



University of
New Haven

University of New Haven
Digital Commons @ New Haven

Electrical & Computer Engineering and Computer
Science Faculty Publications

Electrical & Computer Engineering and Computer
Science

2009

Self-Reported Cyber Crime: An Analysis on the Effects of Anonymity and Pre-Employment Integrity


Ibrahim Baggili

University of New Haven, ibaggili@newhaven.edu

Marcus Rogers

Purdue University

Follow this and additional works at: <http://digitalcommons.newhaven.edu/electricalcomputerengineering-facpubs>

 Part of the [Computer Engineering Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Publisher Citation

Baggili, I., & Rogers, M. (2009). Self-Reported Cyber Crime: An Analysis on the Effects of Anonymity and Pre-Employment Integrity. *International Journal of Cyber Criminology*, 3(2):550-565.

Comments

Dr. Baggili was appointed to the University of New Haven's Elder Family Endowed Chair in 2015.

© 2009 International Journal of Cyber Criminology. All rights reserved. Under a creative commons Attribution-Noncommercial-Share Alike 2.5 India License 550 Copyright © 2009 International Journal of Cyber Criminology (IJCC) ISSN:0974 – 2891 July - December 2009, Vol 3 (2): 550–565



Self-Reported Cyber Crime: An Analysis on the Effects of Anonymity and Pre-Employment Integrity

Ibrahim Baggili¹

Zayed University, United Arab Emirates (UAE)

Marcus Rogers²

Purdue University, West Lafayette, USA

Abstract

A key issue facing today's society is the increase in cyber crimes. Cyber crimes pose threats to nations, organizations and individuals across the globe. Much of the research in cyber crime has risen from computer science-centric programs, and little experimental research has been performed on the psychology of cyber crime. This has caused a knowledge gap in the study of cyber crime. To this end, this research focuses on understanding psychological concepts related to cyber crime. Through an experimental design, participants were randomly assigned to three groups with varying degrees of anonymity. After each treatment, participants were asked to self-report their cyber crime engagement, and pre-employment integrity. Results indicated that the anonymity manipulation had a main effect on self-reported cyber crime engagement. The results also showed that there is a statistically significant negative relationship between self-reported cyber crime engagement and pre-employment integrity. Suggestions for future research are also discussed.

Keywords: Self reported Cybercrime, Anonymity, Pre-employment Integrity, Cyber Crime engagement.

Introduction

Cyber crime is an unlawful act in which a computer/s is/are used as means of committing a crime against a person, property or the government (Babu & Parishat, 2004). Sukhai (2004) explained that an FBI and Computer Security Institute annual survey of 520 companies and institutions reported more than 60% unauthorized use of digital computer systems during a period of 12 months and 57% of all break-ins involved the Internet. Even though these numbers seem large, Sukhai (2004) describes that about 60% of cyber attacks are not even detected. Research indicates that only about 15% of exposed attacks are reported to law enforcement agencies (Sukhai, 2004). In the newer 2006 FBI and Computer Security Institute annual survey of 313 companies and institutions, it was

¹ Assistant Professor and Director of the Advanced Cyber Forensics Research Laboratory, Zayed University, United Arab Emirates. Email: Ibrahim.Baggili@zu.ac.ae

² Professor, Department of Computer and Information Technology, Purdue University, West Lafayette, IN, USA. E-mail: rogersmk@purdue.edu

found that the total losses attributed to security breaches amounted to \$52,494,290 dollars (Gordon et al., 2006). Finally, in the 2008 CSI Computer Crime and Security Survey, it was noted that there is an average loss of \$500,000 with corporations experiencing financial fraud (related to computing) and an extra average of \$350,000 loss at companies that experienced “bot” attacks. The abovementioned figures illustrate that the capital losses attributed to unauthorized use of computers have a substantial damaging bearing on today’s economy. This is also reinforced in the significant average capital loss in the 2008 survey. Due to the negative impact of cyber crime on society, it becomes imperative to understand the social and psychological implications of the cyber crime phenomenon.

Many researchers have focused their efforts on technical aspects related to decreasing cyber crime through computer technology/science prevention and incident response techniques. Rogers (2003) explained that little psychological research is conducted on cyber crime focusing on factors such as personality traits/individual differences, motivation and situational factors associated with the cyber criminals. It is now 2009 and this statement remains true. Two major questions whose answers will remain of important value in social scientific research on cyber crime still need to be examined: What attracts people to cyber criminal activities? And what personality traits/individual differences are associated with cyber criminals?

Literature suggests that one of the major reasons people are attracted to cyber crime is the anonymity they encounter in computer mediated environments (Lipson, 2002; Williams, 2002). The literature further uncovered that experimental research on anonymity derived from Computer Mediated Communication (CMC) is used to explain computer communication and not computer crime. It is necessary to recognize that just because one communicates via computers using technologies like e-mail and chat clients, doesn’t inevitably denote that the act of communication is unlawful and criminal. Therefore, anonymity needs to be extended from CMC research to cyber criminal research. A limited number of empirical studies have examined anonymity theories within the context of cyber crimes, and one specifically is by Hinduja (2008), where the study illuminated the light on deindividuation playing a role in internet software piracy.

Lastly, the seminal psychological studies on cyber crime do not explore anonymity as a situational factor in their experimental procedures (Rogers 1999; Rogers, 2001; Rogers, 2003, Shaw et. al, 1998). Manipulating anonymity in the experimental procedures may shed some light on situational factors that affect the relationship between personality traits/individual differences and cyber crime engagement.

As for the personality traits of cyber criminals, there still remains a plethora of personality constructs that need to be examined. For instance, the influential literature on IT insider threat by Shaw et al. (1998) concluded that pre-employment integrity screening should be performed to decrease cyber crimes arising from within an organization. Due to the Shaw et al. (1998) concluding remarks, this research builds on their work and examines the relationship between cyber criminal activities and an individual’s operationalized pre-employment integrity.

