**Association for Information Systems**
**AIS Electronic Library (AISeL)**

AMCIS 2005 Proceedings

Americas Conference on Information Systems (AMCIS)

2005

# Factors Affecting Illegal Hacking Behavior

Randall Young
*University of North Texas*, youngr@unt.edu

Lingling Zhang
*Chinese Academy of Sciences*, zhangll@gscas.ac.cn

# Factors Affecting Illegal Hacking Behavior

**Randall Young**
University of North Texas
youngr@unt.edu

**Lixuan Zhang**
University of North Texas
zhangl@unt.edu

**ABSTRACT**

The damage caused by illegal hacking has become one of the serious problems facing society. Based on general deterrence theory, social bond theory and social learning theory, the paper proposes a model which examines the factors affecting the likelihood an individual will engage in illegal hacking behavior. Data was gathered from a survey of 127 individuals who attended a hacker's conference. The results indicate that the severity of punishment has a significant positive relationship with the hacking execution while the certainty of punishment has a significant negative relationship with the hacking execution. The results also suggest that the greater an individual's commitment to conventional activities and the stronger the individual's belief in following the norms and rules of society, the less likely he or she will engage in illegal hacking behavior. Finally, interaction with other computer hackers significantly impacts illegal hacking behavior.

**Keywords**

Social Bond Theory, Social Learning Theory, Deterrence Theory, Illegal Hacking

## INTRODUCTION

Computer hacking began with the rise in the use of the personal computer (Skibell, 2002) and has gained widespread significance as the world-wide computer network expanded (Jordan and Taylor, 1998). Hacking can affect both individuals and organizations. Individuals may suffer financial damages if their information is stolen or sold by hackers (Thomas and Loader, 2000). For organizations, hacking can cause loss of consumer confidence and even lead to bankruptcy (Furnell, 2002). Estimated financial losses from fraud, virus attacks, sabotage and denial-of-service pranks rose from $100 million in 1997 to $266 millions in 2000 (Sofaer and Goodman, 2001).

Originally the term hackers referred to innovative programmers at MIT who wanted to explore mainframe computing and were motivated by intellectual curiosity and challenges (Chandler, 1996). However, the term has taken on a negative meaning as the media portrays computer intruders as criminals who purposefully cause serious damage for both corporations and individuals. American Heritage Dictionary (2000) defines a hacker as "*one who uses programming skills to gain illegal access to a computer network or file*".

Theories from criminology can help explain some of the factors behind illegal hacking behavior. Criminology researchers have made tremendous progress in the area of criminal behavior and have developed several strong theories such as general deterrence theory, social bond theory, and social learning theory. For example, general deterrence theory states that to deter people from committing certain behaviors, the expected sanctions in response to the behavior must be higher than the expected benefit the person will receive due to the behavior (Ehrlich, 1973). Due to its cost effectiveness, the United States criminal justice has adopted the approach of increasing the severity of punishment for combating crime (Kahan, 1997).

However, hacking is perceived differently compared to other crimes such as murder or drug trafficking. While the latter may be viewed harshly by the law abiding society, hackers are viewed as talented people with a curiosity about computers. The hacker community will often treat the gifted hackers like celebrities. Evidence of this view is Mark Abene who received a one year prison term for his hacking activities and after his release a large party was thrown for him at an elite Manhattan club (Quittner, 1995). In addition he was voted as one of the top one hundred smartest people in New York by *New York* magazine.

The purpose of this paper is to examine social processes and controls influencing an individual's decision with respect to illegal hacking. Our paper proceeds as follows. We draw upon general deterrence theory, social bond theory and social learning theory to build a research model that examines some factors affecting illegal hacking. Next we analyze data collected from participants in a hacker's conference using logistic regression. Then we present the results and conclusions.

