Copyright © 2010 International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891
Jan – July 2010, July - December 2010 (Combined Issue) Vol 4 (1&2): 643–656

The Risk Propensity and Rationality of Computer Hackers

Michael Bachmann[1]
Texas Christian University, USA

Abstract

Issues concerning computer security have received considerable academic attention in recent years and cyber security has become a top priority for many governments, organizations, and industries. Unfortunately, the attention devoted to cyber crime issues has focused primarily on the technical dimension of computer crime. Today, our knowledge about the persons behind the keyboards remains fragmentary. The current study focuses on one particular subgroup of cyber criminals, the illicit computer hackers. In particular, two personality characteristics commonly ascribed to hackers, strong preference for rational decision-making processes and pronounced risk propensity, are examined and their influence on hacking activities and success is assessed. An abbreviated yet reliable scale to quantify these personality traits in future studies demonstrates the significant relevance both constructs have for predicting hacking-related outcomes. Implications, limitations, and suggestions for future studies are provided.

Keywords: Hacking, Hacker, personality trait, risk propensity.

Introduction

The English verb *hacking* in the context of computers is commonly described as referring to the act of re-designing the configuration of hardware or software systems to alter their intended function. This act requires that the person hacking the system is not only knowledgeable enough to understand its inner workings, but also possesses the creativity necessary for envisioning a modification that will render the system more efficient or able to perform an alternative function.

When the term *hacking* was first introduced as a neologism into the specialized and confined language of computer technicians and programming experts during the 1960s, it was used as a positive label for somebody particularly skilled in developing highly efficient, creative, compact programs and algorithms (Levy, 1984). Over the years, this initially very positive label gradually became highly contested. The increasingly mission-critical nature of computer networks for many industries and the expanding popularity of electronic financial transactions began to interest many people in breaking into computer systems, not in an attempt to understand them or make them more secure, but to abuse, disrupt, sabotage, and exploit them. Today, the term *hacker* is applied to a wide range of computer-savvy persons who differ greatly in their motivations, skills, and usage of their

[1] Assistant Professor, Department of Criminal Justice, Texas Christian University (TCU) Fort Worth, TX, United States of America. Email: m.bachmann@tcu.edu

computer knowledge. This variety aside, the general public tends to stereotype hackers as clever, yet sinister computer criminals who essentially live in cyberspace where they go on thrill-inducing missions to exploit vulnerabilities in other networks and systems.

While this greatly oversimplified, stereotypical representation does not even begin to tell the whole story of who hackers are, it nevertheless includes some elements that seem to be indeed wide-spread personality characteristics within the hacking community. First, hackers are generally thought of as having a heightened need for cognitive challenges (Dalal & Sharma, 2007; Holt & Kilger, 2008; Schell & Melnychuk, 2010). They are eager to learn about the technical intricacies of systems and processes, enjoy exploring their details, and thrive on mastering the intellectual challenges involved in altering or circumventing their functions and limitations. Second, they are also thought of as being thrill-seekers who derive pleasure and excitement from the chase, from overcoming barriers, and from gaining access to other systems (Levy, 1984; Yar, 2005). This second personality characteristic applies particularly to so-called black-hat hackers, persons who do not subscribe to any hacker ethic (Levy, 1984), but who use their skills to break into systems without having the consent of the owner. They engage in illicit activities, a circumstance that introduces greater risks, raises the stakes, and increases the excitement and thrill even more.

While the notion of hackers as persons of heightened rationality and risk propensity is rather intuitive, two questions of interest remain unanswered: (1) how pronounced are heightened-need and thrill-seeking characteristics within the hacking community? (2) Do members of this community differ significantly from the general population? A second set of questions in this context is whether the degree to which hackers exert a preference for rational decision-making processes and for the engagement in particularly risky endeavors influences (3) their overall engagement in hacking activities and (4) their self-reported success as a hacker.

The present study, based on a survey study fielded at a large hacker conference, adds to the current literature on hackers by providing answers to all four questions. The survey instrument included newly devised scales for both personality characteristics. The study tests the validity and reliability of both scales and assesses their ability to cleanly measure both concepts via exploratory factor analysis. It examines both characteristics among respondents who admitted to having engaged in illicit hacking activities further contrasts their prevalence among members of this subgroup to the degree that members of the general public exert them, and assesses the relevance of both factors for the prediction of hacking-related outcomes.

