COMPARING THE COGNITIVE ABILITIES OF HACKERS AND NON-HACKERS USING A SELF-REPORT QUESTIONNAIRE

by

Kellin Nicol Treadway

A Thesis

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Master of Science

Department of Computer and Information Technology
West Lafayette, Indiana
May 2017

ProQuest Number: 10258947

All rights reserved

INFORMATION TO ALL USERS
The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript
and there are missing pages, these will be noted. Also, if material had to be removed,
a note will indicate the deletion.

ProQuest 10258947

Published by ProQuest LLC (2017). Copyright of the Dissertation is held by the Author.

All rights reserved.
This work is protected against unauthorized copying under Title 17, United States Code
Microform Edition © ProQuest LLC.

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 – 1346

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF THESIS APPROVAL

Dr. Kathryn Seigfried-Spellar, Chair

Department of Computer and Information Technology

Dr. Marc Rogers

Department of Computer and Information Technology

Dr. Don Lynam

Department of Psychological Sciences

Approved by:

Professor Jeffrey L. Whitten

Head of the Departmental Graduate Program

For my mother. For my father. For my Spencer.

ACKNOWLEDGMENTS

The completion of this project has been a long time coming, and I could not have made it this far without a number of people who provided support along the way. I would like to thank my thesis committee for bearing with me through this process. Dr. Kate, Dr. Rogers, and Dr. Lynam, thank you for your patience, your assistance, and your faith in me. Furthermore, I would like to thank Stacy Lane in the Department of Computer and Information Technology at Purdue University for all of her long-distance help. Stacy, thank you for your quick responses to my hundreds of emails; I would have been lost and clueless without you. I would also like to thank Brenda Parsons in the Department of Criminology and Criminal Justice at The University of Alabama for just being her amazing, problem-solving self. Brenda, you are a rock star.

I would like to thank my mother for always being my biggest cheerleader and my father for having my back, no matter what. Even though we cannot choose our parents, I would always, always choose both of you. I would like to thank my fiancé, Blake Brasher, for always keeping me grounded (and well-fed when I would forget to eat). Spencer, thank you for talking me off the ledge each and every time; I love you. I would also like to thank the rest of my family, related and otherwise; I am blessed to have so many people to love. Finally, I would like to thank my CJ family. You all shared in the insanity of this process. I love each and every one of you

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CCI-R – Computer Crime Index – Revised (Rogers, Smoak & Liu, 2006).

GPA – grade point average

EECM – Effort Expenditure Comparison Measure (Smith et al., 2013).

IQ – intelligence quotient.

ICAR – International Cognitive Ability Resource (Condon & Revelle, 2014).

SRAPM – Self-Rated Academic Performance Measure (Heaven et al., 2002).

WAIS-R – Weschler Adult Intelligence Scale – Revised (Weschler, 1991)

GLOSSARY

Computer Crime Index – Revised (CCI-R) – a measure of deviant computer behavior (Rogers et al., 2006b).

Hack or hacking behavior – an unauthorized intrusion into a network or computing device (cf., Rogers, 2006).

Hacker – an individual who performs an intrusion into a network or computing device without authorization (cf., Rogers, 2006).

Intelligence quotient (IQ) – the scaled measure of an individual's intelligence (Hernstein & Murray, 1994).

ABSTRACT

Author: Treadway, Kellin N. M.S.
Institution: Purdue University
Degree Received: May 2017
Title: Comparing the Cognitive Abilities of Hackers and Non-Hackers Using a Self Report Questionnaire
Major Professor: Dr. Kathryn Seigfried-Spellar

Hackers are typically represented in the media as having high levels of intelligence, but there is little empirical research available on the topic of IQ and hacking behaviors. Low IQ scores are associated with criminality in general, but higher IQ scores and education are positively correlated with white collar crime, of which criminal hacking behaviors are a subset. Therefore, the present study sought to examine cognitive abilities of self-reported hackers and non-hackers, as well as compare the cognitive abilities scores of different subsets of hackers, in a sample of Mechanical Turk workers using the International Cognitive Ability Resource and the Computer Crimes Index – Revised.

CHAPTER 1. INTRODUCTION

According to a recent Gallup poll, more Americans fear identity theft and cell phone data breaches than they are concerned with physical assaults (Riffkin, 2014). Moreover, the FBI's current Internet Crime Complaint Center (IC3; 2014) report demonstrates recent hacker activity. In 2014, the IC3 received a total of 269,422 complaints, nearly half of which resulted in a financial deficit for an average dollar loss of $6,472 per complaint and a total loss of $800,492,073.00. In addition, researchers at the Ponemon Institute report that, in 2014, nearly half (i.e., 47%) of the population of American adults were victims of a data breach which made their financial information vulnerable to hackers (Pagliery, 2014). Such findings could indicate that the latest surge in data breaches and hacker threats have worked against the public perception of information security in the current tech-savvy society. In such environments, fears can lead to stereotypes, especially when these stereotypes are further reinforced by popular media. Therefore, hackers are often perceived as super-geniuses who can assume control of the nation's critical infrastructures with just a click of the mouse.

1.1 Statement of Purpose

The literature is contradictory on the issue of computer deviants and criminals. According to some previous research (cf., Hernstein & Murray, 1994; Hirschi & Hindelang, 1977; White, Moffit, & Silva, 1989) those convicted of delinquent or criminal behavior are more likely to demonstrate a lower IQ score. However, the commission of most computer-related crimes (i.e., criminal or "black-hat" hacking) typically requires a certain level of technical knowledge and skill (Rogers, 2006). Furthermore, it has been generally assumed that computer hackers are highly intelligent, more so than the average individual.

Therefore, the research on criminal behavior would predict a lower IQ score for those who engage in criminal activities, including computer-related crimes, but the literature on computer hackers would suggest these individuals are equipped with more technical skills and intelligence than the average person. Thus, the present study sought to compare the IQ scores of self-reported computer hackers with self-reported non-hackers in order to determine if IQ scores differ across a sample population of Mechanical Turk “workers.” Although current literature contributes to the knowledge on hackers and hacking behaviors, further research is needed in order to more fully understand these types of individuals.

1.2 Research Questions

Do cyberdeviants vary significantly on cognitive ability scores?

1.3 Significance of the Problem

The lack of knowledge about a topic can sometimes lead to fear of the subject matter. Recently, major hacking attempts and successes have been headlining the news. Target, the United States Postal Service, Anthem health insurance, and many others all share a common trait; they were targeted for large-scale data breaches (Abrams, 2014; Kumparak, 2014; Weise, 2015). In addition, the latest trend in vehicle safety has less to do with air bags and more to do with the security of the car’s onboard computer system (Rushe, 2015). With technology now standard in many cars, trucks, and SUVs, the newest fear amongst car owners is the ability for outsiders to hack into their vehicles’ system controls and override the driver’s input (Rushe, 2015). Most notably, though, was the incident with Sony that occurred in December 2014 when the motion picture production company postponed the release of *The Interview* after a hacker’s threats of violence (Fitzpatrick, 2014). Furthermore, many popular movies (e.g., *Live Free or Die Hard*, *The Matrix*, *The Girl with the Dragon Tattoo*) and television shows (e.g., *Person of Interest*, *CSI: Cyber*, *Mr. Robot*) depict hackers as super-geniuses who can access a country’s critical infrastructure with just a few clicks on a laptop computer (cf., Internet Movie Database [IMdb]).

For those who have less knowledge of technology, such claims by Hollywood may be perceived as true fact, which perpetuates the fear and mystique of computer hackers, and frequent media coverage of data breaches and hacking attempts likely contributes to the American public’s fear associated with such behaviors. For instance, a

Gallup poll from October 2014 indicates the two main criminal concerns in the United States are associated with cybercrime (Riffkin, 2014). Most Americans fear being a victim of identity theft via a store's data breach or a hacking attempt against their cell phone more than they fear being a victim of murder or sexual assault (Riffkin, 2014). For instance, 62-69% of individuals specify they worry frequently over data theft, compared to the 18% who indicate a greater-than-average concern for physical assault (Riffkin, 2014). These findings demonstrate a broad apprehension for computer crimes, as well as a general mistrust of digital security.

However, the term "hacker" was not originally intended to have a negative connotation, and in fact, not every modern hacker has nefarious intentions (Fötinger & Ziegler, 1993; Schell & Holt, 2009). Furthermore, not all hacking behaviors require a high level of technical knowledge and skill (Rogers, 2006). Script kiddies (or novices), for instance, have less technical skill than others who engage in hacking behaviors, as these lower-level hackers use programming code written by more skilled individuals in order to deface websites and otherwise make a nuisance of themselves (Rogers, 2006).

Theoretically, then, what the public perceives as behavior befitting someone with genius-level IQ (i.e., an IQ score which is several deviations above the mean; Herrnstein & Murray, 1994) could be carried out by an individual with an average level of intelligence, as little research exists to suggest a trend in either direction. Therefore, the present study sought to add to the literature on actors involved in computer deviant behavior.

1.4 Assumptions

The assumptions of the present study were as follows:

- Individuals solicited for participation may choose not to complete the survey.
- Participants who begin the survey may not complete it in its entirety.
- Participants responded honestly to the survey questions.

1.5 Limitations

The limitations of the present study were as follows:

- The researcher solicited participants from the Mechanical Turk website.
- The researcher compared cognitive ability scores between different subtypes of self-reported cyberdeviants (e.g., hackers versus virus-writers).
- The researcher compared cognitive ability scores amongst the different levels of cyberdeviant behavior.
- The researcher made these comparisons based on responses collected via a Qualtrics survey, which included a demographics questionnaire, the Computer Crime Index – Revised (CCI-R), and the International Cognitive Ability Resource (ICAR).

1.6 Delimitations

The delimitations of the present study were as follows:

- The present study did not include computer deviancy where the computing device is simply used as the tool to complete the deviant act, such as child pornography or cyberbullying.
- The proposed study will not include the computer deviancy commonly referenced as “pirating,” which is the unauthorized downloading of media or software without payment, due to the marginalization of this behavior in society (cf., Gunter, Higgins, & Gealt, 2010; Rogers, Seigfried, & Tidke, 2006).
- The researcher did not solicit the survey outside of the Mechanical Turk website, which served as the population for the present study.
- Only data from those residing in the United States and above the age of 18 years were included in final data analysis.

1.7 Summary

The rise of data breaches and hacker threats may have contributed to a misbegotten stereotype of hackers as super-geniuses with high IQs, and the fear of hacking behavior is similarly reflected in the public opinion. Although prior research on IQ and criminality suggests a correlation between low IQs and criminal offending, most hacking behaviors require a certain level of technical skill, which might be indicative of a higher IQ.

The present study sought to further the knowledge of hacking behaviors and related IQ scores. The researcher assumes respondents answered the survey questions honestly and that solicited participants may choose not to complete the survey and/or complete only a portion of the survey.

The present study did not include literature or data analysis on “computer-as-a-tool” forms of cyber deviancy (i.e., cyberbullying and child pornography), and only responses from residents of the United States over the age of 18 were included in final data analysis. The researcher solicited these participants via the Mechanical Turk website, and respondents were asked to anonymously answer items from a self-report survey consisting of a demographics questionnaire, an education assessment, the International Cognitive Ability Resource (ICAR), and the Computer Crime Index – Revised (CCI-R).

CHAPTER 2. REVIEW OF THE LITERATURE

The expansive news coverage of recent data breaches (cf., Abrams, 2014; Kumparak, 2014; Weise; 2015), along with the portrayal of computer hackers in popular media, demonstrates a certain public mindset about hackers in general (cf., Furnell, 2002; Holt, Bossler, & Seigfried-Spellar, 2015; Rogers, 1999a; Rogers, 2001; Schell & Dodge, 2002). Therefore, the hacker stereotype persists, as many believe these individuals are extremely intelligent, young, white men with the knowledge and skill to anonymously hack into any secured network and tamper with national security (cf., Holt et al., 2015; Schell & Dodge, 2002).

Furthermore, early literature on network intrusions labeled every type of unauthorized entry as hacking. However, this one-dimensional view of hackers is inaccurate, as this is a diverse group of individuals with varying goals, motivations, intents, and backgrounds (cf., Parker, 1998; Rogers, 1999a; Rogers, 1999b; Rogers, 2001; Rogers, 2010; Schell & Dodge, 2002; Schell & Martin, 2004). Additionally, little to no literature specifically addresses the IQ of hackers, despite the proliferation of research on IQ and general criminality.

2.1 Defining Hacking

Hacking was not always associated with criminal activity (cf., Fötinger & Ziegler, 1993 Schell & Dodge, 2002; Schell & Holt, 2009), and not all hacking behaviors are identical (cf., Parker, 1998; Rogers, 2010; Schell & Dodge, 2002). A hacker is someone who gains unauthorized access to a computer or network (Chiesa, Ducci, & Ciappi, 2009; Fötinger & Ziegler, 1993; Parker, 1998; Rogers, 1999a; Rogers, 1999b; Rogers, 2006; Rogers, 2010; Rogers et al., 2006a; Rogers et al., 2006b; Schell & Dodge, 2002; Schell & Holt, 2009; Holt et al., 2015; Wall, 2007). However, this definition does not take into account the many different sub-types of hacking behavior that exist (cf., Parker, 1998; Rogers, 2010; Shaw, Post & Ruby, 1999).