## LITERATURE REVIEW

Hacking is one of the technologically enabled crimes (Gordon, 1995). Technologies such as the Internet bring electronic commerce, easy access to information and resources and new channels for distributions and advertising. However it also enables new crimes such as hacking (Palmer, 2001). Skorodumova (2004) identifies four stages in hacking development. Stage one starts in the 1960s. The hacker community includes students and professors of major US universities and scientific centers. They were motivated by innovation and exploration of the limits of the technologies. Hacking, in this stage, did not cause any damage to society. In stage two, which lasts from late 1970s to early 1980s, criminal activities started to appear. Hackers intruded on systems, deployed computer viruses and modified sensitive data. In stage three (1980s-1990s), the hacker community merged with the criminal world and subsequently became the target of governments and international human rights organizations. In this period, the most popular attacks were on database control systems, operational systems and network software. In stage four (late 1990s-early 2000s), hacker community became institutionalized. Hackers form associations, meet in conferences and publish books on hacking techniques.

There are several motivational factors behind illegal hacking behavior (Mulhall, 1997). Hackers are thrilled by intellectual challenge and find enjoyment and excitement in bypassing the security controls. Some of them hack for revenge because they are poorly treated employees or were fired while others desire financial gain by selling the information obtained from hacking.

Based on social learning theory, Rogers (2001) found that computer criminals, including hackers, are more likely to engage in moral disengagement. Moral disengagement is the process of justifying and rationalizing aberrant behavior (Bandura, Barbaranelli, Caprara and Pastorelli, 1996). He also found that computer criminals are more likely to associate with other computer criminals. Since his study was conducted in Canada, he called for more research in the United States. Furthering his study, we examine the hacking phenomenon from three theoretical perspectives: general deterrence theory, social bond theory and social learning theory.

## THEORETICAL BACKGROUND

The study is based on three theories from criminology research: deterrence theory, social bond theory and social learning theory. Criminology proves to be a fruitful reference discipline for this study as research in the behavior of deviant individuals is numerous. One critical assumption behind general deterrence theory, social bond theory and social learning theory is that deviant behavior is not fundamentally different from socially acceptable behavior. As Akers (1973, p.7) puts it, "All behavior that humans are capable of performing is natural; none is intrinsically unnatural or deviant, but only so in relation to social definitions, which may vary by time and place."

Researchers have applied some of these theories in computer abuse and software privacy (Hollinger, 1992; Peace, Galletta and Thong, 2003; Lee, Lee and Yoo, 2004). For instance, influence of friends and perceived certainty of being caught is significantly correlated with the extent of software piracy among college students (Hollinger, 1992). Another study examined the computer abuse using general deterrence theory and social control theory (Lee et al., 2004). However, few studies have used these theories from criminology to investigate illegal hacking behavior and this study intends to fill in this gap.

### General deterrence theory

General deterrence theory is one of the most cited theories in criminology literature that has been applied in computer security research (Straub and Welke, 1998; Straub, 1990; Lee and Lee, 2002). The theory has two factors: the severity of punishment and the certainty of punishment. The severity of punishment is measured by the perceived impact of a certain punishment on an individual's life while the certainty of punishment is an individual's perception of the chances of being caught.

General deterrence theory proposes the human actor will make the decision to exhibit or not exhibit deviant behavior based on an internal perception of the benefits and costs of the respective behavior. The idea that in order to reduce crime the cost of committing a crime must exceed the benefit is a staple in the United States criminal justice system. In the IS research arena, several researchers have addressed deterrence measures as a useful strategy for reducing computer abuse (Straub, 1990, Straub and Welke, 1998). In a study using deterrence theory, punishment severity and punishment certainty were found to be significantly related to attitudes toward software piracy (Peace, et al., 2003). In addition, punishment certainty was found to be significantly related to perceived behavioral control of software piracy. As the certainty of being caught increases, an individual perceives less control in committing software piracy (Peace, et al., 2003).

