NJ.

Konicki, S. (2001), "IT on high alert", *Informationweek.com*

Kontzer, T. (2001), "EDS sees security interest at the top", *Informationweek.com*

Levitt, J. (1998), "The keys to security", *Informationweek.com*

Longstaff, T.A. and Ellis, J.T. (1997), "Security of the Internet", *The Froehlich/Kent Encyclopedia of Telecommunications*, Vol. 15, Marcel Dekker, New York, NY, pp. 231-55.

Mandel, M.J. (2001), "Why markets misbehave", *BusinessWeek*, No. 3754, 22 October, p. 95.

Matseuda, R. (1988), "The current state of differential association", *Crime and Delinquency*, Vol. 34, pp. 277-306.

Ricciuti, M. (1999), "Microsoft admits privacy problems, plans fix", *News.com*

Rubenfeld, J. (2001), "Privacy exposed", *The Washington Post*.

Schulman, A. (2001), "The extent of systematic monitoring of employee e-mail and Internet use", *Workplace Surveillance Project at Foundation*.

Stahl, S. (2001), "A question of balance: collabortion vs security", *Informationweek.com*, available at: http://informationweek.com/

Stoll, C. (1989), *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Doubleday, New York, NY.

Strang, R.J. (2000), "Script: how secure is the Internet", interview.

Sullivan, B. (2001), "Security survey", *Computerworld*.

Yee, D. (1999), "Development, ethical trading and free software", *First Monday*, Vol. 4 No. 12, December .

Zaino, J. (2001), "Privacy practices are worth another look", *Informationweek.com*, available at: http://informationweek.com/