Prior to its adoption by computer scientists, the term “hacker” was a Yiddish word that referred to an “inept furniture maker” (Schell & Dodge, 2002; Schell & Martin, 2004). However, modern use of the word originated in the 1960s with an all-male club at

MIT. In its original application, the word “hacker” was considered a term of distinction because it was used for those who could write programming code for “hacks,” or shortcuts, which would better the performance of sluggish computer programs (Fötinger & Ziegler, 1993; Holt et al., 2015; Schell & Martin, 2004; Schell & Holt, 2009).

Despite its innocuous origins, however, “hacking” has taken on a negative connotation over the years, beginning with the “phone phreakers” of the 1960s and ‘70s (Fötinger & Ziegler, 1993; Holt et al., 2015; Parker, 1998; Robson, 2004; Schell & Dodge, 2002; Schell & Holt, 2009; Schell & Martin, 2004). Phreakers, like Kevin Mitnick and “Captain Crunch,” would use various means of making phone calls across state and international borders free of charge (Holt et al., 2015; Parker, 1998; Robson, 2004; Schell & Dodge, 2002; Schell & Martin, 2004). Kevin Mitnick employed social engineering methods, posing as an employee of the phone company to gain access to confidential records and private phone numbers (Holt et al., 2015; Parker, 1998; Robson, 2004; Schell & Dodge, 2002; Schell & Martin, 2004). John “Captain Crunch” Draper would use a whistle given as a free toy inside boxes of cereal bearing his namesake in order to place free phone calls to countries around the world; the sound emitted by the whistle was the perfect frequency to “trick” the telephone system into placing expensive long-distance phone calls at no charge to Draper (Holt et al., 2015; Parker, 1998; Robson, 2004; Schell & Dodge, 2002; Schell & Martin, 2004). For a more detailed account of the history of hacking, see the thorough review provided by McBrayer (2014).

2.1.1. Hacker Subtypes

Hackers who engage in criminal behavior are referred to as black hat hackers or crackers (Holt et al., 2015; Rogers, 2010; Schell & Dodge, 2002; Schell & Martin, 2004; Wall, 2007). These individuals seek to either destroy property or steal information (Holt et al., 2015; Rogers, 2010; Schell & Dodge, 2002; Schell & Martin, 2004; Wall, 2007), and most are motivated by hedonistic goals, such as greed, revenge, or notoriety (Chiesa et al., 2009; Fötinger & Ziegler, 1993; McBrayer, 2014; Schell & Dodge, 2002; Schell & Martin, 2004).

However, not all hackers are criminals (Holt et al., 2015; Rogers, 2010; Schell & Dodge, 2002; Schell & Martin, 2004). White hat hackers adhere to a strict moral code and only hack when directed to do so by a legitimate authority (Holt et al., 2015; Schell & Dodge, 2002; Schell & Martin, 2004). For example, many companies employ white hat hackers to test the company's online security measures in order to find and repair potential breach points (Holt et al., 2015; Schell & Martin, 2004). Additionally, some white hat hackers are also "hunters" who seek out their black hat counterparts (Chiesa et al., 2009). Therefore, many white hats do not acknowledge those who have no respect for the hacking code of ethics (cf., Levy, 2001) as hackers (Chiesa et al., 2009; Fötinger & Ziegler, 1993; Schell & Dodge, 2002). Thus, the main difference between white and black hats can be summed up as follows: "hackers build things, crackers break them" (as cited in Fötinger & Ziegler, 1993, p. 8).

As for the black hats, Parker (1998) initially identified seven subtypes of cybercriminals, including pranksters, career criminals, extreme advocates, and malcontents/addicts/incompetent individuals. Parker (1998) also distinguished between hackers (i.e., those interested in furthering their knowledge or skills who gain access to a computer system or network without permission,), malicious hackers (also known as crackers; i.e., those motivated to inflict damage), and personal problem solvers (i.e., those interested in hacking to solve problems in their personal lives, such as financial issues). Each of Parker's (1998) hacker subtypes are mirrored in Rogers (2006; 2010) taxonomy. However, not every hacking behavior included in Rogers' (2006; 2010) taxonomy are illegal. For instance, one of Rogers' (2006; 2010) hacker categories, the coders/virus-writers, includes some white hats who offer their codes to anti-virus software companies so measures can be taken to protect against new types of malware (Kirwan & Power, 2012).

Furthermore, Rogers (2006) classified hackers along a continuum based on motivation and skillset (see Figure 2.1). Rogers' (2010) latest taxonomy includes the four major groups included in his earlier research (i.e., old school hackers, script kiddies/cyber-punks, professional criminals, and coders/virus-writers; cf., Rogers, 2006), along with several more categories (i.e., hacktivists, identity thieves, cyber-terrorists, internals, and the "Old Guard"; Rogers, 2010).

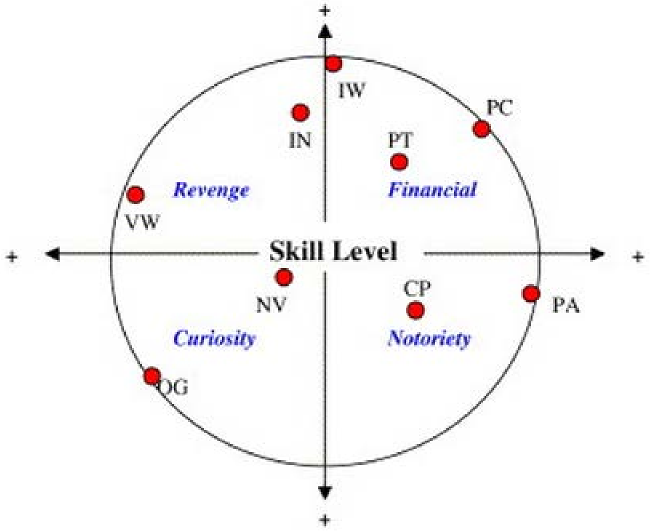


Figure 2.1 Hacker Circumplex
"*Note*: Novice (NV), Cyber-punks (CP), Petty Thieves (PT), Virus writers (VW), Old Guard hackers (OG), Professional Criminals (PC), Information Warriors (IW), Political Activists (PA), PA is included as a discussion point only" (Rogers, 2006, p.100).

Outside of Rogers' (2010) continuum are the "Old Guard," or what Parker (1998) referenced as hackers (i.e., those interested in furthering their knowledge or skills who gain access to a computer system or network without permission). This group consists of "old school" hackers who lack nefarious intent and are more concerned with writing and analyzing lines of code than causing harm (Fötinger & Ziegler, 1993; Rogers, 2010). However, they do feel information should be widely available (Fötinger & Ziegler, 1993; Rogers, 2010). Therefore, these old school hackers share their codes with those who may be less skilled in writing their own code (e.g., script kiddies), thereby indirectly allowing their codes to be used maliciously (Rogers, 2010). For the most part, though, these types of hackers are more interested in upholding the ideals of intellectual challenge and discovery that harkens back to the first generation of hackers (Rogers, 2010).

However, on the low end of the continuum for skillset are the crackers, which includes Parker's (1998) categories for pranksters and malicious hackers; these are the hacker types modernly known as script kiddies and cyber-punks (cf., Fötinger & Ziegler, 1993; Holt et al., 2015; Rogers, 2006; Rogers, 2010; Schell & Dodge, 2002). Those in this group are commonly considered the "typical hacker" (Rogers, 2010). This category of hacker also includes hacktivists, though hacktivists have a different type of motivation than that of script kiddies and cyber-punks, and some exhibit a greater level of skill than that typically attributed to script kiddies and cyber-punks (Rogers, 2010; Schell & Martin, 2004; Wall, 2007).

Script kiddies and cyber-punks are viewed as the “wannabes” of the hacking world, as they lack sophistication and often rely on programming code written by others without understanding the intricacies of it (Holt et al., 2015; Rogers, 2010; Schell & Dodge, 2002). Therefore, this group is more concerned with the results of a hacking attempt than the methods used to execute it (Chiesa et al., 2009; Schell & Dodge, 2002).

Rogers’ (2010) findings suggest script kiddies are most often 12 to 30 year-old white males, which opposes Chiesa et al.’s (2009) results indicating this type of behavior is typically found in adolescents. Cyber-punks are of a similar age, though slightly younger than script kiddies at 12 to 18 years old (Rogers, 2010). Also, cyber-punks tend to favor website defacement (Rogers, 2010). However, both script kiddies and cyber-punks disrespect authority and societal regulations, and they are often motivated by a thrill-seeking ego, as their self-esteem requires constant bolstering by demonstrations of perceived superiority (Chiesa et al., 2009; McBrayer, 2014; Rogers, 2010; Schell & Dodge, 2002).

Therefore, because they like to boast of their escapades, both script kiddies and cyber-punks are frequent and easy targets of police intervention (Chiesa et al., 2009; Rogers, 2010). Hacktivists, on the other hand, may simply be cyber-punks or script kiddies who act in a manner coinciding with their political views (Rogers, 2010). For example, cyber-punks typically deface websites, but a hacktivist may be motivated to deface a website in a certain way so as to make a political statement.

Next on Rogers’ (2010) continuum are identity thieves, which reflects Parker’s (1998) group of personal problem solvers. These thieves target systems to steal credit card data and other information that allows them to use another’s credit to make purchases and large transactions (Rogers, 2010; Wall, 2007).

Although identity thieves are typically more skilled than most crackers (i.e., script kiddies and cyber-punks), they are also less skilled than the professionals (also known as career criminals), an elitist sect of hackers who view their criminal activities as a career and treat their exploits accordingly (Parker, 1998; Rogers, 2010). Identity theft behavior perpetrated by professionals is typically linked to organized crime and corporate espionage (Rogers, 2010), whereas general identity thieves are more akin to Parker's (1998) description of personal problem solvers in that they are motivated by meeting a desire for financial advantage via "quick and easy" methods (Parker, 1998, p. 145; Rogers, 2010).

In his classification of hackers, Parker (1998) listed virus-writers as malicious hackers, but as previously mentioned, not all virus-writers act with malicious intent (cf., Rogers, 2010). Furthermore, not all virus-writers are equally skilled or write their own code (Rogers, 2010). For instance, "click kiddies" can create viruses and malware with just a click of a mouse, which requires far less technological skill and knowledge than the complex programming code used by more advanced virus-writers (Rogers, 2010). In addition, click kiddies, script kiddies, and cyber-punks are usually responsible for unleashing viruses online, as virus-writers are more often motivated by the intellectual challenge of creating the malware than they are interested in causing harm (Kirwan & Power, 2012; Rogers, 2010).

The last group included in Rogers' (2010) continuum are the cyber-terrorists, or those whom Parker (1998) referred to as extreme advocates. Although seemingly similar to hacktivists, this group is concerned with effecting change via severe tactics, and thus, actions from these online terrorists might be misappropriated to malicious virus-writers or cyber-punks (Rogers, 2010; Wall, 2007). Furthermore, cyber-terrorists act more violently and on a larger scale than most hacktivists, as many cyber-terrorists imagine themselves as freedom fighters, waging a cyberwar against those who oppose their views or seek to oppress their liberties (Rogers, 2010).

Likewise, the threat from internal hackers is often cause for concern, as these types of attacks are difficult to defend against (Claycomb, Legg, & Gollmann, 2014; Cummings et al., 2012; Gelbstein, Wuest, & Fridakis, 2012), and they are destructive (Claycomb et al., 2014; Cummings et al., 2012; Gelbstien et al., 2012; Gelbstein, 2014; Randazzo et al., 2005; Rogers, 2010; Schell & Dodge, 2002; Schell & Martin, 2004; Shaw et al., 1999). For instance, Cummings et al. (2012) report an attack by a malicious insider that resulted in a financial deficit of $28 million for one of the companies they surveyed. In addition, Gelbstein et al. (2012) cite research by Forrester, who found financial loss due to downtime after an attack can range from $10,000 to over $1 million *per hour*. Such an event could be disastrous for a company, resulting in loss of integrity and credibility, as well as customers (Gelbstein et al., 2012).

Furthermore, their typically high-ranking position allows internals to inflict damage in the course of otherwise sanctioned activities, either by infecting a computer or computer system (e.g., via malware) or by stealing information (e.g., via keyloggers or spyware; Claycomb et al., 2014; Cummings et al., 2012; Gelbstein, 2014; Schell & Dodge, 2002). Therefore, internal hackers are less likely to be caught than those from outside the company (Schell & Holt, 2009).

Authorized employees must also be able to access certain files and programs in order to do their work, so security measures for these individuals have to be less restrictive; it is easier to block all entry from the outside than to maintain security measures that vary from employee to employee (Gelbstein, 2014). Likewise, many company employees would know how to circumvent security restrictions (Gelbstein et al., 2012). Therefore, relative to their positions as IT professionals, internals are typically more skilled than other types of hackers on Rogers' (2010) continuum.

However, not every internal acts with malicious intent (Claycomb et al., 2014; Cummings et al., 2012; Gelbstein et al., 2012; Gelbstein, 2014). For some, the harm inflicted on the company is unintentional and due to simple user error (Claycomb et al., 2014; Cummings et al., 2012; Gelbstein et al., 2012; Gelbstein, 2014). Although financial gain is most often the primary motive for internal actors (McBrayer, 2014; Randazzo et al., 2005; Wall, 2007), revenge is also a common motivator (Rogers, 2010; Wall, 2007). For instance, attacks against a corporation are more likely to originate from "vengeful insiders" within a company than from those on the outside (Gelbstein et al., 2012; Shaw et al., 1999; Rogers, 2010).

