Effects of Anonymity, Pre-Employment Integrity and Antisocial Behavior on Self-Reported Cyber Crime Engagement: An Exploratory Study

by Ibrahim M. Baggili
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

Graduate School ETD Form 9
(Revised 12/07)

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Ibrahim Baggili

Entitled EFFECTS OF ANONYMITY, PRE-EMPLOYMENT INTEGRITY AND ANTISOCIAL BEHAVIOR ON SELF-REPORTED CYBER CRIME ENGAGEMENT: AN EXPLORATORY STUDY

For the degree of Doctor of Philosophy

Is approved by the final examining committee:

Marcus Rogers
Chair

William Graziano

Thomas Hacker

Richard Mislan

To the best of my knowledge and as understood by the student in the *Research Integrity and Copyright Disclaimer (Graduate School Form 20)*, this thesis/dissertation adheres to the provisions of Purdue University's "Policy on Integrity in Research" and the use of copyrighted material.

Approved by Major Professor(s): Marcus Rogers

Approved by: Gary R. Bertoline July, 12, 2009
Head of the Graduate Program Date

Graduate School Form 20
(Revised 6/09)

PURDUE UNIVERSITY
GRADUATE SCHOOL

Research Integrity and Copyright Disclaimer

Title of Thesis/Dissertation:

Effects of Anonymity, pre-employment integrity and antisocial behvaior on self-reported cyber crime engagement: An exploratory study

For the degree of Doctor of Philosophy

I certify that in the preparation of this thesis, I have observed the provisions of *Purdue University Executive Memorandum No. C-22,* September 6, 1991, *Policy on Integrity in Research.**

Further, I certify that this work is free of plagiarism and all materials appearing in this thesis/dissertation have been properly quoted and attributed.

I certify that all copyrighted material incorporated into this thesis/dissertation is in compliance with the United States' copyright law and that I have received written permission from the copyright owners for my use of their work, which is beyond the scope of the law. I agree to indemnify and save harmless Purdue University from any and all claims that may be asserted or that may arise from any copyright violation.

Ibrahim Baggili
Printed Name and Signature of Candidate

July, 12, 2009
Date (month/day/year)

*Located at http://www.purdue.edu/policies/pages/teach_res_outreach/c_22.html

EFFECTS OF ANONYMITY, PRE-EMPLOYMENT INTEGRITY AND ANTISOCIAL BEHAVIOR ON SELF-REPORTED CYBER CRIME ENGAGEMENT: AN EXPLORATORY STUDY

A Dissertation

Submitted to the Faculty

of

Purdue University

by

Ibrahim M. Baggili

In Partial Fulfillment of the

Requirements for the Degree

of

Doctor of Philosophy

August 2009

Purdue University

West Lafayette, Indiana

To my father.

ACKNOWLEDGEMENTS

I would like to thank everyone for their support. I especially want to thank my father for supporting me, teaching me to never give up, and pursue my dreams. My father has been, and always will be my inspiration. I would also like to thank my committee members. Professor Marcus Rogers, thank you for allowing me to mature my research abilities at my own pace, for always helping me, and continuously believing in me as a future academic colleague. Dr. Graziano, the same goes to you. You have inspired my interest in social psychology, and I learned so much from your extensive experience and advice. Your interest and support has motivated me to pursue new learning opportunities in the interesting world of social psychology. Professor Mislan, my thanks goes to you for helping me understand mobile devices and the need to study them. I would especially like to thank you for giving me the opportunity to be a guest speaker at your conference. Finally, I would have never been able to make it without the support of my loved ones and family members – all of you. To my wife, Meghan, thank you for being patient through our financial hardships while I pursued my dream of becoming Dr. Abe. Thank you all for inspiring me, and letting me grow and achieve a goal that I've always dreamed of achieving. The funny thing is that, now that I have earned my PhD, I feel that my thirst to knowledge has just begun.

TABLE OF CONTENTS

Page

Page

Page

LIST OF TABLES

LIST OF FIGURES

Figure Page

ABSTRACT

Baggili, Ibrahim M. Ph.D. Purdue University, August 2009. Effects of anonymity, self-reported pre-employment integrity and self-reported antisocial behavior on self-reported cyber crime engagement: An exploratory study. Major Professor: Marcus Rogers.

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 dissertation 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, antisocial behavior 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 positive relationship between self-reported antisocial behaviors and cyber crime engagement, and a statistically significant negative relationship between self-reported cyber crime engagement and pre-employment integrity. Suggestions for future research are also discussed.

CHAPTER 1 - INTRODUCTION

Statement of the problem

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 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 someone 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.

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 dissertation builds on their work and examines the relationship between cyber criminal activities and an individual's operationalized pre-employment integrity.

Lastly, research in the pre-computer era has concluded that anonymity induces individuals to engage in antisocial behaviors (Diener, 1979; Zimbardo, 1969). Research in CMC has also indicated that as the level of anonymity increases, individuals are more likely to portray antisocial/disinhibitive behaviors (Tresca, 1998). However, these conclusions have not been validated in the context of cyber criminals. It then becomes necessary to test if our current understanding of antisocial behavior in psychology can be related to cyber criminals. This test may lead to future research aimed at the creation of new antisocial self-reported measures that are predictive of cyber criminals.

Purpose of the study

The purpose of the study is to investigate how cyber crime engagement is related to integrity, anonymity and self-reported antisocial behaviors.

Research questions

This research aims to answer the following questions:

Q_1: Does manipulating someone's anonymity affect their self-reported cyber crime engagement?

Q_2: Is there a significant relationship between the self-reported antisocial behavior and self-reported cyber crime engagement?

Q_3: Is there a significant relationship between self-reported pre-employment integrity and self-reported cyber crime engagement?

Q_4: Does anonymity significantly affect the relationship between self-reported pre-employment integrity and self-reported cyber criminal engagement?

Q_5: Does anonymity significantly affect the relationship between self-reported antisocial behaviors and self-reported cyber criminal engagement?

Q_6: Can self-reported antisocial behavior and pre-employment integrity significantly predict cyber criminal engagement?

Q_7: Are there any interactions between any of the self-reported measures (antisocial behaviors, cyber crime engagement and pre-employment integrity)?

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 and antisocial behavior. 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 operationalizations of antisocial behavior and 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.

CHAPTER 2 – REVIEW OF LITERATURE

The dependency of humans on Information Technology (IT) and the Internet has dramatically increased. Seldom do we see individuals not using a technological device like a cellular phone, a laptop computer or an iPod. IT has penetrated our lives and has had some noticeable implications on our society. The Internet, for instance, has become domesticated and is now used by the majority of Americans for personal and economic reasons (Cummings & Kraut, 2002). One can provide an endless list of statistics on Internet usage and IT released by the U.S. Department of Commerce and other sources, but the impact of technology on humans has become quite obvious.

In the past, humans believed that technology and humans belonged in two different distinct worlds (Saariluoma, 2007). Saarriluoma (2007), the editor in chief of the journal on humans in ICT environments called *Human Technology* points out a famous book written by C.P Snow (1959) called *The two cultures and the scientific revolution*, where Snow (1959) argues that the social and technical disciplines of technology are separated by a high wall. He also argues that in today's world, copious amount of research has indicated that technology is influenced by humanistic ideals. These declarations reveal an interaction of humans with technology, and technology with humans. To better understand the relationship between humans and technology, research needs to be conducted in this area.

A great deal of the research being performed in computing has focused on the positive aspects of human computer interaction. For instance, research on the positive impact of human interaction via electronic mail and chatting has been prominent on the agendas of social and psychological researchers. Research like this has had a constructive influence on our understanding of how and why humans interact electronically. However, paralleling the notion of positive computer use is computer misuse. The drastic increase in the misuse of electronic devices has led toward the cyber crime phenomenon.

There is plenty of speculation of why cyber crime was, and still is on the rise in our society. Literature in CMC has shown that one of the prominent situational factors affecting the electronic interaction of people is anonymity. Research on anonymity has illustrated that the increase in anonymity induces people's engagement in disinhibitive/antisocial behaviors (Diener, 1979; Tresca, 1998; Zimbardo, 1969). Other research in the psychology of cyber criminals has shown that they are more likely to posses certain personality traits, one of which may be the level of personal integrity (Shaw et al., 1998). The following literature review aims to bring the reader up to pace on the writings and research associated with these concepts. First, the concept of cyber crime will be discussed and limited to white collar crime and IT insider threat. Next, the literature on anonymity will be reviewed. Lastly, literature on pre-employment integrity and antisocial behavior will be reviewed.

Cyber crime: what is it?

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). In the California review of law, Brenner (2000) illustrates that according to how the law defines crime, some facets of the definition of traditional crime do not directly apply to “virtual crimes”. A good example that Brenner (2000) discusses is cyber-stalking versus real-life, traditional stalking as an offence. There is a difference between traditional stalking and cyber-stalking in the existence of a threat, such that traditional stalking laws frequently obligate that a stalker has made at least one credible threat to injure his or her victim (Brenner, 2000). However, cyber-stalkers tend to simply threaten their victims and usually that threat is not direct. Cyber-stalkers typically use the cyber world as a medium to harass and threaten their victims, such as posting the victim’s name and address on the Internet along with phony claims that he/she wants to be raped by strangers.

Brenner (2000) also explained that even if a cyber-stalker directly threatens a victim online, a court of law may not find the threat from someone who is physically located very far away to be credible. Another obvious example is that stalking requires the offender to be physically present, yet in cyber-stalking, the offender is not in the victim’s physical presence (“1999 report on cyberstalking,” 2003). These are only two examples that illustrate how cyber crime is different from traditional crime from a law-breaking perspective.

Katyal (2001) states that cyber crime is efficient. Katyal (2001) explains that the advent of personal computers pose major threats to the rule of law and that cyber crime is efficient because a) computers are a powerful substitute for additional people in a criminal enterprise b) computers permit anonymity and secure communications c) cyber criminals are often invisible, remote and unreachable and d) with computers, crime is cheaper to commit and criminals find it easier to escape detection and apprehension (Katyal, 2001, p. 1042). This efficiency can make cyber crime more appealing than traditional crime.

To entirely answer the second question on the types of cyber crime is beyond the scope of this chapter because the author speculates that almost any crime that could be thought of in the physical world can be accomplished in the digital world as well since we live in a technologically enabled society. It would be difficult to cover every single facet of cyber crime in detail, so to limit the scope of this chapter, two major types of cyber crimes will be examined a) high-tech white collar crimes and b) IT insider threat crimes.

The concept of white collar crime is not new. It became part of the English language when Edwin Sutherland gave his presidential address to the American Sociological Society in 1939 (Braithwaite, 1985). However, the definition of white collar crime has changed over time. The original definition by Sutherland was “A crime committed by person of respectability and high social status in the course of his occupation” (Braithwaite, 1985, p.3). Nowadays, the term white collar crime has taken another meaning. The Department of Justice (DOJ) explains “White-collar offenses shall constitute those classes of non-violent illegal activities which principally involve traditional notions of deceit, deception, concealment, manipulation, breach of trust, subterfuge or illegal circumvention." (Baker, 2004, p. 1). There are still debates on the definition of white collar crime, but it is beyond the scope of this chapter to formulate a more concrete description of the term. A good reference guide for the definitional dilemma of white collar crime was presented by the National White Collar Crime Center (NW3C)[1].

The shift towards cyber crime has caused agencies like the NW3C to focus their attention to cyber criminal activities related to white collar crimes. The NW3C releases many reports on white collar crimes associated with computer usage. In their *2005 National Public Survey on White Collar Crime*, they illustrate that white collar crimes are on the rise (Kane & Wall, 2005). Kane and Wall (2005) list categories of white collar crime offenses such as monetary loss over the Internet, illegitimate e-mail fraud, credit card fraud and auction fraud. One can note the impact of computer usage on white collar crime just by considering these aforementioned categories.

In both the first and second categories (monetary loss over the Internet and illegitimate e-mail fraud), the crimes were branded based on Internet usage. In relation to the first category, many modes exist in which one can lose money over the Internet; online gambling is one of them. In the second category, the Internet is required both for the e-mail recipient and the sender in order for that crime to occur. The point is that in both of these categories (monetary loss over the Internet and illegitimate e-mail fraud), a computer is needed in order for the crime to occur. As for credit card fraud and auction

[1] It can be downloaded from their website at http://www.nw3c.org

fraud, these categories may be affected by computer usage as well. One can argue for the increase in the frequency of online credit card centric purchases, which can in turn lead to a plausible contention for the escalation of credit card fraud in computing environments. The same applies to auctions. Websites like eBay have become prominent sources for people to auction their goods and services, thereby increasing the possibility of auction fraud to occur in computer mediated environments.

White collar crimes are becoming more intricate and are often involving hi-tech devices. In the 2005 NW3C *National Public Survey on White Collar Crime*, it was stated "Many white collar crime investigations require specialized investigative techniques, equipment, or training, and many smaller agencies are not prepared to handle such cases. This is especially true of crimes involving a computer" (Kane & Wall, 2005, p3.). The severity of high tech white collar crimes can be shown through data on Internet fraud. In the 2008 annual *Internet Crime Report* by the Internet Crime Complaint Center (IC3), it was stated that Internet fraud statistics based on 72,940 complaints referred to law enforcement in 2008 mostly comprised of complaints relating to Internet fraud. The total dollar loss from all referred fraud cases was $264 (IC3 Report, 2008, p. 3).

One other category of cyber crime is IT insider threat crimes. The insider threat concept is not new and has been of national security interest in the military for centuries. One of the earliest documented insider threat conceptions was by Sun Tzu (544 BC – 496 BC), a Chinese military strategist. In his work, Sun Tzu recognizes the risk of trusted insiders betraying a mission, either by providing information to outsiders (espionage) or by destructive acts (sabotage) (Schwarting, 2005). There seems to be agreement amongst insider threat experts that there exists four major preconditions required for insider threat/betrayal to occur which are a) an opportunity to commit the crime b) a motive for the crime c) an ability to overcome natural inhibitions to criminal behaviors such as moral values, loyalty to employer or co-workers, or fear of being caught and d) a trigger that sets the betrayal in motion (Anderson et al., 2000, p. 90).

In the seminal research conducted by the National Defense Research Institute, they outline two types of opportunity. The first type is the access to information or material that can be exchanged for money or used to achieve a goal. The second type is personal acquaintance with, or easy access to, persons expected to be interested in obtaining such valuable information or material (Anderson et al., 2000, p. 90). The opportunities for the access of information have increased dramatically with the rise of Information Technology. With the wide spread use of photocopy machines, database systems, e-mail, storage media etc., technology has become an insider threat enabler.

As for motives, Anderson et al. (2000) argue that criminal motives are not always linked to money and that money is usually only a surface motive. People that engage in espionage for money have more pressing emotional needs than financial needs. Money is usually viewed as a symbol of power, thus satisfying a personal psychological need. Espionage motive may also be seen as an outlet of anger, as a way of punishing the people in charge for not recognizing one’s talent as means of revenge or a source of excitement (Anderson et al., 2000).

The ability to overcome natural inhibitions may be attributed to numerous variables. Anderson et al. (2000) explain that betrayal is rare because it violates basic moral standards like being loyal to one’s country. It is not fully understood what can cause the erosion of these inhibitions as they argue that any social changes that wear down these inhibitions may increase the frequency of betrayal. However, they do state that if one was categorized as a traitor or if one thinks of him/herself as a traitor, then that can increase the possibility of betrayal. They also mention that economic conditions and feeling of entitlement to better treatment can also play a role in increasing the ability of overcoming natural inhibitions, thereby escalating the frequency of betrayal.

Lastly, there are triggers that increase the frequency of betrayal, such as events that happened during the course of an individual’s personal or professional life, pushing the individual beyond their breaking point. People that are emotionally stable react to situations as such in a positive manner by learning from them and bettering themselves. In contrast, emotionally unstable individuals may act in ways that harm themselves or the organization they work for. They may harm themselves by excessive substance abuse, or the organization through sabotage, espionage, theft or fraud (Anderson et al., 2000). These stressful situations are regarded as triggers, and may be detrimental in the case of emotionally unstable individuals.

Some insider threat studies are now being focused solely on IT insider threat. The leading studies are released by Carnegie Mellon’s Software Engineering Institute – the CERT Coordination Center in conjunction with the United States Secret Service since the concept of the IT insider threat endangers national security. One of their notable studies focused on the Insider IT threat in the banking and finance sector. Their study concluded that most of the incidents in the banking and finance sector were a) not technically sophisticated, b) 81 % of the incidents were planned in advance, c) 81 % of the incidents were motivated by financial gain, rather than the desire to harm the company or information system, d) insiders fit no common profile, e) insider incidents were detected by internal and external individuals (including customers), f) in 30 % of the cases the financial loss exceeded $500,000, g) 83 % of incidents were executed physically from within the insider's organization and took place during normal business hours (Randazzo et al., 2004). Staggering results like these illustrate that the IT insider threat concept is ever apparent today and has a serious unfavorable impact on the economy.

In response to the third question on why people misuse computers and other electronic devices, there have been numerous theoretical speculations on why humans tend to commit crimes in general. These theories do not take into account Information Technology (IT) as a crime enabler or anonymity as a facilitator. For instance, in classical criminology, choice theory asserts that people commit crime because they choose to do so. This theory originated with the writings of Cesare Baccaria, an Italian social thinker in 1744 (McQuade, 2006). Another version of this is the Rational Choice theory. Here, people are regarded as rational thinkers that weigh the potential costs and benefits before committing a crime (Browing, Halci & Webster, 2000). Inherent in both of these theories is the claim that the likelihood of being caught and punished when committing a crime is an important factor when determining why a crime occurs. Another classical theory applied to criminology that attempts to explain why individuals engage in criminal behaviors is the social learning theory (Skinner & Fream, 1997). This theory is closely related to the work by Albert Bandura in which individuals learn by cognition; by observing other’s actions (Blackburn, 1993). Another theory that may be used to explain crime is known as the differential association theory (Sutherland, 1947). In his theory, Sutherland (1947) explained that criminal behaviors are learned from one’s interactions with others, and mostly from key individuals in one’s life such as parents and family members.

To fully explain the various theories of why individuals commit cyber crime is beyond the scope of this literature review. However, the literature review suggested that the classical theories of why people commit crime do not account for anonymity as a major factor in their various models. The literature also suggests that anonymity is an important factor strongly related to computer interaction environments (Katyal, 2003; Tresca, 1998). If that is the case, then anonymity should be studied as a variable affecting cyber crime engagement. This in turn may improve our understanding of the situations inducing individuals to engage in cyber criminal activities.

Anonymity

The word anonymity is derived from the Greek word ανώνυμος (pronounced anonymos) which means without a name, or nameless. A popular definition of anonymity is “The state of not being identifiable within a set of subjects, the anonymity set” (Pfitzmann & Kohontopp, 2001, p.1). Related to anonymity is pseudonymity. Pseudonymity is the use of a false name (Froomkin, 1995). Pseudonymity is especially prevalent in computing environments. Typically, computer users employ either a handle or an e-mail address. A handle or an e-mail address is a pseudonym because it may not be the direct name of an individual, yet it still relates to that specific individual. The definition of anonymity is simple, but the effect anonymity has on our behavior is complicated.

To help in understanding the complexity of anonymity, social scientists should continue to empirically study anonymity. This continuous conception of anonymity is crucial because the definition of anonymity keeps changing. For instance, with the rise of the personal computer, the definition of anonymity has taken new twists. Consequently, due to the rise of electronic communication, especially e-mail, Froomkin (1995) explained that there are four types of anonymity and pseudonymity in relation to e-mails:

1. Traceable anonymity: A system such that a remailer gives the recipient no clues as to the sender's identity but leaves this information in the hands of a single intermediary.
2. Untraceable anonymity: A system in which the author of the message is not known.
3. Untraceable pseudonymity: A system in which the author is known, but the author's real identity is concealed. An example is John signing an e-mail as Alice.
4. Traceable pseudonymity: A system in which one is able to find information required to complete the link between a pseudonym and a real identity. (Froomkin, 1995).

Another theoretical conception of anonymity was proposed by Azechi (2005), as shown in Figure 1. In his proposition, he rationalizes three major levels of anonymity a) visual anonymity b) disassociation of identity and c) lack of identification (Azechi, 2005).

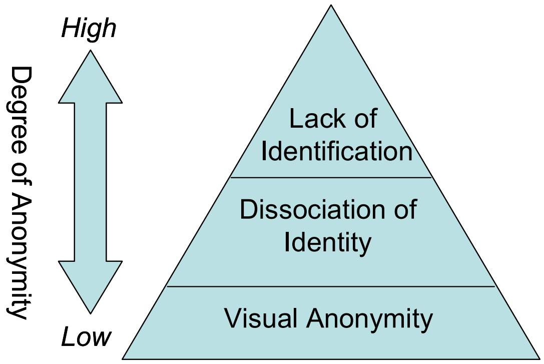


Figure 1. Hierarchical structure of different anonymity conditions (Morio & Buchholz, 2007, p. 3)

Visual anonymity is when individuals communicate without seeing each other. A good example of that is using text-based chatting programs over the Internet. People's physical appearances are obscured in that scenario.

The second level of anonymity is the dissociation of real and online identities. A single individual can create more than one online identity using more than one screen name and avatars (Turkle, 1995). Individuals then have the ability to become more than one person with dissimilar personalities. They also have the ability to adopt new genders and races.

The third level closest to true anonymity is the lack of identifiability. When individuals cannot be identified, their behaviors are not distinguishable from others' behaviors (Douglas & McGarty, 2001). An example of that would be an online forum in which people can post anonymous comments without attaching their usernames to that post.

As seen in both Froomkin (1995) and Azechi (2005), their frameworks spotlight anonymity in relation to electronic communications. One can conclude that anonymity originally meant "without a name" and that the concept has become more intricate.

“Without a name” suggested that anonymity is a single level, whereas research is pointing out that anonymity has multiple levels. The point to take into account is that the meaning of anonymity is affected by the context in which the word is used, as well as the continuous research on the topic. In fact, it has also been shown that the meaning of the word anonymity varies across cultures (Morio & Buchholz, 2007).

In a recent study by Morio and Buchholz (2007), it was shown that people have a different perception of anonymity depending on their culture. Morio and Buchholz (2007) first present the notion that there are two contradicting goals of social interaction – autonomy and affiliation. Autonomy is the ability of an individual to control their own environment as well as the need to be unique and independent from others. Affiliation is when individuals attempt to associate themselves with group members by imitation or compliance (Morio & Buschoolz, 2007, p. 6).

Morio and Buschholz (2007) delineate that there are cross-cultural differences especially in the dimension of Individualism/Collectivism (IC). Some cultures are individualistic, where they emphasize the individual’s goals over the group’s goal. Other cultures are collectivist, and they emphasize the group’s goals over the individual. In their preliminary study, by examining posts from the United States and the Japanese Slashdot.org, they were able to suggest that cross-cultural differences in interpersonal motivation play a role in deciding whether individuals should remain anonymous while communicating online. Their results indicated that individuals in Western societies valued autonomy, while in Eastern societies, they valued affiliation. This signified that Westerners are more likely to gravitate toward concepts with lower levels of anonymity, whereas Easterners seek online activities with higher levels of anonymity (Morio & Buchholz, 2007, p .1).

Despite the relative meaning of the word anonymity in the various contexts, research has continuously shown that it can enhance communication choices (Huber, 1990; Rice, 1987; Sproull & Kiesler, 1991). Understanding the definition of anonymity is important. Comprehending how anonymity affects behavior is also of major value, and the most prevalent symbiotic theory in relation to anonymity effects is deindividuation.

Anonymity & deindividuation

The understanding of the deindividuation theory is ever changing as more research is being conducted. With the advancement of technology and the rise of the personal computer, mobile devices, and various other electronic communication media, the term deindividuation has taken various twists and turns. However, to get an insightful understanding of deindividuation, one has to go back to the earliest research on that subject matter.

The concept of deindividuation is not new and many attribute its originality to Festinger et al. (1952). Nonetheless, in a meta-analysis on deindividuation by Postomes and Spears (1998), they point out that the concept in which the theory of deindividuation stems from is largely based on the classic crowd theory of Gustave Le Bon. In a book written by Gustave Le Bon in 1895 titled *The Crowd: A study of the popular mind*, he discusses the effects of crowds on individuals:

> Whoever be the individuals that compose it, however like or unlike be their mode of life, their occupations, their character, or their intelligence, the fact that they have been transformed into a crowd puts them in possession of a sort of collective mind which makes them feel, think, and act in a manner quite different from that in which each individual of them would feel, think, and act were he in a state of isolation. (p. 9)

Le Bon believed that when individuals are submerged in a crowd they unconsciously lose their individuality. The concept of the crowd was a factor that Le Bon evidently believed played a role in unconsciously manipulating human behavior. Le Bon also deliberated on the anonymity of crowds. In fact, one of the dichotomies of crowds he explained was an “anonymous crowd”. An example of an anonymous crowd is a mass of people walking on the street. But even with the specific dichotomies of crowds presented in his theory, he attempted to formulate a general philosophical account for how individuals are affected by a crowd.

