12-31-2006

A Model for Predicting Hacker Behavior

Nicole Lang Beebe
The University of Texas at San Antonio

Jan Guynes
The University of Texas at San Antonio

A Model for Predicting Hacker Behavior

Nicole Lang Beebe
The University of Texas at San Antonio
Nicole.beebe@utsa.edu

Jan Guynes Clark
The University of Texas at San Antonio
Jan.clark@utsa.edu

ABSTRACT

Unauthorized access to information systems (hacking) continues to plague businesses. Researchers have sought to characterize the motivation and "profile" of various types of hackers in an attempt to better understand their behavior and improve the defensive posture of businesses. Little research, however, has been conducted toward the development of a predictive model to categorize individuals as hackers or potential hackers. Doing so would help target scarce educational and investigative resources. The present study utilizes existing theory in an attempt to empirically develop a discriminant model to categorize an individual's likelihood of engaging in illegal hacking behavior. The independent variables considered include age, gender, education level, professional status, and personal moral philosophy (Forsyth 1980). The dependent variable is behavior (measured by willingness to hack), mediated by attitude toward hacking.

Keywords

Hackers, discriminant analysis, multinomial logistic regression, personal moral philosophy, ethics, hacker profile.

INTRODUCTION

The development and diffusion of information systems and technologies into all aspects of modern society has occurred at a dizzying pace. However, evolution of the ethics that guide the use of these systems and technologies has lagged behind (Marshall, 1999), as illustrated by behavior such as hacking and the creation of malicious code (e.g., worms and viruses). This is exacerbated by a security lag – the time period between diffusion of new technology and the development of related information systems security tools (Dhillon and Backhouse, 2001).

The growing spread of improper computer use, defined as "the unauthorized, deliberate misuse of information systems" (Harrington, 1996), has a significant adverse impact on individuals, organizations, and society. It is estimated that 90% of all businesses are affected, with an annual cost of $17 billion (Austin and Darby, 2003). This is in spite of numerous technological approaches to preventing and detecting computer abuse, suggesting that the solution should also include human and organizational elements (Dhillon and Backhouse, 2001).

The purpose of this study is to explore the potential impact of a limited set of influences on attitudes and beliefs regarding the ethicality of hacking, as well as the subsequent influence of such attitudes and beliefs on behavior (or willingness to behave). The influences explored include basic demographics, ethical ideologies, and professional status. We examined whether these influences can be considered good discriminants in predicting who is likely to engage in illegal hacking behavior.

The remainder of this paper is laid out as follows. The next section provides a brief overview of related research and proposes a theoretical framework from which individuals can be categorized in a predictive manner according to their willingness to engage in illegal hacking behavior. Then we outline our methodology and data analysis procedures, which include confirmatory factor analysis, linear and multinomial logistic regression, and discriminant analysis. Results are then discussed, followed by implications and conclusions.

THEORY & RESEARCH MODEL

A fair amount of research has been dedicated to categorizing types of hackers (Landreth, 1985, Hollinger, 1988, Chantler, 1996, Parker, 1998, Rogers, 1999a, Rogers, 1999b, Denning, 1998), primarily based upon motivation and skill level. Rogers (1999a, 1999b) created a "hacker profile", postulating the individuals most likely to possess the motivation and skill level needed to engage in hacking—illegal or otherwise. The typical profile includes the following attributes:

- Caucasian;
- Male;

- 12-28 years old;
- Middle class;
- Limited social skills, but a strong desire for peer group identification and membership;
- Poor educational performance; and
- Dysfunctional family/home-life.

Several of these demographics have been studied extensively in general ethical decision making studies. Since this is exploratory research, we focused on the variables thought to be the most relevant. Loe et al. (2000) reviewed ethical decision making research and cited 26 studies that considered gender; 15 studies that considered age; 18 that considered educational level; and more than twenty that considered various organizational factors, such as corporate culture, reward/punishment systems, and codes of ethics, which showed that corporate and professional culture typically reduce tendency toward ethical behavior. Based on these studies, the individual with the highest ethical standards would be an older, well-educated, female professional. Therefore, the following are hypothesized:

- H1a: Males are more likely than females to view illegal hacking as ethical.
- H1b: Younger individuals are more likely than older individuals to view illegal hacking as ethical.
- H1c: Less educated individuals are more likely than more educated individuals to view illegal hacking as ethical.
- H1d: Computer users are more likely than computer professionals to view illegal hacking as ethical.