Therefore, due to this homogeneity of intent and skill, the hacker category of internals would include Parker's (1998) group of malcontents, addicts, and irrational people, as well as his classification of malicious hackers. Shaw et al. (1999) further categorize these insider hackers into a subset typology which are similar to the groups in

Rogers' (2010) general taxonomy of cybercriminals, but with their skills focused on internally hacking a corporation rather than externally.

2.2 Intelligence Quotient (IQ)

"IQ" is an acronym for intelligence quotient, though Porter & Carson (2009) extrapolate that the shortened term has now become "self-sufficient" and can stand alone without its original intended meaning. Indeed, IQ was never a measure of true intelligence (Fletcher & Hattie, 2011; Herrnstein & Murray, 1994; Porter & Carson, 2009). Rather, the purpose of modern IQ testing created by Alfred Binet was to categorize Parisian schoolchildren and determine if education could impact their "mental age," which is calculated by dividing the individual's score on the IQ measure by their age in years and multiplying this number by 100 in order to derive a whole number (Fletcher & Hattie, 2011; Nairne, 2013).

However, the vast majority of IQ tests are proprietary in nature, as well as expensive and difficult to administer (cf. Condon & Revelle, 2014; Thorndike, Hagen, & Sattler, 1986; Weschler, 1991). Because most IQ tests involve an assessment of cognitive ability (Condon & Revelle, 2014), the present study includes a measure of cognitive ability similar to and correlating with traditional IQ scales. Therefore, the discussion of IQ also references cognitive ability.

2.2.1. IQ and Criminality

Through his inferiority theory of feeblemindedness, Goddard (1914) was the first to introduce the notion that low IQ scores were a cause for general criminality, stating that half of all criminals have cognitive deficiencies (cf., Mears & Cochran, 2013). Therefore, Goddard (1914) was also a proponent of the sterilization and ostracizing of the mentally disabled in order to lessen criminality in society (cf., Mears & Cochran, 2013). Although Goddard's (1914) ideals would now be considered drastic and unethical, much research in the past several decades demonstrates a correlation between lower IQ scores and criminal offending (Bartels et al., 2010; Beaver & Wright, 2011; Herrnstein & Murray, 1994; Hirschi & Hindelang, 1977; Lynam, Moffitt, & Stouthamer-Loeber, 1993;

Mears & Cochran, 2013; Oleson & Chappell, 2012; Rushton & Templer, 2009; White et al., 1989; Wilson & Herrnstein, 1985).

Lynam et al. (1993) studied data from a group of fourth-grade boys participating in the Pittsburgh Youth Study (PYS). The PYS sample included 508 boys, half of whom were at high risk for delinquency; the other half of the sample served as a comparison group (Lynam et al., 1993). The results of the Lynam et al. (1993) study indicate a significant relationship between delinquency and both verbal IQ and full-scale IQ, with those who were classified as serious delinquents ranging 10 to 11 points lower on IQ scores compared with those categorized as exhibiting lower levels of delinquent behavior. In addition, performance IQ was significantly higher than verbal IQ for those classified as serious delinquents, in contrast to the smaller interaction effect observed for the comparison group of those who reported no delinquent behaviors. Also, the variation between verbal and performance IQ scores was smaller for the black boys than for their Caucasian counterparts.

Although Lynam et al. (1993) controlled for the effect of test performance as a positively correlated factor associated with all three IQ scores (full-scale, verbal, and performance), both the full-scale and verbal IQ scores of delinquents were still significantly lower than those of nondelinquents (Lynam et al., 1993). The results of the Lynam et al. (1993) research support the findings of Hirschi and Hindelang (1977), which found lower IQ scores amidst higher levels of delinquency.

Similar to the Lynam et al. (1993) research, results from the Beaver and Wright (2011) study indicate IQ scores at the county level and crime rates from each type of crime included in data analysis (i.e., property crimes including burglary, larceny, and motor vehicle theft, and violent crimes including robbery and aggravated assault) were significantly related. Higher county-level IQ scores were associated with lower county crime rates for each of the seven types of crime (Beaver & Wright, 2011). These results were still statistically significant, even after controlling for the collective measure of factors which place a location at a high risk for crime (e.g., locations with a high percentage of low-SES inhabitants). These findings support previous research (cf., Bartels et al., 2010, McDaniel, 2006). Beaver and Wright (2011) posit that, due to the significant relationship between IQ scores from each county and crime rates from each type of crime included for analysis, these results indicate a similar association between IQ and all types of criminal activity.

In addition, Bartels et al. (2010) report similar findings in their study on IQ scores and crime rates at the state level. McDaniel (2006) provides an estimate of IQ scores based on the National Assessment of Educational Progress (NAEP)'s standardized test scores on reading and math, and Bartels et al. (2010) utilized this data for their own study comparing state-level IQ scores and crime rates; the statistics on crime were collected between 2005 and 2006 from the FBI's Uniform Crime Report. Results from Bartels et al. (2010) indicate a statistically significant negative correlation between state crime rates and McDaniel's (2006) estimated IQ scores, supporting previous research (cf., Bartels et al., 2010; Beaver & Wright, 2011; Herrnstein & Murray, 1994; Hirschi & Hindelang, 1977; Lynam et al., 1993; Mears & Cochran, 2013; Oleson & Chappell, 2012; Rushton & Templer, 2009; White et al., 1989; Wilson & Herrnstein, 1985). Higher crimes rates (specifically for violent crimes, like murder and aggravated assault, and property crimes, such as burglary, theft, and motor vehicle theft) were associated with lower IQ scores (Bartels et al., 2010).

Furthermore, state-level IQ score was found to be a significant predictor of burglary crimes, and state-level IQ score and race (i.e., black) were both found to be significant predictors for criminal homicide (Bartels et al., 2010). A significant relationship was also found between state-level IQ and race, though these results were not discussed further. Bartels et al.'s (2010) findings mirror those of McDaniel (2006), despite using data collected from the UCR for different years; McDaniel's (2006) data was retrieved from the UCR from 2002-2004.

Similar to Bartels et al.'s (2010) study comparing IQ scores and crime rates at the state level, Rushton and Templer (2009) focused their research on comparing IQ scores and crime rates but at the international level. Rushton and Templer (2009) included a sample of data from a total of 113 countries and three types of violent crimes (i.e., murder, rape, and serious assault). In line with other literature (cf., Bartels et al., 2010; Beaver & Wright, 2011; Lynam et al., 1993), Rushton and Templer (2009) report that higher IQ scores are associated with lower crime rates.

Mears and Cochran (2013) also report a relationship between IQ scores and levels of offending, but findings in their study indicate a curvilinear association. Like Herrnstein and Murray (1994), Mears and Cochran (2013) used the Armed Forces Qualification Test (AFQT) as their measure of IQ. Mears and Cochran (2013) also included other factors along with IQ, such as social class, area of residence (i.e., urban or rural), religious participation, work ethic, and locus of control; levels of criminal offending were measured based on a self-report scale. Participants in the study ranged in age from 14 to 22 years (Mears & Cochran, 2013).

Although higher IQ scores (i.e., scores between 93 and 109) were found to correlate with lower rates of offending, IQ scores in the lowest decile (i.e., scores between 77 and 83) were found to have a similar relationship (Mears & Cochran, 2013). Thus, both high IQ scores and low IQ scores were associated with less criminal offending, and IQ scores falling in the middle range (i.e., scores between 84 and 92) were associated with higher rates of offending. However, the authors caution that their research focused on white males, which could indicate a lack of generalizability to other racial groups (Mears & Cochran, 2013).

Mears and Cochran (2013) also caution that differences in IQ measures, along with other potentially confounding variables (e.g., socioeconomic status) and level of detection by the authorities (cf., Cullen et al., 1997; Herrnstein & Murray, 1994; Hirschi & Hindelang, 1977; Lynam et al., 1993), may muddle some of the literature on the association between IQ scores and levels of criminal offending. For instance, Cullen et al. (1997) have criticized Herrnstein and Murray (1994), stating the relationship between IQ scores and delinquency was less meaningful than portrayed. Instead, Cullen et al. (1997) believe this relationship between IQ and criminality was “at best, modest” (p. 388).

However, utilizing a self-report measure, Moffitt and Silva (1988) found that IQ scores were similar across levels of police detection in 13-year-old delinquents; both discovered and undiscovered acts of delinquency were related to lower IQ scores. Mears and Cochran (2013) also report a similar association between IQ scores and level of offending as previous literature, even after controlling for other variables, such as social status. Furthermore, a large body of literature supports the association between low IQ scores and higher crime rates (cf., Bartels et al., 2010; Beaver & Wright, 2011;

Herrnstein & Murray, 1994; Hirschi & Hindelang, 1977; Lynam et al., 1993; Mears & Cochran, 2013; Oleson & Chappell, 2012; Rushton & Templer, 2009; White et al., 1989; Wilson & Herrnstein, 1985).

2.2.2. IQ and Hacking

Despite the available literature on the association between IQ scores and criminality, the author has found no empirical research to date on the relationship that might exist between IQ scores and deviant computer behaviors, such as hacking. However, Jennings (2014) reported higher education levels of computer criminals in a sample of prisoners in federal and state penitentiaries, compared to other types of incarcerated offenders.

In general, hacking behaviors typically involve some level of technical skill, which has facilitated the perception of the computer deviant as having esteemed intelligence. For example, popular media demonstrates a societal belief that some fields of study are populated by individuals viewed as more intelligent than those in other areas of academia, and recent data from the 2013 SAT® Report on College and Career Readiness support this notion (cf., Lubin, 2013; The College Board, 2013).

In addition, television shows like *The Big Bang Theory* help to propagate the notion that super-geniuses arise from the hard sciences (e.g., physics, biology, engineering), and such perceptions could lead some to believe that those with certain degrees have higher IQs. Furthermore, Owen and Sawhill (2013) report that those in engineering, math, science, and computer-related fields demonstrate the highest earning potential, and previous research offers findings that support the stereotype that hackers emerge from technological, mathematical, or scientific fields. Schell and Holt (2009), Shaw et al. (1999), and Rogers (2010) found most hackers had training as IT professionals. Fötinger and Ziegler (1993) also noted, aside from "the obvious computer science and electrical engineering" (p. 12) fields, hackers tend to associate with areas of math and physics, as well as linguistics and philosophy. In addition, Chiesa et al. (2009) reported chemistry was also a favorite among hackers, as well as computer security.

Furthermore, Coldwell (1994) found science teachers are more likely to be accepting of hacking behaviors than other teachers, with 65% of science teachers reporting a tolerance for computer deviance versus 35% of other teachers. Likewise, undergraduates in a similar discipline also reported an overall acceptance of hacking over their peers (Coldwell, 1994). In turn, these findings support an earlier one from Coldwell (1993), who reported students from “machine-based disciplines” were less likely than those from “people-based disciplines” to distinguish social consequences of hacking (p.11). Coldwell (1993) posited these results call into question what some students consider ethical. Although, a more recent study found no significant difference between degree majors for hacking behaviors specifically (i.e., gaining unauthorized access to a computer system or network), Seigfried-Spellar & Treadway (2014) posit that their results could be indicative of a shift to a more “tech-savvy” society.

2.2.3. IQ and White Collar Crime

Many computer crimes could also be categorized as white collar crimes (cf., Jennings, 2014), and previous research suggests a view on the apparent association of these types of crimes and IQ scores that contrasts the literature on more general crimes (e.g., violent crimes, property crimes) and IQ scores (cf., Benson & Moore, 1992; Lochner, 2004; Murray, 1997; Raine et al., 2012).

Raine et al. (2012) used neuroimaging technology, as well as subsections of the Wechsler Adult Intelligence Scale – Revised (WAIS-R; cf., Wechsler, 1981), to measure executive functioning in a sample of 75 males and 12 females between the ages of 21 and 46. Levels of white collar criminal activity were assessed using the National Youth Survey (cf., Raine et al., 2000), a self-report scale which measures violent crimes (including sex crimes), property crimes, and drug offense. The study’s authors compared subsets of their sample on levels of white collar offending; 21 self-reported white collar criminals (consisting of 18 males and 4 females) were matched on gender, age, and race with their non-white-collar-offending counterparts. Results indicated those who had self-reported as white collar criminals scored higher on the verbal IQ and performance IQ scales, though this finding was non-significant (Raine et al., 2012).

However, the sample in Raine et al.’s (2012) could be of some concern due to the overrepresentation of male participants in a relatively small sample size. Monk-Turner et al.’s (2006) results indicated men were more likely to self-report hacking behaviors, such as pirating software, unauthorized computer or network intrusion, and abuse of privileges related to a job position. In contrast to Monk-Turner et al. (2006), though, Jennings (2014) found women incarcerated in federal and state prisons were more likely to be imprisoned for computer crimes than other types of delinquency. Therefore, the gender discrepancy in Raine et al.'s (2012) study should be considered.

Although Raine et al.'s (2012) findings concerning IQ scores and white collar crime were non-significant, education has also been found to correlate negatively with white collar crime; white collar crime is associated with more education and better grades (Benson & Moore, 1992; Jennings, 2014; Lochner, 2004; Lochner & Moretti, 2004; Walters & Geyer, 2004). In turn, education is positively correlated with IQ (Nairne, 2013). Jennings' (2014) results indicate a greater likelihood for more education in a sample of inmates incarcerated in federal and state prisons. According to Jennings (2014), "for every year of education the prisoner has, their odds of being in prison for computer crime increase significantly" (p. 92). Jennings (2014) posits this result is due to those who were familiar with technology early in life achieving and maintaining white collar careers after graduating college.