Purpose of the study and research questions

The purpose of the study is to investigate how cyber crime engagement is related to anonymity and self-reported pre-employment integrity. This research also aims to answer the following questions:

Q1: Does manipulating someone's anonymity affect their self-reported cyber crime engagement?

Q2: Is there a significant relationship between self-reported pre-employment integrity and self-reported cyber crime engagement?

Q3: Does anonymity significantly affect the relationship between self-reported pre-employment integrity and self-reported cyber criminal engagement?

Q4: Can self-reported pre-employment integrity significantly predict cyber criminal engagement?

Significance of the study

This research builds on the research conducted in other psychological studies by Rogers et al. (2006) and Shaw et al. (1998). Primarily, this research makes a contribution to the experimental literature on the psychology of cyber criminals by extending previous work on integrity. Another notable contribution of this research is the insight it offers into accounting for anonymity when performing psychological research related to cyber crime. It may also have dramatic implications on helping researchers understand if the traditional operationalization of pre-employment integrity can be associated with cyber criminals. The study will also help in testing if traditional pre-employment integrity screening tests may potentially be used to predict computer criminals. Lastly, the results obtained from this research may inspire future research in this area for novel ways of measuring and manipulating anonymity.

Methodology

This study used inferential statistics in order to interpret the data accumulated by assigning participants randomly to one of three groups. The results obtained from the statistical analysis were used to test the following hypotheses:

H1: Decreasing anonymity decreases the amount of self-reported cyber crime.

H2: There is a negative relationship between self-reported cyber crime (CCI) and self-reported pre-employment integrity (PPI).

H3: Anonymity and self-reported pre-employment integrity (PPI) can predict self-reported cyber crime (CCI).

H4: There is an interaction between self-reported pre-employment integrity (PPI) and anonymity when predicting self-reported cyber crime (CCI).

Constructs

The theoretical constructs are presented in Figure 1. In this study, there were two predictors which comprised of one independent variable (anonymity), and one variable of interest (self-reported pre-employment integrity). The dependent variable was self-reported cyber crime.

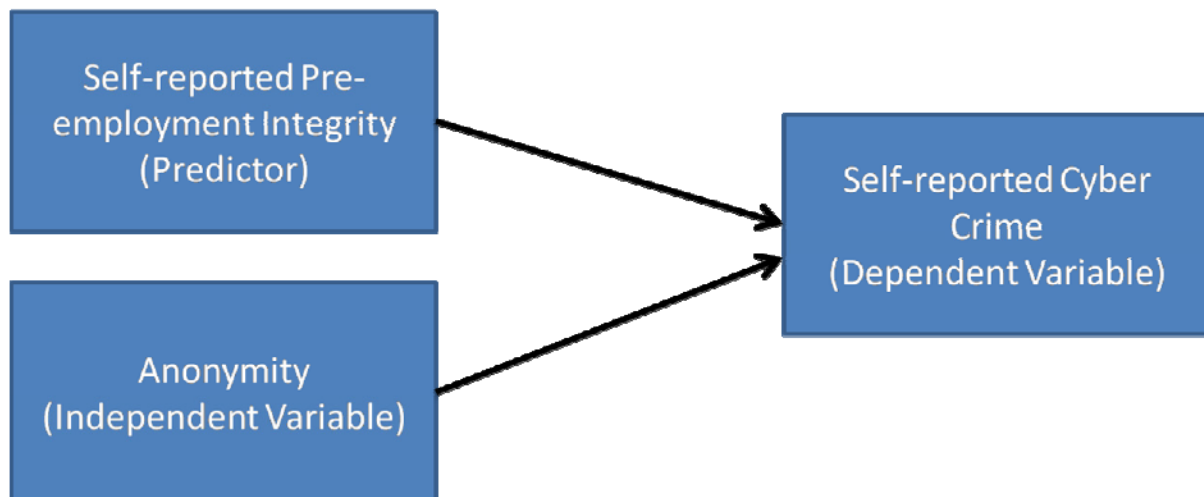


Figure 1. Theoretical Model

Self-reported pre-employment integrity

The self-reported measure for pre-employment integrity was acquired for research purposes from Pearson Consulting Inc. The scale called the Personnel Selection Inventory (PSI-7ST), contains twenty seven Likert items and produced a reliable Chronbach's alpha of .78. This scale was chosen for its extensive use in industry and research.

Anonymity

The IV anonymity was manipulated by randomly assigning participants to one of three groups. The groups were termed 1, 2 and 3. Group 1 (Control Group) was the control group in which participants simply completed an online survey. In group 2 (Computer Group), participants were asked to enter their first name, last name, e-mail address and address on a web form. This was used to manipulate their anonymity and their personal information was not saved anywhere. In the third group (ID Group), participants were asked to raise their hand, and then they were asked to present their Student ID. This was done to manipulate their anonymity at a higher level when compared to Group 2. When participants raised their hand, the researcher attempted to deceive them into thinking that their personal data was being copied from their ID to a paper. These participants were then asked to complete the survey. A manipulation check was also included in the survey to measure the participants' anonymity.

Self reported cyber crime

Little research has been conducted in the area of cyber crime engagement due to the novelty of the cyber crime phenomenon. Rogers (2001) formulated a computer crime index survey to help in determining the level of engagement of people in cyber crime. This self-reported survey is termed Computer Crime Index (CCI). This survey measures the frequency and prevalence of self-reported computer criminal activity and has been effectively used on college students before. Cyber crime has many facets to it. The eight that are measured by the survey are: Software piracy, password cracking, unauthorized access to a system or account, unauthorized alteration or disclosure of data, virus or malicious computer code creation, unauthorized possession or trafficking of passwords, unauthorized possession or trafficking of credit card numbers, possession or use of a device to obtain unauthorized telecommunications service. Using this scale, the higher the CCI

of a person, the higher their level of cyber criminal engagement. The scale produced a reliable Chronbach's alpha of .78.