Although personal moral philosophy has been shown to influence ethical decision making (Schlenker and Forsyth 1977, Forsyth 1980), it has not been extended to explain or predict hacking behavior. Loe et al. (2000) cite 21 different studies that examined the influence of personal moral philosophy on ethical decision making. Personal moral philosophy can be likened to an "ethical compass" that directs one's behavior in ethical situations. Unlike a normal compass, however, the ethical equivalent to North-South-East-West is not universally agreed upon. What some people consider unethical behavior others consider ethical—particularly in IS scenarios (Ellis and Griffith, 2001).

A common approach to categorizing one's "ethical compass" is to use Schlenker and Forsyth's (Schlenker and Forsyth, 1977, Forsyth, 1980) personal moral philosophy (PMP) construct. Using this construct, people are categorized based on their tendencies toward idealism and relativism. These characteristics are independent, but not mutually exclusive (Singhapakdi et al., 1999). Both categories are measured along a continuum, ranging from high to low. Highly idealistic people value decisions based on the welfare of others; they are altruistic, believing the "right" thing can always be done. Conversely, those who are less idealistic believe it may be necessary to harm some people in order to achieve the greater good (Forsyth 1980). Highly relativistic individuals believe decisions must be based on the circumstances of the situation at hand—that universal moral rules should often be relaxed. Less relativistic individuals base decisions on moral rules, rather than the circumstances. Based on the results of these studies, the following are hypothesized:

- H2a: More idealistic individuals are less likely to view illegal hacking[1] as ethical.
- H2b: More relativistic individuals are more likely to view illegal hacking as ethical.
- H3a: Females are more idealistic than males.
- H3b: Females are less relativistic than males.
- H3c: Older individuals are more idealistic than those younger.
- H3d: Older individuals are less relativistic than those younger.
- H3e: More educated individuals are less idealistic than those less educated.
- H3f: More educated individuals are more relativistic than those less educated.

[1] It is important to remember that this study focuses on *illegal* hacking. If we define hacking as gaining unauthorized access from a systems security /or organizational policy perspective, then some hacking (i.e. sanctioned penetration testing) is legal.

- H3g: Computer professionals are more idealistic than computer users.
- H3h: Computer professionals are less relativistic than computer users.

Based on the Theory of Reasoned Action (TRA; Fishbein and Azjen, 1975), it is reasonable to assume that one's attitude toward the ethicality of illegal hacking will influence their behavior. Because measuring actual behavior is often problematic, intention to behave is a widely accepted proxy to behavior and has been frequently shown to have sufficient predictive validity to be used as such (Trevino, 1992). In this study, given the legal risks to respondents in answering questions regarding behavior or behavioral intentions, we utilized "willingness to behave" as a proxy for behavioral intention and behavior itself. Based on this, the following is hypothesized:

- H4: Attitude toward illegal hacking influences one's willingness to hack.

The overall theoretical model is shown in Figure 1. (Note, the arrows indicate correlation, not necessarily causation.)