Similarly, findings from Lochner (2004) are in direct opposition to the literature that indicates education level is positively correlated with crime rates (cf., Lochner & Moretti, 2004). Lochner and Moretti (2004) report higher levels of education are associated with lower rates of the more visible street crimes, such as violent crimes and property crimes (as cited in Lochner, 2004). According to the authors, an average increase of a single year of education would reduce arrest rates for these types of crimes (i.e., violent crimes, property crimes) by at least 10% (Lochner & Moretti, 2004; as cited in Lochner, 2004). However, white collar crime has the opposite effect; Lochner (2004) reports that arrest rates for white collar crimes *increase* by as much as 11% for every extra year of schooling. Both studies used data from the National Longitudinal Survey of Youths, as well as the Uniform Crime Reports and the U.S. Census.

The literature discussed thus far focuses on the quantity of education and its relationship with white collar crime, but Benson and Moore (1992) included a measure of educational quality by comparing the school grades of white collar criminals and so-called common offenders (i.e., those facing incarceration for drug offenses and property crimes). Benson and Moore (1992) examined data regarding defendants in eight district court cases between 1973 and 1978. Their final data analysis included 2,462 white collar criminals and 1,986 common criminals (Benson & Moore, 1992). Results from the study indicate 53.5% of common criminals made poor grades in school, compared to the 24.6% of white collar criminals who reported poor grades (Benson & Moore, 1992). Therefore, white collar offenders were more likely to do better in school (i.e., make better grades) than defendants charged with drug offenses or property crimes (Benson & Moore, 1992).

However, the availability of online vocational schools have increased since the time of Benson and Moore's (1992) research (cf., Allen & Seaman, 2013). Thus, a greater number and larger demographic of individuals now have access to education via online resources (Allen & Seaman, 2013).

2.3 Summary

The term "hacker" applies to a variety of individuals with technical skills that range from the laymen's point-and-click method to the more sophisticated code-writing. Therefore, IQ scores could vary across this range of hackers, and it is possible these scores might not be significantly different from the average population of non-hackers. The research disagrees on the issue of deviant computer behavior and level of IQ, as more traditional forms of criminality are understood to be associated with lower IQ scores, but other types of crime (i.e., white collar crimes) are concomitant with higher IQ scores, as well as higher levels of education. Thus, the computer hacker offers a particular dilemma in regards to understanding the relationship between deviant computer behavior and IQ.

CHAPTER 3. METHODOLOGY

The goals of the present study were as follows: (1) to compare the cognitive ability scores of self-reported cyberdeviants with the cognitive ability scores of self-reported non-cyberdeviants, (2) to compare the cognitive ability scores of self-reported cyberdeviants amongst the various subtypes (i.e., hackers, identity thieves, and virus-writers), and (3) to compare the cognitive ability scores of those who self-report engaging in more general computer deviance with those who report engaging in fewer deviant computer behaviors, all through the use of self-report questionnaires and data analysis. Due to the proprietary nature and lack of flexibility of traditional IQ tests (cf. Condon & Revelle, 2014; Thorndike et al.,1986; Weschler, 1991), a measure similar to and correlating with traditional IQ scales, the International Cognitive Ability Resource (ICAR), was used in the present study.

3.1 Hypotheses

Based on the literature regarding criminal computer behavior, white collar crimes, and IQ scores (Benson & Moore, 1992; Fotinger & Ziegler, 1999; Furnell, 2002; Holt et al., 2015; Jennings, 2014; Lochner, 2004; Lochner & Moretti, 2004; Parker, 1998; Rogers, 1999a; Rogers, 2001; Rogers, 2006; Rogers, 2010; Schell & Dodge, 2002; Walters & Geyer, 2004), the hypotheses for the present study were as follows:

- ICAR Sample Test scores would be significantly higher for the subtypes of self-reported cyberdeviants than non-cyberdeviants (i.e., hackers vs. non-hackers, identity thieves vs. non-identity thieves, and virus-writers vs. non-virus-writers).
- ICAR Sample Test scores would be significantly higher for those who self-report engaging in any of the included cyberdeviant behaviors (i.e., hacking, identity theft, and virus-writing) than those who self-report not engaging in these deviant computer behaviors.
- ICAR Sample Test scores would be significantly higher for those who self-report engaging in more deviant computer behaviors (e.g., hacking, virus-writing,

identity theft) than those who self-report engaging in fewer deviant computer behaviors.

3.2 Sample

Participants for the study were solicited from Amazon's Mechanical Turk; respondents were representative of the general population of Internet users (cf., Buhrmester, Kwang, & Gosling, 2011). The survey solicitation was only available to those designated as "Masters" on Mechanical Turk (i.e., those with a history of quality response rates). APA guidelines for the ethical treatment of participants were followed, and all responses remained anonymous. Based on previous research related to payment amount and questionnaire length (cf., Buhrmeste et al., 2011), each respondent was compensated $0.40 for the completion of the survey, which is a sufficient amount to solicit survey responses (Buhrmester et al., 2011). Funds allotted for paying participants for survey completion were disbursed from the Department of Computer and Information Technology at Purdue University.

3.3 Measures

The anonymous, self-report survey was created and maintained via Qualtrics survey software. All survey items were forced-response with the option for participants to "decline to respond" to any question they chose not to answer. The survey was a multitrait matrix including the following scales: a demographics questionnaire, an education assessment, Condon and Revelle's (2014) International Cognitive Ability Resource (ICAR), and Rogers et al.'s (2006b) Computer Crime Index – Revised (CCI-R). The education assessment and the ICAR measure were randomized to reduce the possibility of responses being altered based on any expectation of education or intelligence from preceding questions.

The demographics questions and the education assessment items were listed first in the survey so as to increase the accuracy of self-reported demographic characteristics (cf., Birnbaum, 2000) and to lessen survey exposure for those who do not meet the criteria for study participation. The CCI-R was the final questionnaire in the survey so as to ensure response accuracy. Participants might self-report differently on the education assessment or the ICAR if the items on the CCI-R were encountered first. For instance, respondents who self-report as hackers might conform to a preconceived notion that hackers are more intelligent individuals who excel in school, and therefore, response data would be skewed.

3.3.1. Demographics Questionnaire

The demographics questionnaire (see Appendix A) was used to determine participants' country of residence, age, sex, marital status, annual income, and ethnicity. Respondents currently residing outside the United States (i.e., not under American legislative jurisdiction) and/or those less than 18 years of age (i.e., minors) were excluded from the study.

3.3.2. Education Assessment

The education assessment for the present study (see Appendix B) was derived from Jennings' (2014) study, the Self-Rated Academic Performance Measure (SRAPM; Heaven et al., 2002), and the Effort Expenditure Comparison Measure (EECM; Smith et al., 2013). The author of the present study compiled an education assessment derived from numerous sources due to the lack of a single questionnaire that would adequately measure a participant's educational history.

Items derived from Jennings' (2014) three-question education scale ask participants to indicate their highest level of attempted and completed education; responses for both questions range from "less than high school" to "Doctoral degree or higher."

Heaven et al.'s (2002) Self-Rated Academic Performance Measure (SRAPM) includes a total of three items, all of which were included in their entirety in the education assessment for the present study. These items ask participants to rate their overall academic performance (with response options ranging from "top 10% of all students" to "below average"), the level of education they hope to obtain, and how often they experience(d) difficulty with schoolwork (Heaven et al., 2002).

Smith et al.’s (2013) Effort Expenditure Comparison Measure (EECM) includes a total of four items, all of which were included in their entirety in the education assessment for the present study. In Smith et al.’s (2013) EECM, participants were asked to compare themselves to other students when answering the following four questions:

- How much effort do you expend in your field of study?
- To what extent do you find the material and work in your field challenging?
- To what extent does your field come easily and naturally to you?
- How much energy does it take you to succeed in your field?

The EECM uses a Likert scale response format ranging from 1 (“a lot less”) to 5 (“a lot more”; Smith et al., 2013).

For the present study, the education scale initially reported a low Cronbach’s alpha (α = .43), indicating a lack of reliability. Based on the subsequent Kuder-Richardson (KR-20) coefficient analysis, the item regarding self-rated academic performance was removed from further data analysis. However, this removal resulted in a Cronbach’s score that was still below acceptable limits (α = .51). Therefore, the education assessment was excluded from further data analysis. This will be explored further in the limitations section (see Chapter 5.2).

3.3.3. International Cognitive Ability Resource (ICAR)

The ICAR Sample Test (see Appendix C) was used to score respondents’ cognitive ability, as it measures similar intelligence constructs as IQ tests (Condon & Revelle, 2014). Furthermore, the ICAR scale was developed specifically for the use of online, self-report research, as it is a performance task measure (Condon & Revelle, 2014). IQ tests are typically administered by doctoral-level psychologists via one-on-one interviews with individual participants, and these types of tests are often expensive and proprietary (Condon & Revelle, 2014; Thorndike et al., 1986; Weschler, 1991). However, Condon and Revelle (2014) propose such IQ assessments are not conducive for research purposes, that the “constraints” of such measures have led cognitive ability research to be excluded from much of the literature on psychological assessment. Instead, the authors (citing Goldberg, 2012) suggest a freely available public domain measure of cognitive ability would offer more flexibility for researchers in the social sciences. Therefore, Condon and Revelle (2014) constructed the International Cognitive Ability Resource (ICAR), an untimed, performance task measure of cognitive ability with constructs similar to traditional IQ tests.

The original ICAR assessment includes 60 items which measure the following four subscales of cognitive ability: verbal reasoning, letter and number series, matrix reasoning, and three-dimensional rotation (Condon & Revelle, 2014). The ICAR Sample Test includes four questions from each subscale for a total of 16 questions (Condon & Revelle, 2014). The verbal reasoning items assess general logic and knowledge skills. The letter and number series prompts the test-taker to complete a sequence of letters or numbers based on the preceding digits in the list. Example questions from the verbal reasoning and letter and number series subscales of Condon and Revelle's (2014) ICAR measure are as follows:

- Verbal reasoning: "If the day after tomorrow is two days before Thursday, then what day is it today?"
- Letter and number series: "In the following alphanumeric series, what letter comes next? V Q M J H"

The matrix reasoning component is based on those used in Raven's Progressive Matrices, a traditional assessment of cognitive ability (Condon & Revelle, 2014). Test-takers are shown geometric shapes presented in a 3 x 3 formation and asked to identify which geometric shape would follow in the established pattern (see Figure 3.1).

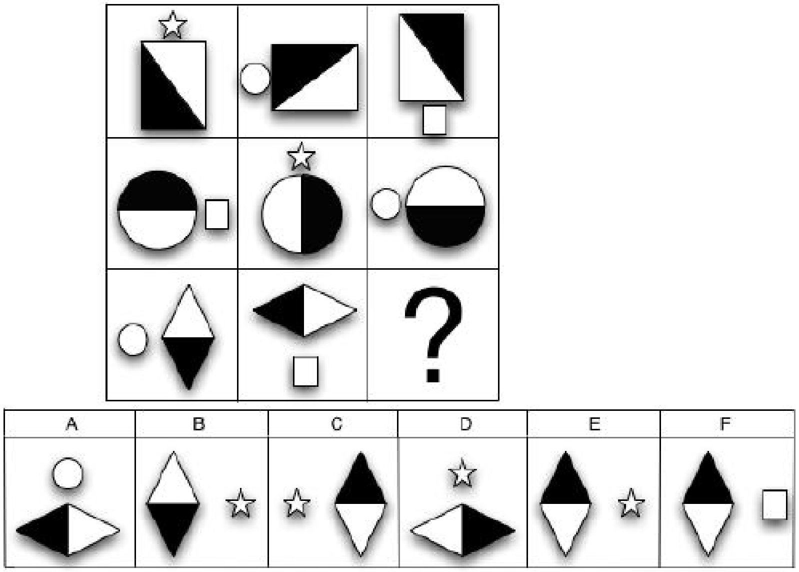
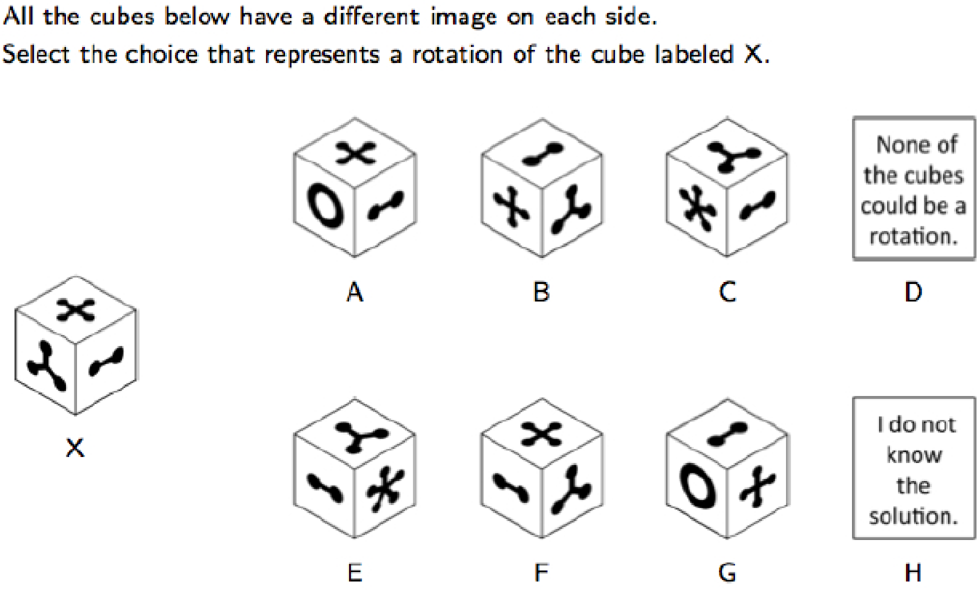


Figure 3.1 Matrix Reasoning Item on the ICAR Sample Test

Finally, the three-dimensional rotation series assesses respondents’ ability to mentally rotate images of cubes similar to dice (see Figure 3.2; Condon & Revelle, 2014).