Research protocol

Participants

Participants in this study included students taking introductory programming and computer graphics classes. They included freshmen, sophomores, juniors and seniors. The total number of participants is (N=163). The gender frequency distribution of the participant pool was as follows:

- 145 males (89%)
- 18 females (11%)

The age and major frequency distribution of the participant pool are illustrated in Figures 2 and 3 respectively.

Figure 2. Participants by Age

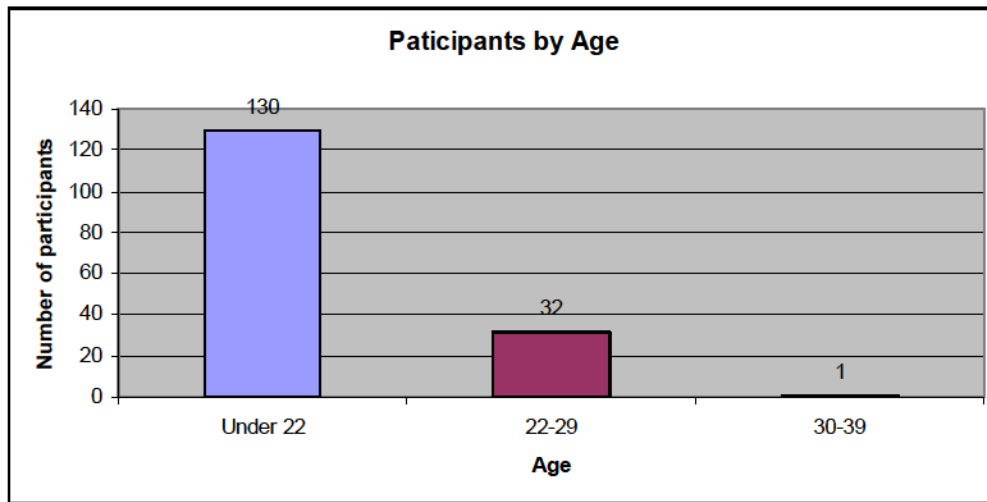
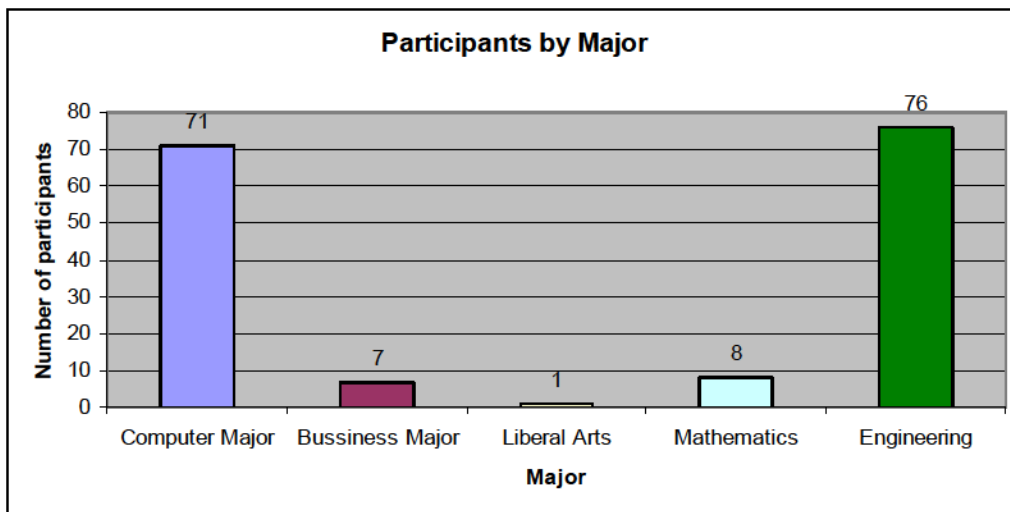


Figure 3. Participants by Major



The participants were (programmatically) randomly assigned to different groups when they accessed the survey (1=Control group, 2=Computer Group and Group 3 = ID group). Cohen (1992) posited that the number of subjects required for a medium effect size at a $p=0.05$ level using General Linear Modeling analysis with three Independent variables is $n=76$, and to illustrate an effect at the $p=.01$ level that there needs to be $n=108$. A-priori power calculations were generated using the program GPower in order to gain better insight for the number of participants needed to get a large effect size. Additionally, the observed power for the General Linear modeling is also reported in results. The calculations for the A-priori power yielded the following:

- For a one-tailed test, with medium effect size (0.5), an alpha of (0.05) and a power (0.8) the recommended sample size is 102.
- For a two-tailed test, with medium effect size (0.5), an alpha of 90.05) and a power of (0.8) the recommended sample size is 128.

In this study, the researchers were able to acquire 163 completed cases ($N=163$). The number of participants $N=163$ is greater than the rule of thumbs indicated by the literature and is also greater than the suggested sample size generated by GPower for both one-tailed and two-tailed tests. This suggested that this study should have reasonable effect size and power.

Study protocol

This study's research protocol included the following steps in order:

1. After reaching the computer laboratory, the participants were asked if they would like to participate in the study.
2. The IRB pre-consent forms were handed out to all the participants that agreed to contribute to the study. The participants were instructed to carefully read and sign the pre-consent forms. The researcher also handed out the post-consent forms and asked the participants to complete and sign those forms when they completed the survey.
3. Participants were then instructed to go to psychdata.com in their web browser and enter the designated survey number and complete the survey.
4. If a participant raised their hand, the researcher approached the participant and performed the ID manipulation by asking the participant to show their student ID (discussed in the abovementioned section). The researcher then faked the writing of the ID information on a paper and the participant was instructed to complete the survey.
5. Once a participant completed the survey, the pre-consent and post-consent forms were signed by the researcher and a copy was given to each of the participants.
6. After all the participants completed the survey, the researcher debriefed the participants about the nature of the research project.