Le Bon explained that there are psychological functions of individuals when immersed in a crowd, calling it a “psychological crowd”. Not only did he state that individuals act differently in a crowd, but he claimed that they become mindless, capable of defying social norms as a result of a single collective group mind. Le Bon’s seminal philosophy on crowd theory initiated interest in psychological research on that matter, and was investigated by the social psychologists Festinger et al. (1952).

Festinger et al. (1952) rationalized deindividuation as a state in which people are not paid attention to as individuals due to being part of a group. Since people are not given proper attention as individuals when submerged in a group, they hypothesized that inner restraints of moral controls are reduced. Therefore, like Le Bon, Festinger et al. (1952) conceived of deindividuation as loosing one's individuality when being part of a larger group. However, there is a difference in the way they both considered why that occurs. On one end, Le Bon hypothesized that it was due to individuals formulating a collective group mind. On the other, Festinger et al. (1952) hypothesized that the loss of a person's individuality, due to being part of the group, decreases internal individual restraints of moral controls.

The next part of the deindividuation phenomenon seems to be the most seminal contribution to the theory when linked to antisocial behaviors and was formulated by Zimbardo in 1969. Zimbardo (1969) took the work on deindividuation and devised a theory that included variables affecting a behavioral outcome. Zimbardo's theory was more objective, specifying that numerous antecedent variables can lead a person to reach a deindividuated state with the most important being anonymity, loss of individual responsibility, arousal, sensory overload, unstructured situations, and mind altering substances. According to Zimbardo (1969), if individuals are subject to the circumstances mentioned above it will lead them to engage in deindividuated behaviors which he defined as "Behavior[s] in violation of established norms of appropriateness" (Zimbardo, 1969, p. 251).

Zimbardo (1969) focused his attention on antisocial behaviors that are a result of deindividuation. However, contrasting the theories offered by Festinger et al. (1952) and Le Bon (1895), Zimbardo (1969) did not limit his deindividuation theory to groups. The deindividuation model he explained could be applied to individualistic related concepts such as suicide and interpersonal hostility. Zimbardo's theory also explained that deindividuation reduces an individual's self-observation, self-evaluation and an individual's concern for social evaluation. This in turn leads to a weakening in controls based on guilt, shame, fear and commitment, which further guides an increase in the display of disinhibited behaviors such as violence and vandalism (Zimbardo, 1969). Zimbardo's model, however, was criticized for two major reasons 1) empirical reasons, and 2) conceptual reasons.

Empirically, Zimbardo's theory failed because his predictions in two distinct experiments, using the same methodology, did not yield the same results. This major problem of validity needed to be addressed. However, the conceptual problem is twofold. Primarily, Zimbardo's model on deindividuation is vague about the mediator variables involved when attempting to predict antisocial behaviors. Secondly, it became clear to psychologists that deindividuation does not only lead to antisocial behaviors, but could also direct individuals to engage in prosocial behaviors, like being more affectionate and generous towards others (Reicher, n.d.). In response to these two issues, a new theory was formulated by Diener in 1980.

Diener went back to the notion of objective self awareness originally conceived by Duval and Wicklund (1972). Diener (1980) asserted that at the heart of the deindividuation theory is the concept of objective self awareness. In this new revised model of deindividuation, the most prominent antecedent variable was the perception of being immersed in a group. Once individuals are submerged in a group, the theory states that they are overloaded with information, thus causing them to lose their objective self awareness, thereby allowing them to lose their internalized self-standards. The decrease in internalized self standards causes individuals to be affected by environmental stimuli. Finally, the environmental stimuli play a major role in determining the outcome of that loss of self awareness, depending on whether the environment promotes antisocial or prosocial behaviors, thus dictating the outcome behavior of that individual.

One of the final noticeable research developments on the classical deindividuation theories was performed by Prentice-Dunn and Rogers (1982) in the 1980s. Prentice-Dunn and Rogers (1982) amalgamated the theories of deindividuation, formulating the notions of private and public self-awareness. Public self-awareness deals with the individual's awareness of being evaluated by others. Private self awareness equates to the concept of objective self-awareness in which individuals assess their behaviors based on their internal self-set standards. In their theory, they explain that when people are lacking in public self-awareness, they are more likely to perform antisocial behaviors. They further articulated that when private-self awareness is decreased, people become more susceptible to external control. An interesting hypothesis that Prentice-Dunn & Rogers do raise, however, is that when individuals are submerged in a group, they lose both their private and public self awareness, thereby leaving individuals unrestrained by either their private or public self awareness.

Despite the relative differences between the classical theories of deindividuation, there are some underlying similarities. Primarily, all the theories consider that there is a difference between an individual and a group. All the theories also have an underpinning agreement that when people are submerged in a large group, their behaviors change. Finally, even though it is not clearly stated in all the theories, most of the deindividuation theories seem share the notion that being deindivduated may increase the possibility of aggressiveness and crime commitment (Diener, Fraser, Beaman & Kelem, 1976; Ellison, Govern, Petri, & Figler, 1995; Rehm, Steinleitner, & Lilli, 1987; Zimbardo, 1975).

The two deindividuation theories proposed by Diener (1980) and Zimbardo (1969) clearly outline anonymity as one of the key causes of deindividuation. Furthermore, using the definition of anonymity mentioned in the earlier part of the chapter "The state of not being identifiable within a set of subjects, the anonymity set" (Pfitzmann & Kohontopp, 2001, p.1), one can deduce that anonymity may be increased or decreased based on the number of individuals in a group. Since all the classical theories of deindividuation explicate that crowd, or groups, affect deindividuation, then one can argue that anonymity is of utmost importance when dealing with behavior prediction in crowds. However, the next step of the deindividuation theory took a novel transformation.

Johnson and Downing (1979) performed an experiment in which individuals were made anonymous to each other by wearing masks and overalls similar to the Ku Klux Klan, or by means of dressing up in nurses' uniforms. The individuals were asked to deliver an electric shock to a person. They found that individuals shocked others less when dressed as nurses, compared to being dressed in a costume similar to the Ku Klux Klan. This indicated that the behaviors individuals engaged in were affected by their awareness of their group identity and abided by the social norm imposed on them by their clothing. The results from this experiment could not be properly explained by the logic of the classical deindividuation theories. Therefore, a newer theory of deindividuation had to be devised.

In a meta-analysis by Postomes and Spears (1998) on deindividuation research, the classical theories of deindividuation were questioned. In their meta-analysis, they examined sixty deindividuation studies and found no reliable support for suggesting that deindividuation is responsible for the increase of antisocial behaviors. In fact, their results indicated that the average effect size is close to zero ($r = 0.09$), illustrating that there is only a marginal support for the notion that deindividuation increases antisocial behaviors. From their study, they concluded that deindividuation effects are more likely to lead to normal behaviors. Their meta-analysis only found one predictor, which was the situational norm. The situational norm is lead by the individuals' perceived norm which is derived from the group context. If individuals thought their behavior was desirable within the group context, they had no difficulty delivering that behavior. The meta-analysis performed by Postomes and Spears (1998) led to the proposition of the Social Identity model of Deindividuation Effects (SIDE).

Compared to the deindividuation models discussed earlier, the SIDE model predicts conformity to norms associated with the social identity of the group rather than conformity to any general norms (Postomes et al., 1998). This proposition illustrates that the SIDE theory is focused on the situation an individual is immersed in and the individual's perception of the group identity. This new model inherited parts from the social identity theory, which was originally developed by Tjafel and Turner (1979) as a way of understanding intergroup discrimination. The basis of the social identity theory is that a person has more than one identity, which is dependent on that individual’s group membership. How the individual perceives themselves as part of the group ultimately affects that individual’s behavior.

Postomes et al. (1998) explain that the SIDE theory contains two major facets that affect the use of anonymity – the cognitive component and the strategic component. The cognitive component of anonymity in SIDE stresses “how group dynamics and individual behavior within groups is mediated by anonymity and the strength on an individual’s identification with the group” and the strategic component “involves the intentional use of anonymity in an attempt to take advantage of the benefits offered by anonymity” (Christopherson, 2007, p. 3048).

SIDE seems more general than the classical deindividuation theories. This could be a reason why it is empirically supported - since any obtained results could fit the general model offered by the SIDE theory. However, like all the other classical deindividuation theories discussed, the SIDE theory still recognizes a difference between the individual and the group. It also implicitly recognizes that submerging an individual in a group will ultimately result in some sort of behavioral change. Finally, it acknowledges the importance of anonymity as a mediator. Since the SIDE theory identifies anonymity as a mediator and distinguishes the differences between an individual and a group, examining anonymity at both the individual and the group levels should not be disregarded.

Anonymity and its research levels

Anonymity can be studied from an individual or a group level. This follows the same philosophy as the deindividuation theory, which parallels the notions of private and public self-awareness. To study the various effects of anonymity on private and public self-awareness, one would require the investigation of anonymity at the individual and the group level.

Anonymity at the individual level

The concept of private self-awareness plays a chief role in the study of anonymity at the individual level. Private self-awareness in the deindividuation theory is strongly coupled with personal privacy. Think about how people may not wish to disclose personal information on a survey, or to a telemarketer. Also think about the times in which people chose to close their curtains in order to maintain their personal privacy. These are only two examples relating to personal privacy, but privacy has clearly become of great concern to individuals in today’s society.

The concept of privacy has existed for a long time and has even been mentioned in Greek philosophy. One early formal attempt to understand privacy is by Bates (1964). Interestingly, even in today’s research and philosophical arguments on privacy, the literature still portrays that there is disagreement on what privacy is and how it affects humans (Austin, 2003; Earp, Anton, Aiman-Smith, & Stufflebeam, 2005; Taylor, 2004). However, with the rise of personal computing, the Internet, and various other technologies like online social networks, the notion of privacy has become of major interest to researchers.

Personal privacy is customarily discussed as a concept in which individuals' ability to control the amount of data and/or communication that they would share with others. Research has indicated that anonymity is an important form of personal privacy and that it provides three functions related to privacy which are 1) recovery 2) catharsis and 3) autonomy (Pedersen, 1997).

Recovery is a sense of rejuvenation that involves active contemplation of one's situation and results in a sense of protection and rest with it being the most important factor associated with anonymity. Catharsis, on the other hand, is the unrestricted expression of thoughts and feelings to others. Autonomy is the chance to experiment with new behavior without the fear of social consequences (Pedersen, 1997).

These three functions can assist in understanding how anonymity affects human behavior during communication. In fact, these functions can be related back to the private and public self-awareness constructs discussed in the deindividuation theory. One can argue that recovery is closely related to private self-awareness and plays a role in assessing one's identity against their internal self-standards. On the other hand, one can argue that catharsis and autonomy can be related to the concept of public-self awareness since they both involve evaluating one's own self against the collective norms.

Anonymity at the group level

An influential group related social psychological concept is known as group polarization. A critical review of the literature performed by Isenberg (1986) is available on that subject matter. Isenberg (1986) explained that "Group polarization is said to occur when an initial tendency of individual group members toward a given direction is enhanced following group discussion" (p. 1). In other words, group polarization is the tendency of individuals to make decisions that are more extreme when in a group than when making decisions independently. In more recent literature, group polarization was shown to also occur in computer mediated communication (Lee, 2007) and is actually heightened in computer mediated communication due to the anonymity offered by computers (Sia, Tan. et al., 2002). Another group social psychological topic is social loafing.

Social loafing is the concept that individuals tend to work less hard when immersed in groups versus working alone. Social loafing is increased by anonymity (Short, Williams, & Christie, 1976). When people are submerged into a group, they tend to think that their responsibilities are decreased, thus causing the responsibility to diffuse amongst group members. One can argue that people work less hard when in a group because individuals may count on other group members to perform their task.

Anonymity at both the individual and group levels has been shown to have effects in classical face-to-face communication literature. Since computers presented humans with an innovative communication medium, the shift in the study of anonymity has transferred towards studying its effects in computer mediated environments. Most of the psychological concepts discussed in face-to-face communication have also been empirically tested in computer mediated situations. In the next section, a basic review of literature dealing with anonymity and computer mediated communication is presented.

Anonymity and computer mediated communication

Using a computer as a medium for communicating with others has become prevalent in society. With the increase in electronic payments, electronic voting, electronic auctions, e-mail and browsing (Diaz, Seys, Claessens & Perneel, 2002), it has become imperative to understand the effects of anonymity on computer usage. Contemplate how sending an e-mail or chatting online may differ from talking to someone face to face. Consider these questions: Have you told someone in an e-mail something you might have not been able to tell them in person? Have you been able to chat online with a total stranger without inhibiting certain feelings because they were not physically there? The philosophical consensus on this topic is that people feel more anonymous when using computers, in comparison to face-to-face communication environments (Christopherson, 2007).

Christopherson (2007) explains that physical appearance is an important social cue in social interactions and that people treat others differently based on gender, race, age, ethnicity, physical disability and attractiveness. Research indicates that these social cues are decreased in computing environments and that individuals are unable to project stereotypes, therefore behaviors based on those stereotypes are diminished (Christopherson, 2007). This led researchers to believe that individuals with less power in society (e.g., women, monitory groups) should have increased power in an online environment (Dubrovsky et al., 1991).

Hypothesizing that the Internet allows individuals to have equal social power is known as the equalization hypothesis (Dubrovsky et al., 1991). The overall principle of the equalization hypothesis stems from the proposition that people are more anonymous when using a computer when compared to face-to-face interactions due to the decrease in physical cues in that communication medium. This may be a reason why researchers like Froomkin (1995) and Tresca (1998) claim that anonymity is heightened in computing environments.

Another reason computer users may have the increased perception of being anonymous is that there may be no obvious way of relating the sending of a message to a user's real identity. Yet, this perception is somewhat misplaced. Consider the following quote:

> A relatively large amount of information can be gleaned from a person's e-mail address and Information Service Provider (ISP). For instance it is possible to (usually) identify a person's gender, country of origin, and workplace / occupation through an e-mail address like jim@hp.co.uk (Gackenbach, 1998, p.52)

From a technical perspective, networked computers use the Internet Protocol (IP) to communicate with each other. Casual Internet users often do not feel that someone's knowledge of their IP address is enough to find out information about their real identities. However, there are numerous ways to employ the use of an IP address to deduce the identity and location of a user through the use of software and data stored by Internet Service Providers (ISPs). Therefore, the perception of being anonymous when using a computer is not well-founded and may be attributed to the lack of technical knowledge possessed by casual computer users. However, the individual difference of technical knowledge even though noted, will not be discussed as it is outside the scope of this chapter. The deindividuation theory will be used as a plausible explanation for the perception of anonymity.

Philosophically, one can also use the various theories of deindividuation to explain anonymity in computer mediated environments, starting with Le Bon's crowd theory. For example, it can be argued that Internet usage has become ubiquitous - synonymous to people walking on the street, which Le Bon termed an "anonymous crowd". Under Le Bon's crowd theory, individuals are ultimately expected to abide by the collective group mind. Therefore, using his theory, computer users are expected to formulate a collective group mind and abide by the social norms imposed by it.

The concept of computer usage can also be explained using Festinger et al. (1952)'s theory. Once again, one has to make the assumption that Internet users are a crowd. If we examine the way people interact using computers for social networking, we can see that they are forming online groups, and becoming part of a larger group of interconnected users of social networks. If we take that perspective, then we can explain that Internet users are becoming part of a crowd, or a group. Consequently, one can explain that individuals using the Internet are not paid attention to as individuals, thus their inner restraints of moral controls are reduced causing them to lose their individuality and behave differently.

Any of the deindividuation theories can be used to philosophically explain people's behaviors in computing environments, however, the most significant empirical support seems to be for the SIDE theory. Numerous studies have examined face-to-face deindividuation and group theories in computer mediated environments, thus showing the effects of anonymity on computer users.

In one study, McKenna and Bargh (1998) focused on the effects of anonymous Internet news groups on gay and lesbians' self-acceptance. The study's results indicated that being part of an anonymous Internet group heightened self-acceptance and the probability of coming out to friends and family. This indicated that being anonymous on the Internet can pose some social advantages, showing that computer usage can be used to promote some prosocial behaviors.

Research has also indicated that group polarization exists in computer mediated communication. It was shown that group polarization is heightened in anonymous computing settings when compared to face-to-face communication environments (Sia et al., 2002). Lee (2007) also reinforced the notion that group polarization is present in computer mediated communication. In Lee's (2007) study, before individuals exchanged their opinions about social dilemmas with three ostensible partners via a computer, participants either shared some personal information (individuated) or not (deindividuated). The results indicated that deindividuation promoted group identification with the partners and induced greater opinion polarization, partly by heightening concerns about public evaluations (Lee, 2007).

There is a vast body of knowledge, including books and academic journals that extend face-to-face communication studies to computer mediated environments. Nevertheless, the body of knowledge relating anonymity and theories of deindividuation mostly to computer mediated communication is merely focused on computer interactions, not on deviant behaviors in computing environments. With the rise of computer usage, a parallel phenomenon known as cyber crime is evolving. The cyber crime phenomenon is associated with antisocial/deviant behaviors in computing environments. The theories relating to anonymity need to be extended, studied and tested in cyber crime related environments to objectively verify if and how anonymity affects cyber criminal behaviors.

Pre-employment integrity tests– one way of decreasing cyber crime

Integrity

The word integrity has Latin and French origins. The Latin origin of the word integrity is *integretatem* which means “Soundness, wholeness”. The French origin of the word is *integrité* which means “Wholeness, perfect condition”. Over the years, various philosophical explanations of what integrity is have been offered, and despite the simplistic definitions of integrity presented above, the concept of integrity can be quite perplexing. For instance, some literature examines integrity in terms of morals, i.e. one that acts with integrity acts morally. However, that may not be the case because people’s morals may be different from one another. To better understand integrity, the sections that follow will offer the philosophical stances of how integrity may be understood.

Integrity by self-integration

Integrity in this philosophical view is considered a matter of people integrating parts of their personality into an agreeable whole (Frankfurt, 1987). This philosophical view has had some criticisms, one of which was by Haflon (1989).

Haflon (1989) explained that the general concept of integrity is associated with honesty and sincerity. If one takes that into account, then the view offered by Frankfrut (1987) is not plausible. To illustrate that through the use of an example, a lawyer may truly and wholeheartedly be dedicated to proving a client's innocence. That lawyer may lie in order to prove a client's innocence while being fully integrated into their selves as explained by Frankfurt (1987), but failing to conform to the standard of honesty and sincerity explained by Haflon (1989). Haflon (1989) was not the only one to pose a critique to this philosophical view of integrity. Others like McFall (1987), Taylor (1981), and Calhoun (1995) offered other criticisms of this view as well.

Integrity by commitment

Another philosophical view of integrity is related to the concept of commitment. A person with integrity is said to hold true to their commitments by not engaging in any desires that break that commitment (Williams, 1981). These commitments have to also conform to one's self at which a person acting with integrity is acting in a way that reflects who they really are, especially in situations where core commitments are questioned (Williams, 1981). However, Calhoun (1995) explains that a person with integrity should act the same in all situations and contexts, and not only in certain situations.

Integrity as standing for something

Calhoun (1995) explained a view of integrity as a social integration and not an internal integration process, and is defined by one's relations to others. Calhoun (1995) explained that a person with integrity stands for something that is valuable and worth doing with relation to the community they are in. This view on integrity does not necessarily deal with morality.

Integrity as moral purpose

Haflon (1989) explains that people with integrity "Embrace a moral point of view that urges them to be conceptually clear, logically consistent, apprised of relevant empirical evidence, and careful about acknowledging as well as weighing relevant moral considerations. Persons of integrity impose these restrictions on themselves since they are concerned, not simply with taking any moral position, but with pursuing a commitment to do what is best."(Halfon 1989, p. 37).

Given the above explanation of integrity, we see that it is largely tied to the concept of moral purpose. However, criticisms can be made to this philosophical account of integrity. For instance, a person that does not persevere on a task having nothing to do with morals will be viewed as a person with no integrity, even though they simply did not complete a task. By reviewing the literature, the biggest critique to this philosophical view of integrity is that it is too narrow in scope, and integrity cannot be fully attributed to moral purpose.

Integrity as a virtue

This is perhaps the widest scope perspective on what integrity is (Cox, La Caze, Levine 2003, p. 41). Virtue is also known as moral excellence. What moral excellence is and how it is defined is associated with traits or qualities that are good. This view of integrity implicitly takes into account the abovementioned views but does not really limit itself to how they are organized.

Discussion

The philosophical literature integrity shows that there is no coherent explanation of what integrity means. Over the years, philosophers have debated on what integrity is and the different types of integrity. Nonetheless, the inconsistency amongst philosophers did not prevent social scientists in exploring ways to measure integrity. Social scientists have been eager to measure a person's integrity for many reasons. One notable reason is employment. Generally, institutions and corporations are not interested in hiring individuals with low integrity, because they might lie or steal on the job, not persevere in completing tasks, or not strive to be good people with excellent morals. In order to measure the integrity of people, integrity tests were created.

Integrity Tests

Pre-employment integrity tests aim at measuring the inclination of individuals to engage in counterproductive activities on the job (Sackett & Harris, 1985). Modern integrity tests are completed using paper and pencil when compared to the early tests that used a polygraph to measure integrity. Integrity tests have generally been developed for use with job applicants and employees. Originally they were designed to predict counterproductive behaviors only, but later research has shown that they helped in predicting variables such as supervisory ratings and employee performance (Ones et al., 1993).

Historical overview of integrity tests

Integrity tests have been used for a long time. The first paper and pencil integrity test was developed in 1948 and was called the Personnel Reaction Blank (Gough 1948). It focused on delinquency measures. In 1951, another scale was developed that focused on the honesty of individuals and was called the Reid Report. The Reid Report included questions that appeared to help in differentiating honest individuals from dishonest ones during polygraph tests. Since the Reid Report, many other scales were developed to measure the integrity of individuals, and a more comprehensive historical overview can be found in Woolley (1991).

Sackett and Harris (1985) indicated that many companies might be using integrity tests for screening about five million applicants on a yearly basis. As of 1997, there were 43 known integrity tests that were in use by industry, and since the use of the polygraph was banned in employment settings in 1988, the use and research in integrity tests has risen (Shmidt, et al., 1997).

Reviewing the literature on integrity tests between 1980 and 1997 illustrated that governmental agencies and psychologists took major interest in integrity testing during the abovementioned time period. This is illustrated in the extensive review on integrity testing performed by the U.S. Congressional Office of Technology Assessment (OTA,

1990) which was in part triggered by the Polygraph act in 1989. Another report was released by the American Psychological Association (APA) during the same time period on integrity testing (Schmidt et. al, 1997). The report by the APA provided a more favorable agreement with the use of integrity tests for employee selection (Schmidt et al., 1997).

There are different ways to measure integrity. One way of assessing integrity is through the use of interviews. However, the one gaining popularity is psychometric testing. Integrity psychometric measures are either overt or covert, but they are all self-reported.

In overt measures, respondents are asked directly about their honesty, criminal history, attitudes towards drug abuse, theft by others and general outlook on issues concerning integrity (Barrett, 2001). Overt measures have been proven to portray inferences with predictive validity and reliability (Wanek, 1999). Some of the overt tests ask responders to report about 74 past illegal and dishonest activities (Schmidt et al., 1997). Some of the most known integrity tests include:

- London House Personnel Selection Inventory (PSI) (London House, Inc. 1975)
- Employee Attitude Inventory (EAI) (London House, Inc., 1982)
- Stanton Survey (Klump, 1964),
- Reid Report (Reid Psychological Systems, 1951)
- Phase II Profile (Lousig-Nont, 1987)
- Milby Profile (Miller and Bradley, 1975)
- Trustworthiness Attitude Survey (Cormack & Strand, 1970).

Sackett et al. (1989) reported that the above tests yield quite similar results, and significant correlations are found amongst them (Ones, 1993).

The other type of integrity tests are covert measures. Sacket et al. (1989) explained that covert tests can help in distinguishing employee thieves from other employees. Covert measures are not immediately clear, and do not ask straight forward questions and are aimed at predicting a broad range of counterproductive behaviors at work such as violence, absenteeism, tardiness, drug abuse, alcohol use and theft. These tests usually examine personality traits such as reliability, conscientiousness, adjustment, trustworthiness, and sociability (Schmidt et al. 1997). Some of the most known covert measures used in integrity testing are:

- Personal Outlook Inventory (Science Research Associates, 1983)
- Personnel Reaction Blank (Gough, 1954)
- Employment Inventory (Paajanen, 1985)
- Hogan's Reliability Scale (Hogan, 1981).

To describe all the abovementioned tests is beyond the scope of this literature review. Detailed explanations of all the above tests can be found in the literature by (Sackett and Harris 1985; Sackett et al., 1989). Lastly, Rafilson and Frost (1989) argued that overt integrity tests are somewhat more reliable than covert measures.

It is noted in the research by Shaw et al. (1998) that pre-employment integrity screening can be one way of screening workers that are more likely to take part in insider threat activities. Insider threat has become closely related to cyber crimes with the rise of the Internet and technology. It then becomes important to test if the psychometric measures in pre-employment integrity may be used in order to predict individuals that are more likely to commit cyber crimes. This can, in turn, illustrate if the current predictors of integrity are applicable even to computer criminals.

Antisocial behavior

As noted in the literature review on anonymity, Diener (1979) and Zimbardo (1969) explained that anonymity may cause an increase in disinhibitive/antisocial behaviors (ASB)s. Zimbardo (1969) simply called them deindividuated behaviors, which are behaviors that deviate from the norm. Tresca (1998) also showed that this type of behavior exists in computer mediated environments and that anonymity induces these behaviors.

