Self-Reported Computer Criminal Behavior: A Psychological Analysis

By

Marcus Rogers, Kathryn Seigfried, Kirti Tidke

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2006 USA

Lafayette, IN (Aug 14th - 16th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment.

As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

available at www.sciencedirect.com

SCIENCE DIRECT®

journal homepage: www.elsevier.com/locate/diin

Digital Investigation

Self-reported computer criminal behavior: A psychological analysis

Marcus K. Rogers[a,*], *Kathryn Seigfried*[b], *Kirti Tidke*[a]

[a]*Department of Computer and Information Technology, Purdue University, 401 N Grant Street, West Lafayette, IN 47907, United States*
[b]*Department of Psychology, John Jay College, 445 West 59th Street, New York, NY 10019, United States*

Keywords:
Computer crime
Psychology
Big-5
Self-reported
Computer deviance
Personality

ABSTRACT

The current research study replicated a study by Rogers et al. (Rogers M, Smoak ND, Liu J. Self-reported criminal computer behavior: a big-5, moral choice and manipulative exploitive behavior analysis. Deviant Behavior 2006;27:1–24) and examined the psychological characteristics, moral choice, and exploitive manipulative behaviors of self-reported computer criminals and non-computer criminals. Seventy-seven students enrolled in an information technology program participated in the web-based study. The results of the study indicated that the only significant variable for predicting criminal/deviant computer behavior was extraversion. Those individuals self-reporting criminal computer behavior were significantly more introverted than those reporting no criminal/deviant computer behavior. This finding is contrary to the findings of the previous study. The current study confirmed that the four psychometric instruments were reliable for conducting research in the field of criminal/deviant computer behavior. The impact of the findings on the field of digital forensic investigations is discussed as well as possible reasons for the apparent contradiction between the two studies.

1. Introduction

Computer crime and those individuals who engage in this deviant behavior have become a part of our digital society (Caloyannides, 2001; Casey, 2002; Furnell, 2002). While the exact damage caused by computer criminals is open for debate, their existence and increase in numbers is unquestioned. The criminal element in our society tends to be the early adopters of technology as it often helps them to become better at their criminal tradecraft (Icove et al., 1995; Marcella and Greenfield, 2002). As more investigations become dependent on digital evidence, the need to assist law enforcement narrows the potential suspects based on digitally derived salient case points becomes increasingly important (Rogers, in press). According to recent surveys on law enforcement needs for computer crime investigations, the ability to obtain reliable and valid offender profiles and better investigative protocols, were rated as pressing issues (Rogers and Zeigfried, 2004; ISTS, 2004).

The field of psychological crime scene analysis has been used with traditional criminal investigations in order to assist investigators in narrowing down the number of potential suspects, conducting proper suspect interviews, and dealing with suspects in a trial/court room setting (Britton, 1997; Douglas et al., 1992; Turvey, 2002). Several researchers have attempted to extend psychological crime scene analysis into the digital/electronic domain with mixed results.

* *Corresponding author*. Tel.: +1 765 496 2021; fax: +1 765 496 3181.
E-mail addresses: rogersmk@purdue.edu (M.K. Rogers), kathryn.seigfried@jjay.cuny.edu (K. Seigfried), kirti810@hotmail.com (K. Tidke).
1742-2876/$ – see front matter © 2006 DFRWS. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2006.06.002

Unfortunately, a lack of empirically derived data on differences between computer criminals, the general public, and traditional criminals has stymied much of the effort to extend psychological crime scene analysis from the physical to the digital domain (Rogers, 2003; Rogers and Ogloff, 2003).

The limited studies on certain subsets of computer criminals such as virus writers, has provided some direction regarding the personality characteristics to include in predictive and risk models (Gattiker and Kelley, 1999; Gordon, 2000, 2003).

Rogers (in press) provides a framework for using salient case points and a rudimentary criminal taxonomy based on the primary components of skill and motivation, in order to assist investigators dealing with digital crime scenes. Again the major weakness of the model is a lack of sufficient data to test the model's assumptions and constructs.

1.1. *Current study*

The purpose of this study was twofold. Firstly it was undertaken to add to the data that are required to test the taxonomy as proffered by Rogers (in press). This was accomplished by following-up and replicating the study conducted by Rogers et al. (2006). The study was exploratory and was one of the first detailed examinations of discriminating characteristics between individuals self-reporting criminal/deviant computer behavior and those individuals self-reporting no such behavior. The respondents in the Rogers et al. (2006) study were Canadian and from a liberal arts department. Rogers et al. (2006) concluded that self-reported computer criminals and non-computer criminals differed significantly on moral choice and exploitive/manipulative behaviors. Self-reported criminals were higher on exploitive/manipulative behaviors, and lower on moral choice internal and moral choice social.