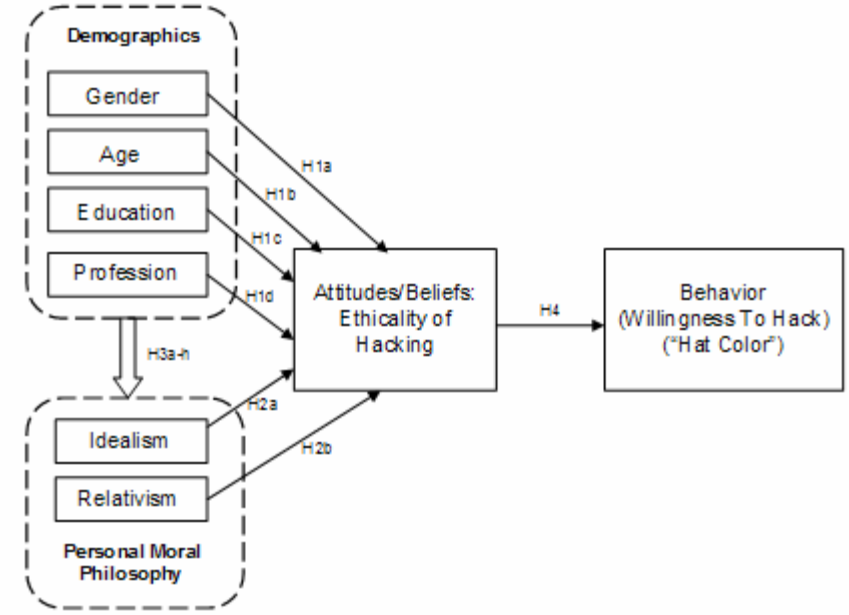

Figure 1. Research Model

METHODS AND RESULTS

Sample

A questionnaire was administered to 130 conference attendees at the 2004 DefCon and BlackHat conferences and 511 students in an introductory information systems course at a large southwestern university. The participants were surveyed on a number of items, including their personal moral philosophy, perceptions of moral intensity of various information systems related scenarios, perspectives about security vs. privacy, various demographics, and their attitudes regarding the ethicality of hacking. Finally, they were asked about their ability and willingness to hack by self-identifying themselves as: (1) hacker ("blackhat"), (2) ex-hacker ("ex-blackhat"), (3) someone with the ability to hack, but only does so with permission ("whitehat"), or (4) not able/willing to hack ("nohat').

Of the 641 surveys administered, 565 were returned (88% response rate[2]). Seven surveys were omitted from the analysis due to incomplete responses, and 12 responses were removed subsequent to outlier analyses[3].

[2] The high response rate was due to extra course credit incentives provided to the student respondents, and the fact that the survey was only provided to DefCon and BlackHat conference attendees who volunteered to complete the survey (who were given incentives via a chance to win electronics equipment).

[3] Observations were deemed outliers when responses varied more than three standard deviations from the mean on any given construct. Subsequent outlier analyses suggested the responses were unreliable.

The sample consisted predominantly of males (59%), and the mean age of the respondents was 25.8 years. Over 64% of the respondents were computer users, as opposed to computer professionals Just over half of the respondents self-identified themselves as being "blackhats," "ex-blackhats," or "whitehats"—that is to say, they had the skills needed to gain unauthorized access to information systems. The majority of the respondents (67.3%) did not have a college degree; one-quarter possessed an undergraduate degree; and approximately 7% possessed a graduate degree. Regarding personal moral philosophy, respondent idealism scores ranged from 1.0 to 8.50 on a nine-point Likert scale, with a mean of 3.85, and standard deviation of 1.60 (lower scores reflect a greater degree of relativism). Respondent relativism scores ranged from 1.0 to 8.33 on a nine-point Likert scale, with a mean of 4.27 and standard deviation of 1.32 (lower scores reflect a greater degree of idealism). Sample descriptive statistics are contained in Tables1a-1e.

1a. Gender	**Total**	**Percentage**
Female	218	39.9%
Male	322	59.0%
Unknown	6	1.1%
Total	546	100.0%
1b. Age	**Total**	**Percentage**
Under 25	325	59.5%
25-34	153	28.0%
35-44	40	7.3%
45-54	18	3.3%
55-64	4	0.7%
Unknown	6	1.1%
Total	546	100.0%
Mean	25.81	
Standard dev.	7.436	
1c. Level of Education	**Total**	**Percentage**
Not Completed High School	8	1.5%
Completed High School	359	65.8%
Undergraduate degree	136	24.9%
Graduate degree	39	7.1%
(blank)	4	0.7%
Total	546	100.0%
1d. Profession (IS Role (ISR))	**Total**	**Percentage**
Computer user	350	64.1%
Computer Professional	188	34.4.4%
Unknown	8	1.5%
Total	546	100.0%
1e. Type of Hacker (self-ID)	**Total**	**Percentage**
Blackhat (hacker)	30	5.5%
Former Blackhat	31	5.7%
Whitehat	217	39.9%
Nohat	266	48.7%
Unknown	2	0.4%
Total	546	100.0%

Table 1. Sample Descriptive Statistics

Construct Operationalization and Instrumentation Validation

Personal Moral Philosophy (PMP)

Forsyth's (1980) Ethics Position Questionnaire (EPQ) was utilized to measure the personal moral philosophy (PMP) of the respondents. The questionnaire (see Appendix A) includes 20 attitude statements, equally divided between the number of questions concerning idealism and relativism. Respondents were asked to indicate their level of agreement or disagreement with each statement via a nine-point Likert scale. Each respondent's idealism and relativism measure was simply a composite mean score of the relevant question answers. Forsyth's (1980) reported coefficient of internal consistency (Cronbach's alpha) for idealism was 0.80 for idealism and 0.73 for relativism; the test-retest measure reported was 0.67 for idealism and 0.66 for relativism.