Despite the wide use of the term "antisocial behavior", there doesn't seem to be a coherent view on what antisocial behaviors are due to the concept's subjectivity. To simply state that they are behaviors that deviate from the norm requires us to define what a norm is, which is an arduous task. Nixon et al. (2003) explained that to properly determine antisocial behaviors one would have to take the following factors into account:

- Context
- Location
- Community tolerance
- Quality of life expectations

From the above list we can conclude that how we define antisocial behavior may differ from one location to another and from one culture to another. For example, something as simple as crossing your legs with the bottom of your shoe facing someone's face is regarded as an insulting antisocial behavior in Arab nations. However, in western localities, that behavior is not regarded as antisocial.

One widely accepted definition of antisocial behavior is the definition by the Crime and Disorder Act (1998). In that definition antisocial behavior is "Acting in a manner that caused or was likely to cause harassment, alarm or distress to one or more persons not of the same household as (the defendant)." The definition offered by the act does not focus on what constitutes antisocial behavior and turns its attention to consequences offered by those behaviors. One may criticize the Crime and Disorder Act (1998) definition as being too general. Armitage (2002) explains that the definition lacks specificity and measurability. Without identifying what constitutes antisocial behaviors, it would be difficult to study those specific behaviors and prevent them from occurring within a locality.

In a 2004 report issued by the Home Office Research Development and Statistics Directorate (RDS), a comprehensive typology of antisocial behavior was developed. The typology included three major types of antisocial behaviors a) Misuse of public space b) Disregard for community / wellbeing c) Acts directed at people and d) Environmental damage ("Defining and measuring antisocial behavior," 2004). Under each of these categories, the report listed numerous specific behaviors that would be regarded as antisocial behaviors.

The impact of antisocial behavior is still a major problem in today's society. The latest preliminary semi-annual report on crime in the United States released as a joint effort between the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ) shows the following crime data between 2008 and 2009 (“Crime in the United States,” 2009):

- 567,041 violent crimes
- 234,889 robberies
- 330,795 aggravated assaults
- 3,220,237 property crimes
- 694,142 burglary crimes
- 481,525 motor vehicle thefts

Even though the above data is only reported by cities with a population of 100,000 and over in the United States, the amount of crimes is staggering. The aforementioned crime types are closely related to our conceptual notion of antisocial behavior, and the study of antisocial behaviors should not cease due to its negative impact on our society and economy.

Operationalization of antisocial behavior

There are two major ways that researchers have attempted to operationlalize antisocial behavior a) Through categorical clinical syndromes and b) Through the legal concept of criminality and delinquency (Morgan & Lilenfeld, 2000).

Morgan and Lilenfeld (2000) explain that antisocial behavior has been operationalized in terms of categorical clinical syndromes such as antisocial personality disorder (ASPD) and conduct disorder (CD). Both of these syndromes are categorized by chronic irresponsible behavior, disregard for the rights of others, poor behavioral controls and an inability to conform to social norms (Morgan & Lilenfield, 2000).

Psychopathic personality has also been associated with antisocial behavior. Psychopathic personality includes features such as lack of remorse or sincerity, dishonesty, egocentricity and impoverished affective reactions (Morgan & Lilenfield, 2000). Some of the instruments that are used to measure Psychopathy are:

- Psychopathic Deviate scale of the Minnesota Multiphasic Personality Inventory (MMPI Pd; Hathaway & McKinley, 1942)
- The Socialization scale of the California Psychological Inventory (CPI So; Gough, 1994)
- Psychopathy Checklist-Revised (PCL and PCL-R; Hare, 1991)

One of the most current and reliable scientific instruments for measuring psychopathy is the Self-Reported Psychopathy Scale that was developed at the University of British Columbia in Canada, and has been widely recognized for its clear factor structure (Williams, Paulhus & Hare, 2005). One of the factor structures in the psychopathy measure is antisocial behavior. This instrument has been used on students and has yielded reliable results. This is also the instrument used as the self-reported antisocial behavior measure in this dissertation.

Antisocial behavior has also been examined through the legal concepts of criminality and delinquency, which encompass unlawful behaviors (Morgan & Lilenfield, 2000). Criminality and delinquency have been shown to be significantly correlated with the abovementioned clinical syndromes (Abram, 1989). Since antisocial behavior has been shown to be highly correlated with criminal offenses, one would also expect that it might be correlated to cyber crimes as well.

Even though researchers have been able to operationalize antisocial behavior, there is still debate on why people portray antisocial behavioral tendencies. Some research illustrates that there are biological influences associated with antisocial behavior (Lykken, 1995; Raine, 1993), some of which are genetics, prenatal and perinatal complications (Raine, Brennan, & Mednick, 1994), psychophysiological abnormalities (Raine, 1997), and differences in neurotransmitter functioning (Berman, Kavoussi, & Coccaro, 1997). Other research points out that antisocial behavior is affected by intelligence (Heilbrun, 1979; Heilbrun & Heilbrun,1985; Henry & Moffitt, 1997). Other theories have also taken a developmental perspective at stating that antisocial behavior is directly affected by family relations especially in terms of parent-child interactions (Patterson et al., 1990).

The literature review on anonymity suggested that antisocial behavior is induced by anonymity, and the literature review on antisocial behavior suggested that it could be measured in terms of criminal activities. It becomes important to test if antisocial behavior is linked to cyber criminal behaviors, and if anonymity affects that relationship.

Tying it all together

Katyal (2001) stated that one of the characteristics of the efficiency of cyber crime is that "Computers permit anonymity and secure communications" (p. 1042). Katyal (2003) also explained "One of the main reasons why crime is pervasive on the Internet is anonymity." (p. 2669). In a more recent news article, a United States Fish and Wildlife Service Special Agent Ed Newcomer explained "The Internet provides anonymity for everyone, and when we go online, the people we're after have no idea who we are" (Burton, 2007, p. 1). It was stated in the news article that cyber crime is increasingly becoming intertwined with wildlife crime as people are selling illegal wild life animals and other wild life related items over the Internet. Therefore, oddly enough, one can argue that the effects of anonymity are also being seen in Internet based wildlife crime.

As it was discussed in the literature review, anonymity may cause individuals to engage in antisocial activities, and individuals that are considered antisocial are characterized by dishonesty (low level of integrity). Therefore, to get a more comprehensive idea of how all these concepts are related, one would have to measure the cyber crime engagement of people, their antisocial behavioral tendencies and their integrity, while manipulating their anonymity. However, to understand the effect of anonymity on cyber criminals, one would first have to examine how anonymity is related to cyber crime.

Stating that anonymity affects cyber crime with no scientific proof is not sufficient and these concepts need to be first studied philosophically and tested scientifically. In fact, Katyal (2003) claims that there is little literature on the relationship of crime to the digital architecture (p. 2261). His claim still stands true today. In order to help make the leap towards a coherent understanding of cyber crime, one of the primary steps researchers have to take is the philosophical conception of how anonymity and deindividuation theory affect cyber criminal activities. In this section, the attempt to interrelate anonymity and the theories of deindividuation will be made. Then that relation will be applied to high-tech white collar crime and IT insider threat. How anonymity is related to the various deindividuation theories is summarized in Table 1.

Table 1. Anonymity and the deindividuation theories

Deindividuation theory	How anonymity is related
Le Bon (1895)	Anonymity is viewed as a mechanism resulting from an individual being submerged in a crowd. This mechanism causes the creation of a collective group mind, causing individuals to become mindless, thereby disobeying orders.
Festinger (1952)	Anonymity is viewed as a mechanism resulting from being submerged in a group, which lifts inner restraints on moral controls.
Zimbardo (1969)	Anonymity is viewed as an antecedent variable leading individuals to the engagement in behaviors in violation of established norms of appropriateness.
Diener (1980)	Anonymity is viewed as a mechanism resulting from being submerged in a group, which removes objective self awareness, thereby allowing individuals to lose their internalized self-standards. The decrease in internalized self standards therefore causes individuals to be affected by environmental stimuli.
Postomes et al. (1998)	Anonymity is viewed as a mechanism that drives two functions. Primarily, anonymity affects the individual's identification with a group (cognitive component). Secondly, anonymity can be used as a mean to reach certain ends by the individual (strategic component).

With the various accounts for the effects of anonymity on behavior, one may use these rationales to foster a better understanding of the effects on both high-tech white collar crime and the IT insider threat problem. Primarily, high-tech white collar crime and IT insider threats can either be individualistic or organized. One can argue that even when a cyber crime is committed strictly by one individual, that individual is still submerged in groups (e.g., internet users, corporate employees, hackers). If the premise that an individual is immersed in a group is made, one can consider the various deindividuation theories and relate anonymity to high-tech collar crime and IT insider crimes.

Using the concept offered by Le Bon (1895), one would simply explain that being part of a computing environment drives an individual to form a collective mind. Having a collective mindset makes people mindless, causing them to defy the law and engage in high-tech white collar crimes or illicit insider IT crimes. If the theory proposed by Festinger (1952) is used, then the claim can be made that anonymity drives the lifting of inner restraints of moral controls, thus causing individuals to perform high-tech white collar crimes or illicit insider IT crimes.

Zimbardo (1969), on the other hand, would view anonymity as an antecedent variable that would cause individuals to engage in high-tech white collar crime or illicit insider IT crimes. When mapping back anonymity as a construct to insider threat theory proposed by Anderson et al. (2000), one may also note that anonymity could be hypothesized as a trigger that may increase the chances of IT insider threat activities, or increase the opportunity of IT insider threat to occur.

Using the Diener (1980) theory of deindividuation, one may explain that anonymity removes objective self awareness, thereby allowing people to lose their internalized self standards. The decrease in internalized self standards causes individuals to be affected by environmental stimuli. If individuals were in environments with stimuli promoting criminal activities, one would expect criminal behavior outcomes in both high-tech white collar crime and IT insider crimes.

Finally, if one were to use the anonymity concept proposed by Postomes et al. (1998), one could argue that anonymity affects the individual's identification with a group. As stated before, the SIDE theory inherits from the social identity theory stating that a person has more than one identity, which is dependent on that individual's group membership. How the individual perceives him/herself as part of the group will ultimately affect that individual's behavior. This notion is parallel to what Anderson et al. (2000) explain on the preconditions of insider threat. If a person feels alienated from the group for various reasons (like not getting a raise compared to other employees), that individual may feel disassociated from the group, thus increasing the probability of engagement in illicit insider crimes. Additionally, if the group identity promotes criminal activities, individuals are more likely to commit high-tech white collar crimes or insider IT crimes.

The situation an individual is placed in plays a major role in dictating behavioral outcomes. The author notes an analogy between the situational concept proposed by the SIDE theory and the trigger concept proposed by Anderson et al. (2000) for preconditions of insider threat. Both of the concepts focus on situational events that individuals may be placed in, possibly pushing them to behave differently. Lastly, Postomes et al. (1998) also argue that anonymity can be used by individuals as means of strategically acquiring what they want, thus, under the SIDE theory, individuals may also use anonymity as a tactical method for performing high-tech white collar crimes or IT insider crimes.

All the theories on deindividuation and anonymity form plausible philosophical explanations for how high-tech white collar crimes and IT insider threat crimes may occur. However, due to the lack of scientific literature in this area, the author cannot predict which theory provides the most precise, plausible explanation for how anonymity is associated to high-tech white collar crime and IT insider threat.

Summary

Even after decades of research on deindividuation, there is still disagreement amongst researchers on the effects of those theories on human behavior. Nevertheless, at the heart of all the theories is the phenomenon of anonymity. One can use the existing deindividuation theories to foster a more complete understanding of how anonymity and cyber crimes are interrelated. It is imperative for scientists to take a step toward understanding how the theories of deindividuation and cyber crime are interrelated, especially in the areas of high-tech white collar crimes and IT insider threat crimes, since they have a detrimental impact on today’s society. Rogers (2001) explained that personality traits and situational factors of cyber criminals should be studied to foster a better understanding of computer criminals.

The literature review illustrated that anonymity is prevalent in cyber environments, and that it enables antisocial behaviors. Therefore, studying the relationship in experimental settings between antisocial behaviors, anonymity and cyber crime becomes essential. Additionally, Shaw et al. (1998) concluded that pre-employment integrity screening should be used as a safeguard to mitigate the amount of IT insider threat – which is a prevalent type of cyber crime. Consequently, it is imperative to investigate the relationship between pre-employment integrity and cyber crime engagement.

CHAPTER 3 - METHODOLOGY

This experimental 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 positive relationship between self-reported cyber crime (CCI) and self-reported antisocial behavior (ASB).

H3: There is a negative relationship between self-reported cyber crime (CCI) and self-reported pre-employment integrity (PPI).

H4: There is a negative relationship between self-reported cyber crime and self-reported antisocial behavior.

H5: Anonymity and self-reported antisocial behavior (ASB) can predict self-reported cyber crime (CCI).

H6: There is an interaction between self-reported antisocial behavior (ASB) and anonymity when predicting self-reported cyber crime (CCI).

H7: Anonymity and self-reported pre-employment integrity (PPI) can predict self-reported cyber crime (CCI).

H8: There is an interaction between self-reported pre-employment integrity (PPI) and anonymity when predicting self-reported cyber crime (CCI).

H9: There is an interaction between self-reported antisocial behavior and self-reported pre-employment integrity when predicting self-reported cyber crime.

Constructs

The theoretical constructs are presented in Figure 2. In this study, there were three predictors which comprised of one independent variable (anonymity), and two variables of interest (self reported antisocial behaviors and self reported pre-employment integrity). The dependent variable was self-reported cyber crime.

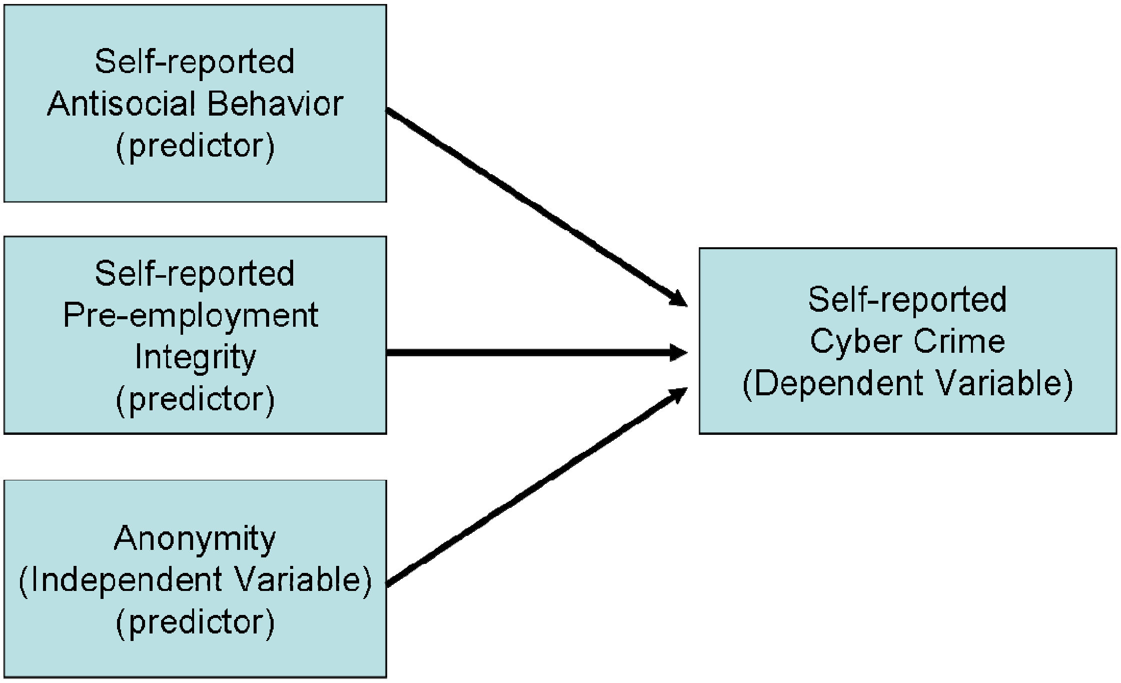

Self-reported Antisocial Behavior (predictor)
Self-reported Pre-employment Integrity (predictor)
Anonymity (Independent Variable) (predictor)
Self-reported Cyber Crime (Dependent Variable)

Figure 2. Theory Diagram

Self-reported antisocial behavior

The self-reported measure of antisocial behavior was extracted from the Self Reported Psychopathy (SRP) scale that has been effectively used on a college population before. It was developed by Paulhus at the University of Biritsh Columbia in Canada and is well recognized for its clear factor structure. The scale contains four sub-scales 1) Interpersonal Manipulation 2) Callous Affect 3) Erratic Lifestyle 4) Antisocial behavior. Due to the scale's clear factor structure, the antisocial self-reported subscale was extracted and used in this study. It included sixteen Likert items and produced a reliable Chronbach's alpha of .78 (See Table 5).

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 Personal Inventory Scale (PSI-7ST), contains twenty seven Likert items and produced a reliable Chronbach's alpha of .78 (See Table 3). 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 Purdue 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 fool 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. The manipulation check was a one Likert scale item "I am anonymous when using this computer".

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. In a doctoral dissertation, 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. The scale produced a reliable Chronbach's alpha of .78 (See Table 4).

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 3 and 4 respectively.

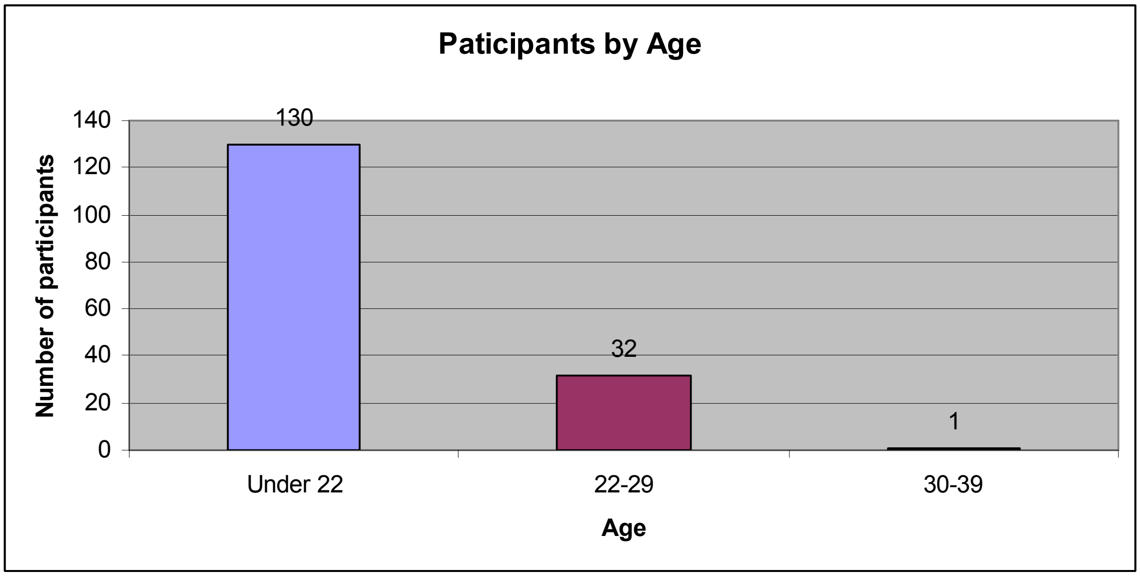


Figure 3. Participants by Age

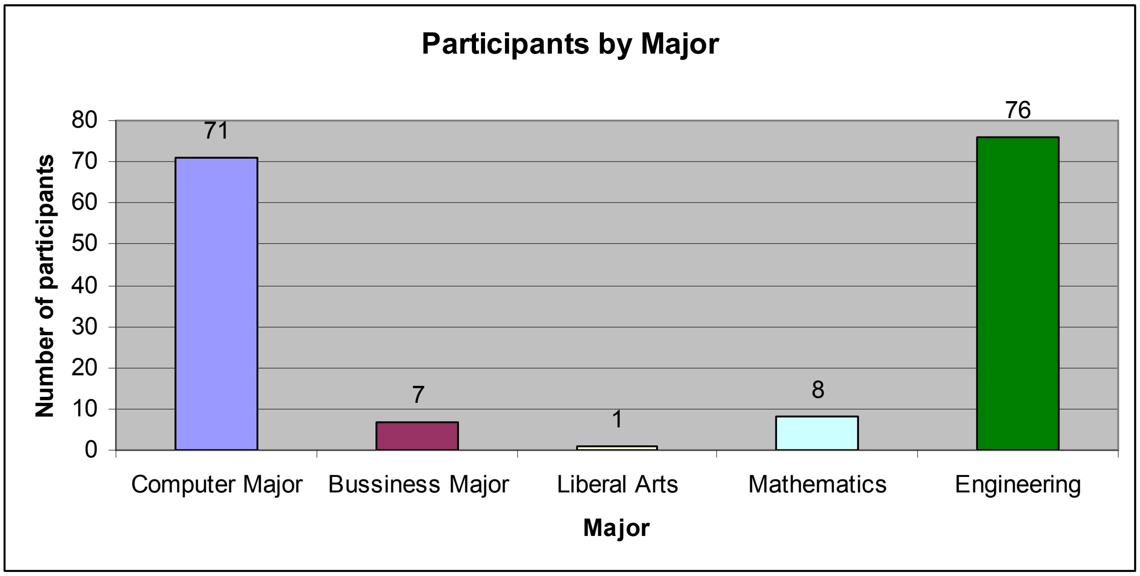


Figure 4. Participants by Major

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 (see 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 researcher was 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

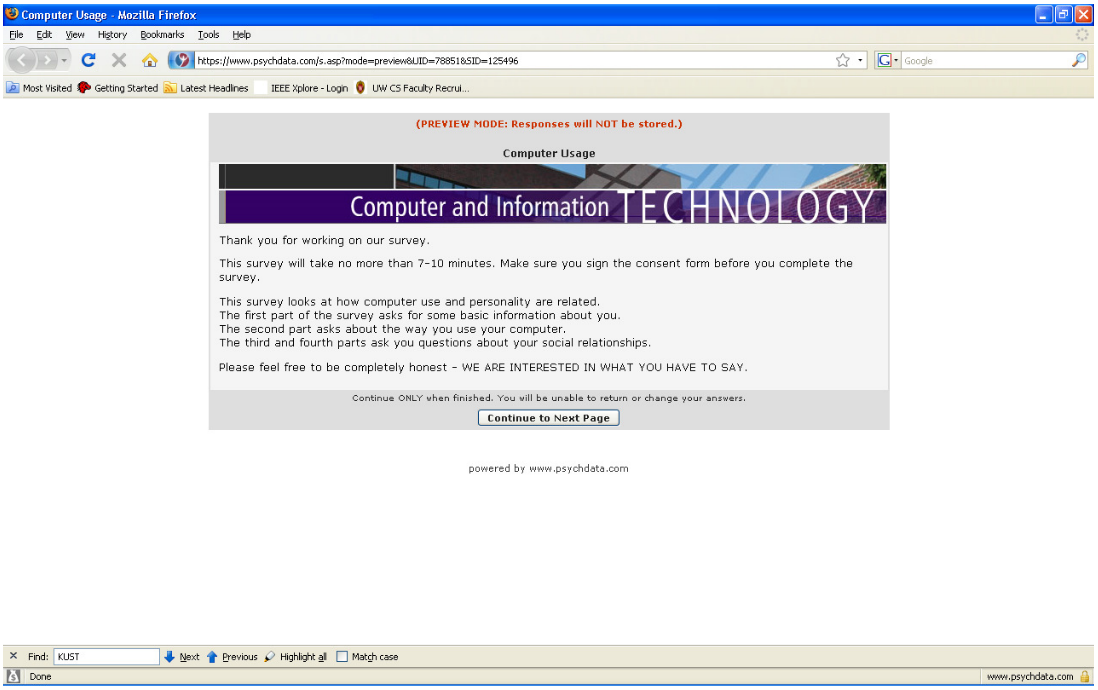
This study's research protocol included the following steps in order:

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 (See Appendix D) 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 5 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 6. The instructions on this page explained to the participant to open and fill out the form displayed in Figure 7. The form in Figure 7 asked the participants to submit their name, e-mail address and address. This served as the computer group’s anonymity manipulation.


Computer Usage - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.psychdata.com/s.asp?mode=preview&UID=78851&SID=125496
Google
Most Visited Getting Started Latest Headlines IEEE Xplore - Login UW CS Faculty Recrui...
Computer and Information TECHNOLOGY
Find: KUST Next Previous Highlight all Match case
Done
www.psychdata.com

(PREVIEW MODE: Responses will NOT be stored.)

Computer Usage

Thank you for working on our survey.

This survey will take no more than 7-10 minutes. Make sure you sign the consent form before you complete the survey.

This survey looks at how computer use and personality are related.
The first part of the survey asks for some basic information about you.
The second part asks about the way you use your computer.
The third and fourth parts ask you questions about your social relationships.