Anonymity manipulation

The participants were asked to complete a secure online survey at psychdata.com. As soon as they reached the first page of the survey shown in Figure 4 and clicked the "Continue to the Next Page" button, the participants were randomly directed to one of three surveys that contained the different anonymity manipulations. After completing the demographics page, if the participants were assigned to the control group, they would

simply complete the survey without an anonymity manipulation. If a participant was randomly directed to the computer group, they would reach the page shown in Figure 5. The instructions on this page explained to the participant to open and fill out the form displayed in Figure 6. The form in Figure 6 asked the participants to submit their name, e-mail address and address. This served as the computer group's anonymity manipulation.

Figure 4. First page of survey

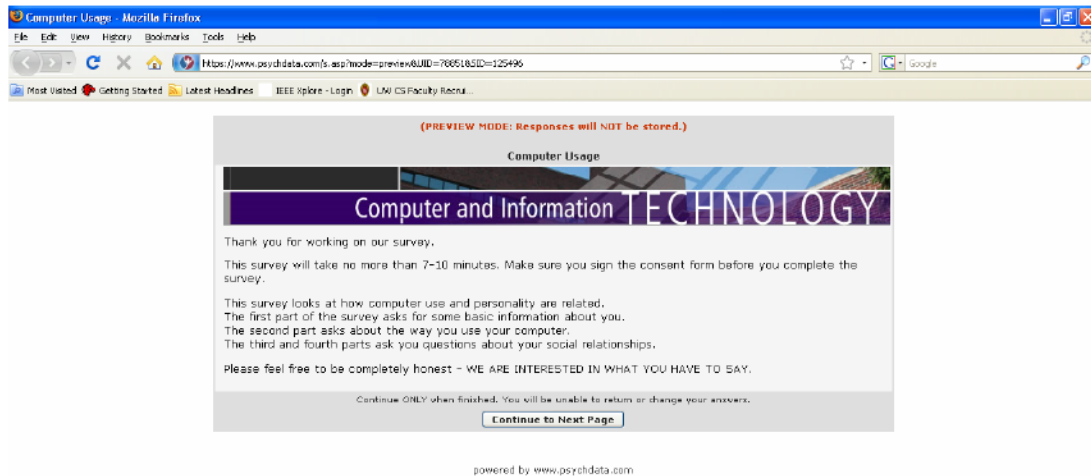


Figure 5. Computer Group

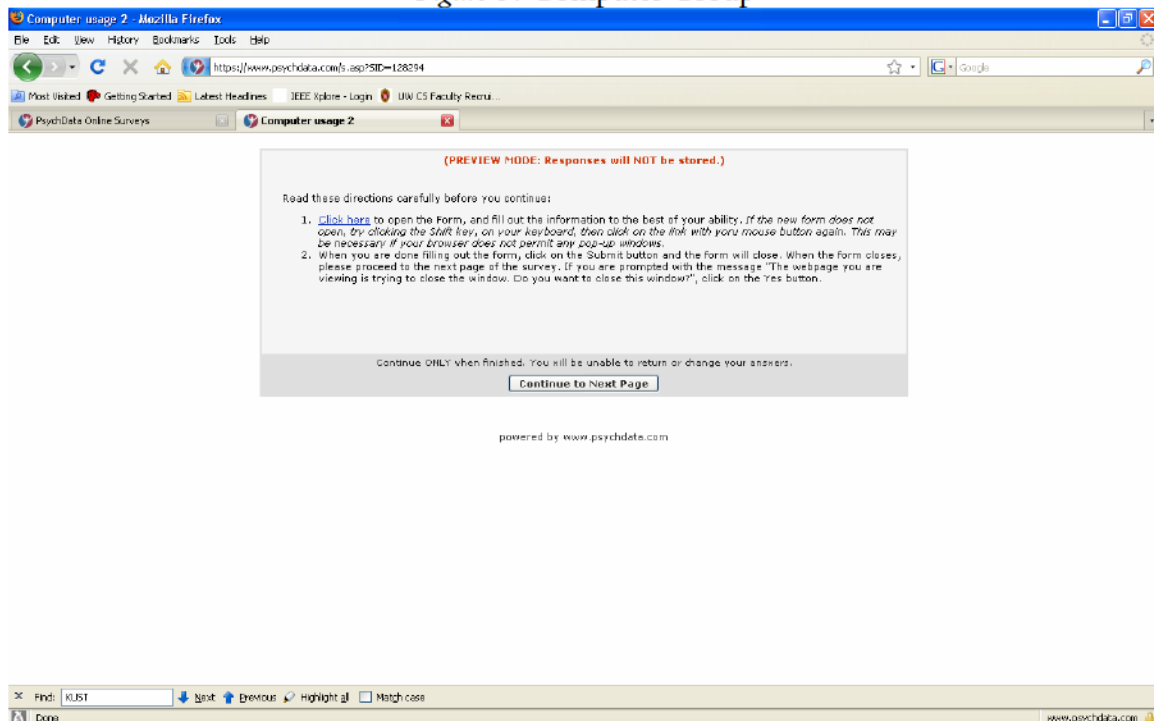


Figure 6. Anonymity Manipulation Form

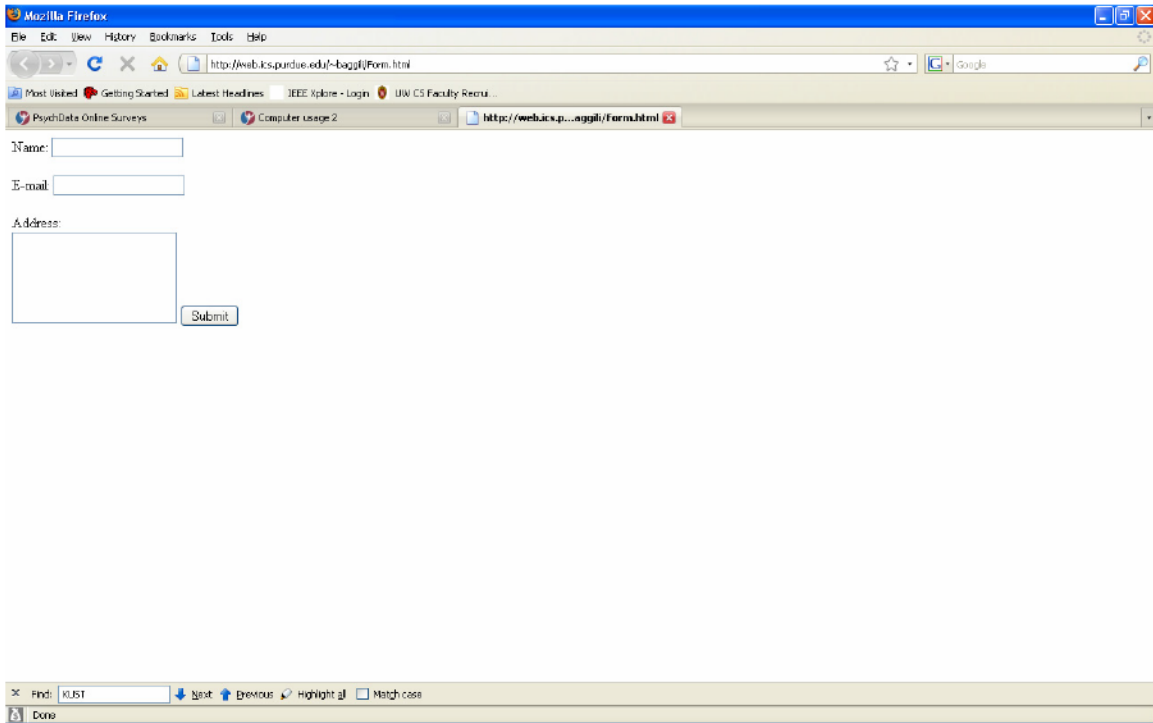
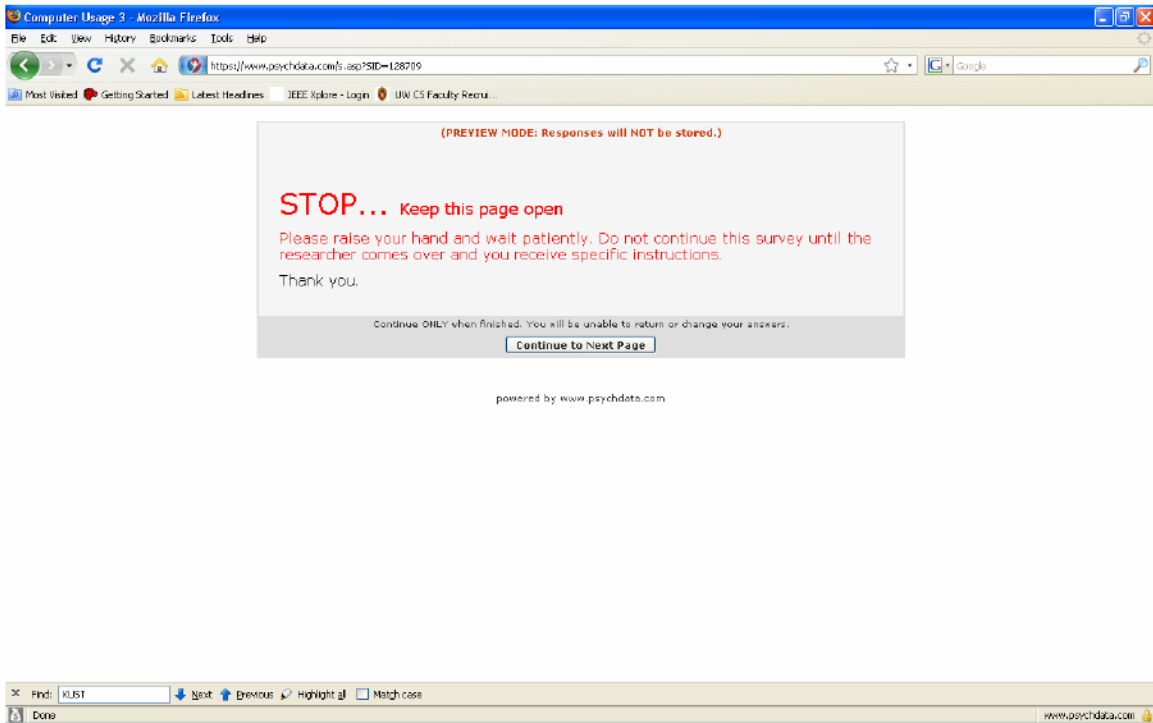


Figure 7. ID Manipulation



After completing the demographics section of the survey, if the participants were randomly directed to the ID group’s survey, they were shown the form in Figure 7 at which they were asked to raise their hand and wait. The researcher then approached the participant and politely asked “May I see your student ID please”. The participant then showed the researcher his/her student ID card at which the researcher faked the participant into thinking that their personal information was being copied from their student ID onto a piece of paper. The researcher then returned the student ID and asked the student to continue the survey by saying “You can now continue the survey, thank you.”