For the purpose of instrument re-validation, we conducted a confirmatory factor analysis (CFA) on Forsyth's EPQ. For this sample, idealism loaded simply on 8 items (3, 6, 7, 11, 14, 16, 17, 19) with an acceptable reliability coefficient (Cronbach's alpha) of α=0.856. Relativism loaded simply on 9 items (1, 2, 4, 5, 8, 13, 15, 18, 20), α=0.771. Items 9, 10, and 12 did not load on either construct, and were therefore dropped from the analyses. (CFA loading tables are available from the authors upon request.)

Attitude Toward Hacking

To measure respondents' attitude toward hacking (ethicality of gaining unauthorized access to information systems), a five-item scale was developed internally (see Appendix B). Two items were included that represented situations wherein no harm was done and wherein the systems were inadequately protected. These were based on previous research regarding the importance of situational consequences, including such elements as magnitude of consequences, temporal immediacy of consequences, probability of effect, and concentration of effect (Jones, 1991) and the basic *hacker ethic* (Arief and Besnard, 2003). Five researchers with experience in information security and computer crime investigations assessed the content validity of the questions. Pre-testing, pilot testing and convergent/discriminant validity tests were not conducted. However, a CFA was conducted based on responses received. The oblique rotation model results in the simpler factor model. In it, one factor with eigenvalue greater than 1.0 emerged, which explains 53% of the total variance. The one-factor model contains all five of the proposed "attitude toward hacking" items, resulting in a five-item scale with reliability of α=0.767.

Behavioral Intention (Willingness to Hack)

In an attempt to measure respondents' behavioral intention regarding illegal hacking behavior, we operationalized behavioral intention via the respondent's willingness to hack. This was approximated by their self-reported hacker type: (1) hacker ("blackhat"), (2) ex-hacker ("ex-blackhat"), (3) someone with the ability to hack, but only does so with permission ("whitehat"), or (4) not able/willing to hack ("nohat'). We asked one question that asked which best described the respondent amongst the following options:

1. "I am willing to use my knowledge and skills to gain unauthorized access to information systems to serve my own goals."
2. "I *used to be willing* to use my knowledge and skills to gain unauthorized access to information systems to serve my own goals."
3. "I have the knowledge and skills to gain unauthorized access to information systems, but I am only willing to use those skills legally and with expressed consent of those affected."
4. "None of the above."

We worded the question toward the respondents' *willingness* as opposed to actual behavior, because the latter could be construed as an admission of criminal activity, thus introducing a higher likelihood for positivity response bias.

Data Analysis and Results

We conducted and report both regression and discriminant analyses for two reasons. First, multinomial logistic regression tends to be more robust when the assumption of equal covariance matrices for the dependent variable levels is violated, which is the case here[4]. On the other hand, logistic regression analysis requires a larger sample size than does discriminant analysis. A general rule of thumb is to have greater than 30 responses in each level of the dependent variable. Because we only have 30 blackhats and 31 ex-blackhats in the sample, our sample does not permit the use of logistic regression in a predictive manner (i.e. divide the sample into a training set and a test set, and subsequently test the model's predictive

[4] The Box's M value was 76.539, which was statistically significant at the α=0.01 level.

capability on the test set). As a result, we elected to include the discriminant analysis results to demonstrate the model's potential predictive ability. (Although the reader is cautioned regarding such results given the inequality of covariance matrices with respect to the dependent variable.) Given the exploratory nature of this study, however, we deemed it important to conduct and present both analyses.

Regression Analysis

Linear regression analysis was employed to determine the ability of gender, age, education level, information systems role (computer user versus computer professional), and PMP type to explain the variance in attitudes toward the ethicality of hacking. As shown in Figure 2, age, information systems role, idealism, and relativism had a statistically significant influence on attitude toward hacking (adjusted R^2=0.138). Contrary to expectations, gender and education level had no impact on one's attitude toward the ethicality of hacking.