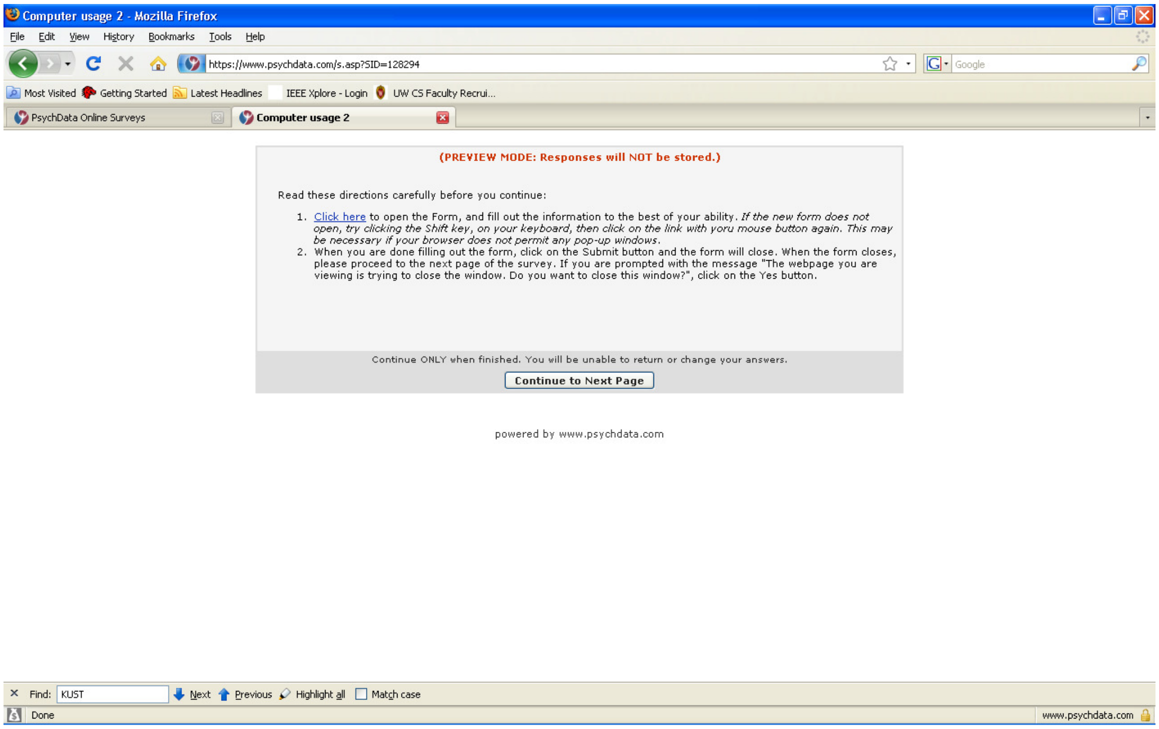
Please feel free to be completely honest - WE ARE INTERESTED IN WHAT YOU HAVE TO SAY.

Continue ONLY when finished. You will be unable to return or change your answers.

Continue to Next Page

powered by www.psychdata.com

Figure 5. First page of survey


Computer usage 2 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.psychdata.com/s.asp?SID=128294
Google
Most Visited Getting Started Latest Headlines IEEE Xplore - Login UW CS Faculty Recrui...
PsychData Online Surveys
Computer usage 2
Find: KUST Next Previous Highlight all Match case
Done
www.psychdata.com

(PREVIEW MODE: Responses will NOT be stored.)

Read these directions carefully before you continue:

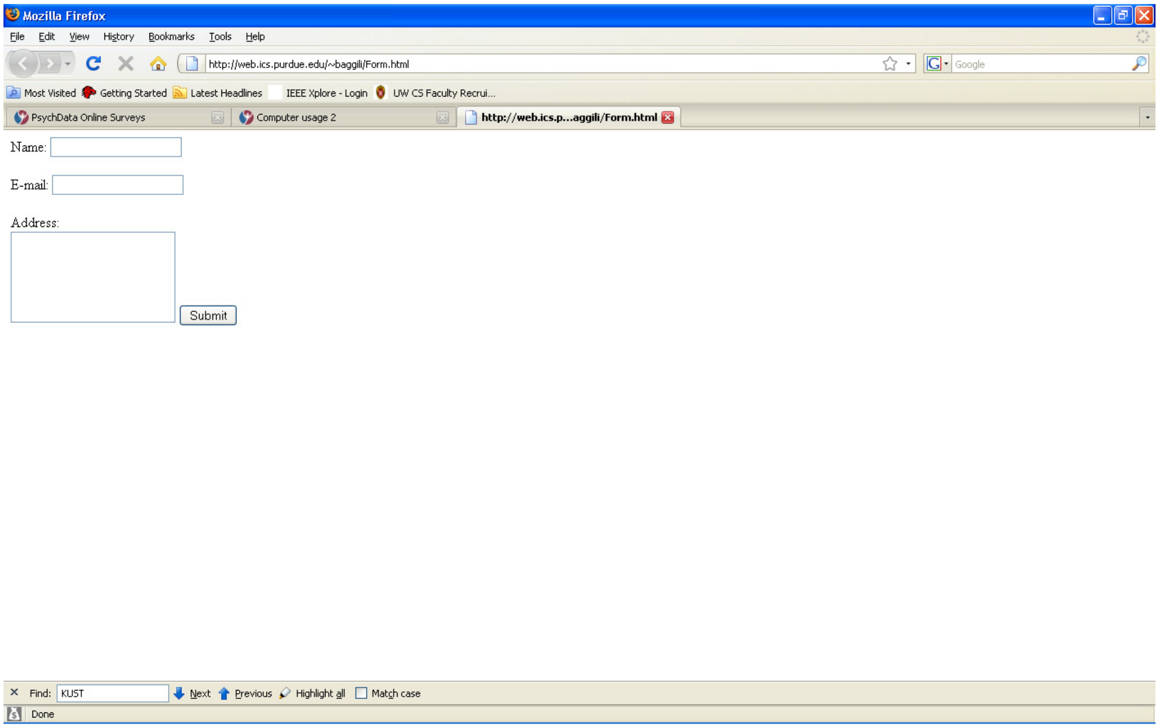
1. Click here to open the Form, and fill out the information to the best of your ability. *If the new form does not open, try clicking the Shift key, on your keyboard, then click on the link with yoru mouse button again. This may be necessary if your browser does not permit any pop-up windows.*
2. When you are done filling out the form, click on the Submit button and the form will close. When the form closes, please proceed to the next page of the survey. If you are prompted with the message "The webpage you are viewing is trying to close the window. Do you want to close this window?", click on the Yes button.

Continue ONLY when finished. You will be unable to return or change your answers.

Continue to Next Page

powered by www.psychdata.com

Figure 6. Computer Group



Name:

E-mail:

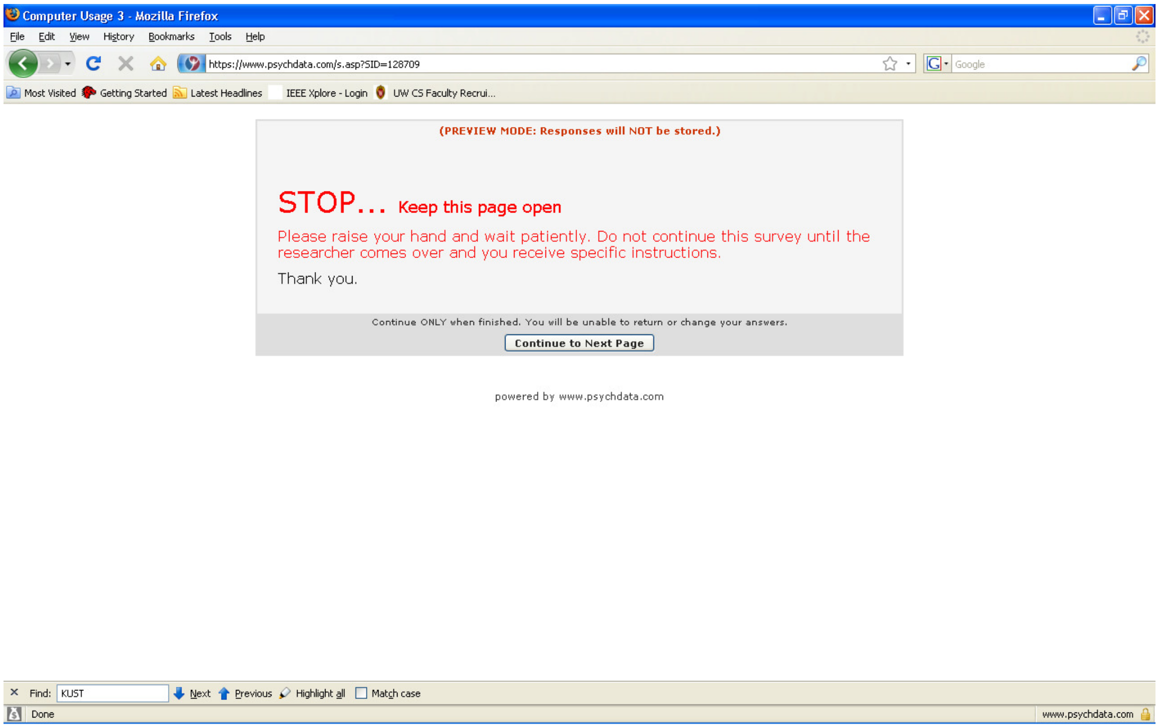
Address:

Submit

Find: KUST

Figure 7. Anonymity Manipulation Form

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 8 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.”


Computer Usage 3 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.psychdata.com/s.asp?SID=128709
Google
Most Visited Getting Started Latest Headlines IEEE Xplore - Login UW CS Faculty Recrui...
Find: KUST Next Previous Highlight all Match case
Done
www.psychdata.com

(PREVIEW MODE: Responses will NOT be stored.)

STOP... Keep this page open

Please raise your hand and wait patiently. Do not continue this survey until the researcher comes over and you receive specific instructions.

Thank you.

Continue ONLY when finished. You will be unable to return or change your answers.

powered by www.psychdata.com

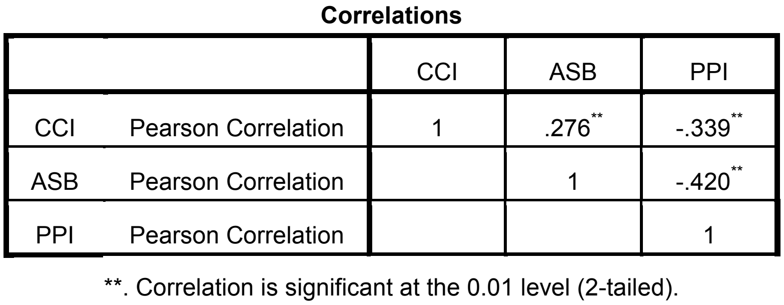
Figure 8. ID Manipulation

Construct validity and reliability

Construct validity

Construct validity deals with how well the constructs of the study were operationalized. Convergent validity is one way of illustrating construct validity (Trochim & Donlley, 2007). Convergent validity refers to the ability to illustrate high correlations between theoretically similar constructs. In this research study, one would expect to see a significant correlation between self-reported antisocial behavior, self-reported cyber crime and self-reported pre-employment integrity. This is illustrated in the zero-ordered correlation matrix in Table 2. The results shown in Table 2 indicate that there is a significant relationship amongst the variables thereby suggesting a high level of convergent and construct validity.

Table 2. Zero ordered correlation



Correlations

		CCI	ASB	PPI
CCI	Pearson Correlation	1	.276**	-.339**
ASB	Pearson Correlation		1	-.420**
PPI	Pearson Correlation			1

**. Correlation is significant at the 0.01 level (2-tailed).

Key: CCI = Cyber crime engagement, ASB = Antisocial behavior, PPI = Pre-employment integrity

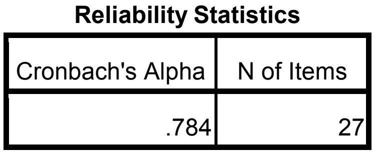
External validity & face validity

Since this dissertation project is a first attempt at looking at the interaction between CCI, ASB and PPI it does not have a strong face and external validity. In order to gain that validity, this research would have to be repeated. If the results obtained by other researchers are similar then this research will gain both external and face validity.

Reliability

The reliability of a study refers to the ability to obtain similar results if a study was conducted multiple times. The most accepted method of assessing the reliability of measures is by assessing the Cronbach's alpha of a measurement. By convention, if the Cronbach's alpha is > 0.7 then the measurement is deemed reliable. In this study, all the survey instruments resulted in a Chronbach's alpha greater than 0.7, thereby suggesting a reasonable reliability. The reliability measures are shown in Tables 3, 4 and 5.

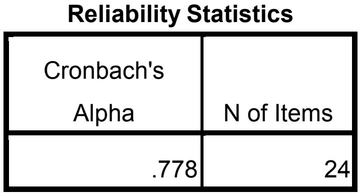
Table 3. The Reliability of the Pre-employment Integrity Measure



Reliability Statistics

Cronbach's Alpha	N of Items
.784	27

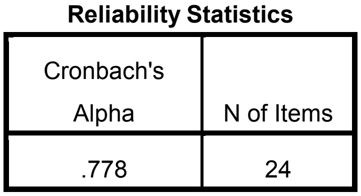
Table 4. The Reliability of the Cyber Crime Engagement Measure



Reliability Statistics

Cronbach's Alpha	N of Items
.778	24

Table 5. The Reliability of the Antisocial Behavior Measure



Reliability Statistics

Cronbach's Alpha	N of Items
.778	24

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. 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 H2, H3 and H4, Pearson's correlation was used. To test predictions and interactions in H5, H6, H7, H8 and H9, General Linear Modeling (GLM) was used.

CHAPTER 4 – RESULTS

Descriptive statistics

Before the data exploration process was started, incomplete responses were deleted. The original data comprised of 201 participants randomly assigned to three groups (Group 1 = 69, Group 2 = 67 and Group 3 = 65). After the incomplete responses were deleted the number of participants decreased to 163 (Group 1 = 61, Group 2 = 57 and Group 3 = 45). In this study, Group 1 is the control group, Group 2 is the computer group and Group 3 is the ID group. It is important to note that all the data will be reported without the exclusion of outliers. The variables measured in this study are related to behaviors that deviate from the norm (antisocial behaviors, computer crime engagement and personal integrity). It is assumed that people may portray varying and extreme self-reported scores on these self-reported measurements due to the nature of the construct being measured. Therefore, an assumption is made that if individuals self-report extreme cases of these measurements, that these cases are part of the normal population. The research also re-checked the coding of the surveys to insure that that the outliers were not a result to coding errors.

Exploratory data analysis for all cases

In this section, the combined descriptive statistics for all groups are reported. First, the test of homogeneity of variance is reported. Next, the normality Q-Q plots for all the self-reported measures are reported. Lastly, outliers are revealed using Box Plots.

The results obtained using Levene's test of homogeneity of variance is shown in Table 6. In Table 6, all the variables Cyber/Computer Crime Index (CCI), Antisocial Behavior (ASB) and Pre-employment Integrity (PPI) portray a large insignificance. Since p > 0.05 for all of the variables, this indicates that the requirement for the homogeneity of variance is met.

Table 6. Levene's Test

		Levene Statistic	df1	df2	Sig.
CCI	Based on Mean	.019	2	160	.981
	Based on Median	.036	2	160	.964
	Based on Median and with adjusted df	.036	2	159.045	.964
	Based on trimmed mean	.023	2	160	.977
ASB	Based on Mean	1.820	2	160	.165
	Based on Median	1.341	2	160	.264
	Based on Median and with adjusted df	1.341	2	130.308	.265
	Based on trimmed mean	1.542	2	160	.217
PPI	Based on Mean	.009	2	160	.991
	Based on Median	.002	2	160	.998
	Based on Median and with adjusted df	.002	2	147.660	.998
	Based on trimmed mean	.007	2	160	.993

Key: CCI = Cyber crime engagement, ASB = Antisocial behavior, PPI = Pre-employment integrity

As for the overall participant statistics for the self-reported measures CCI, PPI and ASB, the results are shown in Table 7.

Table 7. Descriptive Statistics for all cases

		Statistic	Std. Error
CCI	Mean	35.9202	.65688
	Median	36.0000	
	Variance	70.333	
	Std. Deviation	8.38648	
	Minimum	24.00	
	Maximum	60.00	
ASB	Mean	25.0920	.60844
	Median	24.0000	
	Variance	60.343	
	Std. Deviation	7.76810	
	Minimum	16.00	
	Maximum	56.00	
PPI	Mean	105.2699	.83982
	Median	107.0000	
	Variance	114.964	
	Std. Deviation	10.72211	
	Minimum	61.00	
	Maximum	130.00	

Key: CCI = Cyber crime engagement, ASB = Antisocial behavior, PPI = Pre-employment integrity

Next, to illustrate the normality of the population for the three measures, the Q-Q plots are reported. As one can see in Figure 9, the CCI measure is normal since most cases are close to line of best fit. By looking at Figure 10, one can reasonably conclude that the data for ASB are reasonably normal since many of the cases lie close to the line of best fit. Finally, by looking at Figure 11, a conclusion can be made that the data for PPI is roughly normal since most cases lie close to the line of best fit. For all these self-reported measures, some of the extreme cases observed may be due to the nature of the variable being measured since this study deals with non-normative individual differences/personality measures. These extreme cases (outliers) are reported in the Box Plots shown in Figures 12, 13 and 14 for the variables CCI, ASB and PPI respectively.