Methods

To address both questions raised above, a survey measurement instrument was developed and fielded at the Washington D.C. ShmooCon 2008 hacker convention. Since 2004, ShmooCon has developed into one of the largest and most popular annual conventions worldwide. The convention is attended by a diverse audience comprised of American and international hackers and security experts (Grecs, 2008). Fielding a survey at such a popular, yet professional convention presents an opportunity to contact more seasoned hackers and security experts who are involved enough to undergo the efforts and costs involved in attending a professional convention.

Boudreau, Gefan, and Straub (2001) emphasize the need for every survey instrument to be pre-tested to prevent unanticipated encounters during the fielding of the survey. The preliminary draft of the survey instrument was pretested with a convenience sample comprised of six self-proclaimed hackers known to the researcher. There was a general consensus among the reviewers regarding the appropriateness of the items and on the exhaustiveness of the standard answer categories. In a second review step, the revised version of the survey draft was reviewed by two experienced survey researchers since many items were developed specifically for the present study and had not yet been validated. It provided a second scrutiny of the appropriateness of the survey tool as a scientific measurement instrument and the content validity of the individual items. Based on the recommendations of these experts, some modifications and refinements were implemented in the final version of the questionnaire. In a final step, the Institutional Review Board (IRB) permission required to conduct the study was obtained and the study was coordinated with the convention organizers.

Sample

Approximately one-third of the contacted attendees were rejected because they had never attempted a computer intrusion, either because they had just recently become interested in hacking or because they merely accompanied another attendee. A total of 164 questionnaires were distributed among qualified attendees. Most of the persons who agreed to participate in the study filled out the questionnaire on site. Of the 164 distributed surveys, 129 were returned to the researcher. A total of 124 completed surveys were included in the analysis of the study. Overall, the response rate of completed and returned surveys was 75% and an estimated 25% of all eligible attendees were included in the study.

Survey Instrument

Aside from assessing the respondents' general involvement in hacking activities, the survey instrument also included questions measuring the degree of risk propensity, rationality, and faith-in-intuition in the respondents' decision-making processes. The involvement in hacking activities was measured in three different categories: (1) technical intrusions, (2) social engineering attacks, and (3) malware distributions. Each category included a reminder that these items refer exclusively to illicit hacking attacks, not penetration tests under contract or attacks on systems that belonged to the hacker. Respondents were asked to estimate the overall number of times they had engaged in these activities and to provide self-estimated success rates for each type of activity.

The operationalization of the influence and degree of rationality in decision-making processes presented a principally difficult methodological challenge. Typically, such assumptions are measured with either fictional scenarios of nearly real-life decision-making situations (Clarke & Cornish, 2001; Finch, 1987; Harrington, 1996; Kerlinger, 1986) or with social psychological scales (Clarke & Cornish, 2001; Kerlinger, 1986). Scales are typically used because, as MacCrimmon and Wehrung (1990) point out, the concept of risk propensity is too broad to be accurately captured with a single item. The decision to operationalize the three personality traits with social psychological scales in the present study was made because this assessment format better fitted the setting in which the survey was fielded.

All personality-related items were taken from well-established scales abbreviated to keep the overall length of the survey within reasonable limits. Items were selected according to their item-to-total correlations and their factor loads on the respective underlying dimension. To maintain construct validity despite the shortening of the scales, items were also selected based on their ability to measure different aspects of the underlying concept.

The five items measuring risk propensity were taken from different scales and slightly modified for the best thematic fit. The first item "I always try to avoid situations involving a risk of getting into trouble" was modified from a scale developed by Dahlback (1990). The second item, "I always play it safe even when it means occasionally losing out on a good opportunity," was adapted from Gomez-Mejia and Balkin's (1989) "willingness to take risks" scale, which is an advancement of the original scale developed by Slovic (1972) and the modifications introduced by Gupta and Govindarajan (1984). The remaining three items were taken from Dulebohn (2002), who developed them, to measure general risk propensity and who reported a Cronbach alpha of .73 for this three-item scale. The fourth item "I am rather bold and fearless in my actions" was reversed to prevent biases introduced by "acquiescence" response strategies of participants who give superficial answers because they want to get through questions quickly (Krosnick & Fabrigar, 1997).

Two other scales were included to assess the degree to which respondents generally rely on their rationality versus their intuition when making decisions. All items in the rationality and the faith-in-intuition scales were taken from the latest version of the Rational-Experiential Inventory (REI) scale (Pacini & Epstein, 1999). The REI is a well established and supported measurement instrument for rational versus heuristic thinking styles (Epstein, 2003; Epstein, Pacini, Denes-Raj, & Heier, 1996; Handley, Newstead, & Wright, 2000; Pacini & Epstein, 1999).