Although some researchers find that the severity of punishment has little effect on deterrence (Witte, 1983; Decker and Kohfeld, 1990; Von Hirsch, Bottoms, Burney and Wickstrom, 1999), Mendes and McDonald (2001) argue that the probability of arrest is of limited value without the backup of actual punishment. Therefore, in the case of hacking, we argue that severity of punishment and certainty of punishment will influence hacking behavior. This leads to hypotheses 1 and 2:

**H1: Severity of punishment is negatively related to reported execution of illegal hacking activities.**

**H2: Certainty of punishment is negatively related to reported execution of illegal hacking activities**

### Social bond theory

Social bond theory suggests that people with weak bonds to society are more likely to commit deviant acts (Hirschi, 1969). The social bond theory proposes four dimensions: *Attachment, Commitment, Involvement, and Belief* (Hirschi, 1969).

Attachment is the extent to which an individual "has internalized the norms of society" (Hirschi, 1969, p. 18). Evaluating an individual's attachment to specific classes of persons like parents, teachers, and peers is a common measure of attachment. Attachment can be evaluated from two perspectives, one being at the level of people in general and the other at specific classes of people. The theory suggests individuals with a distant attachment to socially conforming others or to human beings as a whole will exhibit a weaker bond to society's rules and therefore are more likely to violate them (Hirschi, 1969).

Commitment is the degree of effort, time, and expense that an individual invests in certain actions which are deemed to be acceptable by law-abiding society (Hirschi, 1969). An individual who has invested time and effort in conventional lines of action may evaluate any deviant behavior in light of the consequences it may have on his or her current position as well as on any future desirable position in society. This dimension posits that individuals with higher degrees of success in conventional activities and/or those with high positive aspirations are less likely to engage in deviant acts as those acts could endanger their current position in society and future ability to achieve certain goals (Hirschi, 1969).

Involvement is the consumption of an individual's time and effort doing "conventional things" (Hirschi, 1969). While it may appear to be very similar to the commitment dimension, it differs in one drastic aspect. While commitment evaluates a person's position in society and future aspirations, involvement looks at how busy a person is. The more involved an individual is in activities that are acceptable by society, the less likely the individual will commit deviant acts.

Belief is the degree to which individuals "believe they should obey the rules of society" (Hirschi, 1969, p.26). Social bond theory "assumes the existence of a common value system within the society or group whose norms are being violated" (Hirschi, 1969, p. 23). Therefore, the theory assumes that individuals have varying degrees of beliefs in the norms and rules of society. The more an individual believes in following the rules of the law-abiding society the less likely they will commit deviant acts. Therefore, the following four hypotheses are derived from social bond theory.

**H3: Attachment is negatively related to the reported execution of illegal hacking activities.**

**H4: Commitment is negatively related to the reported execution of illegal hacking activities.**

**H5: Involvement is negatively related to the reported execution of illegal hacking activities.**

**H6: Belief is negatively related to the reported execution of illegal hacking activities.**

### Social learning theory

Social learning theory proposes that behaviors are maintained and learned by both social and nonsocial conditions. People that have regular contact with delinquent peers are more likely to commit crimes (Akers, 1973). People learn how to commit crime "by observing the behavior of others and by imitating this pattern" (Rice, 1999, p. 43). Just like people learn how to conform to society's norm, they also need to learn how to depart from these norms (Calhoun, Light and Keller, 1989).

Hacking requires sophisticated techniques and expertise. They are often trained by other experienced hackers (Jordan and Taylor, 1998). Hackers often draw on the collective wisdom of the hacking community. For example, they meet in conferences such as DefCon or 2600, and they also interact in cyberspace. Thus we hypothesize that contact with other hackers is related to hacking behavior.

**H7: Interaction with other individuals performing hacking is positively related to reported execution of illegal hacking activities**

The model for the paper is shown in Figure 1. The dependent variable is a binary variable asking the respondents if they "participated in a hacking activity that would be considered outside the bounds of that allowed by the court system within the past year".