Data analysis

The data was first explored. Thirty eight incomplete participant responses were deleted from the data set. The data was then analyzed using exploratory and descriptive statistics. These statistics were used to test for normality and homogeneity of variance to see if parametric tests can be used to analyze the data. The results indicated that the data was roughly normal, and that paramedic tests could be applied. To test H1, Analysis of Variance (ANOVA) was used to examine the effect of the anonymity manipulation on the self-reported CCI score. To test the strength of relationships in H1 and H2, Pearson’s correlation was used. To test predictions and interactions in H3 and H4, General Linear Modeling (GLM) was used.

Hypotheses analyses

The purpose of the study was to investigate how self-reported cyber crime engagement is related to self-reported integrity, anonymity and self-reported antisocial behaviors. In this section all the hypotheses will be tested. All the tests were 2-tailed tests. Additionally, the alpha for all ANOVA and GLM analysis was set at the 0.05 level, whereas for the correlation analysis, the alpha was set at the 0.01 level.

Hypothesis 1

H1: Decreasing anonymity decreases the amount of self-reported cyber crime.

To test this hypothesis a one way ANOVA was used with anonymity being a factor and CCI and PPI being dependents. The results of the ANOVA are displayed in Tables 1 and 2.

Table 1. Descriptive Statistics

Dependent Variable: CCI			
Group	Mean	Std. Deviation	N
1.00 (Control)	37.3770	8.33499	61
2.00 (Computer)	33.5088	7.92402	57
3.00 (ID)	37.0000	8.52270	45
Total	35.9202	8.38648	163

Table 2. ANOVA Results

Tests of Between-Subjects Effects						
Dependent Variable: CCI						
Source	Type III Sum of Squares	Degrees of Freedom	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	513.390 ^a	2	256.695	3.775	.025	.045
Intercept	207255.145	1	207255.145	3047.709	.000	.950
Group	513.390	2	256.695	3.775	.025	.045
Error	10880.573	160	68.004			
Total	221707.000	163				
Corrected Total	11393.963	162				

a. R Squared = .045 (Adjusted R Squared = .033)

The descriptive statistics in Table 1 illustrates that the mean decreases from the Control Group to the Computer Group and from the Control group to the ID Group. The ANOVA results indicated that there is a statistically significant effect for the anonymity manipulation ($F(2,160) = 3.78, p = .025, \text{partial } \eta^2 = .045$). In order to know if there was a significant effect in the decrease of anonymity between the Computer Group and the ID Group, a post-hoc Tukey's test was used. The results from Tukey's test are shown in Table 3.

Table 3. Tukey's Test

Multiple Comparisons							
Dependent Variable: CCI							
	(I) Group	(J) Group	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
	p	p				Lower Bound	Upper Bound
Tukey HSD	1.00	2.00	3.8683 [*]	1.51916	.032	.2743	7.4622
		3.00	.3770	1.62049	.971	-3.4566	4.2107
	2.00	1.00	-3.8683 [*]	1.51916	.032	-7.4622	-.2743
		3.00	-3.4912	1.64446	.088	-7.3816	.3991
	3.00	1.00	-.3770	1.62049	.971	-4.2107	3.4566
		2.00	3.4912	1.64446	.088	-.3991	7.3816

Based on observed means.
 The error term is Mean Square(Error) = 68.004.
 *. The mean difference is significant at the .05 level.

Tukey's post-hoc test suggested that there is statistically significant difference between Groups 1 and 2 (Control and Computer) ($p = .032$). It also showed a marginal difference between groups 2 and 3 (Computer and ID) ($p = .088$). Therefore, based on the ANOVA and the post-hoc test, H1 is accepted.

Hypothesis 2

H2: There is a negative relationship between self-reported cyber crime (CCI) and self-reported pre-employment integrity (PPI).

To test this hypothesis, a Pearson’s correlation was used. The results are shown in Table 4.

Table 4. CCI and PPI Correlation

Correlations			
		CCI	PPI
CCI	Pearson Correlation	1	-.339**
PPI	Pearson Correlation		1
** . Correlation is significant at the 0.01 level (2-tailed).			

Key: CCI = Computer crime engagement, PPI = Pre-employment integrity

The results in Table 4 show a statistically significant negative correlation between CCI and PPI $r(161) = -.339, p < .01$. Since the relationship is significant H2 is accepted.

Hypotheses 3 and 4

H3: Anonymity and self-reported pre-employment integrity (PPI) can predict self-reported cyber crime (CCI).

H4: There is an interaction between self-reported pre-employment integrity (PPI) and anonymity when predicting self-reported cyber crime (CCI).

To test H3 and H4, a univariate GLM was executed using CCI as the dependent variable. Anonymity was a categorical variable between participants factor and PPI was a continuous between participants predictor (Analogous to covariate). The results from this analysis are shown in Table 5.

Table 5. GLM Results (Pre-employment integrity x Anonymity)

Source	Type II Sum of Squares	df	Mean Square	F	Sig.	Partial Squared	Eta	Observed Power ^b
Corrected Model	2091.134 ^a	5	418.227	7.058	.000	.184		.998
Intercept	7274.457	1	7274.457	122.768	.000	.439		1.000
Group	21.855	2	10.927	.184	.832	.002		.078
PPI	1555.509	1	1555.509	26.252	.000	.143		.999
Group * PPI	22.235	2	11.117	.188	.829	.002		.079
Error	9302.830	157	59.254					
Total	221707.000	163						
Corrected Total	11393.963	162						

Key: PPI = Pre-employment integrity, Group = Anonymity group

From Table 5 we can infer the following:

- There is no statistically significant effect for our anonymity manipulation, ($F(2,157) = .184, p = .832, \text{partial } \eta^2 = .002$).
- There is a statistically significant effect for PPI, ($F(1,157) = 26.25, p < .01, \text{partial } \eta^2 = .143$).
- There is no significant interaction between our anonymity manipulation and PPI, ($F(2,157) = .188, p = .829, \text{partial } \eta^2 = .002$).