The full version of the REI consists of 40 items in two main scales measuring the preference for analytical-rational or intuitive-experiential information processing. Each of the main scales is further divided into subscales of self-assessed effectiveness and engagement in both thinking styles. More precisely, "rational effectiveness" refers to the confidence persons have in their logical reasoning, whereas "rational frequency" or "engagement" refers to the pleasure derived from rational thinking (Handley et al., 2000). Conversely, "experiential ability" measures the confidence in relying on personal intuitions and "experiential engagement" measures the enjoyment of using intuition as the basis of one's decision making. The internal consistency reliabilities are reported with .87-.90 for the two REI scales and .79-.84 for the four subscales (Epstein, 2003). The full version of the REI scale was abbreviated in the survey. The questionnaire contained five items from each of the two REI scales. Three of the five items in each scale were taken from the ability subscales and two from the engagement subscale. All items were anchored on appropriately labeled seven-point Likert-type scales to allow for fine distinctions in the measurement of the variables (Sommer & Sommer, 2002), and to increase the ability to reach the upper limits of reliability (Krosnick & Fabrigar, 1997; Nunnally, 1978). The survey instrument concluded with measures of basic socio-demographic information.

Analysis

The regression models used for testing expectations regarding the impact of rationality and risk propensity on the involvement and success in hacking operated with two indices derived from the abbreviated personality scales as independent variables. To ensure the appropriate operationalization of all personality variables in the regression models, the validity and reliability of the personality constructs was assessed prior to the calculation of the regression models. When estimating the validity of a theoretical construct, two aspects are of particular importance: discriminant and convergent validity (Schnell, Hill, & Esser, 1999; Trochim, 2002). Since the scales used to measure the personality constructs were abbreviated and partially modified, the validity and reliability of these scales were analyzed in an exploratory validation phase.

Exploratory Factor Analysis

According to Thompson (2004), an exploratory factor analysis (EFA) should be conducted when the relationships between individual items and underlying factors are not exactly known. The particular type of EFA used was a principal component analysis with promax rotation and Kaiser normalization (calculated with SPSS 17.0). As Hair and his colleagues suggested, the selection of an orthogonal or oblique rotation should be made according to the specific demands of a particular research problem (Hair, Anderson, Tatham, & Black, 1998). According to Hair et al., orthogonal rotation methods are most appropriate when the research goal is to reduce the number of items in a construct, regardless of how meaningful the resulting underlying factors are. On the other hand, if the intent is to create or verify theoretically meaningful constructs, oblique rotation methods are better suited. Since the purpose of this factor analysis was to reveal the appropriateness of the scales used in this study, promax rotation, an oblique rotation method, was chosen. All 15 items were entered into the EFA and three factors were extracted. Table 1 presents the EFA results for all three personality variables.

Table 1 shows that the EFA produced three factors with eigen values greater than 2.0, a level that confirms the independence of the concepts. The high eigen values of all three factors also indicated that the factors explained large fractions of the variance within their respective set of variables. The three-factor solution accounted for 63.4% of the total variance, a value above the generally accepted 60% level in social research (Hair et al., 1998; Thompson, 2004). To assess the factor loadings in the individual item analysis, guidelines from Kim and Mueller (1978) were used. According to these guidelines, loadings of 0.4 to 0.54 are considered fair; 0.55 to 0.62 are considered good; 0.63 to 0.70 are considered very good; and over 0.71 are considered excellent.

As Table 1 shows, all of the 15 items loaded higher than 0.55 on their respective factors, and none of the items loaded higher than 0.4 on any other factors. Thus, all three constructs were extracted cleanly as factors. The fact that none of the items loaded on multiple factors indicated high levels of discriminant validity for all three personality constructs. Similarly, the high to excellent loadings of all individual items on their respective factors further suggested that all three constructs also had high levels of convergent validity. Based on the positive EFA results, all of the 15 items were retained in the analysis.

All 15 items correlated highly with their respective scales. The lowest item-to-total correlation of any item was 0.42, which shows that all items contributed in a meaningful way to the scale scores. The high internal consistency of all three scales is further reflected in their high Cronbach's alpha values. The risk propensity scale reached an alpha level of 0.83; the rationality scale, a level of 0.75; and the experience scale, a level of 0.86. All three values were within 0.70 and 0.90, the range that is typically considered to be ideal for internal consistency measures (Hair et al., 1998).