Secondly, the study was used to further validate and test the reliability of several newer or repurposed psychometric tests (computer crime index, big-5 factor questionnaire, exploitive manipulative and dishonesty scale and moral decision making scale), as these have not been extensively tested in relation to computer crime. The lack of validated and reliable psychometric instruments for research in non-traditional criminal behavior is a corollary problem with there being a lack of empirical research by the behavioral sciences in the area of criminal/deviant computer behavior.

2. Method

2.1. *Participants*

The participants for the study were 77 students from a mid-western university enrolled in the college of technology. Eighty-seven percent of the respondents were male and 13% were female (see Table 1). The mean age was 21. Forty-one percent of the respondents were sophomores, and 92% were enrolled in the computer technology program. Students were used in order to be consistent with the previous study by Rogers et al. (2006) and allow a valid comparison. Furthermore, students are representative of the larger population of interest (i.e., individuals 17–30 years of age who anecdotally make up the majority of those individuals engaged in deviant/criminal behavior).

Table 1 – Respondent demographics

Participants	Percentage (frequency)	
	Computer criminals	Non-computer criminals
Gender		
Male	86.8 (59)	88.9 (8)
Female	13.2 (9)	11.1 (1)
Total	100 (68)	100 (9)
Age		
18–20	51.4 (35)	33.3 (3)
21–23	39.7 (27)	44.4 (4)
24–27	7.4 (5)	22.2 (2)
28 or older	1.5 (1)	0
Total	100 (68)	100 (9)
Year in college		
Freshman	7.4 (5)	0
Sophomore	45.6 (31)	33.3 (3)
Junior	10.3 (7)	11.1 (1)
Senior	36.8 (25)	55.6 (5)
Total	100 (68)	100 (9)
Ethnicity		
White	85.3 (58)	77.8 (7)
Asian American	8.8 (6)	11.1 (1)
African American	1.5 (1)	0
Indian	1.5 (1)	0
Asian	1.5 (1)	11.1 (1)
Asian (India)	1.5 (1)	0
Total	100 (68)	100 (9)
Major		
Comp. tech	91.2 (62)	100 (9)
Comp. graphics	1.5 (1)	0
Comp. science	1.5 (1)	0
Other	5.9 (4)	0
Total	100 (68)	100 (9)

The participants were categorized as being computer criminal or non-computer criminal based on their self-reported online behaviors as measured by the computer crime index (see Section 2.2). Participants reporting that they had engaged in:

- guessing passwords;
- using another person's password without authorization;
- looking at others' files without authorization;
- changing others' files without authorization;
- using or writing a virus;
- obtaining someone else's credit information without authorization; and
- using a device to obtain free phone calls

were classified as computer criminals. Those individuals reporting no such activity were classified as non-computer criminals. Illegal software use was not considered in this study, as this has become such a marginalized activity that it would effectively negate there being any non-computer criminals. It is also speculated that the dynamics of software piracy are different than for those behaviors included in the study (Rogers and Ogloff, 2003).

Table 2 – Zero ordered correlation

	Class	Open	Agree	Consc	Neur	IV	SV	HED	Emad	Ext
Class	1	0.151	−0.105	−0.133	−0.037	−0.036	−0.161	0.181	0.146	−0.291**
Open		1	0.503	0.476	0.518	0.272	0.057	−0.065	−0.211	0.234
Agree			1	0.332	0.313	0.190	0.146	−0.104	−0.149	0.590
Consc				1	0.464	0.038	−0.056	−0.314	−0.172	0.219
Neur					1	0.212	−0.026	−0.237	−0.204	0.143
IV						1	0.554	0.113	−0.609	0.112
SV							1	0.303	−0.394	0.228
HED								1	0.214	−0.056
Emad									1	−0.193
Ext										1

Class, criminal classification; open, openness; ogree, agreeableness; consc, conscientious; neur, neurotic; IV, internal moral choice; SV, social moral choice; HED, hedonistic moral choice; Emad, EMAD total; ext, extraversion total.
**$p < 0.01$.

2.2. *Instruments*

The participants answered four computer based Likert-scale questionnaires related to their computer criminal activities, personality characteristics, and behavior in general:

1. Computer crime index (CCI): the CCI measures the frequency and prevalence of self-reported criminal computer activity (e.g., virus writing, obtaining passwords, unauthorized use of a computer or account, etc.). The reported Cronbach's alpha was 0.71.[1]
2. Big-5 factor questionnaire: this measure is a self-report questionnaire assessing personality traits based on five factors: extraversion, agreeableness, conscientiousness, neuroticism, and openness to experience. The reported Cronbach's alphas for each subscale were as follows: extraversion = 0.88, agreeableness = 0.87, conscientiousness = 0.70, neuroticism = 0.80, and openness to experience = 0.85.
3. Exploitive manipulative amoral dishonesty scale (EMAD): the EMAD is a self-report scale that measures the degree of exploitive and manipulative behavior. The reported Cronbach's alpha for the EMAD total was 0.90.
4. Moral decision making scale (MDKS): the MDKS is a self-report questionnaire that measures participants' moral decision making across three subscales: internal, social, and hedonistic.
5. The reported Cronbach's alphas for the subscales were as follows: internal = 0.63, social = 0.63, and hedonistic = 0.72.