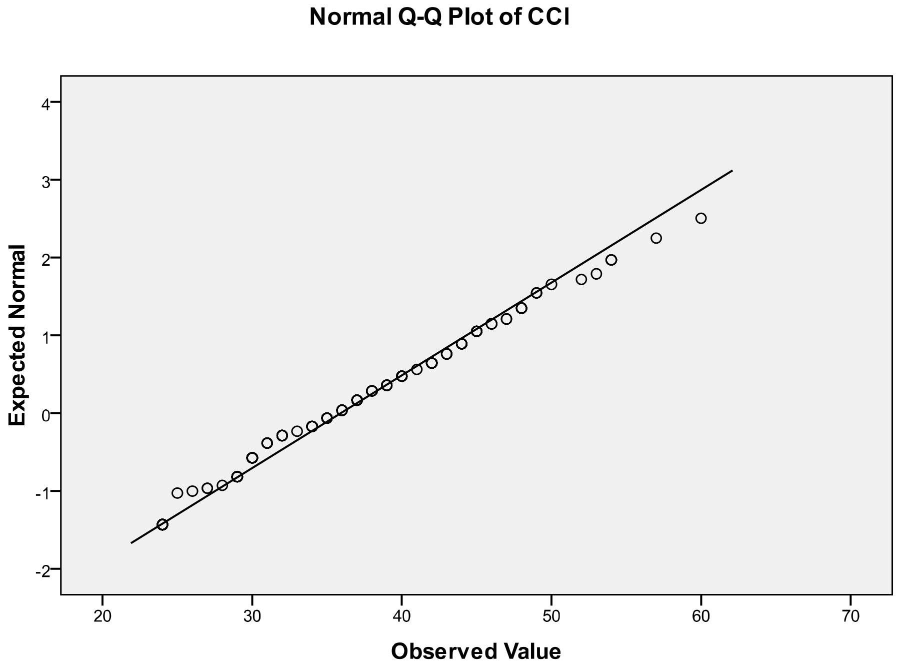


Figure 9. Q-Q Plot for cyber crime engagement

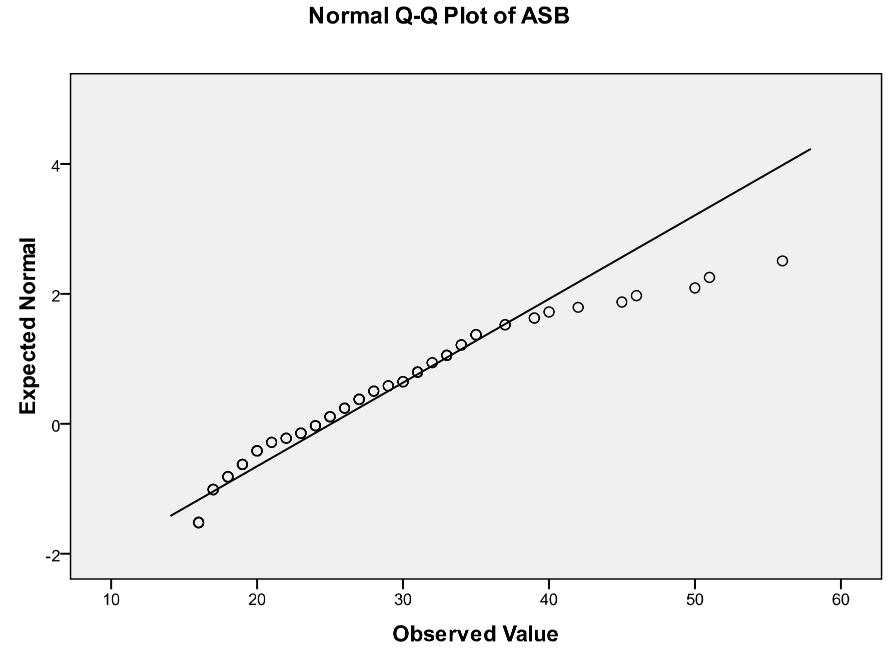


Figure 10. Q-Q Plot for antisocial behavior

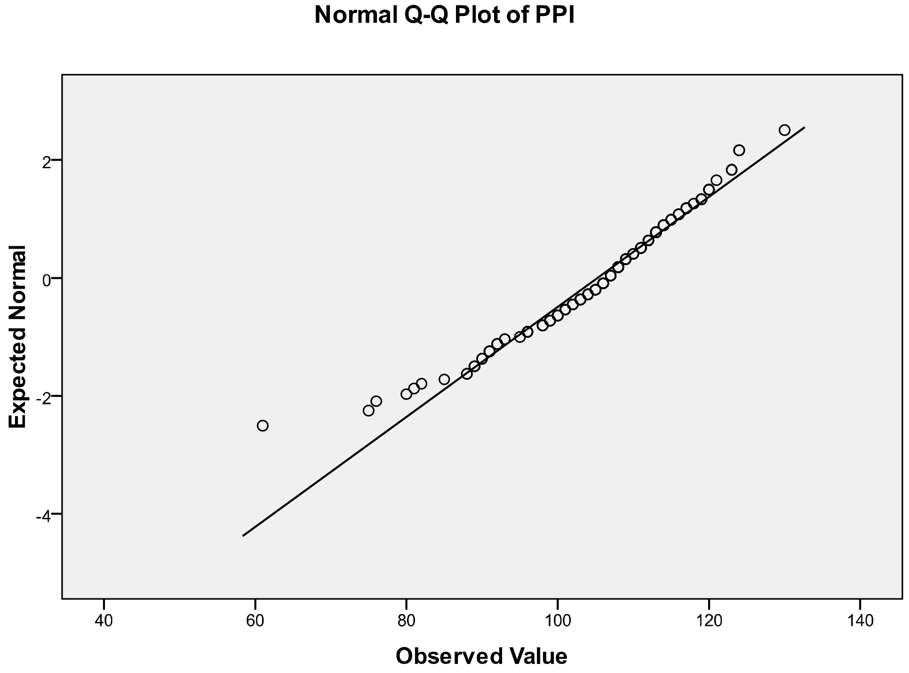


Figure 11. Q-Q Plot for pre-employment integrity

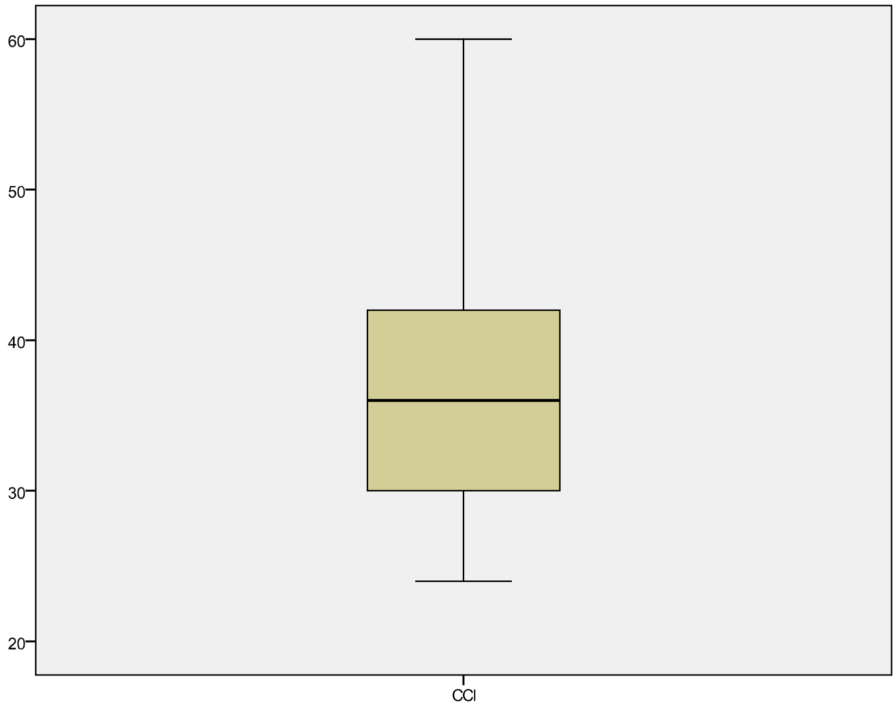


Figure 12. Box Plot for cyber crime engagement

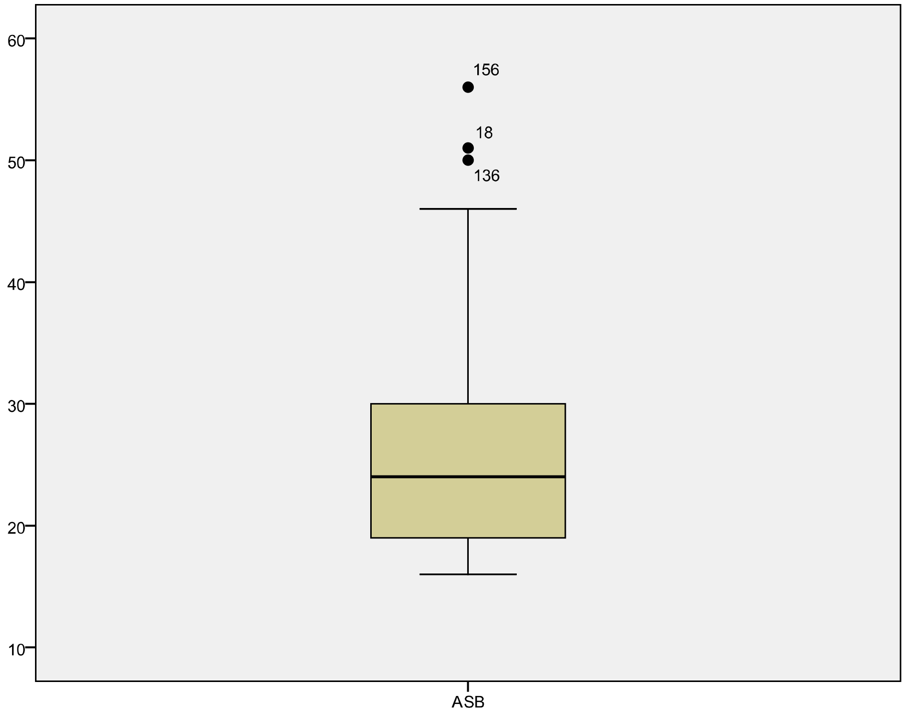


Figure 13. Box Plot for antisocial behavior

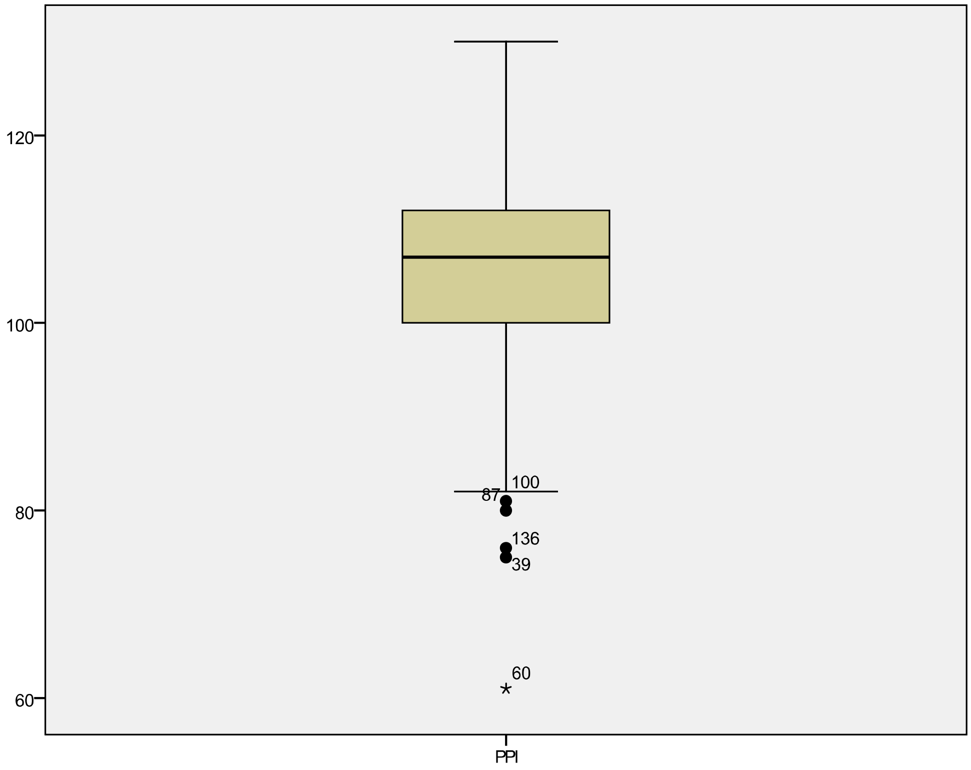
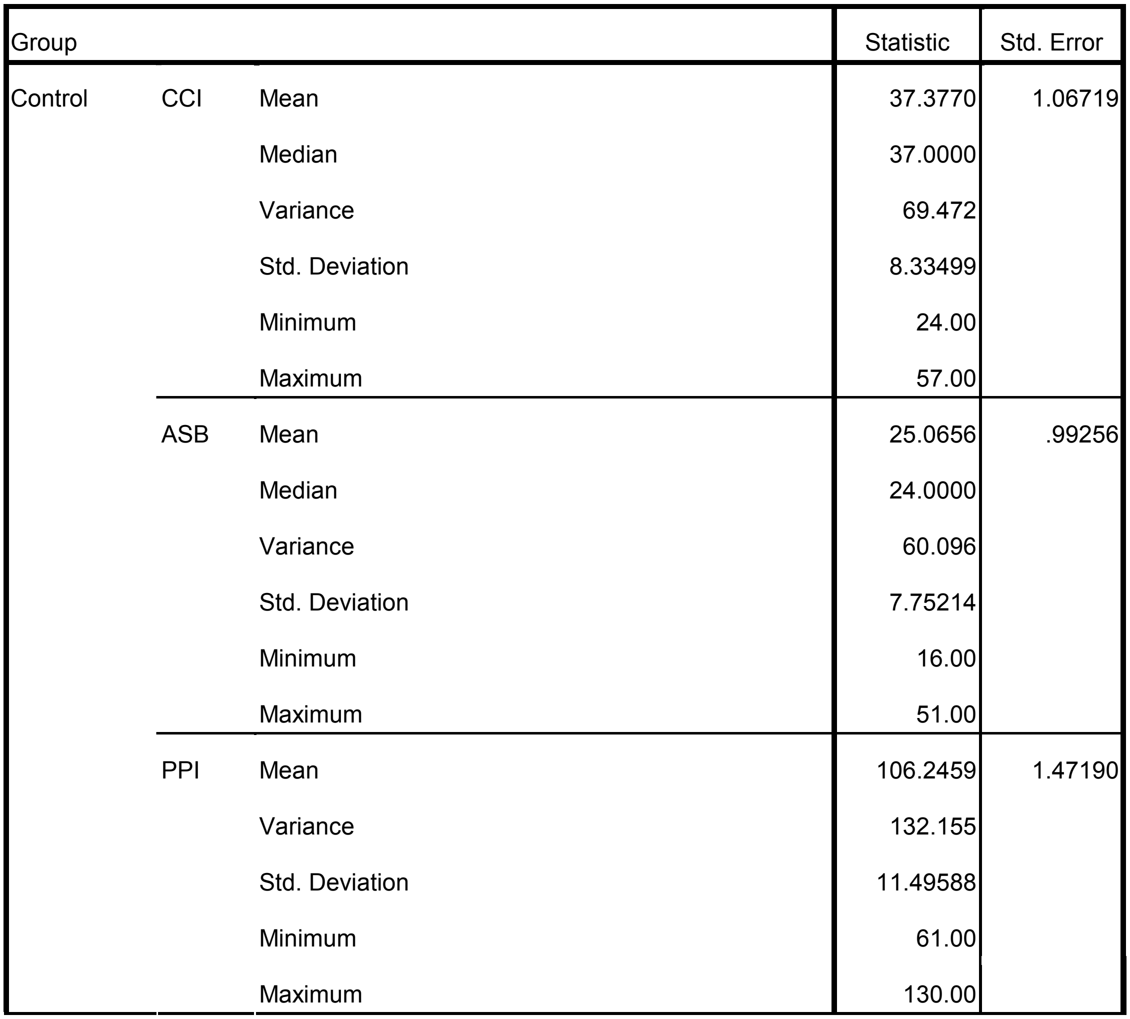


Figure 14. Box Plot for pre-employment integrity

Exploratory data analysis for control group (Group 1)

In this section, descriptive statistics for CCI, ASB and PPI are reported. Then, the Q-Q plots are shown to establish normality. Next, Box Plots are reported to illustrate the extreme cases for CCI, ASB and PPI.

Table 8. Descriptive Statistics for Control Group



Group			Statistic	Std. Error
Control	CCI	Mean	37.3770	1.06719
		Median	37.0000	
		Variance	69.472	
		Std. Deviation	8.33499	
		Minimum	24.00	
		Maximum	57.00	
	ASB	Mean	25.0656	.99256
		Median	24.0000	
		Variance	60.096	
		Std. Deviation	7.75214	
		Minimum	16.00	
		Maximum	51.00	
	PPI	Mean	106.2459	1.47190
		Variance	132.155	
		Std. Deviation	11.49588	
		Minimum	61.00	
		Maximum	130.00	

Key: CCI = Cyber crime engagement, ASB = Antisocial behavior, PPI = Pre-employment integrity

Table 9. Q-Q Plots for Control Group

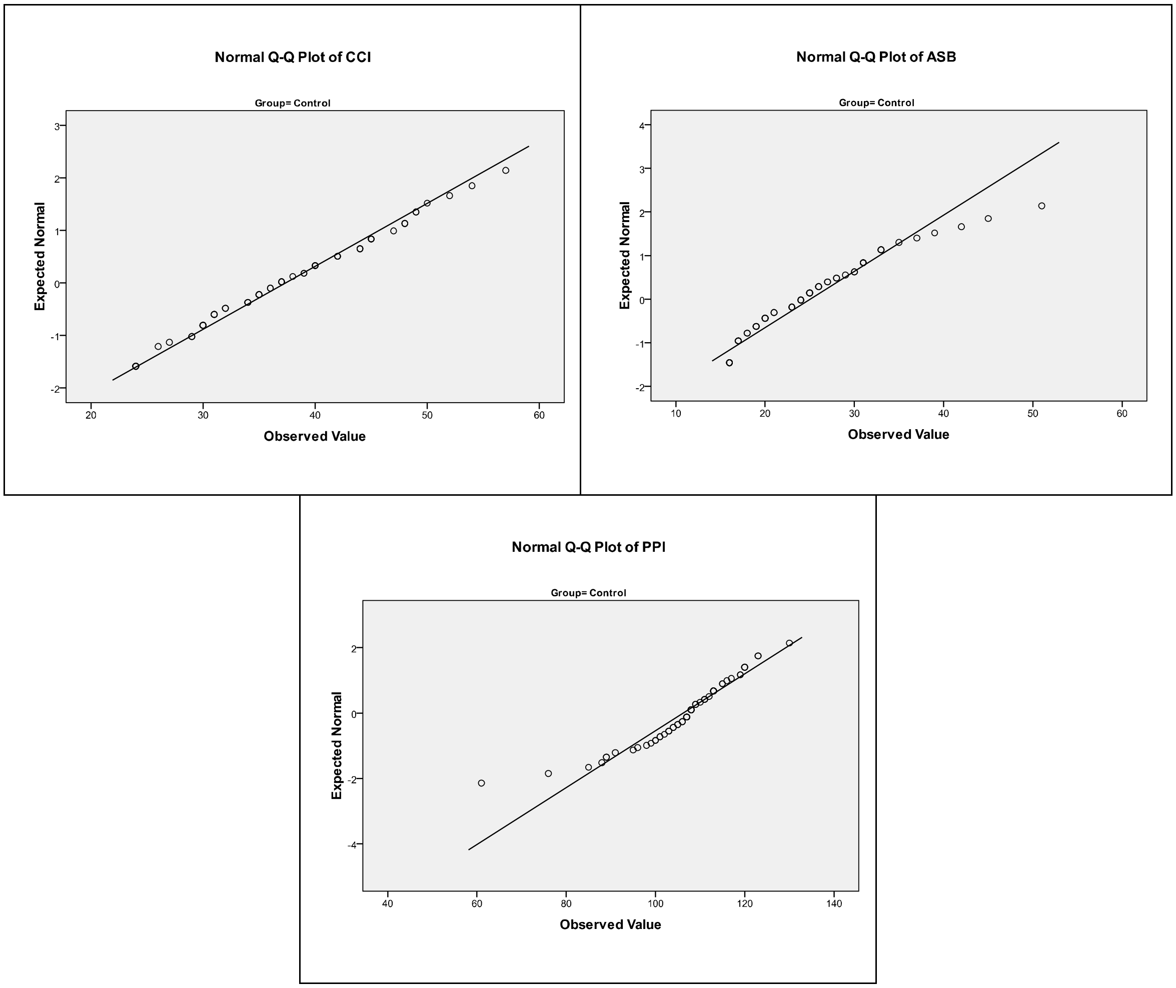
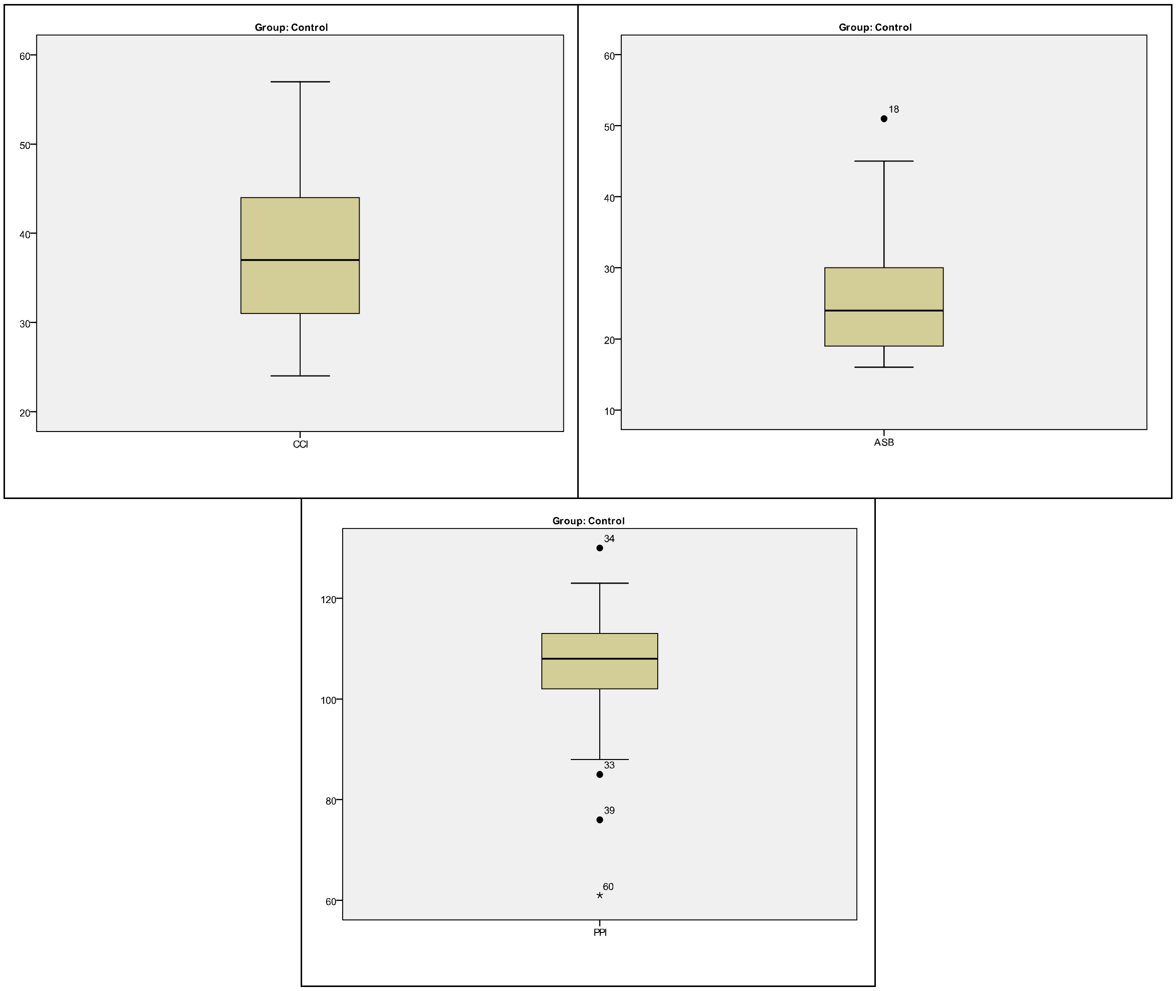


Table 10. Box Plots for Control Group



Exploratory data analysis for computer group (Group 2)

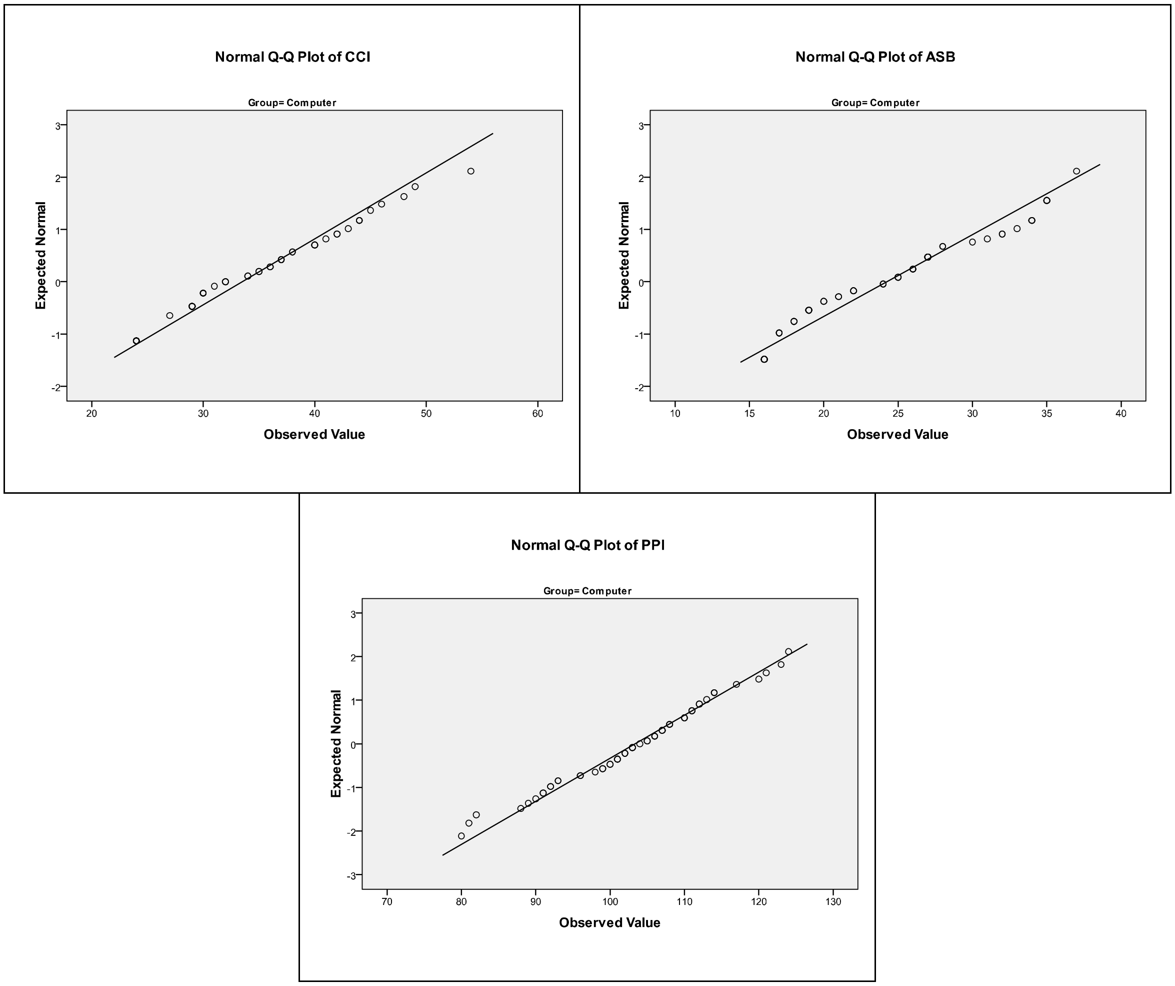
In this section, descriptive statistics for CCI, ASB and PPI are reported. Then, the Q-Q plots are shown to establish normality. Next, Box Plots are reported to illustrate the extreme cases for CCI, ASP and PPI.

Table 11. Descriptive Statistics for Computer Group

Computer	CCI	Mean	33.5088	1.04956
		Median	32.0000	
		Variance	62.790	
		Std. Deviation	7.92402	
		Minimum	24.00	
		Maximum	54.00	
	ASB	Mean	24.2632	.84646
		Median	24.0000	
		Variance	40.840	
		Std. Deviation	6.39064	
		Minimum	16.00	
		Maximum	37.00	
	PPI	Mean	103.3684	1.33950
		Median	104.0000	
		Variance	102.273	
		Std. Deviation	10.11299	
		Minimum	80.00	
		Maximum	124.00	

Key: CCI = Cyber crime engagement, ASB = Antisocial behavior, PPI = Pre-employment integrity

Table 12. Q-Q Plots for Computer Group

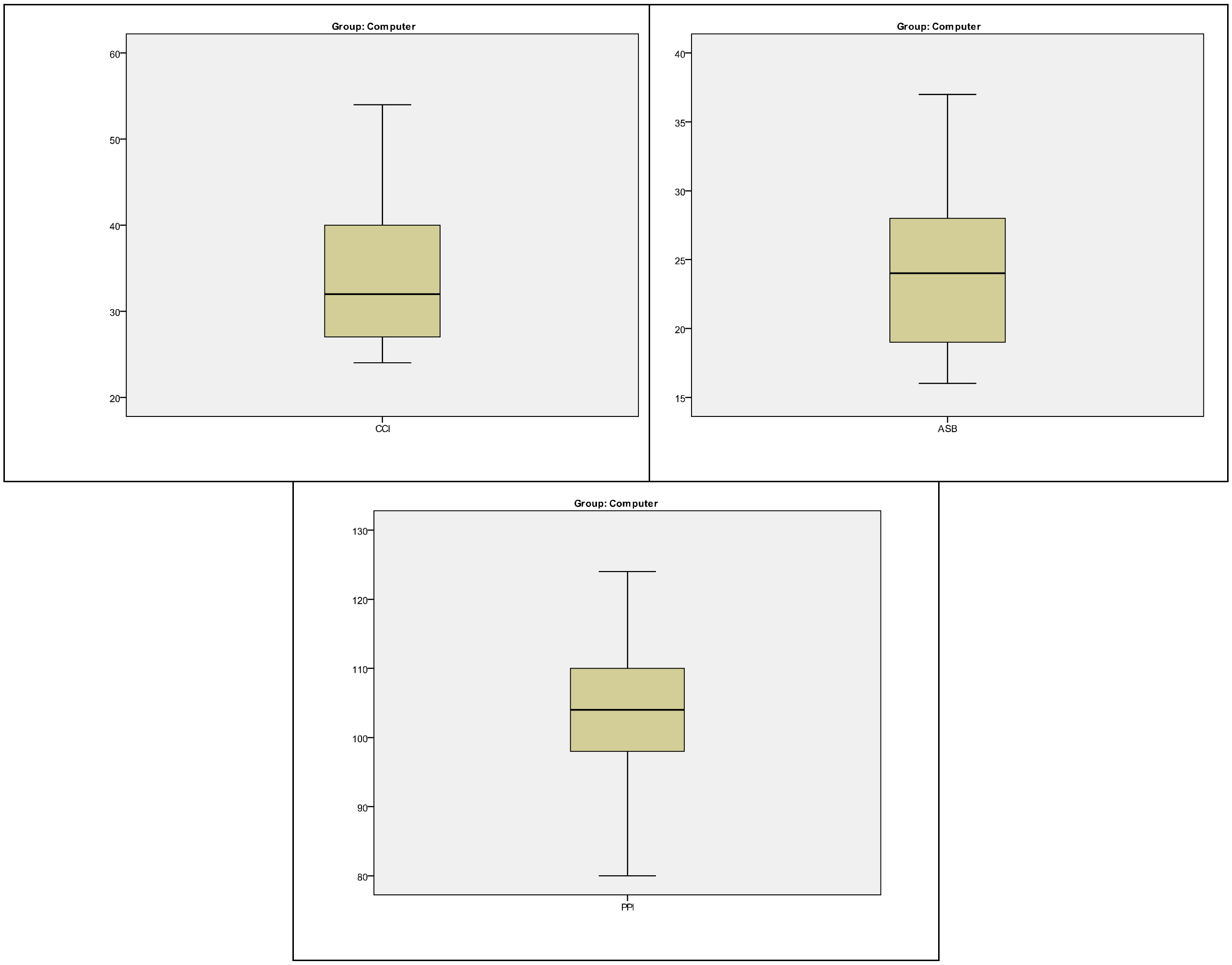


Normal Q-Q Plot of CCI

Normal Q-Q Plot of ASB

Normal Q-Q Plot of PPI

Table 13. Box Plots for Computer Group



Exploratory data analysis for ID group (Group 3)

In this section, descriptive statistics for CCI, ASB and PPI are reported. Then, the Q-Q plots are shown to establish normality. Next, Box Plots are reported to illustrate the extreme cases for CCI, ASB and PPI.