Overall, the loading patterns of the REI items in this factor analysis compared favorably to the factor analysis findings for the complete scales reported by Handley and colleagues (2000). The similarity between the patterns of both factor analyses confirms the appropriateness of the item selections that were used to create the abbreviated scales. The comparison to Handley's results further reveals an important finding.

Table 1: Personality Scales, Item, Factor, and Index Analysis

		Item to total correlation		Factors[1]	
Items			1	2	3
Risk propensity scale (α=.83)					
I always try to avoid situations involving a risk of getting into trouble.		.65	.81		
I always play it safe even when it means occasionally losing out on a good opportunity.		.69	.88		
I am a cautious person who generally avoids risks.		.71	.83		
I am rather bold and fearless in my actions.[2]		.52	.63		
I am generally cautious when trying something new.		.53	.65		
Rationality items (α=.75)					
I usually have clear, explainable reasons for my decisions.		.62		.79	
I don't reason well under pressure.[2]		.55		.81	
Thinking hard and for a long time about something gives me little satisfaction.[2]		.44		.57	
I prefer complex to simple problems.		.42		.57	
I enjoy solving problems that require hard thinking.		.63		.82	
Intuition-experience items (α=.86)					
Using my gut-feelings usually works well for me in working out problems in my life.		.57			.73
I trust my initial feelings about situations.		.66			.82
I like to rely on my intuitive impressions.		.79			.87
I often go by my instincts when deciding on a course of action.		.79			.86
I don't think it is a good idea to rely on one's intuition for important decisions.[2]		.61			.86
Eigenvalue			2.71	2.21	4.31
Variance explained (%)			18.1	14.8	28.7
Cumulative variance (%)			18.1	32.9	61.6
Indices	α	N	Range		(sd)
Summative risk propensity index	.83	124	5-35	22.1	6.1
Summative rationality index	.75	124	11-35	27.2	5.0
Summative intuition index	.86	124	10-35	23.6	5.3

[1] Principal Component Analysis with Promax Rotation Method and Kaiser Normalization. Loadings less than .4 not shown. [2] Items were reversed.

When compared to the general public sampled in Handley's study, the sample of hackers yielded a significantly higher average rationality value (5.4 compared to 3.4 in Handley's analysis, $t(123) = 17.94$, $p < .001$). Hackers also reported a significantly higher confidence in their experience-based decision making (4.7 compared to 3.4, $t(123) = 7.85$, $p < .001$), even though this difference was not as large as the one found between the two rationality measures. These comparisons suggest two important differences between hackers and the general public: (1) hackers prefer a more analytical and rational thinking style than the average person, and (2) display a generally higher confidence in their ability to make decisions, regardless of whether these decisions are based on rational considerations or on intuition and experience.

Influence of Personality Characteristics on Hacking Involvement and Success

The expectation that risk propensity exerts an influence on the total number of illicit hacking attempts was tested using a linear regression model. The dependent variable total number of hacking attempts was calculated as a summative index of the total number of technical intrusions, social methods, and malware distributions a person had attempted. The wide range of the index (from 1 to 23,000) and the rounded estimates many respondents gave to the questions about the total number of attacks caused the dependent variable to have a platykurtic shape with a multimodal, rounded peak, and wide shoulders. Despite the significant deviation from the mesokurtic shape of a normal distribution, the distribution of the dependent variable was not significantly skewed, and was therefore included in the regression.

Table 2: OLS Regression Coefficients for estimated Effects of Rationality and Risk Propensity on Total Amount of Hacking Attacks

	Model 1		Model 2	
Variable	B	β	B	β
Hypothesized characteristics				
Rationality index	174.60 *	.21 (74.72)	192.51 **	.23 (74.23)
Risk propensity index	228.44 ***	.33 (61.96)	243.44 ***	.35 (61.26)
Sociodemographic controls				
Age			-19.42	-.03 (68.87)
Female			16.69	.00 (1613.7)
Non-White			-17.10	-.00 (1279.4)
Education			-539.06	-.16 (368.80)
Marital status				
Living as married			1940.18	.16 (1073.5)
Married			510.49	.06 (956.86)
Unemployed			4110.45 **	.27 (1623.2)
Student			-2226.61 **	-.25 (829.90)
Constant	1981.59	(2215.30)	5438.62	(3345.22)
R-squared	.12		.29	

Note. Standard errors are listed in parenthesis.
**p*<.05. ***p*<.01. ****p*<.001.