All the cubes below have a different image on each side.
Select the choice that represents a rotation of the cube labeled X.

A
B
C
None of the cubes could be a rotation.
D
X
E
F
G
I do not know the solution.
H

Figure 3.2 Three-Dimensional Rotation Item on the ICAR Sample Test

The ICAR Sample Test is meant to be a brief, but valid, measure of cognitive ability, used specifically for self-report purposes in research (Condon & Revelle, 2014). The 16 questions selected for the ICAR Sample Test were chosen based on their difficulty in relation to the other items on the original, 60-item ICAR measure. Of the item subscales, the three-dimensional rotation tasks were determined to be the most difficult (i.e., more respondents incorrectly answered the questions assessing this type of skill), and the verbal reasoning questions were found to be the least difficult (Condon & Revelle, 2014). The ICAR Sample Test questions were randomized for the present study, based on Condon and Revelle's (2014) research.

In total, Condon and Revelle (2014) analyzed data from 96,958 respondents across 199 countries; 78.1% of the sample originated from the United States. Condon and Revelle (2014) found strong correlations between the ICAR scale and standardized tests (0.59 for the SAT and 0.52 for the ACT), as well as traditional IQ tests. The Shipley-2 scale (cf. Shipley et al., 2009; 2010) includes two composites, and scores on these composites were positively associated with the ICAR Sample Test (0.82 and 0.81), as well as the Wonderlic Personnel Test (0.64 and 0.60), the Full-Scale IQ scores for the Weschler Abbreviated Scale of Intelligence (0.77 and 0.72), and the Full-Scale IQ scores for the Weschler Adult Intelligence Scale (0.86 and 0.85; Condon & Revelle, 2014; Shipley et al., 2010). Therefore, the ICAR scale has been shown to correlate with traditional measures of cognitive ability (Condon & Revelle, 2014).

Although it was a concern that an online, untimed, self-report measure of cognitive ability would lead to higher reported scores, Condon and Revelle's (2014) findings indicate this was not the case; respondents' scores varied sufficiently across the sample. Participants were more likely to incorrectly answer over half of the questions included on the full 60-item ICAR measure. Likewise, items assessing three-dimensional rotation received incorrect responses more often than not (Condon & Revelle, 2014).

Additional findings from Condon and Revelle (2014) indicate adequate internal consistency for the 16-item ICAR Sample Test ($\alpha = 0.81$; $\omega_{total} = 0.83$) and good internal consistency for the full 60-item ICAR measure ($\alpha = 0.93$; $\omega_{total} = 0.94$). Overall, the ICAR Sample Test in the present study reported an adequate Cronbach's alpha ($\alpha = .75$), a finding which is similar to Condon and Revelle's (2014) overall Cronbach's alpha for the ICAR Sample Test ($\alpha = 0.81$).

As for the subscales, reliability analyses conducted by Condon and Revelle (2014) on items from the full 60-item measure indicate internal consistencies ranging from adequate for the matrix reasoning, letter and number series, and verbal reasoning items (α

= 0.68, α = 0.77, and α = 0.76 respectively) to good internal consistency for the three-dimensional rotation items (α = 0.93). For the present study, the ICAR Sample Test subscales had the following reported Cronbach's alphas: verbal reasoning (α = .61), letter and number series (α = .63), matrix reasoning (α = .51), and three-dimensional rotation (α = .62). Due to the low Cronbach's score, the matrix reasoning subscale was removed from analysis because of its lack of reliability. Therefore, only 12 of the original 16 items from the ICAR Sample Test were included in data analyses; these items were taken from the subscales measuring verbal reasoning, letter and number series, and three-dimensional rotation skills. This will be explored further in the limitations section (see Chapter 5.2).

3.3.4. Computer Crime Index – Revised (CCI-R)

Rogers et al.'s (2006) CCI-R (see Appendix D) was used to categorize cyberdeviants and non-cyberdeviants. The primary measure of the CCI-R is the actor's intent (i.e., whether they acted knowingly and purposefully). The initial version of the Computer Crime Index was created by Rogers (2001) and included a measure based on social learning theory (cf., Akers, 1977; Skinner & Fream, 1997; Rogers, 2001). Subsequent research led to the current form of the Computer Crime Index – Revised (CCI-R), which includes a similar format as the original; the items associated with social learning theory were removed, and questions regarding deviant computer behavior were added (cf., Rogers, 2001; Rogers et al., 2006a; Rogers et al., 2006b).

The CCI-R is a self-report questionnaire with a total of 66 items divided into three sections, all of which include a closed-response, Likert scale format (Rogers, 2001; Rogers, 2006b). In the first section, respondents were asked to use a scale to indicate the time period they last participated in the described behaviors, ranging from "Never" to "5 or more years ago" (Rogers, 2001; Rogers et al., 2006b). In the subsequent sections of the CCI-R, respondents were asked how many times in the previous three years they engaged in the behaviors and at what age they first committed the listed acts (Rogers, 2001; Rogers et al., 2006b). The same set of 22 questions were repeated in each of the three sections, which increases the reliability of respondents' answers (Bryman, 2012).

The behaviors listed in the CCI-R include items related to hacking (i.e., the unauthorized access of a computer system or network), pirating (i.e., illegally downloading media without payment), identity theft, virus-writing, and cyberbullying (Rogers et al., 2006b; Seigfried-Spellar & Treadway, 2014; Seigfried-Spellar, O'Quinn, & Treadway, 2014). Based on the coding techniques of Seigfried-Spellar and Treadway (2014) and Seigfried-Spellar et al. (2014), categories for the CCI-R were determined as follows: 36 items that address hacking behaviors, 9 items that correspond with identity theft, 9 items that correspond with virus-writing, and 6 items which address cyberbullying behaviors. As the present study did not include cyberbullying data, the items related to online bullying behaviors were not included on the survey. Furthermore, due to the marginalization of pirating behavior in society (Gunter et al., 2010; Rogers et al., 2006a; Seigfried-Spellar & Treadway, 2014), this behavior was also excluded from the present study.

Therefore, the final item count for the portion of the CCI-R to be used in the present study was 60, and only those behaviors corresponding with hacking (i.e., gaining unauthorized access to a computer system or network), identity theft, and virus-writing were included. For example, the following statements were used to classify respondents' deviant computer behavior in Rogers' (2001; 2006b) CCI-R:

1) Hacking: knowingly accessing a computer system or network without authorization
2) Identity theft: knowingly electronically obtaining another person's credit card information without permission
3) Virus-writing: knowingly writing or using a program that would infect a computer or network.

The CCI-R has been used extensively in previous research (cf., Rogers et al., 2006a; Rogers et al., 2006b; Seigfried-Spellar & Rogers, 2010; Seigfried-Spellar & Treadway, 2014; Seigfried-Spellar et al., 2014). For the present study, the CCI-R scale reported a good Cronbach's alpha (α = .97), indicating the CCI-R survey items were reliable at measuring the underlying constructs. Therefore, the CCI-R is a well-tested, measure of deviant computer behavior that is both valid and reliable.

3.4 Design and Procedure

The research instrument for the present study was an anonymous, Internet-based questionnaire created and hosted via Qualtrics online survey software (to which Purdue has a license). Therefore, no identifying information was recorded or requested of participants (e.g., IP addresses, names), resulting in greater self-disclosure about potentially sensitive topics (Mueller, Jacobsen, & Schwarzer, 2000). Participants also had the option of declining to answer any question with which they felt uncomfortable for any reason.

Due to the accessibility of the general population of Internet users via Amazon’s Mechanical Turk website, data collection was completed within a month of the first posting of the survey solicitation (December 2016). This method of data collection was chosen for the present study due to the attainability of anonymous respondents, which also accounts for the popularity of online data collection methods in research (Mueller et al., 2000).

The author of the present study has had success in previous research studies using anonymous, Internet-based questionnaires created and hosted via Qualtrics survey software (cf., Seigfried-Spellar et al., 2014; Seigfried-Spellar & Treadway, 2014; Treadway & Seigfried-Spellar, 2015), as well as Amazon’s Mechanical Turk (cf., Treadway & Seigfried-Spellar, 2015). Furthermore, previous literature has indicated that sampling from a population of Mechanical Turk workers offers better generalizability than other sampling methods (such as snowball sampling), as it allows researchers to collect data from a diverse demographic of individuals quickly and at a low cost to the researcher (cf., Berinsky, Huber, & Lenz, 2011; Buhrmester et al., 2011).

3.4.1. Statistical Analyses

Following the collection of data, statistical analyses were conducted via the Statistical Package for the Social Sciences (SPSS) version 22. Prior to analysis, statistical significance was set at the alpha level of .05, which is acceptable for social science research (Field, 2013). In order to ascertain data regarding the demographics of the sample, frequencies and cross-tabulations of the following variables were conducted: age, sex, marital status, employment status, ethnicity, annual income, education level completed, and status as a student.

In order to test the hypothesis that cognitive ability scores would be higher for self-reported hackers, identity thieves, and virus-writers than those self-reporting not engaging in these behaviors, the number of ICAR items correct was calculated into the variable of ICAR items answered correctly. Dichotomous variables were also calculated for each of the individual cyberdeviant behaviors based on responses from the CCI-R. Those who self-reported engaging in hacking, identity theft, and/or virus-writing behavior were coded as a value of 1, whereas those who self-reported as not engaging in these behaviors were coded with a value of 0. A dichotomous variable was also created for cyberdeviants (1) versus non-cyberdeviants (0) based on responses from the CCI-R. Level of cybercrime was assessed based on responses from the CCI-R and categorized as ranging between engaging in one behavior (1) to engaging in all three behaviors (3).

Initially, Pearson correlations tested for significant relationships between the individual cyberdeviant behaviors (all dichotomous variables), as well as general cyberdeviancy (dichotomous variable) and level of cyberdeviancy (continuous variable), and number of items answered correctly on the ICAR Sample Test (continuous variable). Based on the significant findings from the correlational analyses, linear regressions were conducted in order to determine the level of predictive quality of cyberdeviancy for higher scores on the ICAR Sample Test (i.e., a higher total of items answered correctly). A forced entry linear regression is appropriate for analyses when only one independent variable (e.g., ICAR Sample Test score) and one dependent variable (e.g., hacker vs. non-hacker) are being studied simultaneously (cf. Field, 2013). Independent samples t-tests (used to compare means between two separate groups) and a one-way ANOVA (compares means between multiple groups) were also conducted where appropriate, based on correlational significance.

3.5 Summary

The present study explored the variance in cognitive ability scores between subtypes of cyberdeviants and non-cyberdeviants (i.e., hackers, identity thieves, and virus-writers), general cyberdeviants and non-cyberdeviants, and level of cyberdeviant behavior. These aims were accomplished through the use of a self-report survey consisting of a demographics questionnaire, an education assessment, and Rogers et al.'s (2006b) Computer Crime Index – Revised (CCI-R), along with the International Cognitive Ability Resource (ICAR) Sample Test, a performance task scale created by Condon and Revelle (2014). Responses to the survey were downloaded to SPSS, and the data was analyzed using frequencies, correlations, t-tests, ANOVAs, and linear regressions.

CHAPTER 4. RESULTS

Following the collection of data, statistical analyses were conducted via the Statistical Package for the Social Sciences (SPSS) version 22. Frequencies were conducted to determine the demographic makeup of the sample, and Pearson’s *r* correlational analyses were performed to establish a relationship between variables. An analysis of variance (ANOVA) was calculated in order to compare the group means (e.g., average ICAR scores for the hacker group and average ICAR scores for the non-hacker group). In addition, a linear regression was conducted so as to determine the predictive quality (if any exists) of cyberdeviant behavior on ICAR (e.g., if ICAR scores can be predicted by hacking behavior).

4.1 Sample

A total of 498 Mechanical Turk workers initiated the survey; 319 were included in final data analysis. Exclusion from final data analysis was based upon a number of factors, such as age (*n* = 7), and missing data (i.e., incomplete item responses due to attrition or answering with “decline to respond,” along with incorrect answers for the validation question; *n* = 172).

As shown in Table 4.1, the majority of participants were white non-Hispanic (*n* = 258, or 80.9%), between 25 and 54 years of age (*n* = 241, 75.5%), single or married (*n* = 277, 86.8%), employed full-time (*n* = 208, 65.2%), earning less than $70,001 per year (*n* = 271, 85.0%), had completed at least a Bachelor’s degree (*n* = 268, 84.0%), and were not currently students (*n* = 273, 85.6%). The sample was split nearly evenly between males (*n* = 151, 47.3%) and females (*n* = 167, 52.4%) on sex, with one respondent identifying as transgender (0.3%; see Table 4.1).