We contend that one's ethicality toward hacking and one's willingness to hack are two separate entities. Multinomial logistic regression analysis[5] was employed to test the influence of attitude toward illegal hacking on willingness to illegally hack. Figure 2 also shows that attitude toward hacking explains approximately 14% of the variance in willingness to illegally hack. The odds functions are provided below:

$$\text{Prob(blackhat)/Prob(not a hacker}^{6}\text{)} = e^{4.485} \times e^{-1.109(HA)}$$

$$\text{Prob(ex-blackhat)/Prob(not a hacker)} = e^{1.201} \times e^{-0.496(HA)}$$

$$\text{Prob(blackhat)/Prob(not a hacker)} = e^{1.408} \times e^{-0.229(HA)}$$, where HA = Attitude toward Hacking

Finally, the regression results show that although gender was not a good predictor of one's ethicality toward hacking, it was (along with information systems role (ISR)), a significant predictor of idealism; and age and education had a statistically significant influence on relativism (see Figure 2).

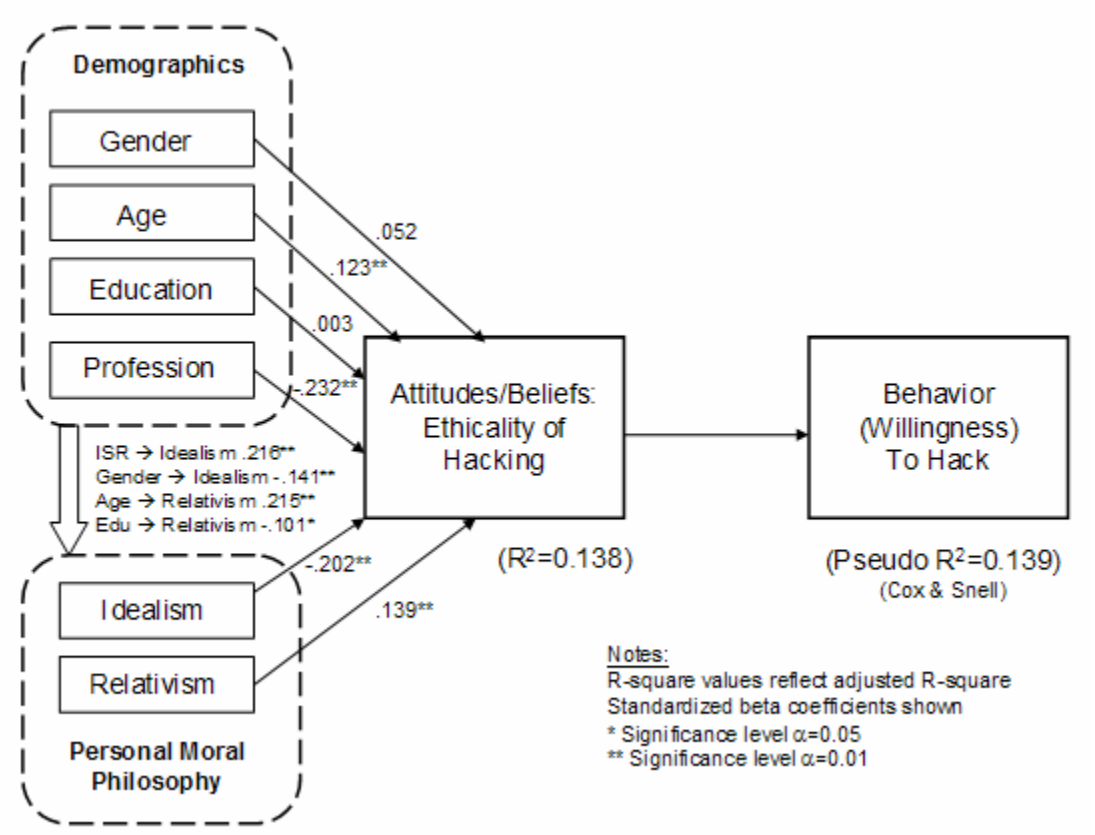

Figure 2. Regression Results

[5] The dependent variable is categorical with four categories: (1) blackhats, (2) ex-blackhats, (3) whitehats, and (4) nohat.

[6] Not a hacker, past or present.