As could be guessed intuitively, the effect of the risk propensity variable (*p*<.001 in both models) was stronger than the effect of the rationality variable. Nevertheless, a significant effect was also found for the rationality variable (*p*<.05 in Model 1 and *p*<.01 in Model 2). The effects of both variables are shown in Table 2.

The risk propensity of respondents influenced the number of total hacking attempts as predicted. Persons with a higher risk propensity engaged in significantly more hacking attempts. Surprisingly, the level of rationality also exerted a significant influence on the number of total hacks. Hackers with a preference for analytic-rational thinking styles also committed significantly more attacks. One possible explanation for this finding is provided in the second regression model in this study. The model shows that hackers with a preference for analytic-rational thinking styles report to be more successful in their hacks, a circumstance that could lead them to become more involved.

Two of the sociodemographic control variables entered in the saturated model also exerted a significant effect on the number of hacks. Unemployed hackers reported a significantly higher number of hacking attacks than hackers who were employed (*p*<.01). One possible explanation for this finding could be related to the circumstance that hacking is a time-consuming activity. Unemployed hackers simply have more time at their hands to dedicate to hacking. Time considerations could also be the reason why student hackers report to commit significantly fewer attacks (*p*<.01). The majority of students in the sample were part-time students who had full-time jobs. Another possible explanation is offered by Laub and Sampson (1993, 2003), who emphasize that stable careers inhibit the engagement in illegal activities. According to Laub and Sampson (2003), stable work and career relations create strong ties to society that decrease the likelihood of engagement in criminal activities (p. 6).

The second regression shown in Table 3 demonstrates the influence of the two hacker personality characteristics, risk propensity and rationality, on the overall success of hacking activities. To reflect the overall success of all hacking activities most accurately, the success rates of the three different attack methods (technical intrusions, social methods, and malicious code distributions) were weighed with the proportion of total hacking attempts that was accounted for by the respective attack method. The three products were then summarized into the total success rate for all methods. For example, if a hacker reported having undertaken a total of 100 hacking attempts, out of which 70 were technical intrusions, 20 were social engineering attacks, and 10 were distributions of malicious code, the total success rate for this hacker was calculated as the sum of the success rate of technical intrusions multiplied by 0.7. The success rate of social methods was then multiplied by 0.2, and the success rate of malicious code distributions multiplied by 0.1.

The regression results presented in Table 3 clearly support the predictions regarding the influence of the personality traits on hacking success. Despite the low number of cases in the models (n=124), a circumstance that usually causes high in-group variances, both models were highly significant (Model 1 and 2 *p*<.001).

In the first model, the two personality characteristics alone explained 11% of the variance in the success of hacking attacks. In this model, both variables exerted a highly significant influence on the dependent variable (*p*<.01). Moreover, rationality turned out to be the most influential variable in both models. As could be expected, the effect of rationality on the success of hacking attacks was positive and the effect of risk propensity negative. The higher the preference for an analytic-rational approaches to thinking and the lower the risk propensity of a hacker, the more successful this hacker is.

Table 3: OLS Regression Coefficients for Estimated Effects of Rationality and Risk Propensity on Hacking Success

	Model 1		Model 2	
Variable	B	β	B	β
Hypothesized characteristics				
Rationality index	.14 **	.29 (.04)	.14 **	.30 (.04)
Risk propensity index	-.09 **	-.23 (.04)	-.09 *	-.23 (.04)
Sociodemographic controls				
Age			.00	.00 (.04)
Female			.13	.01 (.97)
Non-White			-1.66 *	-.19 (.77)
Education			-.12	-.06 (.22)
Marital status				
Living as married			-.41	-.06 (.64)
Married			.20	.04 (.57)
Unemployed			-1.30	-.15 (.97)
Student			-1.03 *	-.20 (.97)
Constant	4.09 **	(1.27)	5.03 **	(2.00)
R-squared	.11		.21	

**p*<.05. ***p*<.01. ****p*<.001

The inclusion of the socio-demographic control variables in the second, saturated model had only a slight impact on the effect of both personality variables. While the standardized coefficients for both variables remained roughly the same, the inclusion of the control variables reduced the effect of risk propensity to a *p*<.05 significance level. Overall, the inclusion of the additional variables raised the amount of explained variance to 21% in the second model.