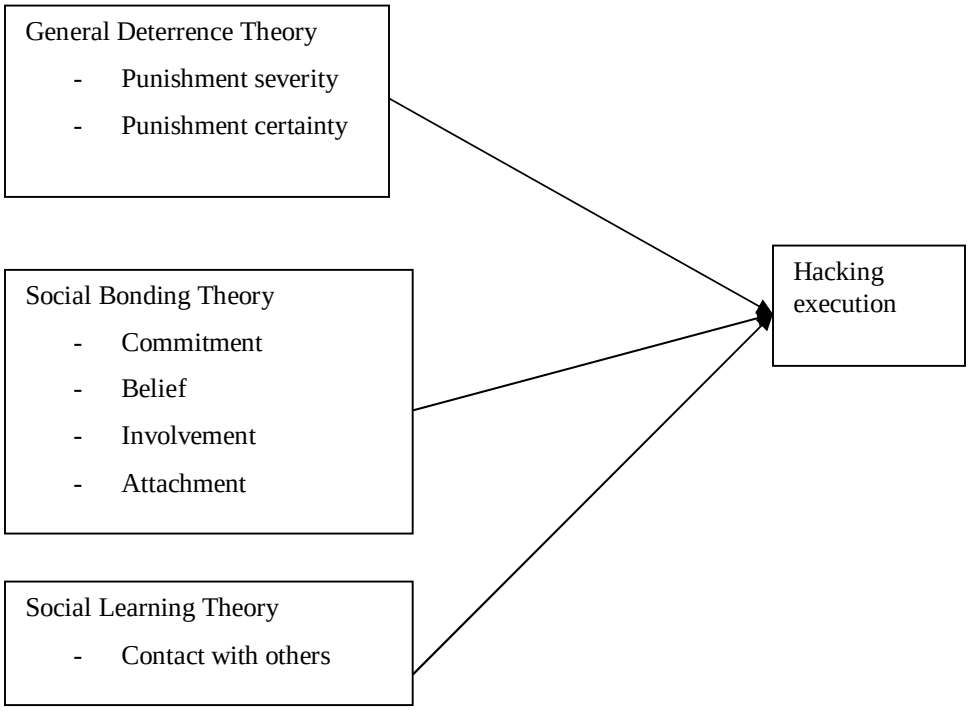


**Figure 1: Theoretical Model**

## METHODOLOGY

One of the authors went to DefCon in August 2003 and handed out surveys to the conference attendees. DefCon is the largest annual computer hacker convention held annually in Las Vegas (Schwartau, 2003). Most of the attendees are hackers or people who are interested in hacking. The survey was anonymous. A total of 155 surveys were collected during the three day conference. 28 surveys are unusable as the respondents either answered every question the same or failed to answer the majority of the questions. Therefore, the usable sample size is 127.

All survey items were developed by the authors after consulting the literature. All items are measured on a 5 point Likert scale with anchors ranging from "Strongly agree" to "Strongly disagree". For the variable attachment, we measured the attachment to older adults to represent the attachment construct. Due to the observation of many researchers (Mulhall, 1997; Jordan and Taylor, 1998) that the majority of illegal hackers are young adolescent males, we wanted to examine the attachment to older adults under the assumption that older adults (like parents and teachers) are more likely to represent the law-abiding society. The dependent variable is engaging in the illegal hacking act in the past year. The respondents were asked if they have participated in a hacking activity that would be considered outside the bounds of that allowed by the court system within the past year. The answer for the question is worded in yes or no format. The questionnaire was reviewed by academic experts for content validity. The survey was finalized after several modifications.

## DATA ANALYSIS AND RESULTS

### Reliability and validity

Principal components factor analysis with a varimax rotation is used to assess construct validity and to refine the scale items. A factor loading of 0.40 was determined to be the lowest acceptable loading assuming a power level of 80 percent (Hair, Anderson, Tatham and Black, 1998). Cronbach's alpha is used to assess the reliability of the survey with 0.70 being the lower limit (Nunnally, 1978). Two items were deleted because of the cross-loading with other items. The construct involvement does not show adequate reliability so it is not included in the analysis. The other constructs demonstrate adequate reliability and validity.

### Analysis using logistic regression

Logistic regression was conducted to test all hypotheses since the dependent variable is a binary variable. It measures the statistical relationship between social bond factors, social learning factors, deterrence factors and hacking execution.