Discriminant Analysis

Discriminant analysis was employed to determine the ability of individual characteristics (demographic variables and personal moral philosophy) to predict one's willingness to illegally hack. We found the model was unable to realistically distinguish between blackhat hackers and ex-blackhat hackers. When attempting to predict at that level of granularity, the predictive ability of the model (success rates) dropped to 58.8% for the training set and less than 50% (48.1%) for the test set. Considering the fact that both blackhat and ex-blackhat hackers demonstrate or have demonstrated a willingness to illegally hack, we explored the predictive ability of the model when combining these two groups of people. When doing so, the prediction success rates increase to 62.7% for the training set and 54.1% for the test set. We argue such combination is justified, since our goal is to predict willingness to illegally hack, as opposed to actual, current behavior.

Information systems role (a.k.a. "profession" or "ISR"), gender ("Gender"), idealism ("Ideal"), and attitude toward hacking ("HA") were significant predictors of one's willingness to illegally hack. The resultant Fisher's linear discriminant functions are as follows:

$$D_1 \text{ (blackhat or former blackat hacker)} = -30.597 + 12.189(ISR) + 8.831(Gender) + 2.396(Ideal) + 3.525(HA)$$

$$D_2 \text{ (whitehat hacker)} = -36.331 + 12.951(ISR) + 9.666(Gender) + 2.295(Ideal) + 4.176(HA)$$

$$D_3 \text{ (not a hacker)} = -34.396 + 10.840(ISR) + 10.294(Gender) + 2.066(Ideal) + 4.287(HA)$$

Where,

ISR = 1 if computer user; 2 if computer professional

Gender = 1 if male; 2 if female

Ideal = Idealism score (continuous scale 1-9; lower score is more idealistic)

HA = Attitude toward hacking score (continuous scale 1-9; lower score reflects positive attitude toward hacking ("It is OK to hack"))

Note that Fisher's functions are based on discriminant scores. The objective is to find the highest score, using the discriminant functions (above formulas) and independent variable values for an individual. To predict hacker type, one must input the ISR, gender, idealism, and HA values—the highest score corresponds to the prediction decision.

The discriminant functions for predicting hacker type ("hat color") resulted in a 62.7% success rate for the test (learning) sample set and a 54.1% success rate for the validation sample set. Thus, the discriminant functions using gender, information systems role, level of idealism, and attitude toward the ethicality of hacking results in correct classifications greater than 50% of the time.

DISCUSSION

Based upon results of the linear and logistic regression analyses, we found support for the following hypotheses:

- H1b: Younger individuals are more likely than older individuals to view illegal hacking as ethical.
- H1d: Computer users are more likely than computer professionals to view illegal hacking as ethical.
- H2a: More idealistic individuals are less likely to view illegal hacking as ethical.
- H2b: More relativistic individuals are more likely to view illegal hacking as ethical.
- H3a: Females are more idealistic than males.
- H3d: Older individuals are less relativistic than those younger.
- H3g: Computer professionals are more idealistic than computer users.
- H4: Attitude toward illegal hacking influences one's willingness to hack.

Surprisingly, gender and age had no impact on one's view of the ethicality of hacking. Gender did, however, impact one's willingness to hack. The findings show that individual characteristics, including demographic variables and personal moral philosophy do influence one's attitude toward the ethicality of hacking, which in turn influences one's willingness to illegally hack computer systems. The influence of demographic variables serves to empirically validate previous theory and replicate

previous findings. The influence of personal moral philosophy on one's attitude toward the ethicality of hacking represents new theory via theoretical extension, which was empirically validated in this study.

It is interesting to note that one's level of relativism did not emerge as a good discriminant in predicting willingness to illegally hack; further discussion is warranted. As previously stated, the long-standing and widely accepted basic *hacker ethic* states that illegal hacking is acceptable if the target systems are inadequately protected and/or if no harm is done from the hacking activity (Arief and Besnard, 2003). These situational characteristics could reasonably be considered conditions when the rules should be relaxed in the eyes of a relativist. If the long-standing hacker ethic is indeed valid today, hackers can be assumed to be relativists. Thus, we would expect relativism to emerge as a discriminating variable in predicting willingness to illegally hack. The fact that it did not calls into question the presumed veracity of the self-reported hacker ethic – an important potential implication of this study.

While the resultant discriminant functions presented are limited in their utility, due to discrimination success rates of just slightly greater than 50%, the research shows promise for future discriminant analysis research regarding "profiling" hackers. The somewhat low, albeit statistically significant explained variance in attitude toward illegal hacking (13.8%) and willingness to illegally hack (13.9%), suggests that identification of additional explanatory variables would improve the discriminant functions. In other words, this research showed that hacker profiling (prediction of hacker type based on individual characteristics) is feasible with an exceptionally parsimonious model, which suggests that a more complex model would improve the ability to profile potential hackers.