Nevertheless, the impact of the individual socio-demographic variables was surprisingly small. Only two of the variables reached a significant level. The variables of age and sex had virtually no impact on the dependent variable. Particularly for the age variable, this finding was surprising because it implies that hackers of all ages report roughly the same success rates. In contrast to the age variable, the complete absence of a gender effect in the data is unfortunately not very meaningful because only seven of the respondents were females. Since seven respondents are not enough cases to allow a confident generalization of the results, future studies with more female hackers are needed to confirm this finding. The only two socio-demographic variables in the second model to reach a significant level were race and student status. Students report significantly lower success rates than persons who are not or no longer studying. Also, when compared to White hackers, hackers belonging to minority groups report a significantly lower success rate (*p*<.05). Again, this finding also has to be interpreted with caution, given the small number of minority hackers in the present sample.

Discussion and Conclusion

Hackers do in fact have a considerably higher need for cognition and higher risk propensity than the general public. They tend to prefer rational thinking styles over intuitive approaches and they demonstrate a particularly high confidence in their ability to reach optimal decisions through a rational deliberation process. They prefer complex problems over simple ones and they enjoy solving problems that require hard thinking more than the average person. Second, they are also more prone to engage in potentially risky behaviors than members of the broader population.

Both personality characteristics exerted significant importance for the prediction of hacking related outcomes. Rationality and risk propensity turned out to be valuable predictors of self-reported hacking success. Hackers with a stronger preference for rational decision-making processes seem to engage in preparation, reconnaissance, and attack routines that yield higher success rates than the methods employed by others with a less pronounced preference for rational deliberations. They also engage in significantly more overall hacking attempts. It appears that they are more confident in ability to successfully attack a target and they also employ more thoughtful attack routines that yield higher success rates. Hackers with a less pronounced preference for rational decision-making processes appear to be less confident in their ability to successfully attack targets, and they engage in fewer attempts to attack them. The importance of rationality as a factor is further underscored by the finding that it was the most important factor in both regression models. The second personality characteristic, the propensity to engage in risky behaviors, also has a significant impact for both hacking success and the overall involvement in hacking. Respondents with a more pronounced risk propensity engaged in more hacking attempts, but reported overall less success. The study established both factors as essential dimensions of cybercrime offender typologies.

A number of criminological theories could be offered as a larger framework for the findings in the present study. In particular, the rational choice perspective emphasizes the importance of the offender's ability to weigh deliberately the outcomes of alternative actions and to take risks willingly (Clarke & Cornish, 1985, 2001; Cornish, 1994; Cornish & Clarke, 1986). The present study, however, does not lend exclusive support to the rational choice perspective. For instance, the general theory of crime classifies both personality traits measured in this study as two of the six components that comprise low self-control (Gottfredson & Hirschi, 1990). Future studies should examine all six dimensions of low self-control and investigate the influence of this personality construct on hacking activities. Furthermore, Jaishankar (2008) proposed the "space transition theory," the first criminological theory that was explicitly designed for the application to crimes committed in cyberspace. Space transition theory provides an explanation for why otherwise law-abiding persons, who do not commit crimes in the terrestrial world, engage in cyber-criminal activities. Jaishankar argues that people behave differently when they move from one space to another. They engage in cybercrime activities because they are aware of the greatly diminished chances of becoming apprehended. Future cyber-criminological studies should devote special attention to this first exclusively cybercrime-related theory and test whether it is indeed better suited for the explanation of cybercrimes than traditional criminological theories.

The conclusions that can be derived from this study are not limited to contributions to the scientific discourse about cybercrime offenders. They also hold some important implications for the efforts to combat cybercrimes. Experts agree that present efforts to combat cybercrimes are facing a multitude of challenges. Aside from the resource shortages and other practical difficulties, law enforcement efforts are also hampered by a shortage of substantive and reliable information for the creation of cybercrime-offender profiles. Detailed profiles of the different types of cyber-criminals, their skill levels, and their motivations are critical because they provide helpful guidance for the investigation of cybercrimes and thereby increase the effectiveness of current prosecution efforts. A more effective response by the criminal justice system is an urgent need—because it would increase the number of convicted cybercriminals and more important, because it would also have a preventive deterrence effect on the illegal parts of the hacking community.

From a broader standpoint, the findings of this study suggest that effective deterrence might be a strategy when dealing with highly rationally acting offenders. Unfortunately, present efforts to curb cybercrimes are hardly suited to exerting a pronounced deterrence effect. Despite the annually increasing number of cybercrimes, only a relatively few high profile cybercrime cases are presently successfully tried, many of them without swift or severe punishments (Brenner, 2006). The ongoing uncertainty of punishments is particularly problematic because it severely undermines any efforts to deter criminal behavior in cyberspace. Indeed, the high risk awareness that appears to be rooted in rational decision-making processes suggests that many hackers are aware of the current improbability of becoming detected and prosecuted.