The significance of the regression coefficients of the independent variables was examined to determine if the hypotheses were supported. Wald statistics were used in the significance test. Table 1 shows the results. Punishment severity, punishment certainty, commitment, norm and interaction with other hackers are significantly related to hacking execution ($p<0.01$) while attachment is not. However, contrary to the hypothesis 1, punishment severity is positively significantly related to the illegal hacking behavior. Therefore, H1 and H3 are rejected while H2, H4, H6 and H7 are supported.

The model was also assessed for its discriminating power. As there are 72 respondents who did not engage in illegal hacking last year and 54 who did, guessing which hackers executed illegal hacking would result in a 57.02% accuracy $((54/126)^2+(1-54/126))^2 = 0.5702$. However, logistic regression had a classification accuracy of 89.7%, which is much better than by random choice.

| Variables | Parameter Estimate | Wald Chi-square | Odd ratio | p-value |
|---|---|---|---|---|
| Commitment | -1.781 | 7.595 | 0.167 | 0.006 |
| Attachment | -0.409 | 1.125 | 0.664 | 0.289 |
| Belief | -1.085 | 5.442 | 0.338 | 0.020 |
| Punishment Severity | 1.445 | 5.446 | 4.240 | 0.020 |
| Punishment Certainty | -2.332 | 20.920 | 0.097 | 0.000 |
| Interaction | 0.975 | 10.005 | 2.651 | 0.002 |

**Table 1: Summary of Logistic Regression**

## DISCUSSION AND CONCLUSION

Hypothesis 1 and 2 propose that severity of punishment and certainty of punishment have a negative relationship with illegal hacking behavior. Hypothesis 1 is rejected. The findings suggest that severity of punishment is significantly related to illegal hacking behavior in the positive direction. One possible reason is that many individuals engage in illegal hacking behavior to acquire peer recognition and respect. The perceived severity of punishment may be positively related to any increase in the perceived peer recognition from committing the act. Hypothesis 2 is supported, which shows that as the likelihood of getting caught increases the tendency to commit the illegal hacking behavior decreases. If hackers perceive that there is a large possibility that they will get caught, they are less likely to engage in illegal hacking activities.

Hypotheses 3, 4 and 6 suggest that attachment, commitment and belief are negatively related to the illegal hacking behavior. Hypothesis 3 is rejected. Attachment is not significantly related to illegal hacking performance. However, commitment and belief are significantly related to illegal hacking execution. The higher an individual's commitment to society's conventions the less likely he or she will act out illegal behavior as it could jeopardize his or her current and future standing in society. An individual may perceive that committing a crime and getting caught will have a drastic effect on their current and future status in society. An individual who perceives he or she has little to lose will feel less constrained by society and therefore is more likely to engage in illegal hacking behavior. When an individual believes in following the conventions of society, the he or she is less likely to engage in illegal hacking activities. This demonstrates that the more value an individual places on conventional society values and norms the less likely he or she will exhibit behaviors that go against society's norms and values.

Hypothesis 7 is supported. Interaction with other hackers is positively related to illegal hacking execution. The higher the reported contact with individuals and friends who exhibit illegal hacking behavior the more likely an individual will exhibit the behavior.

While the U.S legal system considers the act of hacking into a computer system illegally to be a crime, the community can not assume it can be controlled by implementing the same measure that are currently used to control other crimes. The U.S. government and the community must implement efficient measures to control the problem as society will become more dependent on computers for survival.

**REFERENCES**

1. Akers, R. (1973). Deviant behavior: a social learning approach, Belmont, California, Wadsworth.

2. Bandura, A., Barbaranelli, C., Caprara, G., and Pastorelli, C (1996). Mechanisms of moral disengagement in the exercise of moral agency, Journal *of Personality and Social Psychology*, 71, 364-374.

3. Calhoun, C., Light, D., and Keller, S. (1989). Sociology, Alfred A. Knopf, New York.

4. Chandler, A. (1996). The changing definition and image of hackers in popular discourse, *International Journal of the Sociology of Law*, 24, pp. 229-251.