Because of the aforementioned results only part of H3 is accepted. Anonymity did not have a significant effect. However, PPI had a highly significant effect. Therefore, the part of the hypothesis in which PPI can be used to predict CCI is accepted. However, the part of H3 in which Anonymity may be used to predict CCI is rejected. H4 is rejected since there was no significant interaction between Anonymity and PPI.

Summary of findings

From a correlation standpoint, self-reported pre-employment integrity (PPI) was significantly correlated with cyber crime engagement (CCI). Primarily, the predictors: anonymity and PPI had significant main effects on self-reported cyber crime engagement (CCI). However, it was apparent through the GLM analysis that when the predictive model is evaluated with the two factors, PPI is the stronger of the two. What is interesting to note is that using anonymity as a main predictor by itself yielded a significant model. However, as soon as PPI was introduced into the model, it became the stronger predictor.

As for the anonymity manipulation we observe an interesting trend. The largest anonymity effect took place when participants were manipulated by asking them to complete a web form that included their name, e-mail address and address. However, in the ID group, when participants were asked to show their physical student ID to the researcher, there was only a marginal effect of the anonymity manipulation. This was an interesting finding since one would expect that the physical ID manipulation would make participants feel less anonymous when compared to the Computer group. However, the findings indicated otherwise. The findings from this study illustrated that looking at someone's ID only created a marginally significant manipulation effect and the results in that group were similar to the control group.

Hypotheses discussion

Hypothesis 1

As it was described in the results, hypothesis 1 was supported. Decreasing the level of anonymity did decrease the level of self-reported cyber crime. These results are in line with research by Tresca (1998) and Zimbardo (1969). However, using Tukey's post analysis test, we see that anonymity only marginally decreased between the ID group and the Control Group these results may also be similar to research by Hartnett and Seligsohn (1967). In their research, Hartnett and Seligsohn (1967) examined the effects of varying degrees of anonymity on responses of different types of psychological questionnaires. They varied four levels of anonymity:

1. Respondent was completely anonymous: respondents to the questionnaires were told explicitly not to put either their name or student identification number on either the questionnaire or answer sheets.

2. Some identity information requested: respondents were asked to put their name and student identification number on the questionnaire sheet, but only the questionnaire number on the answer sheet.
3. Complete identification requested but respondents assured that their responses would not be identified.
4. Complete identification requested. No assurance regarding anonymity provided. (Seligsohn and Hartnett, 1967, p. 97)

Seligsohn and Hartnett (1967) results indicated that anonymity was a marginal factor only when the survey dealt with information that was highly private in nature. On the contrary, in a computer mediated environment study, Kilner and Hoadley (2005) found that they were able to reduce the occurrence of negative comments on an online forum by 89%. They manipulated anonymity by making the participants' usernames visible.

The results from this research support the conclusions portrayed in the aforementioned research. The anonymity manipulation had a significant effect on the Computer Group, however, it had a marginal effect on the ID group, even though the surveys were online.

One can speculate why there was a difference in the effect of the anonymity manipulation. One reason could be that individuals did not regard the survey items as "highly sensitive and private data". Another reason could be that participants thought that the ID manipulation was a standard procedure performed by the experimenter; therefore, it had no effect on self-reported cyber crime. Both of these plausible explanations should be tested so that we can have a better understanding of the difference between the ID and Computer manipulation.

Hypothesis 2

As shown in the results, hypothesis 2 was supported. The literature suggested that overt PPI measures have items that relate to criminal/illegal activities (see literature review). In specific, one would expect that these two are negatively correlated because logically; individuals with high levels of integrity should portray low levels of criminality.

Hypothesis 3 & Hypothesis 4

H3 was partially accepted. The accepted part indicated that PPI is a predictor of CCI. The hypothesis that anonymity is a predictor of CCI was rejected. H4 was also rejected. Primarily, it is intuitive that one may use people's integrity to predict their crime engagement. This was apparent in the literature by Shaw et al. (1999). Additionally, as explained in the literature review, inherent in the overt measures of PPI is the concept of criminal activities.

This preliminary finding may suggest that irrespective of the level of anonymity that individuals may be placed in, an individual's integrity plays a larger role in predicting their cyber criminal engagement. The finding in this study indicated that integrity is a stable predictor, because in all the tested GLM models, it remained a highly significant predictor. Rationally, we expect individuals with high levels of integrity to be less likely to engage in cyber crime activities regardless of their level of anonymity.

H4 was rejected and no interaction was found between PPI and anonymity. This finding is sensible because the concepts of anonymity and PPI are independent from one another. Anonymity can exist without PPI and vice versa.

Implications for future research

This study illustrated that manipulating one's anonymity has a significant effect on one's self reported cyber crime engagement. This is an important finding and should be taken into account when participants in a study are asked to self-report their cyber-crime engagement using a web-based survey. This finding may also suggest that anonymity is highly related to cyber crime and therefore more research needs to be conducted on its effects on cyber criminal behaviors.

The results obtained from the study also suggest that a new validated way of measuring one's anonymity while using a computer should be devised. This research illustrates that it is quite important to be able to quantify that anonymity to enable future researchers to measure the level of perceived and actual anonymity participants have. It might be that anonymity is an individual difference that also interacts with the level of anonymity gained by situational factors, and that would be an important hypothesis to test, since most literature views anonymity as a situational factor.

The results obtained from this study suggested that participants in the ID group scored similarly to the control group. This illustrated that the ID manipulation may not have fully worked as was discussed before. It is important to study why the ID manipulation did not have a significant effect on self-reported cyber crime engagement (CCI). One hypothesis to test is to see if participants generally associate anonymity in today's world with computing environments. Another hypothesis one could test is to see whether participants regard the ID manipulation as part of the experimental protocol, and therefore it has no effect on their CCI.