Unquestionably, the establishment of effective deterrence efforts as an integral part of cybercrime prevention strategies will not be an easy undertaking. The vast range of cybercrime activities and the multitude of different offenders considerably complicate the selections of the most appropriate deterrence policies. The most effective deterrence strategies for leisure-time juvenile hackers will most likely be unfit to deter destructive computer-security experts or other seasoned hackers from attacking computer systems for monetary gains. Nonetheless, deterrence should be pursued as a mitigation strategy, because even limited accomplishments can prevent some crime incidents and provide some protection from an increasingly serious problem.

Limitations and Suggestions for Future Research

Though it produced valuable insights, one set of potential shortcomings to the present study involves the sampling frame and the sample size of the study. The study analyzed only data from one particular convention, a circumstance that constricts the confidence with which the present findings can be generalized to larger populations. Additional datasets from different conventions are needed to enable researchers to draw comparisons between them and to assess the reliability and validity of the present data. Once multiple studies from different conventions exist, meta-studies will eventually be able to compare the results of these studies and extract highly reliable and valid findings.

Although repeated studies from different conventions will eventually generate valid and generalizable results, these results will, to a certain degree, be generalizable only to the subset of hackers who consider attending hacker conventions or, more narrowly, have already attended them. Whether systematic and consistent differences exist between hackers, those who potentially attend conventions and those who do not, remains to be seen

The present study was one of the first attempts to generate quantifiable information about the hacking underground, and it was naturally limited in manifold ways. As does every extension of our knowledge, the present study provides some answers but also raises many more questions. Future studies need to include other measurements of attitudes, social networks, personal background information, and many other aspects to refine and extend our understanding of hackers. Such studies could specify and detail many additional characteristics in a more precise way.

The long list of current unknowns about hackers' calls to mind that cyber criminology is only beginning to develop and that our knowledge about cybercrime offenders remains fragmentary at best. The present study yielded some important insights into the minds of hackers. Nevertheless, it was but one step toward the establishment of cyber criminology as a distinct subfield of criminological research. A long and difficult road is still ahead for this young field of criminological research.

References

Boudreau, M. C., Gefen, D., & Straub, D. W. (2001). Validation in Information Systems Research: A State-of-the-art Assessment. *MIS Quarterly, 11*(1), 1-16.

Brenner, S. (2006). Defining Cybercrime: A Review of State and Federal Law. In R. D. Clifford (Ed.), *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime* (pp. 13-94). Durham, NC: Carolina Academic Press.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offender's decisions: A framework for research and policy. In T. M. & N. Morris (Eds.), *Crime and Justice* (Vol. 6). Chicago: University of Chicago Press.

Clarke, R. V., & Cornish, D. B. (2001). Rational Choice. In R. Paternoster & R. Bachman (Eds.), *Explaining Criminals and Crime: Essays in Contemporary Criminological Theory*. Los Angeles: Roxbury.

Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. In R. V. Clarke (Ed.), *Crime Prevention Studies* (Vol. 3). Monsey, NY: Criminal Justice Press.

Cornish, D. B., & Clarke, R. V. (Eds.). (1986). *The Reasoning Criminal*. New York: Springer Verlag.

Dahlback, O. (1990). Personality and risk-taking. *Personality and Individual Differences, 11*(12), 1235-1242.

Dalal, A. S., & Sharma, R. (2007). Peeping into a Hacker's Mind: Can Criminological Theories Explain Hacking? *ICFAI Journal of Cyber Law, 6*(4), 34-47.

Dulebohn, J. H. (2002). An investigation of the determinants of investment risk behavior in employer-sponsored retirement plans. *Journal of Management 28*(1), 3-26.

Epstein, S. (2003). Cognitive-experiential self-theory of personality. In T. Millon & M. J. Lerner (Eds.), *Comprehensive Handbook of Psychology, Volume 5: Personality and Social Psychology* (pp. 159-184). Hoboken, NJ: Wiley & Sons.

Epstein, S., Pacini, R., Denes-Raj, V., & Heier, H. (1996). Individual differences in intuitive-experiential and analytical-rational thinking styles. *Journal of Personality and Social Psychology, 71*(2), 390-405.

Finch, J. (1987). The Vignette Technique in Survey Research. *Sociology, 21*(1), 105-114.

Fisher, R. J. (1993). Social desirability bias and the validity of indirect questioning. *Journal of Consumer Research, 20*(2), 303-315.