2.3. *Hypotheses*

The hypotheses were that individual's self-reporting deviant computer activities (classified as computer criminals for this study) would be:

1. More introverted;
2. More open to experience;
3. More neurotic;
4. More exploitive and manipulative; and
5. Of lowest scoring on social moral choice

than those individuals self-reporting no deviant/computer criminal behavior.

3. Results

3.1. *Descriptive statistics*

Eighty-eight percent of respondents were classified as computer criminals (see Table 1). Other demographic information is presented in Table 1.

3.2. *Correlations*

A zero ordered correlation analysis indicated that computer criminal classification was negatively correlated with extraversion total ($r = -0.29$, $p < 0.01$; see Table 2).

3.3. *Analysis of variance*

Additionally, the data were analyzed using a one-way ANOVA, which revealed that the computer criminal group scored significantly lower on extraversion total than the non-computer criminal group ($M = 40.81$ and $M = 50.22$, $F\ (1,\ 75) = 6.96$, $p < 0.01$; see Table 3).

3.4. *Predictive model*

Finally, a logistic regression analysis was conducted in order to determine a predictive model. The analysis included a single dependent variable, computer criminal behavior, and nine manipulated variables (extraversion, openness to experience, agreeableness, conscientiousness, neuroticism, moral choice

[1] Cronbach's alpha is a measure of reliability of a scale. By convention 0.60 is considered the lowest acceptable level. Obviously, the higher the level the better.

Table 3 – Analysis of variance – extraversion total

Source	df	SS	MS	F
Extraversion total				
Between groups	1	704.29	704.29	6.96**
Within groups	75	7586.36	101.15	
Total	76	8290.36		

**$p < 0.01$.

hedonistic, moral choice internal, and moral choice social). Due to the explorative nature of the study, a forward stepwise Wald procedure was used. The results indicated that only one variable, extraversion total, was significant in predicating computer criminal behavior ($W = 5.70$, $p < 0.05$) (see Table 4). In addition, extraversion total reduced the classification error by 43% (Tau-P = 0.43).

4. Discussion

The reliability analysis for the instruments indicated that the subscales were within acceptable parameters. The moral choice questionnaire subscales were somewhat low for internal and social choice (Chronbach's alpha = 0.63), which may indicate that these subscales suffer from multidimensionality. This could be responsible for a failure to find any significant effect for moral choice internal and moral choice social, during the hypotheses testing and needs to be explored further.

The results indicated that only extraversion total was significant in relation to deviant/criminal computer behavior, none of the other hypotheses were supported. The finding that low extraversion (introversion) was a significant predictive variable is contrary to previous research (c.f., Rogers et al., 2006). The logistic regression analysis also confirmed that extraversion total was a significant risk factor in determining deviant/criminal computer behavior. According to the results, a one standard deviation increase in extraversion total scores would decrease the risk of the individual engaging in the deviant/criminal behaviors (Exp(B) = 0.87).[2]

It would be imprudent to draw sweeping conclusions about the role of extraversion/introversion based on the results of a single study. While the media has portrayed those individuals who are involved in criminal computer behavior (hackers) as being socially underdeveloped and introverted, this study does not provide an endorsement for such a sweeping generalization.

The finding that moral reasoning was not a significant variable is also contrary to the findings of Rogers et al. (2006) and somewhat at odds with Rogers and Ogloff (2003) who concluded that a lack of internalization of societal norms was a significant factor in unethical and aberrant computer behavior. This may be more of factor with the construction of the instrument used than a real difference between the studies.

[2] With logistic regression analysis, if the risk score is less than 1.00 it indicates a decrease in the risk for every increase (one standard deviation) in the variable.

Table 4 – Logistic regression – forward stepwise Wald

	B	S.E.	Wald	df	Exp (B)	95% C.I. for Exp (B)	
						Lower	Upper
Step 1							
Extraversion total	−0.14	0.06	5.70*	1	0.87	0.78	0.98
Constant	8.31	2.84	8.60	1	4079.06		

*$p < 0.05$.

In the current study, there was no significant difference between self-reported computer criminals and non-computer criminals in relation to exploitive/manipulative behaviors. Again this is contrary to Rogers et al. (2006) where exploitive/manipulative behavior was found to be a significant factor, respondents' self-reporting computer criminal behavior scored higher on exploitive/manipulative than non-computer criminals. The exact reason for this contradiction is not speculated at this time, but warrants further consideration and examination.