Table 4.1 Demographics for Self-Reported Cyberdeviants vs. Non

Variable		Non-Cyberdeviant	Cyberdeviant	Total
		(*n* = 159)	(*n* = 160)	(*N* = 319)
Sex	Male	74 (46.5)	85 (53.5)	151 (47.3)
	Female	77 (29.2)	56 (21.2)	167 (52.4)
	Transgender	0 (0)	1 (.6)	1 (.3)
Age Groups (years)	18-24	14 (8.8)	24 (15.0)	38 (11.9)
	25-34	57 (35.8)	69 (43.1)	126 (39.5)
	35-44	34 (21.4)	32 (20.0)	66 (20.7)
	45-54	28 (17.6)	21 (13.1)	49 (15.4)
	55-64	19 (11.9)	11 (6.9)	30 (9.4)
	65+	7 (4.4)	3 (1.9)	10 (3.1)
Education	high school or GED	16 (10.1)	17 (10.6)	33 (10.3)
	some college	35 (22.0)	26 (16.3)	61 (19.1)
	Associate's Degree	18 (11.3)	36 (22.5)	54 (16.9)
	Bachelor's Degree	60 (37.7)	60 (37.5)	120 (37.6)
	Master's Degree	21 (13.2)	20 (12.5)	41 (12.9)
	PhD, JD, etc.	9 (5.7)	1 (0.6)	10 (3.1)
Ethnicity	White (non-Hispanic)	133 (83.6)	125 (78.1)	258 (80.9)
	Hispanic	1 (0.6)	9 (5.6)	10 (3.1)
	Black	15 (9.4)	12 (7.5)	27 (8.5)
	Other than listed	8 (5.0)	14 (8.8)	22 (6.9)
	Decline to Respond	2 (1.3)	0 (0)	2 (0.6)
Marital Status	Single	62 (39.0)	77 (48.8)	140 (43.9)
	Married	75 (47.2)	62 (38.8)	137 (42.9)
	Divorced, Separated, or Widowed	19 (11.9)	20 (12.5)	39 (12.2)
	Decline to Respond	3 (1.9)	0 (0)	3 (0.9)
Employment	Full-time	102 (64.2)	106 (66.3)	208 (65.2)
	Part-time	34 (21.4)	27 (16.9)	61 (19.1)
	Unemployed	23 (14.5)	25 (15.6)	48 (15.0)
	Decline to Respond	0 (0)	2 (1.3)	2 (0.6)
Student	No	141 (88.7)	132 (82.5)	273 (85.6)
	Yes	18 (11.3)	28 (17.5)	46 (14.4)
Income	less than $10,000	17 (10.7)	17 (10.6)	34 (10.7)
	$10,001 - $20,000	19 (11.9)	23 (14.4)	42 (13.2)
	$20,001 - $40,000	51 (32.1)	52 (32.5)	103 (32.3)
	$40,001 - $50,000	20 (12.6)	21 (13.1)	41 (12.9)
	$50,001 - $70,000	27 (17.0)	24 (15.0)	51 (16.0)
	$70,001 - $99,999	14 (8.8)	16 (10.0)	30 (9.4)
	more than $100,000	9 (5.7)	7 (4.4)	16 (5.0)
	Decline to Respond	2 (1.3)	0 (0)	2 (0.6)

Note. Values represent frequency with percentages in parentheses.

As demonstrated in Table 4.1 the sample was split nearly evenly between cyberdeviants (*n* = 160, 50.2%) and non-cyberdeviants (*n* = 159, 49.8%). A total of 158 (49.5%) participants self-reported engaging in hacking behavior; 33 (10.3%) reported engaging in identity theft; and 34 (10.7%) reported engaging in virus-writing. Of those who self-reported as cyberdeviants, the majority reported engaging in only one type of cyberdeviant behavior (*n* = 120, 37.6%); 15 (4.7%) reported engaging in 2 types of cyberdeviant behaviors, and 25 (7.8%) reported engaging in all types of cyberdeviant behaviors.

On average, participants answered approximately 5 out of 12 ICAR questions correctly (*M* = 4.86, *SD* = 2.78). Likewise, the largest portion of respondents (*n* = 44, 13.8%) answered 5 out of 12 questions correctly; 90.3% (*n* = 264) answered fewer than 9 questions correctly. A total of 7 (2.2%) participants answered all 12 ICAR questions correctly; 16 (5.0%) scored a zero on the ICAR measure, meaning all questions were answered incorrectly. As for each of the 4-item ICAR subscales, participants scored an average of 2.49 for the verbal reasoning items, 1.76 for the letter and number series items, and 0.61 for the three-dimensional rotation items.

4.2 Results

4.2.1. Hackers vs. Non-Hackers

In order to test the hypothesis that ICAR scores would be significantly higher for self-reported hackers than non-hackers, a point biseral (r_{pb}) correlation was calculated for the number of ICAR items correct and the hacking behavior variables. However, the relationship between number of ICAR items correct and hacking behavior was non-significant, $r_{pb}(319) = -.07$ with $p = .11$.

Similarly, a point biseral (r_{pb}) correlation was also calculated for each of the ICAR subscales (verbal reasoning, letter and number series, matrix reasoning, and three-dimensional rotation) and the hacker variable. However, the relationship between each of these subscales and hacking was non-significant (see Table 4.2).

Table 4.2 Correlations of ICAR Sample Test and Subscales with Cyberdeviancy

	Non vs. CD	Level of CD	Hacking	Identity Theft	Virus-Writing
Total ICAR Score	-.064 (.126)	-.193** (.000)	-.069 (.108)	-.220** (.000)	-.221** (.000)
Verbal Reasoning	-.037 (.256)	-.196** (.000)	-.037 (.255)	-.250** (.000)	-.251** (.000)
Letter & Number Series	-.065 (.125)	-.152** (.003)	-.072 (.101)	-.154** (.003)	-.165** (.002)
3D Rotation	-.044 (.218)	-.075 (.090)	-.049 (.193)	-.076 (.089)	-.060 (.142)

Note. p values in parentheses.
** Correlation is significant at the .01 level
* Correlation is significant at the .05 level
Non vs. CD = Non vs. Cyberdeviant; Level of CD = level of cyberdeviant behavior; 3D Rotation = three-dimensional rotation
Listwise *N* = 319

It was hypothesized that hackers would score higher on the ICAR measure than non-hackers. However, due to the lack of significant findings between ICAR score and hacking, no further analyses were conducted for the hacking variable.

4.2.2. Identity Thieves vs. Non-Identity Thieves

A point biseral (r_{pb}) correlation was calculated for the ICAR items correct and the identity theft behavior variables in order to test the hypothesis that ICAR scores would be significantly higher for self-reported identity thieves than non-identity thieves. There was a significant, medium, negative relationship between total number of ICAR items correct and identity theft behavior, indicating those who self-reported as an identity thief demonstrated lower ICAR total scores, $r_{pb}(319) = -.22$ with $p < .01$ (see Table 4.2). The strength of this relationship (.2 or higher) is typically satisfactory in social science research (cf. Field, 2013).

Similarly, a point biseral (r_{pb}) correlation was also calculated for each of the included ICAR subscales (verbal reasoning, letter and number series, and three-dimensional rotation) and the identity theft variable. There were significant, negative relationships between the verbal reasoning, $r_{pb}(319) = -.25$ with $p < .01$, and letter/number series, $r_{pb}(319) = -.15$ with $p < .01$, ICAR subscale scores with identity theft behavior, indicating self-reported identity thieves scored lower on these subscales. These relationships were moderate and weak in strength, respectively (see Table 4.2). Based on these significant findings, an independent samples t-test was conducted in order to compare means between identity thieves and non-identity thieves on ICAR score, as well as the verbal reasoning and letter and number series ICAR subscales. On average, identity thieves reported significantly lower ICAR total scores than non-identity thieves (see Table 4.3).

Table 4.3 Mean Differences for ICAR Sample Test and Subscale Scores with Identity Theft Behavior

	Identity Thief	*M*	*SE*	df	*t*
ICAR Total Score	yes	3.06	.38	317	4.02**
	no	5.07	.16		(.000)
Verbal Reasoning	yes	1.52	.20	317	4.60**
	no	2.60	.08		(.000)
Letter & Number Series	yes	1.15	.18	44.658	3.45**
	no	1.83	.08		(.001)

Note. p values in parentheses.
The three-dimensional rotation subscale was not included as there were no significant differences found between identity theft behavior and scores on the three-dimensional rotation items.
** Significant at the .01 level
* Significant at the .05 level
Listwise *N* = 319

As for the ICAR subscales, identity thieves scored significantly lower on verbal reasoning, letter and number series, and matrix reasoning than non-identity thieves (see Table 4.3).

Therefore, a backward linear regression was conducted for identity theft behavior with the ICAR verbal reasoning subscale and the ICAR letter and number series subscale. As suggested by the analysis of variance (ANOVA), the final model significantly improved the ability to predict identity theft behavior, $F(1, 317) = 21.19$ with $p < .01$. The final model predicted 9% of the variance in identity theft behavior. According to the linear regression, the best predictive model for identity theft behavior included the verbal reasoning subscale ($t = -4.60$, $p < .01$). Diagnostics suggested no problems with multicollinearity; variance inflation factor (VIF) values were less than 2.0, the condition index was less than 30, and each variance proportion row had only one value greater than .50.

A forced entry linear regression was also conducted for the variables of identity theft behavior and ICAR total score. As suggested by the analysis of variance (ANOVA), the model significantly improved the ability to predict ICAR total score based on identity theft behavior, $F(1, 317) = 16.18$ with $p < .01$. This finding indicates ICAR total score significantly predicted identity theft behavior ($t = -4.02$, $p < .01$), with the model explaining 5% of the variance. Diagnostics suggested no problems with multicollinearity; variance inflation factor (VIF) values were less than 2.0, and the condition index was less than 30.

Based on the significant findings of lower ICAR scores for identity thieves, the hypothesis that identity thieves would score higher on the ICAR measure than non-identity thieves was refuted.

4.2.3. Virus-Writers vs. Non-Virus-Writers

In order to test the hypothesis that ICAR scores would be significantly higher for self-reported virus-writers than non-virus-writers, a point biseral (r_{pb}) correlation was calculated for the ICAR items correct and the virus-writing behavior variables. There was a moderate, negative relationship between total number of ICAR items correct and virus-writing behavior, indicating lower ICAR scores for those self-reporting as a virus-writer; this relationship was significant, $r_{pb}(319) = -.21$ with $p < .01$.

Similarly, a point biseral (r_{pb}) correlation was also calculated for each of the ICAR subscales (verbal reasoning, letter and number series, and three-dimensional rotation) and virus-writing. There were significant, negative relationships between the verbal reasoning, $r_{pb}(319) = -.25$ with $p < .01$, and letter and number series, $r_{pb}(319) = -.17$ with $p < .01$, ICAR subscale scores and virus-writing behavior, indicating lower scores on these subscales for those self-reporting as a virus-writer; these relationships moderate and weak in strength, respectively (see Table 4.2)

Based on these significant findings, an independent samples t-test was conducted in order to compare means between virus-writers and non-virus-writers on ICAR items correct, along with the ICAR subscales assessing verbal reasoning and letter and number series. On average, virus-writers scored significantly lower on the ICAR scale; virus-writers correctly answered fewer ICAR questions overall than non-virus-writers (see Table 4.4).

Table 4.4 Mean Differences for ICAR Sample Test and Subscale Scores with Virus-Writing Behavior

	Virus-Writer	*M*	*SE*	df	*t*
ICAR Total Score	yes	3.09	.43	317	4.03**
	no	5.07	.16		(.000)
Verbal Reasoning	yes	1.53	.21	317	4.61**
	no	2.60	.08		(.000)
Letter & Number Series	yes	1.12	.20	317	2.98**
	no	1.84	.08		(.003)

Note. p values in parentheses.
The three-dimensional rotation subscale was not included as there were no significant differences found between virus-writing behavior and scores on the three-dimensional rotation items.
** Significant at the .01 level
* Significant at the .05 level
Listwise *N* = 319

Virus-writers also scored significantly lower on each of the subscales (i.e., verbal reasoning, letter and number series, and matrix reasoning) than their counterparts (see Table 4.4).

Therefore, a backward linear regression was conducted for virus-writing behavior and the following variables: verbal reasoning subscale and letter and number series subscale. As suggested by the analysis of variance (ANOVA), the final model significantly improved the ability to predict virus-writing behavior, $F(1, 317) = 21.27$ with $p < .01$, with the final model predicting 6% of the variance in virus-writing behavior. According to the linear regression, the best predictive model for virus-writing behavior included the verbal reasoning subscale ($t = -4.61$, $p < .01$). Diagnostics suggested no problems with multicollinearity; variance inflation factor (VIF) values were less than 2.0, the condition index was less than 30, and each variance proportion row had only one value greater than .50.

A forced entry linear regression was also conducted for the variables of virus-writing behavior and ICAR total score. As suggested by the analysis of variance (ANOVA), the model significantly improved the ability to predict ICAR total score based on virus-writing behavior, $F(1, 317) = 16.22$ with $p < .01$, meaning virus-writing behavior could significantly predict ICAR score (*t* = -4.03, *p* < .01); the model explained 5% of the variance. Diagnostics suggested no problems with multicollinearity; variance inflation factor (VIF) values were less than 2.0, and the condition index was less than 30.

Because virus-writers demonstrated lower ICAR scores than non-virus-writers, the hypothesis that virus-writers would score higher on the ICAR measure than non-virus-writers was not supported.

4.2.4. Cyberdeviants vs. Non-Cyberdeviants

In order to test the hypothesis that ICAR scores would be significantly higher for self-reported cyberdeviants than non-cyberdeviants, a point biseral (r_{pb}) correlation was calculated for the ICAR items correct and the cyberdeviant behavior variables. However, the relationship between number of ICAR items correct and cyberdeviant behavior was non-significant, $r_{pb}(319) = -.07$ with $p = .13$.