Gomez-Mejia, L. R., & Balkin, D. B. (1989). Effectiveness of individual and aggregate compensation strategies *Industrial Relations, 28*(3), 431-445.

Gottfredson, M., & Hirschi, T. (1990). *A General Theory of Crime*. Palo Alto, CA: Stanford University Press.

Grecs. (2008). ShmooCon 2008 Infosec Conference Event. Retrieved April 25, 2010, from http://www.novainfosecportal.com/2008/02/18/shmoocon-2008-infosec-conference-event-saturday/

Gupta, A. K., & Govindarajan, V. (1984). Business unit strategy, managerial characteristics, and business unit effectiveness at strategy implementation. *Academy of Management Journal, 27*(1), 25-41.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate Data Analysis*. Englewood Cliffs, NJ: Prentice Hall.

Handley, S. J., Newstead, S., E., & Wright, H. (2000). Rational and Experiential Thinking: A Study of the REI. In R. Riding & S. G. Rayner (Eds.), *International Perspectives on Individual Differences: Cognitive Styles* (Vol. 1). Stamford, CT: Ablex Publishing.

Harrington, S. J. (1996). The Effect of Codes of Ethics. and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. *MIS Quarterly, 20*(3), 257-278.

Higgins, K. J. (2006). Hacker Profiling Stirs Controversy. Retrieved February 12, 2010, from http://www.darkreading.com/security/management/showArticle.jhtml?articleID=208804181

Holt, T., & Kilger, M. (2008). *Techcrafters and Makecrafters: A Comparison of Two Populations of Hackers*. Charlotte, NC: 2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing.

Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 281-283). Upper Saddle River, NJ: Pearson.

Kerlinger, F. N. (1986). *Foundations of Behavioral Research* (3 ed.). New York, NY: Rinehart & Winston.

Kim, J.-O., & Mueller, C. W. (1978). *Introduction to Factor Analysis: What It Is and How To Do It (Quantitative Applications in the Social Sciences)*. Newbury Park, CA: Sage.

Krosnick, J., & Fabrigar, L. (1997). Designing Rating Scales for Effective Measurement in Surveys. In L. Lyberg, P. Biemer, M. Collins, E. de Leeuw, C. Dippo, N. Schwarz & D. Trewin (Eds.), *Survey Measurement and Process Quality* (pp. 141-164). New York: Wiley.

Laub, J. H., & Sampson, R. J. (1993). Turning points in the life course: Why change matters to the study of crime. *Criminology, 31*(3), 301-326.

Laub, J. H., & Sampson, R. J. (2003). *Shared Beginnings, Divergent Lives: Delinquent Boys to Age 70*. Cambridge, MA: Harvard University Press.

Levy, S. (1984). *Hackers: Heroes of the Computer Revolution*. New York: Doubleday.

MacCrimmon, K. R., & Wehrung, D. A. (1990). Characteristics of risk taking executives. *Management Science, 36*(4), 422-435.

Nunnally, J. C. (1978). *Psychometric Theory* (2 ed.). New York: McGraw-Hill.

Pacini, R., & Epstein, S. (1999). The relation of rational and experiential processing styles to personality, basic beliefs, and the ratio-bias phenomenon. *Journal of Personality and Social Psychology, 76*(6), 972-987.

Schell, B. H., & Melnychuk, J. (2010). Female and Male Hacker Conference Attendees: Their Autism-Spectrum Quotient (AQ) Scores and Self-Reported Adulthood Experiences. In T. J. Holt & B. H. Schell (Eds.), *Corporate hacking and technology driven crime: Social dynamics and implications* (pp. 144 - 169). Hershey, PA: IGI Global.

Schnell, R., Hill, P. B., & Esser, E. (1999). *Methoden der Empirischen Sozialforschung* (6 ed.). Muenchen: Oldenbourg.

Slovic, P. (1972). Information processing, situation specificity and the generality of risk-taking behavior. *Journal of Personality and Social Psychology, 22*(2), 128-134.

Sommer, R., & Sommer, B. (2002). *A practical guide to behavioral research: Tools and techniques* (5 ed.). New York: Oxford University Press.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 255-276.

Thompson, B. (2004). *Exploratory and Confirmatory Factor Analysis: Understanding Concepts and Applications*. Washington, DC: American Psychological Association.

Trochim, W. M. K. (2002). *The research methods knowledge base* (2 ed.). Cincinnati, OH: Atomic Dog Publishing.

Yar, M. (2005). Computer Hacking: Just Another Case of Juvenile Delinquency? *The Howard Journal, 44*(4), 378-399.