Table 14. Descriptive Statistics for ID Group

ID	CCI	Mean	37.0000	1.27049
		Median	37.0000	
		Variance	72.636	
		Std. Deviation	8.52270	
		Minimum	24.00	
		Maximum	60.00	
	ASB	Mean	26.1778	1.38363
		Median	24.0000	
		Variance	86.149	
		Std. Deviation	9.28168	
		Minimum	16.00	
		Maximum	56.00	
	PPI	Mean	106.3556	1.53253
		Median	108.0000	
		Variance	105.689	
		Std. Deviation	10.28051	
		Minimum	75.00	
		Maximum	124.00	

Key: CCI = Cyber crime engagement, ASB = Antisocial behavior, PPI = Pre-employment integrity

Table 15. Q-Q Plots for ID Group

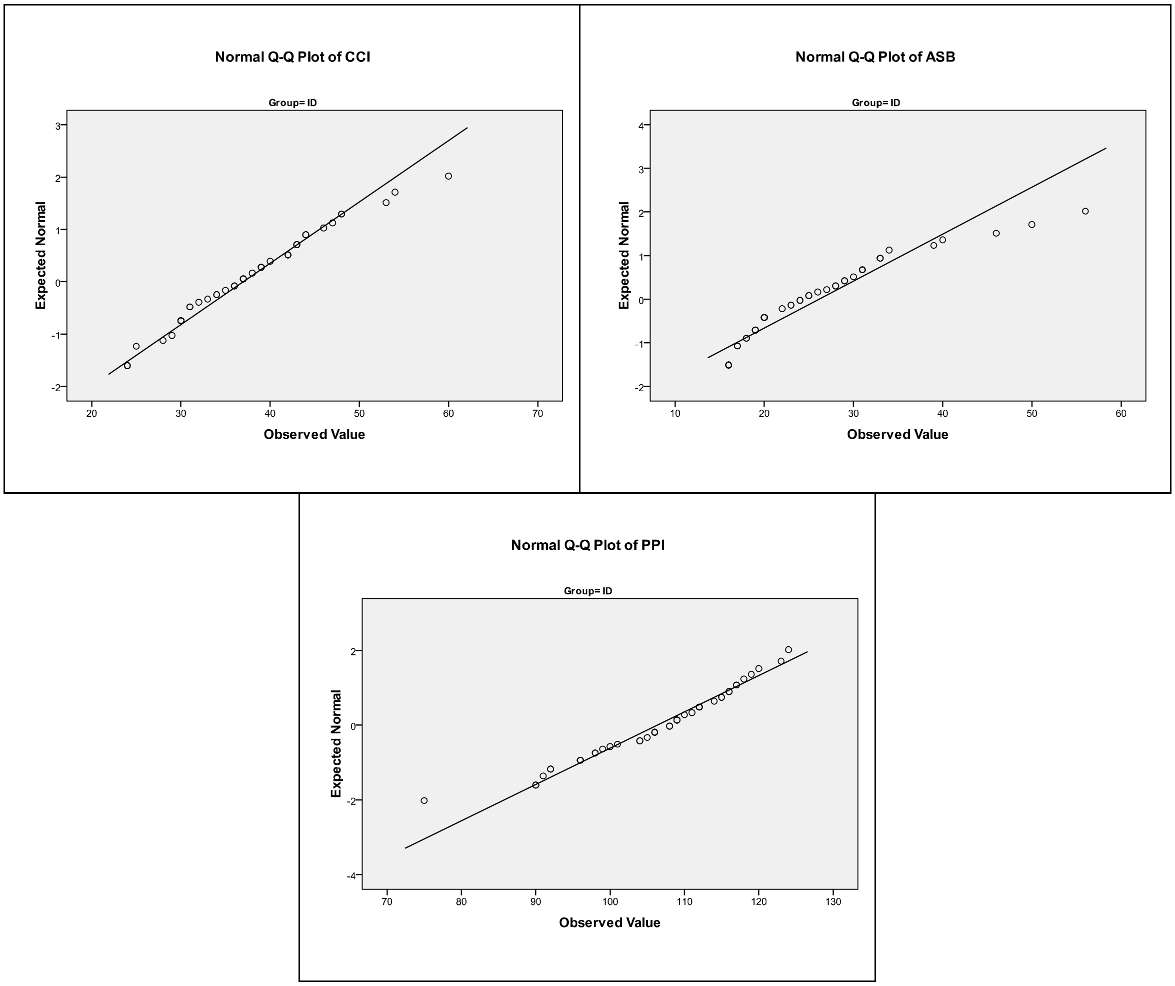
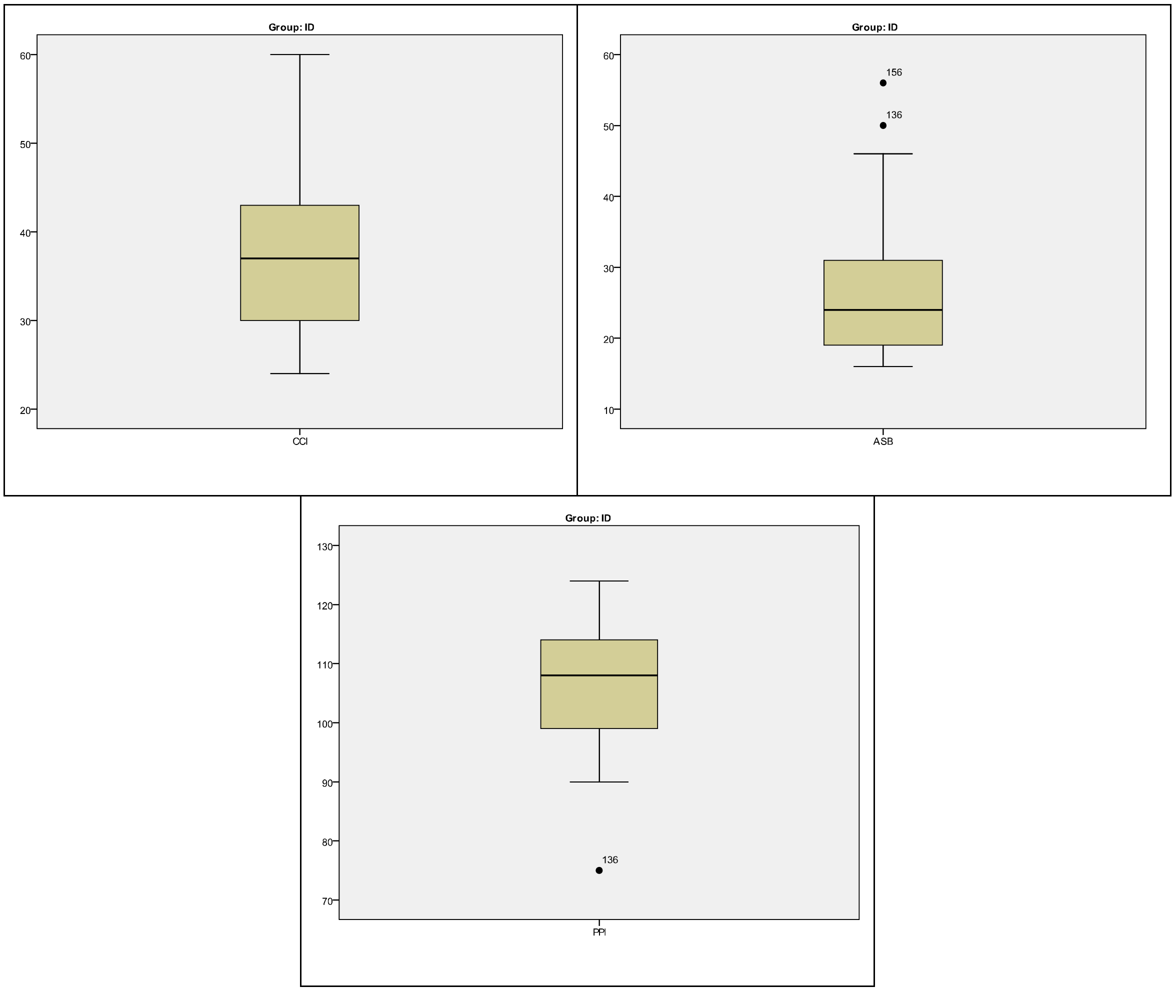


Table 16. Box Plots for ID Group



Possible moderation

The data was explored for anonymity acting as a moderator. If there was no moderation, one would expect to find the following correlations to be roughly equal across all three groups:

$$\text{PPIxCCI}_{\text{(Control Group)}} = \text{PPIxCCI}_{\text{(Computer Group)}} = \text{PPIxCCI}_{\text{(ID Group)}}$$

$$\text{ASBxCCI}_{\text{(Control Group)}} = \text{ASBxCCI}_{\text{(Computer Group)}} = \text{ASBxCCI}_{\text{(ID Group)}}$$

The results from the correlations are as follows:

<u>Control Group</u>

ASB*CCI: r = 0.278 Sig = 0.30

PPI*CCI: r = -4.32 Sig = 0.001

<u>Computer Group</u>

ASB*CCI: r = 0.441 Sig = 0.001

PPI*CCI: r = -0.396 Sig 0.002

<u>ID Group</u>

ASB*CCI: r = 0.121 Sig = 0.428

PPI*CCI: r = -2.80 Sig = 0.063

From the above results, we can deduce that the correlation between ASB and CCI increases in the computer group, and then decreases in the ID group when compared to the control group. As for the correlation between PPI and CCI, we see that the correlation decreases in the computer group and the ID group when compared to the control group. These exploratory results were reported to inspire future research on anonymity acting as a moderator to these variables. These preliminary findings indicate that the anonymity manipulation may have affected the strength of the relationship between the variables, thus making it a plausible moderator.

Discussion of exploratory data analysis

The above mentioned results can be summarized by stating that the data is roughly normal. Some of the cases that seem like outliers in the normality tests as well as the Box Plots when all the cases are analyzed and when the cases were looked at per group are regarded as normal in this study's case. As discussed before, this is due to the constructs being measured. Since the constructs being measured deal with antisocial behaviors, cyber crime and integrity, some individuals may portray extreme cases of these attributes. The Q-Q plots showed that the data is roughly normal and Levene's test showed that the requirement for the homogeneity of variance is met. These results suggested that parametric tests could be applied to the data set. These parametric tests were used to test the hypotheses and this is shown in the next section. Lastly, preliminary analysis of the correlations between ASB and CCI, and PPI and CCI indicate the possibility of the anonymity acting as a moderator.

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, ASB and PPI being dependents. The results of the ANOVA are displayed in Tables 17 and 18.

Table 17. 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 18. ANOVA Results

Tests of Between-Subjects Effects

Dependent Variable:CCI

Source	Type III Sum of Squares	df	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 17 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, partial η2 = .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 19.

Table 19. Tukey's Test

Multiple Comparisons

Dependent Variable:CCI

	(I) Group	(J) Group	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						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.

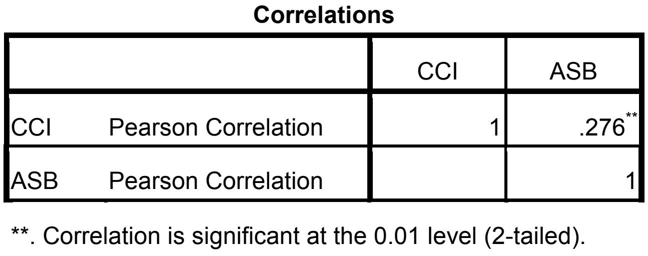
Tukey's post-hoc test suggested that there is statistically significant difference between Groups 1 and 2 (Control and Computer) (p = .032). It also showed a marginal difference between groups 2 and 3 (Computer and ID) (p = .088). Therefore, based on the ANOVA and the post-hoc test, H1 is accepted.

Hypothesis 2

H2: There is a positive relationship between self-reported cyber crime (CCI) and self- reported antisocial behavior (ASB).

To test this hypothesis, a Pearson's correlation was used. The results are shown in Table 20.

Table 20. Correlation ASB and CCI



Correlations

		CCI	ASB
CCI	Pearson Correlation	1	.276**
ASB	Pearson Correlation		1

**. Correlation is significant at the 0.01 level (2-tailed).

Key: CCI = Computer crime engagement, ASB = Antisocial behavior

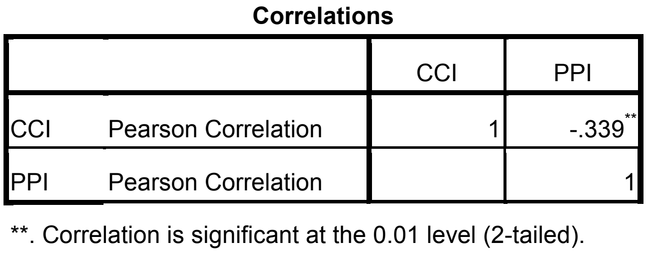
The results in Table 20 indicate that there is a statistically significant positive correlation between CCI and ASB r(161) = .276, p < .01. Since the relationship is significant H2 is accepted.

Hypothesis 3

H3: 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 21.

Table 21. 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

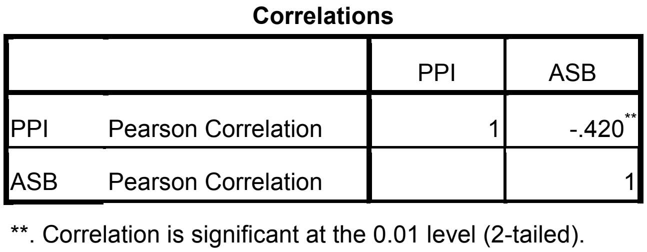
The results in Table 21 show a statistically significant negative correlation between CCI and PPI r(161) = -.339, p < .01. Since the relationship is significant H3 is accepted.

Hypothesis 4

H4: There is a negative relationship between self-reported pre-employment integrity and self-reported antisocial behavior.

To test this hypothesis, a Pearson's correlation was used. The results are shown in Table 22.

Table 22. PPI and ASB Correlation



Correlations

		PPI	ASB
PPI	Pearson Correlation	1	-.420**
ASB	Pearson Correlation		1

**. Correlation is significant at the 0.01 level (2-tailed).

Key: PPI = Pre-employment integrity, ASB= Antisocial behavior

The results in Table 22 illustrate a statistically significant negative correlation between PPI and ASB r(161) = -.420, p < .01. Since the relationship is significant H4 is accepted.

Hypotheses 5 and 6

H5: Anonymity and self-reported antisocial behavior (ASB) can predict self-reported cyber crime (CCI).

H6: There is an interaction between self-reported antisocial behavior (ASB) and anonymity when predicting self-reported cyber crime (CCI).

To test H5 and H6, a univariate GLM was executed using CCI as the dependent variable. Anonymity was a categorical variable between participants factor and ASB was a continuous between participants predictor (analogous to covariate). The results form this analysis is shown in Table 23.

Table 23. GLM Results (Antisocial behavior x Anonymity)

Source	Type II Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Observed Power[b]
Corrected Model	1567.642[a]	5	313.528	5.009	.000	.138	.982
Intercept	11484.635	1	11484.635	183.496	.000	.539	1.000
Group	410.645	2	205.323	3.281	.040	.040	.616
ASB	782.035	1	782.035	12.495	.001	.074	.940
Group * ASB	272.217	2	136.109	2.175	.117	.027	.440
Error	9826.321	157	62.588				
Total	221707.000	163					
Corrected Total	11393.963	162					

Key: Group = Anonymity group, ASB = Antisocial behavior

From Table 23, we can infer the following:

- There is a statistically significant main effect for our anonymity manipulation, (F(2,157) = 3.28, p = .040, partial η^2 = .04).
- There is a statistically significant effect for ASB, (F(1,157) = 12.495, p = .001, partial η^2 = .074).
- There is no significant interaction between our anonymity manipulation and ASB, (F(2,157) = 2.175, p = .117, partial η^2 = .027).

Because of the aforementioned results, H5 is accepted since anonymity and ASB had significant effects. However, H6 is rejected since there was no significant interaction between Anonymity and ASB.

Hypotheses 7 and 8

H7: Anonymity and self-reported pre-employment integrity (PPI) can predict self-reported cyber crime (CCI).

H8: There is an interaction between self-reported pre-employment integrity (PPI) and anonymity when predicting self-reported cyber crime (CCI).

To test H7 and H8, 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 form this analysis is shown in Table 24.

Table 24. GLM Results (Pre-employment integrity x Anonymity)

Source	Type II Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	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 24 we can infer the following:

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

Because of the aforementioned results only part of H7 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 H7 in which Anonymity may be used to predict CCI is rejected. H8 is rejected since there was no significant interaction between Anonymity and PPI.

Hypothesis 9

H9: There is an interaction between self-reported antisocial behavior and self-reported pre-employment integrity when predicting self-reported cyber crime.

To test H9, a univariate GLM was executed using CCI as the dependent variable. ASB was a continuous between predictor and PPI was a continuous between participants predictor (Analogous to covariates). The results form this analysis is shown in Table 25.

Table 25. GLM Results (Pre-employment integrity x Antisocial behavior x Anonymity)

Source	Type II Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Observed Power[b]
Corrected Model	2755.073[a]	11	250.461	4.378	.000	.242	.999
Intercept	1282.902	1	1282.902	22.424	.000	.129	.997
Group	94.680	2	47.340	.827	.439	.011	.190
PPI	622.100	1	622.100	10.874	.001	.067	.906
ASB	243.468	1	243.468	4.256	.041	.027	.536
Group * PPI	80.635	2	40.318	.705	.496	.009	.167
Group * ASB	72.181	2	36.091	.631	.534	.008	.154
ASB * PPI	282.276	1	282.276	4.934	.028	.032	.598
Group * ASB * PPI	73.430	2	36.715	.642	.528	.008	.156
Error	8638.890	151	57.211				
Total	221707.000	163					
Corrected Total	11393.963	162					

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

From Table 25, we can infer the following about the interaction:

- There is a statistically significant effect for the interaction of pre-employment integrity X antisocial behavior, (F(1,151) = 4.93, p < .01, partial η^2 = .032).

Due to the aforementioned results H9 is accepted because the interaction effect was significant.

CHAPTER 5 – DISCUSSIONS AND CONCLUSIONS

The purpose of the study was to investigate how self-reported cyber crime engagement is related to pre-employment integrity, anonymity and antisocial behaviors. The data analysis from this research has provided some possible answers to the questions raised. The data analysis also posed some new questions for future research.

Summary of findings

From a correlation standpoint, self-reported anti social behaviors (ASB) and pre-employment integrity (PPI) were significantly correlated with cyber crime Engagement (CCI). Primarily, all predictors (ASB, anonymity and PPI) had significant main effects on self-reported cyber crime engagement (CCI). However, it was apparent through the GLM analysis in Chapter 4 (Table 25) that when the predictive model is evaluated with all three factors, PPI is the strongest of the three. The second strongest is the predictive model in which PPIxASB is the predictor (interaction effect between PPI and ASB). The third most significant model predicting CCI is using ASB as a main effect predictor.

What is interesting to note that using anonymity as a main predictor by itself yielded a significant model. When ASB and anonymity are both used as predictive variables, the model is still significant. However, as soon as PPI was introduced into the model, it became the strongest predictor. ASB still remained a significant predictor although its significance level decreased, but the effect of anonymity stopped being significant when PPI was introduced into the predictive model.

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).

One of the first notable research initiatives on the levels of anonymity was performed in 1967 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. (Hartnett & Seligsohn, 1967, p. 97).

Hartnett and Seligsohn (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 in this dissertation 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.

Lastly, it is important to note that there is plausible evidence that the ID manipulation might have worked. The original sample size of the ID group was sixty five participants, but only forty five participants fully completed the survey. This is a 30 % decrease in the number of participants for the ID group. This indicates that participants in the ID group might have felt that their anonymity was stripped away. The decrease in the anonymity of individuals in the ID group might have caused the twenty participants to cease participation because they felt that their responses would have not been anonymous and that their privacy was compromised.

Hypothesis 2

As it was described in the results, hypothesis 2 was supported. The results indicated that there is a significant correlation between antisocial behavior (ASB) and self-reported cyber crime. As noted in the literature review, ASB been examined through the legal concepts of criminality and delinquency, which encompass unlawful behaviors

(Morgan & Lilenfield, 2000). Even though the criminal offenses used in prior research did not include cyber crimes, the results in this study indicate that there is still a significant correlation between ASB and cyber crime.

ASB is highly linked with psychopathy (see literature review). The ASB measure in this study was a sub-measure extracted from a psychopathy survey. It could be that the psychopathy personality trait is highly associated with cyber criminals and that is why ASB is significantly correlated with self-reported cyber crime. However, ASB measures have been typically related to traditional crime, and the results in this study indicate that it can also be related to cyber crime.

Hypothesis 3

As shown in the results, hypothesis 3 was supported. The literature suggested that overt PPI measures have items that relate to criminal/illegal activities (see literature review). Since cyber crimes are illegal activities, one would expect that pre-employment integrity (PPI) is linked to antisocial behavior (ASB). In specific, one would expect that these two are negatively correlated because logically; individuals with high levels of integrity should portray low levels of ASB. Since hypothesis 3 was supported, the intuitive idea that ASB and pre-employment integrity are negatively correlated was supported.

Hypothesis 4

As was stated in the results, hypothesis 4 was supported. According to the literature review, ASB has been examined through the legal concepts of criminality and delinquency, which encompass unlawful behaviors (Morgan & Lilenfield, 2000). Since ASB has been shown to be highly correlated with criminal offenses, one would also expect that it might be correlated to cyber crimes as well because cyber crimes are criminal offenses. The results reinforced the findings in the literature.

Hypothesis 5 & Hypothesis 6

As the results indicated, H5 was accepted and H6 was rejected. Over the years, literature on anonymity has shown that it can be an enabler to antisocial behaviors (Tresca, 1998; Zimbardo,1969). Consequently, one would expect that increasing or decreasing the level of anonymity may predict one's engagement in ASBs. This prediction is intuitive. Take stealing a car as an example. One would expect that criminals would less likely steal a car in the presence of others because they would feel less anonymous.

H6 was not supported. This finding makes sense because the concepts of anonymity and ASB are independent from one another. Anonymity can exist without ASB and vice versa. The fact that anonymity may enable ASB to increase or decrease does not necessarily mean that they interact as variables. Independent from one another, they seem to be significant predictors of cyber crime engagement, but their interaction does not seem to produce enough predictive significance of cyber crime engagement.

Hypothesis 7 & Hypothesis 8

H7 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. H8 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. (1998). Additionally, as explained in the literature review, inherent in the overt measures of PPI is the concept of criminal activities.

In this testing scenario, even though anonymity was shown to be a significant predictor of CCI when ASB was in the model, it stops being significant in this model. This is because PPI had a larger significant predictive effect on CCI than ASB. This significant predictive power accounted for a larger portion of the relationship than anonymity.

This preliminary finding may suggest that irrespective of the level of anonymity that individuals may be placed in, an individuals' 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 less likely engage in cyber crime activities regardless of their level of anonymity.

H8 was rejected and no interaction was found between PPI and anonymity. H6 however, was not supported. This finding is sensible because the concepts of anonymity and PPI are independent from one another. Anonymity can exist without PPI and vice versa.

Hypothesis 9

As was shown in the results, H9 was accepted. According to the literature review, the overt integrity measures have items that relate to criminal/illegal activities (see literature review). In overt measures, some of the items respondents are asked directly about are their, criminal history, attitudes towards drug abuse, theft by others (Barrett, 2001) and illegal and dishonest activities (Schmidt et al., 1997). All the aforementioned constructs are regarded as antisocial behaviors. Therefore, one would intuitively expect that there is an interaction between ASB and PPI. This notion was supported since this study found a significant interaction between ASB and PPI, when predicting CCI.

Limitations

This study has some limitations. Primarily, this study has the methodological limitation of self-reported surveys. Additionally, only one question in the survey was used as a manipulation check for anonymity. When that manipulation check was analyzed against the various groups, there was no significant correlation between the manipulation check and the group. This could be attributed to the inability to quantify a reliable manipulation check using a one Likert scale item. There is also the slight chance that the anonymity was not the factor being manipulated during the experimental procedures.

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.

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. A simple one item Likert scale manipulation check did not properly quantify a participant's self-reported level of anonymity. 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.

Lastly, the ASB measure used in this study is extracted from the psychopathy scale as mentioned before. It would be important to test if all the other subscales in psychopathy may be used as predictors of self-reported cyber crime. The other variables may enable future researchers to create a more statistically significant predictive model.

Contribution of the study

Primarily, this study looks 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 antisocial behavior and pre-employment integrity as individual differences relating to cyber crime engagement. The results illustrate that there is a significant relationship amongst those variables and that they are correlated to cyber crime. Additionally, this study illustrated that individual differences that were originally operationalized to measure non-cyber related constructs may be used as significant predictors 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.