A possible reason for the different findings between the two studies may lie in the fact that in the Rogers et al. (2006) study the respondents were Canadian and from a liberal arts department, where as in the current study, the respondents were primarily American and from an information technology department. However, while the predominant nationalities of the respondents differed, both studies had representation from non-Caucasian/non-white groups and were relatively balanced in this demographic, which somewhat negates the different nationalities argument. Furthermore, Canadian and US culture and society are very similar and share popular media (e.g., TV, movies, music). The factor of having respondents from different departments with supposedly different focuses on information technology, may be a plausible explanation for the different findings; however, an analysis of the amount of use of technology, time spent online, etc. between the two groups was remarkably similar.[3]

5. Conclusion

It may appear odd to include psychological traits, characteristics, and morality, in a discussion about digital forensics, but if we consider that like any other crime, people are involved, the inclusion of these behavioral science topics becomes self-evident. Computer crime and digital forensics is as much about the individuals involved in this deviant behavior as it is about the technology (Furnell, 2002; Rogers and Ogloff, 2003). Therefore research focusing on people is vital if we have any real hope of coming to grips with the phenomena of computer crime.

The current study adds to the growing body of knowledge in the area of identifying discriminant characteristics that can be used to help construct taxonomies and profiles for computer criminals. In order to have any investigative utility,

[3] The details of this comparison are available upon request from the contact author.

current models need to be matured and validated. This can only be accomplished with the aid of large data sets, and frameworks that have been empirically tested; the findings from this and other studies will be used for this purpose.

Computer crime is not expected to decrease in the foreseeable future. The number of investigations will continue to increase at a staggering rate. As such, investigators require assistance with digitally derived evidence, digital crime scenes, and logically, assistance in dealing with those criminals engaged in computer crimes.

REFERENCES

Britton P. The jigsaw man. London, England: Transworld Publishers; 1997.

Caloyannides M. Computer forensics and privacy, Artech house computer security series. Boston, MA: Artech House; 2001. xvii, 392 p.

Casey E. Handbook of computer crime investigation: forensic tools and technology. San Diego, CA: Academic Press; 2002. xiv, 448 p.

Douglas J, Burgess W, Burgess A, Ressler R. Crime classification manual. San Francisco: Jossey-Bass; 1992.

Furnell S. Cybercrime: vandalizing the information society. Boston: Addison-Wesley; 2002. xi, 316 p.

Gattiker UE, Kelley H. Morality and computers: attitudes and differences in moral judgments. Information Systems Research 1999;10(3):233–54.

Gordon S. Virus writers: the end of the innocence? [cited 9.08.2003]. Available from: http://www.research.ibm.com/antivirus/SciPapers/VB2000SG.htm; 2000.

Gordon S. Convergence of virus writers and hackers: fact or fantasy? 2003.

Icove DJ, Seger KA, VonStorch W. Computer crime: a crimefighter's handbook, Nutshell handbook. 1st ed. Sebastopol, CA: O'Reilly & Associates; 1995. xxi, 437 p.

ISTS. Law enforcement tools and technologies for investigating cyber attacks: a national research and development agenda [cited 9.09.2004]. Available from: http://www.ists.dartmouth.edu; 2004.

Marcella AJ, Greenfield R. Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes. Boca Raton, FL: Auerbach Publications; 2002. xx, 443 p.

Rogers MK, Ogloff JRP. A comparative analysis of Canadian computer and general criminals. Canadian Journal of Police & Security Services 2003;1(4):366–76.

Rogers M, Zeigfried K. The future of computer forensics: a needs analysis survey. Computers and Security 2004;(3):12–6.

Rogers MK, Smoak N, Liu J. Self-reported criminal computer behavior: a big-5, moral choice and manipulative exploitive behavior analysis. Deviant Behavior 2006;27:1–24.

Rogers M. The role of criminal profiling in computer forensic investigations. Computers and Security 2003;22(4):293–8.

Rogers, M. The development of a meaningful hacker taxonomy: a two dimensional approach. Digital Investigations, in press.

Turvey BE. Criminal profiling: an introduction to behavioral evidence analysis. 2nd ed. Amsterdam, Boston: Academic Press; 2002. xxviii, 717 p.

Marcus K Rogers, PhD, CISSP, CCCI is the Chair of the Cyber Forensics Program in the Department of Computer and Information Technology at Purdue University. He is an Associate Professor and also a research faculty member at the Center for Education and Research in Information Assurance and Security (CERIAS).

Kathryn Seigfried (BA), is a graduate student at John Jay College where she is pursuing her Masters degree in forensic psychology, with a focus on cyber criminals.

Kirti Tidke (MSc), is a recent graduate from the Masters of Science Program from the Dept. of Computer and Information Technology at Purdue University.