Similarly, a point biseral (r_{pb}) correlation was also calculated for each of the ICAR subscales (verbal reasoning, letter and number series, matrix reasoning, and three-dimensional rotation) and the cyberdeviancy variable. However, the relationship between each of these subscales and cyberdeviant behavior was non-significant (see Table 4.2).

Due to the lack of significant findings between ICAR score and cyberdeviancy, no further analyses were conducted for the cyberdeviancy variable; the hypothesis that cyberdeviants would score higher on the ICAR measure than non-cyberdeviants was not supported.

4.2.5. Level of Cyberdeviancy

In order to test the hypothesis that ICAR scores would be significantly higher for more levels of cyberdeviancy, a zero-order correlation was calculated for the ICAR items correct and cyberdeviancy variables. There was a significant, moderate, negative relationship between total number of ICAR items correct and level of cyberdeviant behavior, indicating lower scores for those self-reporting more cyberdeviant behaviors (see Table 4.2).

Similarly, a zero-order correlation was also calculated for each of the ICAR subscales (verbal reasoning, letter and number series, and three-dimensional rotation) and level of cyberdeviancy. There was a significant, weak, negative relationship between the verbal reasoning and letter and number series subscale scores and level of cyberdeviant behavior, meaning those who self-reported as engaging in more types of cyberdeviant behaviors scored lower on these subscales (see Table 4.2).

Based on these significant findings, a one-way ANOVA was conducted to compare means between level of cyberdeviant behavior and the following variables: ICAR total, ICAR verbal reasoning subscale, ICAR letter and number series subscale. There was a significant mean difference between level of cyberdeviancy and the verbal reasoning ICAR subscale, $F(3, 315) = 9.04$ with $p < .01$. *Post hoc* tests revealed that those engaging in either 0 or 1 types of cyberdeviant behavior reported lower verbal reasoning scores than those engaging in all 3 behaviors (for both 0 and 1 behaviors, Bonferroni, $p < .01$; Hochberg's GT2, $p < .01$; Games-Howell, $p < .01$). There was also a significant mean difference between level of cyberdeviancy and the letter and number series ICAR subscale, $F(3, 315) = 3.50$ with $p = .02$. *Post hoc* tests revealed that those engaging in either 0 or 1 types of cyberdeviant behavior reported lower letter and number series scores than those engaging in all 3 behaviors (for both 0 and 1 behaviors, Bonferroni, $p = .02$; Hochberg's GT2, $p = .02$; Games-Howell, $p < .01$).

In addition, a significant mean difference was also found between level of cyberdeviancy and ICAR total score, $F(3, 315) = 6.75$ with $p < .01$. *Post hoc* tests revealed that those engaging in either 0 or 1 types of cyberdeviant behavior reported lower letter and number series scores than those engaging in all 3 behaviors (for both 0 and 1 behaviors, Bonferroni, $p < .01$; Hochberg's GT2, $p < .01$; Games-Howell, $p < .01$).

Bonferroni, Hochberg's GT2, and Games-Howell *post hoc* analyses were conducted for each ANOVA for the following reasons: Bonferroni *post hoc* analysis controls for Type I error (i.e., the presence of a false positive). Hochberg's GT2 *post hoc* analysis is appropriate when sample sizes vary greatly. Lastly, Field (2013) suggests conducting Games-Howell *post hoc* analysis for every ANOVA test because equality of population variances is uncertain.

It was hypothesized those who engaged in more cyberdeviant behaviors would demonstrate higher ICAR scores than those who engaged in fewer cyberdeviant behaviors. Because those who engaged in all three cyberdeviant behaviors scored significantly lower on the ICAR scale than those who engaged in only one or none of these behaviors, this hypothesis was refuted.

4.3 Summary

The present study explored the variance in cognitive ability scores between subtypes of cyberdeviants and non-cyberdeviants (i.e., hackers, identity thieves, and virus-writers), general cyberdeviants and non-cyberdeviants, and level of cyberdeviant behavior. These aims were accomplished through the following data analyses: frequencies, point biseral and zero-order correlations, one-way ANOVAs, and linear regressions. There were no significant differences between hacking behavior and ICAR score or education; there were also no significant differences found for cyberdeviancy versus non-cyberdeviancy. However, significant differences were found between ICAR total scores, ICAR subscale scores (verbal reasoning and letter and number series,) for virus-writers/non-virus-writers, identity thieves/non-identity thieves, and among level of cyberdeviant behavior. As there were no significant differences between hackers versus non-hackers and cyberdeviants versus non-cyberdeviants, and because identity thieves and virus-writers scored lower on the ICAR measure and two of the subscales (verbal reasoning and letter and number series), the hypotheses regarding higher scores for cyberdeviants was not supported.

CHAPTER 5. DISCUSSION

5.1 Discussion

In general, more traditional crimes (i.e., violent and property crimes) have been associated with lower IQs (Bartels et al., 2010; Beaver & Wright, 2011; Herrnstein & Murray, 1994; Hirschi & Hindelang, 1977; Lynam et al., 1993; Mears & Cochran, 2013; Oleson & Chappell, 2012; Rushton & Templer, 2009; White et al., 1989; Wilson & Herrnstein, 1985). In contrast, white collar crimes (of which the majority of computer crimes are included) are associated with higher IQs (Benson & Moore, 1992; Jennings, 2014; Lochner, 2004; Lochner & Moretti, 2004; Walters & Geyer, 2004). Furthermore, computer hackers are frequently stereotyped as having high levels of intelligence (cf., Furnell, 2002; Holt et al., 2015; Rogers, 1999a; Rogers, 2001; Schell & Dodge, 2002), which is also evidenced by the common social assumption seen in popular media (e.g., television shows like USA Network's *Mr. Robot*) in which hackers are elevated to "super-genius" levels of intelligence. Therefore, it is a common social assumption that hackers (a term also typically used as a catch-all for all types of computer deviance; cf. Seigfried-Spellar and Treadway, 2014) are extremely intelligent, as their techniques are frequently lauded in popular media.

Thus, it was expected that ICAR Sample Test scores (a measure of cognitive ability akin to traditional IQ tests; cf. Condon & Revelle, 2014) would be higher for cyberdeviants than non-cyberdeviants. It was also hypothesized that those who engaged in more types of cyberdeviant behavior (e.g., three behaviors versus one) would also score higher on the ICAR Sample Test. However, the results of the present study did not support expectations. Regarding ICAR Sample Test score, there were no significant differences between hackers and non-hackers. This lack of significant findings could be due to group-member diversity. Hackers are a heterogeneous group, as this category includes the Old Guard computer hackers (who are more skilled and typically motivated by the intellectual challenge associated with hacking), along with the less-skilled cyber-punks and script kiddies (Fotinger & Ziegler, 1999; Holt et al., 2015; Parker, 1998; Rogers, 2006; Rogers, 2010).

In addition, many hackers have training as IT professionals (Rogers, 2010; Schell & Holt, 2009; Shaw et al., 1999), and in fact, many companies employ white hat hackers to test digital security measures (Holt et al., 2015; Schell & Dodge, 2002; Schell & Martin, 2004). These employees (i.e., internals) are also more likely to have high-ranking positions within the company (Claycomb et al., 2014; Cummings et al., 2012; Gelbstein, 2014; Schell & Dodge, 2002). Based on the literature regarding area of training and hacking behaviors (cf. Schell & Holt, 2009; Shaw et al., 1999; Rogers, 2010; Seigfried-Spellar & Treadway, 2014), it might be that education in a particular field, such as computer and information technology, would correlate with higher IQ scores. According to The College Board (2013), those with planned majors in the field of computer science scored above average on the SATs (i.e., a combined score of 1558 versus 1498).

Furthermore, not every hacking behavior requires advanced technological skill. Social engineering, using trickery to convince someone to share viable resource information, is just one low-tech method of gaining desired access and data (Holt et al., 2015). For instance, Kevin Mitnick obtained confidential manuals from the phone company by posing as a legitimate company employee (Flanagan & McMenamin, 1992; Holt et al., 2015; Robson, 2004). After serving time in prison for his activities, Mitnick now works as a computer security consultant (Robson, 2004), but the core of Mitnick's strategy is still applicable today. For example, reporters for Jimmy Kimmel Live, a popular late-night television show, took to the streets in one episode to ask passersby for their online passwords through a series of roundabout questions (Morris, 2015). The interviewees freely gave up their passwords, seemingly without much thought, demonstrating the ease of obtaining confidential information with the right questions (Morris, 2015).

As for the other cyberdeviant subtypes, significant differences were found for ICAR Sample Test scores with identity thieves and virus-writers, but these relationships were not in the anticipated direction. When compared to their non-cyberdeviant counterparts, ICAR scores were lower for virus-writers and identity thieves. Although these findings refute the hypotheses regarding cyberdeviancy, the results tend to support the research on traditional crimes and IQ. For instance, Lynam et al. (1993) found a significant relationship between delinquency and both verbal IQ and full-scale IQ, with those who were classified as serious delinquents ranging 10 to 11 points lower on IQ scores compared with those categorized as exhibiting lower levels of delinquent behavior. In the present study, both identity thieves and virus-writers scored lower on the ICAR verbal reasoning subscale, along with the letter and number series subscale. Therefore, identity theft behavior and virus-writing behavior, as measured in the current study, more closely resemble traditional crime than white collar crime (i.e., lower IQs are typically associated with violent crime and property crime; Bartels et al., 2010; Beaver & Wright, 2011; Herrnstein & Murray, 1994; Hirschi & Hindelang, 1977; Lynam et al., 1993; Mears & Cochran, 2013; Oleson & Chappell, 2012; Rushton & Templer, 2009; White et al., 1989; Wilson & Herrnstein, 1985).

Like hackers, identity thieves and virus-writers are also diverse subgroups, though usually less varied than those in the hacker subgroup (Holt et al., 2015; Parker, 1998; Rogers, 2010). For instance, there are a number of low-skilled ways in which someone can steal personal information. Card skimmers, for example, are low-tech devices that account for 80% of scams directed at ATMs (Krebs, 2017). These skimmers can be purchased online for less than $100, and for the average consumer, they are extremely difficult to detect, and they can also be fairly easy to install (Krebs, 2017). For example, in May 2016, a number of these skimming devices were discovered in various Wal-Mart stores; they were attached to the credit card machines in the self-checkout aisles (Krebs, 2017).

Similarly, keyloggers are another type of device that are inexpensive, simple to use, and easy to hide (Keelog.com, 2017; Mitchell, 2016). Keyloggers are available in both hardware and software versions and are used to record key strokes, allowing for theft of sensitive data (Mitchell, 2016). For instance, a keylogger installed on a personal computer could record the username and password for banking websites, email accounts, and any other amount of confidential information because it logs data typed on the user's keyboard (Mitchell, 2016). Retailing for less than $50, hardware versions of the device typically resemble an ordinary flash drive but with a USB port on one end. This allows the device to act as a bridge between a USB-connected keyboard and the computer (Keelog.com, 2017). Software keyloggers, on the other hand, usually come in the form of a Trojan, a type of malware which runs quietly in the background of computing applications without alerting the user to its presence (Holt et al., 2015). Either form of keylogger can easily steal valuable information without the victim's knowledge (Holt et al., 2015; Keelog.com, 2017).

Likewise, the availability of online black markets can make it easier for identity thieves and malware enthusiasts alike to obtain harmful information (Holt et al., 2015). Back in the age of Kevin Mitnick and the phone phreakers, computer knowledge was shared through hands-on learning, along with face-to-face interactions with like-minded individuals. A fair amount of trial and error was also involved (Flanagan & McMenamin, 1992; Holt et al., 2015; Robson, 2004). Now, interested parties need only pay for the data they want, whether it is stolen credit card information or a computer virus; little technical knowledge is required (Holt et al., 2015). For instance, click-kiddies (i.e., those who do not write their own programming code) can simply buy a virus, obtain instructions through YouTube and other websites on how to implement the malware, and release it, all without an extensive background in computer programming (Holt et al., 2015). Therefore, the ease of access and ready availability of malware and personal data could explain why both identity thieves and virus-writers scored lower on the ICAR measure than their non-cyberdeviant counterparts; a great level of knowledge is no longer required for a cybercriminal to achieve their goals (Holt et al., 2015).

Furthermore, it was also expected that cyberdeviants would score higher on the ICAR measure than non-cyberdeviants, but this was not the case. It was also expected that ICAR Sample Test scores would be significantly higher for those who self-report engaging in more deviant computer behaviors (e.g., hacking, virus-writing, identity theft) than those who self-report engaging in fewer deviant computer behaviors. This hypothesis was based on the presumption that engaging in more types of cyberdeviant behavior would indicate a more versatile technological background (cf. Rogers, 2010; Schell & Holt, 2009; Shaw et al., 1999). However, ICAR scores were lower for those who engaged in all cyberdeviant behaviors compared with those who engaged in only one or none of these behaviors.

In addition to the heterogeneity of cyberdeviant groups, the present study also did not differentiate between the behaviors of black hat hackers and white hat hackers. The CCI-R is a measure used to determine deviant computer behavior (Rogers, 2006b).

Therefore, those who self-reported not engaging in this type of behavior were categorized as non-cyberdeviant, rather than non-technically literate. In other words, the present study did not compare those familiar with technology against those unfamiliar with technology; it compared those who used technology in a deviant manner against those who did not. This could explain the lack of significance between hackers versus non-hackers and cyberdeviants versus non-cyberdeviants.