Conclusions

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 two predictors (self-reported anti social behavior (ASB) and self-reported pre-employment integrity (PPI). It illustrated that PPI is the strongest predictor, followed by the interaction between PPIxASB, followed by ASB, followed by anonymity (ranked in order of model strength based on the data analysis performed). It further suggested that using the experimental design presented, the manipulation of anonymity by seeing a participant's ID only has a marginal effect. Lastly, the results suggested that using a one Likert scale item for quantifying a participant's level of anonymity is not viable (given the fact that anonymity was manipulated in the first place).

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.

REFERENCES

REFERENCES

1999 Report on cyberstalking: A new challenge for law enforcement and industry. A report to the attorney general to the vice president. Retrieved April 25, 2006, from http://www.usdoj.gov/criminal/cyber crime/cyberstalking.htm

Abram, K. M. (1989). The effect of co-occurring disorders on criminal careers: Interaction of antisocial personality, alcoholism, and drug disorders. *International Journal of Law and Psychology, 12*, 133–148.

Anderson, R., Bozek, T., Longstaff, T., Metizler, W., Skroch, M., & Van Wyk, K. (2000). Research on mitigating the insider threat to information systems - # 2: Proceedings of a workshop held august 2000. Retrieved November 26, 2007, from http://www.rand.org/pubs/conf_proceedings/CF163/CF163.pdf

Armitage, R. (2002) Tackling antisocial behaviour: what really works. NACRO Community Safety Practice Briefing.

Austin, L. (2003). Privacy and the question of technology. *Law and Philosophy*, 22(2), 119-116.

Azechi, S. (2005). Information humidity model: explanation of dual modes of community for social intelligence design, *AI & Society,* 19(1), 110-112

Babu, M., & Parishat, M.G. (2004). What is cyber crime?. Retrieved November 27, 2007, from http://www.crime-research.org/analytics/702/

Baker, J. (2004). The sociological origins of “white collar crime”. Retrieved November 26, 2007, from http://www.heritage.org/Research/LegalIssues/lm14.cfm

Bates, A. (1964). Privacy – a useful concept?, *Social Forces,* 42(4), 429-434.

Barrett, P. 2001. Pre-Employment Integrity Testing: Current Methods, Problems and Solutions. *British Computer Society: Information Security Specialist Group*. Milton Hill, Oxford.

Berman, M. E., Kavoussi, R. J., & Coccaro, E. F. (1997). Neurotransmitter correlates of human aggression. In D. M. Stoff, J. Breiling, & J. D. Maser (Eds.), *Handbook of antisocial behavior* (pp. 305–313). New York: John Wiley & Sons.

Blackburn, R. (1993). *The psychology of criminal conduct: Theory, research and practice*. Toronto: John Wiley & Sons.

Braithwaite, J. (1985). White collar crime. *Annual Review of Sociology*, 11, 1-25.

Brenner, S. (2000). Is there such a thing as a “virtual crime”? *California Criminal Law Review.* Retrieved April 25, 2006, from http://www.boalt.org/CCLR/v4/v4brenner.htm

Browing. G., Halci. A. & Webster. F. (2000). *Understanding Contemporary Society: Theories of the Present*. Sage Publications.

Burton, K. (2007). Internet crime; where anonymity cuts both ways. Retrieved September, 25, from http://www.crime-research.org/articles/wildlife-internet-crime

Calhoun, C. (1995). Standing for Something. *Journal of Philosophy*, XCII: 235–260.

Christopherson, K. (2007). The positive and negative implications of anonymity in Internet social interactions: on the Internet, nobody knows you're a dog. *Computers in Human Behavior*. 23(6), 3038-3056.

Cormack, R.W., & Strand, A.L. (1970). *Trustworthiness Attitude Survey*. Oakbrook, IL: Personnel Systems Corporation.

Cox, D., La Caze, M., & Levine, M.P. (2003). *Integrity and the Fragile Self*. Aldershot: Ashgate.

Crime and disorder act. (1998). Retrieved July 2, 2009 from http://www.opsi.gov.uk/acts/acts1998/ukpga_19980037_en_1

Crime in the United States. (2009). Retrieved May 26, 2009 from http://www.fbi.gov/ucr/2008prelim/downloads.htm

Cummings, J. N., & Kraut, R. (2002). Domesticating computers and the Internet. *The Information Society*, 18(3), 1-18.

CSI Computer Crime and Security Sruvey. (2008). Retrieved May 25, 2009 from http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf

Defining and measuring antisocial behavior. (2004). Retrieved July 2, 2009 from http://uk.sitestat.com/homeoffice/rds/s?rds.dpr26pdf&ns_type=pdf&ns_url=%5Bhttp://www.homeoffice.gov.uk/rds/pdfs04/dpr26.pdf%5D

Diaz, C. Seys, S., & Preneel, B. (2002). Towards measuring anonymity. In Hannes Federath (Ed.), *Designing Privacy Enhancing Technologies*, Lecture Notes in computer Science. San Francisco, CA.

Diener, E., Fraser, S. C., Beaman, A. L. & Kelem, R. T. (1976). Effects of deindividuation variables on stealing among Halloween trick-or-treaters. *Journal of Personality and Social Psychology*, 33(2), 178-183.

Diener, E. (1979). Deindividuation, self-awareness, and disinhibition. *Journal of Personality and Social Psychology*. 37, 1160-1171.

Diener, E. (1980). Deindividuation: The absence of self-awareness and self-regulation in group members. In P.B. Pauhus (Ed.), *Psychology of group influence* (pp. 209-242). Hillsade, NJ: Erlbaum.

Douglas, K., & McGarty, C. (2001). Identifiability and self-presentation: computer mediated communication and intergroup interaction. *British Journal of Social Psychology*. 40(3), 399-416.

Dubrovsky, V. J., Kiesler, B. N., & Sethna, B. N. (1991). The equalization phenomenon status effect in computer-mediated and face-to-face decision-making groups. *Human-Computer Interaction*. 2(2), 119-146.

Duval, S. & Wicklund, R. A. (1972). *A theory of objective self-awareness*. New York: Academic Press.

Earp, J.B., Anton, A.I., Aiman-Smith, L., & Stufflebeam, W.H. (2005). Examining Internet privacy policies within the context of user privacy values. *Engineering Management IEEE Transactions*, 52(2), 227-237.

Ellison, P., Govern, J., Petri, H., & Figler, M. (1995). Anonymity and aggressive driving behavior: A field study. *Journal of Social Behavior and Personality*, 10, 265-272.

Festinger, L., Pepitone, A. & Newcomb T. (1952). Some consequences of deindividuation in a group. *Journal of Abnormal and Social Psychology*, 47, 382-389.

Frankfurt, H. (1971). Freedom of the Will and the Concept of a Person. *Journal of Philosophy*, LXVIII: 5–20.

Froomkin, A. M. (1995). Anonymity and its enmities. *Journal of Online Law*, *4*. Retrieved April 1, 2007, from http://www.wm.edu/law/publications/jol/95_96/froomkin.html

Gackenbach, J. (1998). *Psychology and the Internet: Intrapersonal, Interpersonal, and transpersonal implications*. San Diego, CA : Academic Press.

Gordon, L., Loeb, M., Lucyshyn, W., & Richardson, R. (2006). CSI/FBI Computer crime and security survey. Retrieved November 29, 2007 from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

Gough, H.G. (1948). A sociological theory of psychopathy. *American Journal of Sociology.* 53:359- 366.

Gough, H.G. (1954) *Personnel Reaction Blank*. Palo Alto, CA: Consulting Psychologists Press.

Gough, H. G. (1994). Theory, development, and interpretation of the CPI Socialization Scale. *Psychological Reports, 75*, 651–700.

Halfon, M. (1989). *Integrity: A Philosophical Inquiry*. Philadelphia: Temple University Press.

Hare, R. D. (1991). *The Hare Psychopathy Checklist-Revised.* Toronto: Multi-Health Systems.

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.

Hathaway, S. R., & McKinley, J. C. (1942). *Minnesota Multiphasic Personality Inventory.* Minneapolis: University of Minnesota Press.

Heilbrun, A. B. (1979). Psychopathy and violent crime. *Journal of Consulting and Clinical Psychology, 47*, 509–516.

Heilbrun, A. B., & Heilbrun, M. R. (1985). Psychopathy and dangerousness: Comparison, integration and extension of two psychopathic typologies. *British Journal of Clinical Psychology, 24*, 181–195.

Henry, B., & Moffitt, T. E. (1997). Neuropsychological and neuroimaging studies of juvenile delinquency and adult criminal behavior. In D. M. Stoff, J. Breiling, & J. D. Maser (Eds.), *Handbook of antisocial behavior* (pp. 280–288). New York: John Wiley & Sons.

Hogan, R. (1981). *Hogan Personality Inventory*. Minneapolis: National Computer Systems Inc.

Huber, G.P. (1990). A theory of the effects of advanced information technologies on organizational design, intelligence, and decision making. In J. Fulk & C. W. Steinfield (Eds.), *Organizational and communication technology* (pp. 237-74). Newbury Park, CA: Sage.

IC3 2005 Internet Crime Report. (2005). Retrieved September 25, 2007 from http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf

IC3 2008 Internet Crime Report. (2008). Retrieved June 16, 2009 from http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf

Isenberg, D. J. (1986). Group polarization: a critical review and meta-analysis. *Journal of Personality and Social Psychology*, 50(6), 1141-1151.

Johnson, R. D., & Downing, L. L. (1979). Deindividuation and valence of cues: effects of prosocial and antisocial behavior. *Journal of Personality and Social Psychology*, 37(9), 1532-1538.

Kane, J., & Wall, A. (2005). The 2005 national public survey on white collar crime. Retrieved December 5, 2007, from http://www.nw3c.org/research/site_files.cfm?fileid=b3d1badb-51ca-4acf-bd34-fdeb6b7a4ef1&mode=p

Katyal, N.K. (2001). Criminal law in cyberspace. *University of Pennsylvania Law Review,* 149(4), 1003-1114.

Katyal, N.K. (2003). Digital architecture as crime control. *The Yale Law Journal,* 112(8), 2261-2289.

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.

Klump. (1964). C.S. *Stanton Survey*. Charlotte, NC: Stanton Corporation.

Lee, E. (2007). Deindividuation effects on group polarization in computer-mediated communication: The role of group identification, public self-awareness, and perceived argument quality, *Journal of Communication*, 57(2), 385-403.

Le Bon, G. (1895). *The crowd: A study of the popular mind*. Retrieved November 12, 2007, from http://www.gwiep.net/library/LeBon_-_Crowd.html

Levemore, S. (1996). The anonymity tool. *University of Pennsylvania Law Review*, 144-5, 2191-2236.

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

London House, Inc. (1997). *Personnel Selection Inventory*. Park Ridge, IL: London House Press.

Lousig-Nont. (1987). G.M. *Phase II Profile*. Las Vegas, NV: Self-published.

Lykken, D. T. (1995). *The antisocial personalities.* Hillsdale, NJ: Lawrence Erlbaum Associates.

McFall, L. (1987). Integrity. *Ethics*,98, 5–20. Reprinted in John Deigh (ed.), *Ethics and Personality*, Chicago: University of Chicago Press, 1992.

McKenna, K., & Bargh, J. (1998). Coming out in the age of the Internet: Identity “demarginalization” through virtual group participation. *Journal of Personality and Social Psychology*, 75, 681–694.

McQuade, S.C. (2006). Understanding and Managing Cyber crime. New York, NY. Pearson.

Miller, J.F., & Bradley, P. (1975). Milby Profile. Minneapolis: Milby Systems Inc.

Morgan, A., Lilienfeld, S. (2000). A meta-analytic review of the relation between antisocial behavior and neuropsychological measures of executive function. *Clinical Psychology Review,* 20(1), 113-136.

Morio, H., & Buchholz, C. (2007). How anonymous are you online? Examining online social behaviors from a cross-cultural perspective [Electronic version]. *AI & Society.*

Nixon, J., Blandy, S., Hunter, C., Jones, A. & Reeve, K. (2003) *Developing Good Practice in Tackling Anti-Social Behaviour in Mixed Tenure Areas.* Sheffield: Sheffield Hallam University.

Ones, D.S.; Viswesvaran, C.; and Schmidt, F.L. Meta-analysis of integrity test validities: Findings and implications for personnel selection and theories of job performance. *Journal of Applied Psychology.* 78:4, 1993.

Paajanen, G. (1985). *PDI Employment Inventory*. Minneapolis: Personnel Decisions, Inc.

Patterson, G. G., DeBaryshe, B., & Ramsey, E. (1990). A developmental perspective on antisocial behavior. *American Psychologist, 44,* 329-335.

Pedersen, D. (1997). Psychological functions of privacy. *Journal of Environmental Psychology*, 17(2), 147-156.

Pfitzmann, A., & Kohntopp, M. (2001). Anonymity, Unobservability and Pseudoymity – A proposal for Terminology. In Hannes Federath (Ed.), *Designing Privacy Enhancing Technologies,* Lecture Notes in Computer Science, LNCS 2009, pp. 1-9, Springer-Verlag.

Postomes, T., & Spears, R. (1998). Deindividuation and antinormative behavior: A meta-analysis. *Psychological Bulletin*, 123(3), 238-259.

Postomes, T., & Spears, R. (2002). Behavior online: does anonymous computer communication reduce gender inequality? *Personality and Social Psychology Bulletin*, 28(8), 1073-1083.

Prentice-Dunn, S., & Rogers, R. (1980). cues and aggressive models on subjective deindivduation and aggression. *Journal of Personality and Social Psychology*, 39, 104-113.

Prentice-Dunn, S., & Rogers, R. (1982). Effects of public and private self-awareness on deindividuation and aggression. *Journal of Personality and Social Psychology*, 43, 503-513.

Rafilson, F.M., & Frost, A.G. (1989). Overt integrity tests versus personality-based measures of delinquency: An empirical comparison. *Journal of Business Psychology, 3,* 269-277.

Raine, A. (1993). *The psychopathology of crime.* San Diego: Academic Press.

Raine, A., Brennan, P. A., & Mednick, S. A. (1994). Birth complications combined with early maternal rejection at age 1 year predispose to violent crime at age 18 years. *Archives of General Psychiatry, 51*, 984–988.

Randazzo, M., Keeny, M., Kowalski, E., Cappelli, D., & Moore, A. (2004). Insider threat study: illicit cyber activity in the banking and finance sector. Retrieved November 27, 2007 from http://www.cert.org/archive/pdf/bankfin040820.pdf

Reicher, S. *The psychology of crowd dynamics*. (n.d.). Retrieved November 13, 2007, from http://www.uni-kiel.de/psychologie/ispp/doc_upload/Reicher_crowd%20dynamics.pdf

Reid Psychological Systems. (1951). *Reid Report*. Chicago, IL: Reid Psychological Systems.

Rehm, J., Steinleitner, M., & Lilli, W. (1987). Wearing uniforms and aggression: A field experiment. *European Journal of Social Psychology*, 17, 357-360.

Rice, R.E. (1987). Computer mediated communication and organizational innovation. *Journal of Communication,* 37(4), 65-69.

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.

Saarilouma, P. (2007). Making it possible. *Human Technology*, 3(1), 1-3.

Sackett, P.R., & Harris, M.M. (1985) Honesty testing for personnel selection. A review and critique. In H.J. Bernadin and D.A. Bownas (Eds) *Personality Assessment in Organizations*. New York: Praeger.

Sackett, P.R., Brusis, L.R., & Callahan, C. (1989). Integrity testing for personnel selection: An update. *Personnel Psychology,* 42:491-529.

Science Research Associates. (1983). *Personal Outlook Inventory*. Parkridge, IL: Science Research Associates.

Schwarting, I. (2005). The insider problem revisited: Position paper. In *Proceedings of the 2005 workshop on New security paradigms NSPW '05*, *Lake Arrowhead, California*, *20 – 23 September 2005* (pp. 79-81). New York, NY: ACM.

Sia, C., Tan, B. C. Y., & Wei, K. (2002). Group polarization and computer-mediated communications: effects of communication cues, social presence, and anonymity. *Information Systems Research*, 13(1), 70-90.

Shaw, E., Ruby, K., & Post, J. (1998). The insider threat to information systems: the psychology of the dangerous insider. *Security Awareness Bulletin*, 2(98).

Schmidt, F., Viswesvaran, V., & Ones, D. (1997). Retrieved June 26, 2009, from http://www.nida.nih.gov/pdf/monographs/monograph170/069-095_Schmidt.pdf

Short, J., & Williams, B., & Christie, B. (1976). *The social psychology of telecommunication*. New York: John Wiley.

Skinner, W., & Fream, A. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency*, 34, 495-518.

Snow, C. P. (1959). *The two cultures and the scientific revolution*. Cambridge, UK: Cambridge University Press.

Sproull, L., & Keisler, S. (1991). *Connections: New ways of working in the networked organization.* Cambridge, MA: The MIT Press.

Sukhai, N. (2004). Hacking and cyber crime. New York, NY. *ACM Press*.

Sutherland, E. (1947). *Principles of criminology (4thed.)*. Philadelphia: Lippincott.

Tajfel, H. & Turner, J. C. (1979). An integrative theory of intergroup conflict. In W. G. Austin & S. Worchel (Eds.), *The Social Psychology of Intergroup Relations*. Monterey, CA: Brooks-Cole.

Taylor. C. (2004). Consumer privacy and the market for customer information. *The RAND Journal of Economics*, 35 (4), 631-650.

Taylor, G. (1981). Integrity. *Proceedings of the Aristotelian Society*, Supplementary Volume 55: 143–159.

Tresca, M. (1998). The impact of anonymity on disinhibitive behavior through computer-mediated communication. Retrieved April 01, 2007, from http://www.msu.edu/user/trescami/thesis.htm

Trochim, W., & Donnelly, J. (2007). *The research methods knowledgebase*, 3e: Atomic Dog Publishing.

Turkle, S. (1995). *Life on the screen: identity in the age of the Internet*. Simon & Schuster. New York: Simon & Schuster.

U.S. Congressional Office of Technology Assessment. (1990). *The use of integrity testing for pre-employment screening*. (OTA-SET-442). Washington, DC: Supt. of Docs., U.S. Govt. Print. Off.

Wanek, J.E. (1999) Integrity and honesty testing: What do we know? How do we use it? *International Journal of Selection & Assessment*. Vol 7(4), 183-195.

Williams, B. (1981). *Moral Luck: Philosophical Papers 1973–1980*. Cambridge: Cambridge University Press.

Williams, K., Paulhus, D. & Hare, R. (2007). Capturing the Four-Factor Structure of Psychopathy in College Students Via Self-Report. Journal of Personality Assessment, 88 (2), 205-219.

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

Woolley, R. (1991). "An Examination of the Construct and Criterion-related Validity of Overt and Personality Oriented Predictors of Counter-productivity." Masters thesis, University of British Columbia, Vancouver.

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.

Zimbardo, P.G. (1975). Transforming experimental research into advocacy for social change. In M. Deutsh & Hornstein (Eds.), *Applying social psychology*: *Implications for research, practice and training* (pp. 33-66). Hillsdale, NJ: Lawerence.

APPENDICES

Appendix A – Control Survey

Computer usage 1

The first thing we will ask you to do is to answer the following general demographic questions. Please choose the answer that best describes you. There are also two questions that are related to your computer use.

1) Gender

[-Select- ▾]

- Male
- Female

2) Age

□ Under 22

□ 22 - 29

□ 30 - 39

□ 40 - 49

□ 50 - 59

□ 60 - 69

□ 70 and over

3) What best describes your academic major?

○ Computers

○ Business

○ Liberal Arts

○ Mathematics

○ Engineering

4) I use computers:

○ I don't unless I have to ○ A little ○ Moderately ○ A lot

5) I am anonymous when using the Internet:

○ Disagree strongly ○ Disagree ○ Neutral ○ Agree ○ Agree strongly

-------------------------------------Page Break--------------------------------------

Below are a number of items related to activities that relate to computer use. Some of these items may be regarded as antisocial. Please respond to these items as honestly as possible and be aware that your answers to the questions are only going to be used for research purposes.

WHEN WAS THE MOST RECENT TIME THAT YOU:

		Never	Within the past month	Within the past year	1-4 years ago	5 or more years ago
6)	Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?	○	○	○	○	○
7)	Tried to guess another's password to get into his/her computer account or files?	○	○	○	○	○
8)	Accessed another's computer account or files without his/her knowledge or permission just to look at the information or files?	○	○	○	○	○
9)	Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?	○	○	○	○	○
10)	Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or trojan horse)?	○	○	○	○	○
11)	Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?	○	○	○	○	○
12)	Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?	○	○	○	○	○
13)	Knowingly used, made, or gave to another person a device to obtain free long distance phone calls?	○	○	○	○	○

HOW OFTEN IN THE PAST THREE YEARS HAVE YOU:

		Never	Once	2-3 times	4-5 times	6+ times
14)	Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?	○	○	○	○	○
15)	Tried to guess another's password to get into his/her computer account or files?	○	○	○	○	○
16)	Accessed another's computer account or files without his/her knowledge or permission just to look at the information or files?	○	○	○	○	○
17)	Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?	○	○	○	○	○
18)	Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or trojan horse)?	○	○	○	○	○
19)	Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?	○	○	○	○	○
20)	Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?	○	○	○	○	○
21)	Knowingly used, made, or gave to another person a device to obtain free long distance phone calls?	○	○	○	○	○

HOW OLD WERE YOU THE FIRST TIME YOU:

		Does not apply to me	16 or less	17-18	19-20	21 or older
22)	Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?	○	○	○	○	○
23)	Tried to guess another's password to get into his/her computer account or files?	○	○	○	○	○
24)	Accessed another's computer account or files without his/her knowledge or permission just to look at the information or files?	○	○	○	○	○
25)	Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?	○	○	○	○	○
26)	Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or Trojan horse)?	○	○	○	○	○
27)	Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?	○	○	○	○	○
28)	Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?	○	○	○	○	○
29)	Knowingly used, made, or gave to another person a device to obtain free long distance calling?	○	○	○	○	○

30) I am anonymous when using this computer:

○ Disagree strongly

○ Disagree

○ Neutral

○ Agree

○ Agree strongly

-------------------------------------Page Break-------------------------------------

Please rate the degree to which you agree with the following statements about you. You can be honest because your name is detached from the answers.

		Disagree Strongly	Disagree	Neutral	Agree	Agree Strongly
31)	I have never been involved in delinquent gang activity.	○	○	○	○	○
32)	I have never stolen a truck, car or motorcycle.	○	○	○	○	○
33)	I have tricked someone into giving me money.	○	○	○	○	○
34)	I have assaulted a law enforcement official or social worker.	○	○	○	○	○
35)	I have never tried to force someone to have sex.	○	○	○	○	○
36)	I have never attacked someone with the idea of injuring them.	○	○	○	○	○
37)	I have broken into a building or vehicle in order to steal something or vandalize.	○	○	○	○	○
38)	I have never been arrested.	○	○	○	○	○
39)	I have taken hard drugs (e.g., heroin, cocaine).	○	○	○	○	○
40)	I never shoplifted from a store.	○	○	○	○	○
41)	I was convicted of a serious crime.	○	○	○	○	○
42)	Every now and then I carry a weapon (knife or gun) for protection.	○	○	○	○	○
43)	I have threatened people into giving me money, clothes, or makeup.	○	○	○	○	○
44)	I have close friends who served time in prison.	○	○	○	○	○
45)	I purposely tried to hit someone with the vehicle I was driving.	○	○	○	○	○
46)	I have violated my probation from prison.	○	○	○	○	○

-------------------------------------Page Break-------------------------------------

Please answer the following questions as honestly as possible.

This part of the survey was not included for Copyright reasons (PPI survey)

Please click on "Submit"

powered by www.psychdata.com

Appendix B – Computer Group Survey

Computer usage 2

The first thing we will ask you to do is to answer the following general demographic questions. Please choose the answer that best describes you. There are also two questions that are related to your computer use.

1) Gender

-Select- ▾

- Male
- Female

2) Age

□ Under 22

□ 22 - 29

□ 30 - 39

□ 40 - 49

□ 50 - 59

□ 60 - 69

□ 70 and over

3) What best describes your academic major?

○ Computers

○ Business

○ Liberal Arts

○ Mathematics

○ Engineering

4) I use computers:

○ I don't unless I have to ○ A little ○ Moderately ○ A lot

5) I am anonymous when using the Internet:

○ Disagree strongly ○ Disagree ○ Neutral ○ Agree ○ Agree strongly

-------------------------------------Page Break--------------------------------------

Read these directions carefully before you continue:

1. Click here to open the Form, and fill out the information to the best of your ability. *If the new form does not open, try clicking the*

Shift key, on your keyboard, then click on the link with your mouse button again. This may be necessary if your browser does not permit any pop-up windows.

2. When you are done filling out the form, click on the Submit button and the form will close. When the form closes, please proceed to the next page of the survey. If you are prompted with the message "The webpage you are viewing is trying to close the window. Do you want to close this window?", click on the Yes button.

-------------------------------------Page Break-------------------------------------

Below are a number of items related to activities that relate to computer use. Some of these items may be regarded as antisocial. Please respond to these items as honestly as possible and be aware that your answers to the questions are only going to be used for research purposes.