Several limitations of this study and its findings should be noted. The limitations fall into the categories of instrumentation, sampling, and methodology (data analysis techniques selected given sampling issues). Instrumentation issues are three-fold. First, the EPQ measuring personal moral philosophy (PMP) fails to perform up to stated expectations in this application. It is reportedly a two-factor model, but those two factors—idealism and relativism—only explain approximately 54% of the variance in responses. Scales that explain 70% of the variance with factors having eigenvalues greater than 1.0 are preferred. Improved PMP scales may cause idealism and relativism to emerge as more powerful discriminants.

The second instrumentation issue is similar to the first, but pertains to the scale measuring attitudes toward the ethicality of illegal hacking. This scale was developed and used without adequate validity testing, especially convergent and discriminant validity testing. This might explain the poor performance of the scale from the perspective of explained variance. While the reliability was reasonably acceptable (α=0.767), the model only explained 53% of the overall response variance.

The last instrumentation issue pertains to positivity bias. Despite the fact that the surveys were anonymous, the respondents are likely to have answered the attitude and behavior willingness questions in a positive manner, independent of their true attitude or willingness to behave in an unethical manner. The reason for this is two-fold. First, the respondents were either students in an academic environment in which they are striving to please, or they were attendees at a known hacker's conference, therefore placing their general honesty into question. Additionally, the subject matter involved illegal activity. While we attempted to minimize positivity bias by measuring self-assessed hacker type, rather than actual behavior or behavioral intention, the respondents were likely to minimize their willingness to engage in such activity for fear of self-incrimination.

The second category of problems associated with this research involves sampling issues. Overall, there is a lack of heterogeneity in the sample, particularly with respect to age. Additionally, there is a disproportionate number of respondents in each category (i.e. many more users than professionals, many more non-hackers than whitehat hackers, many more whitehat hackers than blackhat hackers, etc.). The result of such homogeneity and disproportionate subsamples is lack of variability and unbalanced prior probabilities, which naturally limits the ability of the proposed variables to emerge as good discriminators. Given these issues, though, it is reasonable to assume our findings are downward biased. In that case, discrimination success rates ranging from 54-61% are actually rather promising.

CONCLUSION

The theoretical basis underlying the hypotheses appears sound. As Loe et al. (2000) point out in their review of empirical literature pertaining to ethics, there is ample support for the hypotheses presented. Research, albeit limited and largely non-empirical, into the profiling of hackers suggests the proposed theory is extensible to the domain of ethical decision making in information systems in general and hacking in particular. It appears that the sample frame is inadequate in its lack of heterogeneity and representativeness, as it pertains to the hacker population, to support the development of a discriminant model for predicting who will be hackers. Future research should seek to gain responses from more blackhat hackers.

ACKNOWLEDGMENTS

This research was supported via a grant from the Center for Information Assurance and Security (CIAS) at the University of Texas at San Antonio. The authors wish to thank CIAS personnel, as well as Dr. Tim Goles, Barbara Hewitt, and Carlos

Alberto Dorantes for their assistance in distributing the survey and coding the results. The authors also wish to thank Dr. Nandini Kannan for her comments on an earlier version of this paper.