5. Decker, S., and Kohfeld, C.W. (1990) Certainty, severity and the probability of crime, *Policy Study Journal* (19:1), 2-21.

6. Ehrlich, L. (1973) Participation in illegitimate activities: a theoretical and empirical investigation, *Journal of Political Economy*, 81, 521-564.

7. Furnell, S. (2002) Cybercrime: vandalizing the information society, Boston; London: Addison-Wesley.

8. Gordon, S. (1995) Technologically enabled crime: shifting paradigms for the year 2000, *Computer and Security*, 14, 5, 391-402.

9. Hair, J.F, Anderson, R.L., Tatham, R., and Black, W. (1998) Multivariate data analysis, New York: Prentice Hall.

10. Hirschi, T. (1969) Causes of delinquency, University of California Press, Berkley, CA.

11. Hollinger, R. (1992) Crime by computer: correlates of software piracy and unauthorized account access, *Security Journal*, *2*, 1, 2-12.

12. Jordan, T., and Taylor, P. (1998) A sociology of hackers, *Sociological Review*, 46, 4, 757-780.

13. Kahan, D. (1997) Between economics and sociology: the new path of deterrence, *Michigan Law Review* 95, 8, 2477-2498.

14. Lee, S.M., Lee, S-G., and Yoo, S. (2004) An integrative model of computer abuse based on social control and general deterrence theories, *Information and Management*, 41, 707-718.

15. Lee, J. and Lee, Y. (2002) A holistic model of computer abuse within organizations, *Information Management and Computer Security*, 10, 2/3, 57-77.

16. Mendes, S and McDonald, M. (2001) Putting severity of punishment back in the deterrence package, *Policy Studies Journal* , 29, 4, 588-610.

17. Mulhall, T. (1997) Where have all the hackers gone? part 3 ------ motivation and deterrence, *Computer and Security* 16, 4, 1997, 291-297.

18. Nunnally, J. C. (1978) Psychometrics methods, New York: McGraw-Hill.

19 Peace, A.G., Galletta, D.F., and Thong, J.L. (2003) Software piracy in the workplace: a model and empirical test, *Journal of Management Information Systems*, 20, 1, 153-177.

20. Quittner, J. (1995) Hacker homecoming, *Time* 145, 3, Jan, 23rd, 61.

21. Palmer. C.C. (2001) Ethical hacking, *IBM Systems Journal* 40, 3, 769-780.

22. Rice, P. (1999) The adolescent: development, relationships and culture, Allyn and Bacon: Boston. .

23. Rogers, M.K. (2001) A social learning theory and moral disengagement analysis of criminal computer behavior: an exploratory study, Unpublished Dissertation.

24. Schwartau, W. (2003) DefCon: all in good fun, *Network World*, Aug 25th, p. 47

25. Skibell, R. (2002) The myth of the computer hacker, *Information, Communication & Society*, 5, 3, 336-356.

26. Skorodumova, O.(2004) Hackers as information space phenomenon, *Social Sciences* 35, 4, 105-113.

27. Sofaer, A.D., and Goodman, S.E. (2001) The transnational dimension of cybercrime and terrorism, Stanford, Hoover Institution Press.

28. Straub Jr, D. W. (1990) Effective IS security: an empirical study, *Information Systems Research, 1*, 3, 255-277.

29. Straub Jr, D.W., and .Welke, R. (1998) Coping with systems risk: security planning models for management decision making, *MIS Quarterly* , 22, 4, 441-469.

30. Thomas, D., and Loader, B.D. (2000) Cybercrimes: law enforcement, security and surveillance in the information age, London, Routledge.

31. Von Hirsch, A., Bottoms, A.E., Burney, E and Wickstrom, P-O. (1999) Criminal deterrence and sentence severity, Hart, Oxford.

32. Witte, A.D. (1983) Economic Theories, In S.H. Kalish (Ed.), Encyclopedia of crime and justice, 1, Free Press, New York, 316-322.