WHEN WAS THE MOST RECENT TIME THAT YOU:

		Never	Within the past month	Within the past year	1-4 years ago	5 or more years ago
6)	Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?	○	○	○	○	○
7)	Tried to guess another's password to get into his/her computer account or files?	○	○	○	○	○
8)	Accessed another's computer account or files without his/her knowledge or permission just to look at the information or files?	○	○	○	○	○
9)	Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?	○	○	○	○	○
10)	Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or trojan horse)?	○	○	○	○	○
11)	Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?	○	○	○	○	○
12)	Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?	○	○	○	○	○
13)	Knowingly used, made, or gave to another person a device to obtain free long distance phone calls?	○	○	○	○	○

HOW OFTEN IN THE PAST THREE YEARS HAVE YOU:

		Never	Once	2-3 times	4-5 times	6+ times
14)	Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?	○	○	○	○	○
15)	Tried to guess another's password to get into his/her computer account or files?	○	○	○	○	○
16)	Accessed another's computer account or files without his/her knowledge or permission just to look at the information or files?	○	○	○	○	○
17)	Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?	○	○	○	○	○
18)	Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or trojan horse)?	○	○	○	○	○
19)	Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?	○	○	○	○	○
20)	Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?	○	○	○	○	○
21)	Knowingly used, made, or gave to another person a device to obtain free long distance phone calls?	○	○	○	○	○

HOW OLD WERE YOU THE FIRST TIME YOU:

		Does not apply to me	16 or less	17-18	19-20	21 or older
22)	Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?	○	○	○	○	○
23)	Tried to guess another's password to get into his/her computer account or files?	○	○	○	○	○
24)	Accessed another's computer account or files without his/her knowledge or permission just to look at the information or files?	○	○	○	○	○
25)	Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?	○	○	○	○	○
26)	Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or Trojan horse)?	○	○	○	○	○
27)	Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?	○	○	○	○	○
28)	Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?	○	○	○	○	○
29)	Knowingly used, made, or gave to another person a device to obtain free long distance calling?	○	○	○	○	○

30) I am anonymous when using this computer:

○ Disagree strongly

○ Disagree

○ Neutral

○ Agree

○ Agree strongly

--------------------------------------Page Break--------------------------------------

Please rate the degree to which you agree with the following statements about you. You can be honest because your name is detached from the answers.

		Disagree Strongly	Disagree	Neutral	Agree	Agree Strongly
31)	I have never been involved in delinquent gang activity.	○	○	○	○	○
32)	I have never stolen a truck, car or motorcycle.	○	○	○	○	○
33)	I have tricked someone into giving me money.	○	○	○	○	○
34)	I have assaulted a law enforcement official or social worker.	○	○	○	○	○
35)	I have never tried to force someone to have sex.	○	○	○	○	○
36)	I have never attacked someone with the idea of injuring them.	○	○	○	○	○
37)	I have broken into a building or vehicle in order to steal something or vandalize.	○	○	○	○	○
38)	I have never been arrested.	○	○	○	○	○
39)	I have taken hard drugs (e.g., heroin, cocaine).	○	○	○	○	○
40)	I never shoplifted from a store.	○	○	○	○	○
41)	I was convicted of a serious crime.	○	○	○	○	○
42)	Every now and then I carry a weapon (knife or gun) for protection.	○	○	○	○	○
43)	I have threatened people into giving me money, clothes, or makeup.	○	○	○	○	○
44)	I have close friends who served time in prison.	○	○	○	○	○
45)	I purposely tried to hit someone with the vehicle I was driving.	○	○	○	○	○
46)	I have violated my probation from prison.	○	○	○	○	○

--------------------------------------Page Break--------------------------------------

Please answer the following questions as honestly as possible.

This part of the survey was not included for Copyright reasons (PPI survey)

powered by www.psychdata.com

Appendix C – ID Group Survey

Computer Usage 3

The first thing we will ask you to do is to answer the following general demographic questions. Please choose the answer that best describes you. There are also two questions that are related to your computer use.

1) Gender

-Select- ▾

- Male
- Female

2) Age

□ Under 22

□ 22 - 29

□ 30 - 39

□ 40 - 49

□ 50 - 59

□ 60 - 69

□ 70 and over

3) What best describes your academic major?

○ Computers

○ Business

○ Liberal Arts

○ Mathematics

○ Engineering

4) I use computers:

○ I don't unless I have to ○ A little ○ Moderately ○ A lot

5) I am anonymous when using the Internet:

○ Disagree strongly ○ Disagree ○ Neutral ○ Agree ○ Agree strongly

-------------------------------------Page Break--------------------------------------

STOP... Keep this page open

Please raise your hand and wait patiently. Do not continue this survey until the researcher comes over and you receive specific instructions.

Thank you.

-------------------------------------Page Break-------------------------------------

Below are a number of items related to activities that relate to computer use. Some of these items may be regarded as antisocial. Please respond to these items as honestly as possible and be aware that your answers to the questions are only going to be used for research purposes.

WHEN WAS THE MOST RECENT TIME THAT YOU:

		Never	Within the past month	Within the past year	1-4 years ago	5 or more years ago
6)	Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?	○	○	○	○	○
7)	Tried to guess another's password to get into his/her computer account or files?	○	○	○	○	○
8)	Accessed another's computer account or files without his/her knowledge or permission just to look at the information or files?	○	○	○	○	○
9)	Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?	○	○	○	○	○
10)	Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or trojan horse)?	○	○	○	○	○
11)	Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?	○	○	○	○	○
12)	Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?	○	○	○	○	○
13)	Knowingly used, made, or gave to another person a device to obtain free long distance phone calls?	○	○	○	○	○

HOW OFTEN IN THE PAST THREE YEARS HAVE YOU:

		Never	Once	2-3 times	4-5 times	6+ times
14)	Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?	○	○	○	○	○
15)	Tried to guess another's password to get into his/her computer account or files?	○	○	○	○	○
16)	Accessed another's computer account or files without his/her knowledge or permission just to look at the information or files?	○	○	○	○	○
17)	Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?	○	○	○	○	○
18)	Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or trojan horse)?	○	○	○	○	○
19)	Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?	○	○	○	○	○
20)	Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?	○	○	○	○	○
21)	Knowingly used, made, or gave to another person a device to obtain free long distance phone calls?	○	○	○	○	○

HOW OLD WERE YOU THE FIRST TIME YOU:

		Does not apply to me	16 or less	17-18	19-20	21 or older
22)	Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?	○	○	○	○	○
23)	Tried to guess another's password to get into his/her computer account or files?	○	○	○	○	○
24)	Accessed another's computer account or files without his/her knowledge or permission just to look at the information or files?	○	○	○	○	○
25)	Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?	○	○	○	○	○
26)	Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or Trojan horse)?	○	○	○	○	○
27)	Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?	○	○	○	○	○
28)	Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?	○	○	○	○	○
29)	Knowingly used, made, or gave to another person a device to obtain free long distance calling?	○	○	○	○	○

30) I am anonymous when using this computer:

○ Disagree strongly

○ Disagree

○ Neutral

○ Agree

○ Agree strongly

-------------------------------------Page Break-------------------------------------

Please rate the degree to which you agree with the following statements about you. You can be honest because your name is detached from the answers.

		Disagree Strongly	Disagree	Neutral	Agree	Agree Strongly
31)	I have never been involved in delinquent gang activity.	○	○	○	○	○
32)	I have never stolen a truck, car or motorcycle.	○	○	○	○	○
33)	I have tricked someone into giving me money.	○	○	○	○	○
34)	I have assaulted a law enforcement official or social worker.	○	○	○	○	○
35)	I have never tried to force someone to have sex.	○	○	○	○	○
36)	I have never attacked someone with the idea of injuring them.	○	○	○	○	○
37)	I have broken into a building or vehicle in order to steal something or vandalize.	○	○	○	○	○
38)	I have never been arrested.	○	○	○	○	○
39)	I have taken hard drugs (e.g., heroin, cocaine).	○	○	○	○	○
40)	I never shoplifted from a store.	○	○	○	○	○
41)	I was convicted of a serious crime.	○	○	○	○	○
42)	Every now and then I carry a weapon (knife or gun) for protection.	○	○	○	○	○
43)	I have threatened people into giving me money, clothes, or makeup.	○	○	○	○	○
44)	I have close friends who served time in prison.	○	○	○	○	○
45)	I purposely tried to hit someone with the vehicle I was driving.	○	○	○	○	○
46)	I have violated my probation from prison.	○	○	○	○	○

--------------------------------------Page Break--------------------------------------

Please answer the following questions as honestly as possible.

This part of the survey was not included for Copyright reasons (PPI survey)

Please click on "Submit"

powered by www.psychdata.com

Appendix D – Consent and Post Consent Forms

Research Project Number_______________

RESEARCH PARTICIPANT CONSENT FORM

Anonymity and computer usage
Dr. Marcus Rogers
Purdue University
Department of Computer and Information Technology

Purpose of Research: In this research, the experimenters are interested in individual differences in how people use computers to answer questions. You will be asked to complete several popular measures used in psychological research. You will then be trained to answer a couple of questions, and see the correct answers. Finally, you will have the opportunity to answer a number of challenging questions that will increase by difficulty.
Specific Procedures to be Used: You will be asked to sit and complete a survey presented on the computer. This will include a variety of questions about yourself and your personality. You will then be asked to answer a couple of questions that increase by difficulty.
Duration of Participation: Your participation will take no more than 60 minutes.
Benefits to the Individual: There are no direct benefits to participating in this study. However, you may have the opportunity to learn about differences in how people use computers.
Risks to the Individual: Minimal: The risks to the participants are minimal. They are not greater than those ordinarily encountered in daily life, although you may feel emotionally uncomfortable due to a couple of questions we will ask you to answer.

Confidentiality: Only researchers associated with this study will have access to the responses associated with this study. The project's research records may be reviewed by departments at Purdue University responsible for regulatory and research oversight. Strict confidentiality of the data will be upheld. Your responses will not be associated with any identifying information; your name will not be attached to your responses at any point. The anonymous data will be kept in the Cyber Forensics Lab's locked file cabinet for five years.

Voluntary Nature of Participation: You do not have to participate in this research project. If you agree to participate you can withdraw your participation at any time without penalty. You do not have to answer any question you find objectionable.

Human Subject Statement: If you have any questions about this research project, you can contact Dr. Marcus Rogers, 49-42561 (or by email, rogersmk@purdue.edu). If you have concerns about the treatment of research participants, you can contact the Committee on the Use of Human Research Subjects at Purdue University, 610 Purdue Mall, Hovde Hall Room 307, West Lafayette, IN 47907-2040. The phone number for the Committee's secretary is (765) 494-5942. The email address is irb@purdue.edu.

I HAVE HAD THE OPPORTUNITY TO READ THIS CONSENT FORM AND HAVE THE RESEARCH STUDY EXPLAINED. I HAVE HAD THE OPPORTUNITY TO ASK QUESTIONS ABOUT THE RESEARCH PROJECT AND MY QUESTIONS HAVE BEEN ANSWERED. I AM PREPARED TO PARTICIPATE IN THE RESEARCH PROJECT DESCRIBED ABOVE. I WILL RECEIVE A COPY OF THIS CONSENT FORM AFTER I SIGN IT.

______________________________ ______________________________
Participant's Signature Date

____
Participant's Name

______________________________ ______________________________
Researcher's Signature Date

Research Project Number: ________________________

RESEARCH PARTICIPANT POST-CONSENT FORM
Anonymity and computer usage
Dr. Marcus Rogers
Purdue University
Department of Computer and Information Technology

Purpose of Research: The purpose of the research is to study the links among being anonymous, personal integrity and anti social behavior on the use of computers. If you were asked for your name, e-mail address, and street address, you are no longer anonymous (but in truth that information was not stored). When you were trained to answer the questions that vary by difficulty, you had to push a button to see the correct answer. We then asked you to start answering the question to the best of your ability. Later on, when we showed the same indicator that showed up when viewing the correct answer, we used this situation to see if you actually attempted to take advantage of, to get the correct answer (before answering the questions).

Specific Procedures Used: Being anonymous or not anonymous was totally determined by random assignment. It did not reflect any evaluation of you as an individual; it was merely chance.

Why Deception Was Necessary: Deception is necessary for this research so that the experimenters can measure reactions to the level of anonymity. To see how people respond naturally, we could not reveal this aspect of the experiment prior to recording your responses. When people know about the purpose of some experiments ahead of time, they often cannot or will not behave as they normally would do.

Confidentiality: Only researchers associated with this study will have access to the responses associated with this study. The project's research records may be reviewed by departments at Purdue University responsible for regulatory and research oversight. Your responses will not be associated with any identifying information. Each participant will receive an experimental number that will be attached to his or her materials. There will be no way to identify you from your responses. Strict confidentiality of data will be upheld. In addition, all of your data will be discarded if you decide to indicate that preference below.

Human Subject Statement: If you have any questions about this research project, you can contact Dr. Marcus Rogers 49-42561 (or by email, rogersmk@purdue.edu). If there are concerns about the treatment of research participants, you can contact the Committee on the Use of Human Subjects at Purdue University, 610 Purdue Mall, Hovde Hall Room 307, West Lafayette, IN 47907-2040. The phone number for the Committee's secretary is (765) 494-5942. The email address is irb@purdue.edu.

I HAVE BEEN FULLY DEBRIEFED BY THE EXPERIMENTER. I HAVE HAD THE OPPORTUNITY TO READ THIS CONSENT FORM AND HAVE THE RESEARCH STUDY EXPLAINED. I HAVE HAD THE OPPORTUNITY TO ASK QUESTIONS ABOUT THE RESEARCH PROJECT AND MY QUESTIONS HAVE BEEN ANSWERED. I AM PREPARED TO PARTICIPATE IN THE RESEARCH PROJECT DESCRIBED ABOVE. I WILL RECEIVE A COPY OF THIS CONSENT FORM AFTER I SIGN IT. AS A RESULT,
____ PLEASE DISCARD ALL DATA COLLECTED
____ I GIVE PERMISSION TO HAVE MY DATA USED IN THIS RESEARCH PROJECT

(***Please initial one of the above options***)

______________________________ ____________________
Participant's Signature Date

____
Participant's Name

______________________________ ____________________
Researcher's Signature Date

VITA

VITA

IBRAHIM MOUSSA BAGGILI

614 South Street, Apartment 5
Lafayette, IN 47901
765-409-2138
baggili@purdue.edu
http://baggili.weebly.com

EDUCATION: Purdue University, West Lafayette, IN

Ph.D. in Computer and Information Technology, Cyber Forensics, *Expected Aug 2009*
Dissertation: *An exploratory study on the relationship between anonymity, antisocial behaviors, integrity and computer crime.*
Advisor: Marcus K. Rogers

Master of Science in Computer and Information Technology, Computer Programming Technology, May 2005
Thesis: *Diabetic e-management system*

Bachelor of Science in Computer and Information Technology, Network Engineering Technology, Dec 2002

Course experience in the following areas:

- Development with web services
- Business oriented application development with focus in enterprise applications
- Two-Tier and three tier application development
- Web application development
- Database administration & development
- Programming event driven and object oriented
- Development with component objects
- Organizational leadership skills
- Communication: personal, small group, and technical
- Management of Information Technology
- E-commerce and E-business applications

- The business of E-commerce
- Engineering forensics
- Technology from a Global Perspective
- Wide Area Networks and Local Area Network technologies
- System administration
- Network security
- Relational database design
- Mobile Computing
- Biometric Technologies
- Project management
- System analysis and design
- Quality of Management
- Organizational Behavior and Human Resources
- Research analysis and design methodologies
- Digital Forensics
- Small Scale Digital Device Forensics
- Curriculum development
- Philosophy of Science
- Forensic Accounting

CERTIFICATIONS: **Computer Forensics**

Access Data boot camp certification (Passed the Practical Skills Assessment

Access Data – Windows Forensics, Registry and Applied decryption.

ACADEMIC HONORS: **Bilsland Dissertation Fellowship**

A limited amount of students are awarded a dissertation fellowship out of a school-wide pool of applicants. The amount of the award was $23,000. The award is given to Ph.D. students in the final stages of their dissertations 2008-2009.

Department School Travel Grant/Support

The department covered the expenses of presenting some of my publications at conferences.

Graduate Student TAship and Stipend

A TAship was provided to me since the beginning of my masters. Jan 2003 – August 2009.

Nominations

- Nominated for "The Chancellor's List", 2005-2006, "The highest academic honor to which graduate students can aspire"
- Nominated for the "Outstanding Innovations in "Helping Students Learn", Purdue University 2006

Distinctions and Honors

- Bachelor of Science with distinction, Purdue University, Dec 14, 2002
- Associate of Science with distinction, Purdue University, Dec 15 2001

- Recognized by the National Society of Collegiate Scholars
- Honors and Dean’s list, 8 semesters consecutively

TEACHING EXPERIENCE:

Purdue University, West Lafayette, IN
Graduate Lecturer, 05 to present
Application Development Course

- Provided continuous help for the students.
- Formulated programming assignments in the .NET environment for students to learn the new technology.
- Graded, created and assessed programming assignments.

Purdue University, West Lafayette, IN
Graduate Lecturer, 09
Graduate Course on Cyber Forensics

- I was designated as the fill-in instructor for the course when the main instructor was not available.
- Facilitated class discussions on various topics.
- Directed students towards finding topics for their research projects.

Purdue University, West Lafayette, IN
Teaching Assistant/Mobile Lab Coordinator, 03-05
Enterprise Application Development and Mobile Development
Application Development courses/Network Administrator

- Performed network administration duties for the lab utilizing Win 2K Server, Win 2K clients, Proxy server, Ghosting, IIS and firewalls, ISA server and SQL server.
- Graded assignments that utilized the Pocket PC .NET compact framework for mobile devices in the C# programming environment.
- Graded assignment that utilized the full .NET framework in the C# programming language.

Purdue University, West Lafayette, IN
Teaching Assistant, Jan 03 – May 03
Local Area Networking

- Provided continuous help for the students.
- Provided help to students in server OS environments that included 2000 Server, Novell, Netware 5.1 and Linux.
- Graded and assessed technical documentations.
- Installed a VPN server for student dial-up into the laboratory’s internal network.
- Programmed an Online Student Peer Evaluation System (OSPES).

OTHER WORK EXPERIENCE:

Security Triangle, Amman, Jordan
Founder and consultant, 05-07

- Managed ongoing projects for the company.
- Worked on network engineering projects.
- Aided in the design and programming of software systems for corporate use.
- Formed and closed various Information Technology contracts.
- Performed research in new and growing areas in the Cyber Forensics field.

Purdue University, West Lafayette, IN
CERIAS and CNIT Researcher, 05-09

- Created and worked with other graduate students on various research projects:
    - SMS author attribution experiment
    - SMIRK (SMS management and Information Retrieval Kit)
    - FOX (Forensics on EXIF)
    - Anonymity survey creation
    - Hand geometry biometrics project
    - SMS author attribution
- Wrote a preliminary grant proposal

BISYS Education Services Indianapolis, IN
Policies, Procedures and Standards Developer, S03

- Formulated a Project Management, and Project Management Office manual for internal and corporate testing.
- Documented Information Technology policies, procedures and standards.
- Documented and formulated Security related policies, procedures and standards.
- Documented and formulated application development policies, procedures and standards.

Purdue University, Herrick Labs West Lafayette, IN
Electronic Shop Assistant / Webmaster/Application Developer, 02

- Designed an information system that includes point-to-point sales, with a database backend and a bar code scanner interface.
- Documented program and conducted software testing methodologies.
- Trained end users, and provided extensive training guides.
- Installed and maintained Apache web server for windows.
- Maintained the local network and technical help desk.

Total, Abu Dhabi, United Arab Emirates
IT Intern, S02

- Built an Access database program, for specific logistical purposes.
- Worked at the help desk, and helped configure 60 new workstations using Ghost.

- Facilitated with a network design that included a network that had to be setup and configured through a satellite connection, for communication on an offshore oilrig.
- Researched various software products that allowed the company to manage an inventory database of oilrig related pipes and parts.

Chi Phi Fraternity, Kappa Zeta Chapter West Lafayette, IN
Graduate Advisor/Alumni Relations, Sp 03 – F05

- Contacted alumni for continuous projects and ongoing events.
- Formulated projects for incoming new members, for raising capital.
- Advised active members on academic matters.
- Advised the Executive Council on various events, projects and budgets.

PUBLICATIONS: **Books:**

Baggili, I. Ravai, G. (2007). *Step into programming with visual basic .NET*. Kendall Hunt.
Baggili, I. Ravai, G. (2008). *Step into programming with visual basic .NET*. (2nd Edition).Kendall Hunt.

Journal Articles/Proceedings/Magazines

Mohan, A., Baggili, I., Rogers, M. (2009). Optimal parameters for authorship attribution of SMS messages using an N-gram approach. In publication.

Yousef, A., Baggili, I. Mymryk, J. Bartlett, G. (2009). Laboratory Inventory Network Application. In publication.

Baggili, I. Mohan, A. Rogers, M. (2009). Forensics on EXIF: An investigative tool. In publication.

Baggili, I., Mislan, R., & Rogers, M. (2007). Mobile phone forensics tool testing: A database driven approach. *International Journal of Digital Evidence*. 6(2).

Baggili, I., Kiley, M. (2007). Digital forensics: a brief overview of critical issues. *Forensic magazine.* Issue: October/November.

Baggili, I. (2006). Forensic scene documentation using mobile technology. *Conference on digital forensics, security and law*. Las Vegas, Nevada.

Baggili, I., Lutes, K. (2006). Diabetic e-management system. *Information technology new generations.* Las Vegas, Nevada.

Baggili, I. (2006). Search and seizure from a digital perspective: a reflection on Kerr’s Harvard Law. *Forensic Focus*: *computer forensics news, information and community.*

CONFERENCE OR SYMPOSIUM COORDINATION:

Chair, *ITNG: Digital Forensics track. A conference with the proceedings that are published in* IEEE. 2007.

PROFESSIONAL ACTIVITIES:

Reviewer and program committee, *Informing Science & Information Technology Education joint Conference* (InSITE). 2006.

CONFERENCE PARTICIPATION

Represented Jordan at the International Citizen of the year award ceremony, 2007 that was given to President Martin C. Jischke of Purdue University.

Presented at the 2nd Mobile Phone Forensics World Conference (2009). Topic: SMS Management and Information Retrieval Kit (SMIRK) & Data mining in cell phone forensics. (Invited guest speaker)
Presented at the Third International Conference of Information

Technology: New Generation, 2006, Las Vegas, Nevada with an IEEE conference proceeding publication. Topic: Diabetic E-Management System.

Presented at the first annual ADFSL (Association of Digital Forensics Security and Law), 2006, Las Vegas, Nevada, with a JDFSL (Journal of Digital Forensics Security and Law) conference proceeding publication. Topic: Crime Scene Documentation using Mobile Technology.

WorkLife / Wellness / EAP Symposium, April 2005. Topic: Diabetic e-Management System.

E-enterprise, Discovery Park, Purdue University 2004. Topic: Diabetic e-Management System.

Regenstrief Center Health Care Delivery Systems Workshop, Purdue University 2004. Topic: Diabetic e-Management System

Indiana Health Industry Forum, Indianapolis, IN, 2004. Topic: Diabetic e-Management System.

IGLC, Indiana Greek Leadership Conference, West Lafayette, IN, 2003.

MEDIA:

Featured in a live TV program in Jordan (JTV), as one of the most accomplished young Jordanians, and for being the first Arabic person to pursue a PhD in Digital Forensics.

Featured in technology a program on Sama Dubai TV in the United Arab Emirates, as the first Arabic person to pursue a PhD in Cyber Forensics.

Featured in Al Dustour newspaper, in Jordan, as the first Arabic person to pursue a PhD in Cyber Forensics and as well as for being a very accomplished individual.

Featured in Al Ghad newspaper, in Jordan, as the first Arabic person to purse a PhD in Cyber Forensics as well as for being a very accomplished young individual.

Featured in Al Arab Al Yawm newspaper, in Jordan, as the first Arabic person to pursue a PhD in Cyber Forensics as well as for being a very accomplished young individual.

REFERENCES

Reference 1 – Major advisor
Dr. Marc Rogers
Professor/University Faculty Scholar
Director - Cyber Forensics Program/ Cyber Forensics Masters Area of Specialization

Purdue University
Department of Computer and Information Technology
401 N Grant St.,West Lafayette, IN 47907
Phone: 765-494-2561, Fax: 765-496-1212
E-mail: rogersmk@purdue.edu

Reference 2 – PhD committee member
Dr. William Graziano
Professor of Psychological Sciences
Purdue University
Department of Psychological Sciences
Rm. PSYC 2170
703 Third Street, West Lafayette, IN 47907-2081
Phone: (765) 494-7224, Fax: (765) 496-1264
E-mail: graziano@purdue.edu

Reference 3 – Coauthor of a book and course manager
Guity Ravai
Continuous Lecturer
Purdue University
Department of Computer and Information Technology
Knoy Hall of Technology, Room 239
401 N Grant St.,West Lafayette, IN 47907

Phone: (765) 496-6005, Fax: (765) 496-1212
E-mail: guity@purdue.edu

Reference 4 – PhD committee member
Richard P. Mislan (ABD)
Assistant Professor
Purdue University
Department of Computer and Information Technology
Knoy Hall of Technology, Room 223
401 N Grant St.,West Lafayette, IN 47907
Phone: (765) 494-2563, Fax: (765) 496-1212
E-mail: rmislan@purdue.edu