REFERENCES

1. Arief, B. and Besnard, D. (2003) University of Newcastle upon Tyne, Newcastle, UK, pp. 1-17.
2. Austin, R. D. and Darby, C. A. R. (2003) The Myth of Secure Computing, *Harvard Business Review*, 120-128.
3. Chantler, N. (1996) Infowar, Florida.
4. Denning, D. (1998) Information Warfare & Security, Addison-Wesley, Reading.
5. Dhillon, G. and Backhouse, J. (2001) Current Directions in IS Security Research: Towards Socio-Organizational Perspectives, *Information Systems Journal*, 11, 11.
6. Ellis, T. S. and Griffith, D. (2001) The Evaluation of IT Ethical Scenarios Using a Multidimensional Scale, *The DATA BASE for Advances in Information Systems*, 32, 32, 75-85.
7. Fishbein, M. and Azjen, I. (1975) Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research, Addison-Wesley, MA.
8. Forsyth, D. R. (1980) A Taxonomy of Ethical Ideologies, *Journal of Personality and Social Psychology*, 39, 39, 175-184.
9. Harrington, S. J. (1996) The Effects of Codes of Ethics and Personal Denials of Responsibility on Computer Abuse Judgments and Intentions, *MIS Quarterly*, 20, 20, 257-278.
10. Hollinger, R. (1988) Computer Hackers Follow a Guttman-Like Progression, *Social Sciences Review*, 72, 72, 199-200.
11. Jones, T. M. (1991) Ethical Decision Making by Individuals in Organizations: An Issue-Contingent Model, *Academy of Management Review*, 16, 16, 231-248.
12. Landreth, B. (1985) Out of the Inner Circle, Microsoft Books, Redmond, WA.
13. Loe, T. W., Ferrell, L. and Mansfield, P. (2000) A Review of Empirical Studies Assessing Ethical Decision Making in Business, *Journal of Business Ethics*, 25, 25, 185-204.
14. Marshall, K. P. (1999) Has Technology Introduced New Ethical Problems? *Journal of Business Ethics*, 19, 19, 81-90.
15. Parker, D. (1998) Fighting Computer Crime: A New Framework for Protecting Information, John Wiley & Sons, Inc., New York.
16. Rogers, M. (1999a) A New Hacker Taxonomy, Masters Thesis, University of Manitoba, Winnipeg.
17. Rogers, M. (1999b) The Psychology of Hackers: The Need for a New Taxonomy, www.infowar.com.
18. Schlenker, B. R. and Forsyth, D. R. (1977) On the Ethics of Psychological Research, *Experimental Social Psychology*, 13, 13, 369-396.
19. Singhapakdi, A., Vitell, S. J. and Frank, G. R. (1999) Antecedents, Consequences, and Mediating Effects of Perceived Moral Intensity and Personal Moral Philosophies, *Journal of the Academy of Marketing Science*, 27, 27, 19-35.
20. Trevino, L. K. (1992) Moral Reasoning and Business Ethics: Implications for Research, Education and Management, *Journal of Business Ethics*, 11, 5,6, 445-464.

APPENDIX A - ETHICS POSITION QUESTIONNAIRE (EPQ)

NOTE: Questions 1-10 measure idealism; question 11-20 measure relativism.

1. People should make certain that their actions never intentionally harm another even to a small degree.
2. Risks to another should never be tolerated, irrespective of how small the risks might be.
3. The existence of potential harm to others is always wrong, irrespective of the benefits to be gained.
4. One should never psychologically or physically harm another person.
5. One should not perform an action which might in any way threaten the dignity and welfare of another individual.
6. If an action could harm an innocent other, then it should not be done.
7. Deciding whether or not to perform an act by balancing the positive consequences of the act against the negative consequences of the act is immoral.
8. The dignity and welfare of the people should be the most important concern in any society.
9. It is never necessary to sacrifice the welfare of others.
10. Moral behaviors are actions that closely match ideals of the most "perfect" action.
11. There are no ethical principles that are so important that they should be a part of any code of ethics.
12. What is ethical varies from one situation and society to another.
13. Moral standards should be seen as being individualistic; what one person considers to be moral may be judged to be immoral by another person.
14. Different types of morality cannot be compared as to "rightness."
15. Questions of what is ethical for everyone can never be resolved since what is moral or immoral is up to the individual.
16. Moral standards are simply personal rules that indicate how a person should behave, and are not be applied in making judgments of others.
17. Ethical considerations in interpersonal relations are so complex that individuals should be allowed to formulate their own individual codes.
18. Rigidly codifying an ethical position that prevents certain types of actions could stand in the way of better human relations and adjustment.
19. No rule concerning lying can be formulated; whether a lie is permissible or not permissible totally depends upon the situation.
20. Whether a lie is judged to be moral or immoral depends upon the circumstances surrounding the action.

APPENDIX B – ATTITUDE TOWARD HACKING MEASURES

(HA1) I feel it is okay for a person to access information systems without authorization.

(HA2) I feel it is okay to get into information systems without the system owner's consent.

(HA3) In my opinion, an individual should not be held accountable or punished for accessing information systems that were not properly safeguarded.

(HA4) In my opinion, it is wrong to access information systems without permission.

(HA5) I feel it is okay for a person to access information systems without authorization if no harm is done.