Contribution of the study

Primarily, this study looked at the effect of anonymity on self-reported cyber crime. The results illustrated that anonymity did have a main effect on self-reported cyber crime engagement. Secondly, this study looked at pre-employment integrity as an individual difference related to cyber crime engagement. The results illustrate that there is a significant relationship when pre-employment integrity is correlated to cyber crime engagement. Additionally, this study illustrated that the pre-employment integrity measure originally operationalized to measure a non-cyber related construct may be used as significant predictor of self-reported cyber crime engagement.

The practical implication of this study is related to cyber criminal screening. Since this study illustrated that self-reported pre-employment integrity may significantly predict self-reported cyber crime, it sheds light for the potential of researching psychometric pre-employment integrity tests for screening cyber criminal employees. However, in order to strengthen that relationship, perhaps a new pre-employment integrity screening measure could be devised that takes cyber crime activities into account.

Conclusion

Research in cyber crime behavior and psychology is still young. Because of the sparse literature on this subject matter, this study was exploratory in nature. This study needs to be re-created and validated with other participants in order to get a better understanding for the validity and reliability of the obtained results.

Even though this study was exploratory, it significantly adds to the body of knowledge in this area. This study illustrated that self-reported cyber criminal behavior (CCI) may be

significantly predicted using one independent variable (Anonymity) and the predictor (self-reported pre-employment integrity (PPI)).

Successive research in this area should attempt to use a better manipulation technique for the ID group. Additionally, in the future, researchers should attempt to use the full psychopathy scale, and should test other covert and overt PPI measures to examine if they are valid predictors of self-reported cyber crime. Future researchers should also attempt to use a larger population sample, and measure other individual differences to see their effects on self-reported cyber crime.

This study aimed at exploring psychological constructs that deal with cyber crime. As people are becoming increasingly technology-dependent, we continue to see growth in cyber criminal activities. In order to mitigate cyber criminal activities, the continuous pursuit of research to understand cyber criminals continues to be of importance and value.

Limitations

This study has some limitations. Primarily, this study has the methodological limitation of self-reported surveys. There is also the slight chance that the anonymity was not the factor being manipulated during the experimental procedures since the ID group manipulation was not stronger than the Computer Group.

Another limitation of the study is the sample used as well as the sample size. Primarily, the number of males is significantly larger than the number of females. Second, all the students recruited had similar ages and majors (technology students). Third, the number of participants (N=163) is reasonable but not very high. If the ratio of males to females is improved, the participant sample came from a more diverse population and the number of participants was increased, the study's results would become more generalizable.

Finally, a significant limitation is the generalizability of the findings. The findings of this study cannot be generalized to all the populations. In order for this study to gain more external validity, it would have to be repeated for different populations with larger sample sizes.

References

- Babu, M., & Parishat, M.G. (2004). What is cyber crime?. Retrieved November 10, 2009, from <http://www.crime-research.org/analytics/702/>
- CSI Computer Crime and Security Survey. (2008). Retrieved May 25, 2009 from <http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2008.pdf>
- Gordon, L., Loeb, M., Lucyshyn, W., & Richardson, R. (2006). CSI/FBI Computer crime and security survey. Retrieved November 10, 2009 from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf
- Hinduja, S. (2008). Deindividuation and Internet Software Piracy. *CyberPsychology & Behavior*, 11(4), 391-398.
- Rogers, M. (1999). Modern-day Robin Hood or moral disengagement: understanding the justification for criminal computer activity. Retrieved June 27, 2009, from <http://homes.cerias.purdue.edu/~mkr/moral.doc>
- Rogers, M. (2001). A social learning theory and moral disengagement analysis of criminal computer behavior: an exploratory study. Retrieved June 27, 2009, from <http://homes.cerias.purdue.edu/~mkr/cybercrime-thesis.pdf>

- Rogers, M. (2003). Preliminary findings: understanding criminal computer behavior: a personality trait and moral choice analysis. Retrieved June 27, 2009, from <http://homes.cerias.purdue.edu/~mkr/CPA.doc>
- Rogers, M., Seigfried, K., Tidke, K. (2006). Self-reported computer criminal behavior: A psychological analysis. *The International Journal of Digital Forensics & Incident Response*, 3, 116-120.
- Sukhai, N. (2004). Hacking and cyber crime. New York, NY. *ACM Press*.
- Lipson, H. (2002). Tracking and tracing cyber-attacks: technical challenges and global policy issues. Retrieved June 27, 2009, from <http://www.cert.org/archive/pdf/02sr009.pdf>
- Williams, P. (2002). Organized crime and cyber-crime: implications on business. Retrieved June 27, 2009, from <http://www.cert.org/archive/pdf/cybercrime-business.pdf>
- Shaw, E., Ruby, K., & Post, J. (1998). The insider threat to information systems: the psychology of the dangerous insider. *Security Awareness Bulletin*, 2, 1-10.
- Cohen, J (1992). A power primer. *Psychological Bulletin*, 112, 155-159.
- Hartnett, R. T., & Seligsohn, H. C. (1967). The effects of varying degrees of anonymity on responses to different types of psychological questionnaires. *Journal of Educational Measurement*, 4(2), 95-103.
- Kilner, P., & Hoadly, M. (2005). Anonymity options and professional participation in an online community of practice. *Conference on computer support for collaborative learning* (pp. 272-280). Taipei: Taiwan.
- Tresca, M. (1998). The impact of anonymity on disinhibitive behavior through computer-mediated communication. Retrieved November 10, 2009, from <http://www.msu.edu/user/trescami/thesis.htm>
- Zimbardo, P. G. (1969). The human choice: Individuation, reason, and order versus deindividuation, impulse, and chaos. In W. J. Arnold and D. Levine (Eds.), 1969 Nebraska Symposium on Motivation (pp. 237-307). Lincoln, NE: University of Nebraska Press.