Likewise, many of the techniques addressed by the CCI-R require low levels of technological skill (Rogers, 2006b). For instance, one of the questions addressing hacking behaviors asks if the reader has ever attempted to guess someone else's password in order to gain access to private information (Rogers, 2006b). Based on this question alone, the interviewers for Jimmy Kimmel's television show would classify as hackers. Another item pertaining to virus-writing specifically questions respondents on whether or not they have ever "written or *used*" (emphasis added) any form of malware (Rogers, 2006b). The questions regarding identity theft also address simple possession and/or use of another's credit card information, which does not intrinsically require technical skill or knowledge (Rogers, 2006b). Therefore, it may be that the CCI-R is more equipped to measure those with a broad range of technological skill, which could explain why there were no significant differences in ICAR score between hackers versus non-hackers and cyberdeviants versus non-cyberdeviants. It could also explain the negative relationship between identity thieves versus non-identity thieves, virus-writers versus non-virus-writers, and level of cyberdeviancy.

Due to an ever-increasing population of digital natives (i.e., those who are born into a digital society, and therefore, inherently more comfortable with technology), it could be these low-tech forms of hacking, identity theft, and virus-writing might one day become as prevalent as pirating, though results from the present study indicated fairly static trends in cyberdeviancy rates. For instance, in the present study, approximately 50% of participants reported engaging in hacking behavior, compared to the 57% of college students who reported engaging in hacking behaviors in Seigfried-Spellar and Treadway's (2014) study. Additionally, virus-writers in the present study comprised 11% of the sample, falling in between the prevalence rates of 9% (Seigfried-Spellar & Treadway, 2014) and 17% (Rogers et al., 2006) in previous research. Likewise, 10% of the sample in the current study consisted of identity thieves, whereas Selwyn (2008) and Seigfried-Spellar and Treadway (2014) report identity thieves comprised 13% and 6% of their samples, respectively. In contrast to Seigfried-Spellar and Treadway's (2014) findings of greater involvement in cyberdeviant behaviors, however, the majority of participants in the current sample reported engaging in only one type of cyberdeviant behavior versus multiple forms of cyberdeviancy.

Based on the findings in the current study, then, the author concludes the hypotheses were not supported by the results. Virus-writers, who are considered to be the more tech-savvy of the cyberdeviant group, and identity thieves, also a highly skilled group, were found to have significantly lower ICAR scores than their non-cyberdeviant counterparts. As Seigfried-Spellar and Treadway (2014) posited, the shift toward a society of digital natives might be a factor in research pertaining to cyberdeviancy. For instance, a simple Google search yields multiple results for easy "how-to" guides on hacking and other related cyberdeviant behaviors, available in both text and video form. Therefore, the stereotype of hackers as individuals with genius-level IQs might have been true years ago (though no such literature exists on the subject), but there is currently no support for this perception.

5.2 Limitations

For the present study, the sample was derived from the Mechanical Turk website, and it has been shown that Mturk workers are representative of the general population of Internet users (cf., Buhrmester et al., 2011). However, a sample including only Internet users, specifically those already familiar with navigating a survey-response website, does not accurately represent the general population of Americans, many of whom are inexperienced with technology. For instance, 73% of Americans own a computer, 68% own a smartphone, and only 45% own a tablet (Anderson, 2015). Therefore, the present study included those already familiar with technology, at least on a basic level.

It is also possible that respondents simply "clicked through" the online questionnaire instead of answering the questions honestly. On average, respondents spent approximately 15 minutes completing the survey ($M = 14.73$). For comparison, the

Qualtrics estimated response time for the survey was 17 minutes. However, 6.3% (*n* = 20) of the sample finished the survey in five minutes or less, which could indicate that these respondents did not actually read and truthfully answer the questions.

The present study was also limited by the reliability of the education and ICAR measures. Due to the low reliability of the education scale, it was omitted from analysis altogether; questions regarding demographic information (e.g., student status) were retained solely for the purpose of identifying descriptive data. The low reliability of this scale may be a consequence of meshing the EECM, the SRAPM, and various items from the Jennings (2014) measure. The EECM measures effort expended in schoolwork, whereas the SRAPM is a scale of academic performance. As for the ICAR Sample Test, the matrix reasoning subscale was excluded from analysis, also due to insufficient reliability; the remaining subscales measured just below the cut-off for adequate reliability in social science research (cf. Field, 2013), but were retained for the purpose of exploratory analysis due to the reliability of the overall ICAR Sample Test.

The low Cronbach's scores for the ICAR subscales could be due to a number of factors. Condon and Revelle (2014) only report reliability analyses conducted on subscale items from the full 60-item measure, whereas the subscale reliability analysis in the present study was conducted for a much smaller number of items (i.e., four). In addition, Condon and Revelle (2014) found 56% of their sample were currently enrolled in college/university or graduate/professional school; only 14% of respondents in the present study identified as current students. In addition, approximately 12% of Condon and Revelle's (2014) participants had earned some form of college degree, and 15% had not completed high school, whereas the majority of participants in the current study had completed at least a Bachelor's degree.

Moreover, Condon and Revelle (2014) analyzed data from respondents across 199 countries, with 78.1% of the sample originating from the United States. In the present study, those living outside of the United States were excluded from survey participation. Minors (i.e., those under the federally recognized age of maturity) were also excluded from the present study, whereas Condon and Revelle's (2014) respondents ranged in age from 14 to 90 years. Furthermore, Condon and Revelle's (2014) ICAR measure is relatively new and as yet untested outside of the original study. All of the aforementioned could be factors related to the low reliability of the ICAR subscales.

5.3 Conclusion

The current study was the first to compare the differences between cyberdeviants and non-cyberdeviants on cognitive ability. Although the hypotheses were not supported, the current study found no evidence that would indicate cyberdeviants are more intelligent than non-cyberdeviants, which dispels the myth of the “super-genius” computer hacker. These findings also indicate the literature on IQ and white collar crime may not be applicable to cyberdeviant behavior. When discussing the application of criminological theory to cybercriminal behavior, Wall (1998) categorized cyberdeviancy as not quite “old wine in new bottles,” or “new wine in old bottles,” but instead, “new wine, but no bottles!” (as cited in Holt et al., 2015, p. 283). In other words, cyberdeviancy and cybercriminality might be a different set of behaviors altogether.

Future research might include a population more diverse than general Internet users in order to increase external validity; the issue of respondents completing the survey too quickly should also be addressed. In addition, respondents’ field of study or profession should also be recorded, as this might impact test scores (cf. The College Board, 2013). Seigfried-Spellar and Treadway (2014) examined the individual differences in computer deviants across majors, but GPA was not included in their analyses. Therefore, future research might benefit from exploring the possible differences in cognitive ability and academic success (such as GPA, standardized test scores, etc.), as well. Also, significant differences might be found in cognitive ability scores between cyberdeviants and traditional criminals (e.g., those who engage in violent crimes), which should be considered. Further thought should also be expended for the measures used in such research, due to the lack of reliability for the education scale and the low reliability of the ICAR Sample Test. Moreover, as the CCI-R tends to include low-tech behaviors and exclude legal forms of computer skills, perhaps a scale measuring different levels of computer literacy and legality should be adopted. Regardless, further research into the possible relationship between cyberdeviant behaviors and IQ scores/education is necessary.

APPENDIX A: DEMOGRAPHICS QUESTIONNAIRE

1. What is your current country of residence?
   a. United States
   b. Other (please specify): _________
   c. decline to respond
2. What is your age in years? ______
   a. decline to respond
3. What is your sex?
   a. male
   b. female
   c. decline to respond
4. What is your marital status?
   a. single
   b. married
   c. civil union
   d. separated
   e. divorced
   f. widowed
   g. decline to respond
5. What is the closest approximation of your annual income?
   a. less than $10,000
   b. $10,001 - $20,000
   c. $20,001 - $40,000
   d. $40,001 - $50,000
   e. $50,001 - $70,000
   f. $70,001 – $99,999
   g. more than $100,000
   h. decline to respond
6. What is the combined closest approximation of annual income for your parents?
   a. less than $20,000

   b. $20,001 - $40,000
   c. $40,001 - $50,000
   d. $50,001 - $70,000
   e. $70,001 - $99,999
   f. more than $100,000
   g. decline to respond

7. What is your ethnicity?
   a. white
   b. black
   c. Hispanic
   d. Native American
   e. other
   f. decline to respond

APPENDIX B: EDUCATION ASSESSMENT

1. What is the highest level of education you have attempted?
    a. less than high school
    b. high school degree or high school equivalency exam (i.e., GED)
    c. some college
    d. Associate’s degree
    e. Bachelor’s degree
    f. Master’s degree
    g. Doctoral degree or higher
    h. decline to respond
2. What is the highest level of education you have completed?
    a. less than high school
    b. high school degree or high school equivalency exam (i.e., GED)
    c. Associate’s degree
    d. Bachelor’s degree
    e. Master’s degree
    f. Doctoral degree or higher
    g. decline to respond
3. Are you currently a student?
    a. no
    b. yes
    c. decline to respond
4. What is your most recent GPA?
    a. less than 1.0
    b. 1.1 – 2.0
    c. 2.1 – 3.0
    d. 3.1 – 3.7
    e. 3.8 – 3.9
    f. 4.0 or higher
    g. decline to respond

5. How would you rate yourself in terms of general academic performance (i.e., where would you usually come in assessments at school)?

    a. top 10% of all students
    b. top one-third of all students
    c. above average, but not top one-third
    d. about average
    e. below average
    f. decline to respond

6. What level of education would you expect to attain eventually?

    a. High school degree
    b. Associate’s degree
    c. Bachelor’s degree
    d. Master’s degree
    e. Doctoral degree or higher
    f. decline to respond

7. Generally speaking, when you were in school, how often did you/do you experience difficulty with schoolwork?

    a. almost always
    b. most of the time
    c. neutral
    d. sometimes
    e. hardly ever
    f. decline to respond

Please answer the following questions regarding your general school experience using the following scale: A lot less (1), a little less (2), average (3), a little more (4), a lot more (5), or decline to respond (6).

8. Compared with other students, how much effort do you expend in your field of study?	1	2	3	4	5	6

9. Compared with other students, to what

extent do you find the material and work in your field challenging?	1	2	3	4	5	6
10. Compared with other students, to what extent does your field come easily and naturally to you?	1	2	3	4	5	6
11.) Compared with other students, how much energy does it take you to succeed in your field?	1	2	3	4	5	6

APPENDIX C: INTERNATIONAL COGNITIVE ABILITY RESOURCE (ICAR)

The following items contains mathematical, verbal reasoning, and spacial orientation Tasks. You may use a calculator.

1. What number is one fifth of one fourth of one ninth of 900?
    a. 2
    b. 3
    c. 4
    d. 5
    e. 6
    f. 7
    g. I don’t know the answer
2. Zach is taller than Matt and Richard is shorter than Zach. Which of the following statements would be most accurate?
    a. Richard is taller than Matt
    b. Richard is shorter than Matt
    c. Richard is as tall as Matt
    d. It’s impossible to tell
3. Joshua is 12 years old and his sister is three times as old as he. When Joshua is 23 years old, how old will his sister be?
    a. 35
    b. 39
    c. 44
    d. 47
    e. 53
    f. 57
4. If the day after tomorrow is two days before Thursday, then what day is it today?
    a. Friday
    b. Monday
    c. Wednesday
    d. Saturday

   e. Tuesday
   f. Sunday

5. In the following alphanumeric series, what letter comes next? K N P S U
   a. S
   b. T
   c. U
   d. V
   e. W
   f. X
6. In the following alphanumeric series, what letter comes next? V Q M J H
   a. E
   b. F
   c. G
   d. H
   e. I
   f. J
7. In the following alphanumeric series, what letter comes next? I J L O S
   a. T
   b. U
   c. V
   d. X
   e. Y
   f. Z
8. In the following alphanumeric series, what letter comes next? Q S N P L
   a. J
   b. H
   c. I
   d. N
   e. M
   f. L
9. Which of the following completes the series?

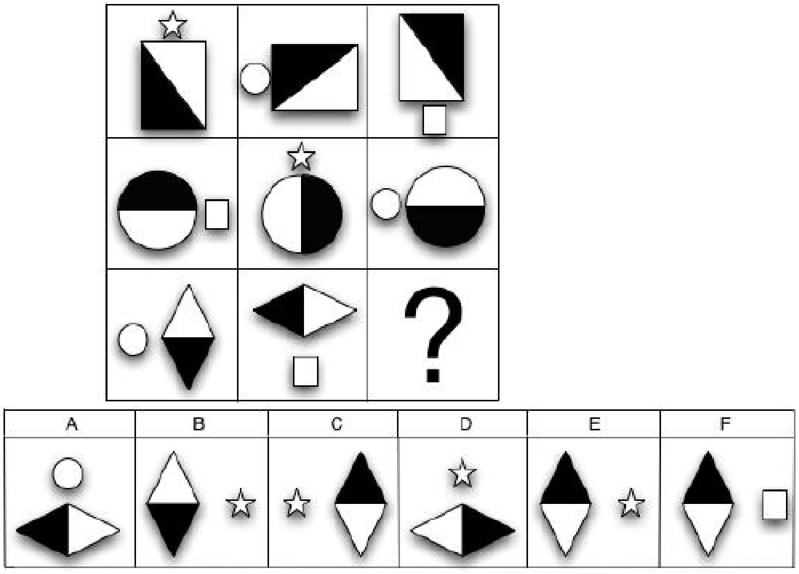


Figure C.1 MX45 Matrix Reasoning Item of the ICAR Sample Test

a. A
b. B
c. C
d. D
e. E
f. F

10. Which of the following completes the series?

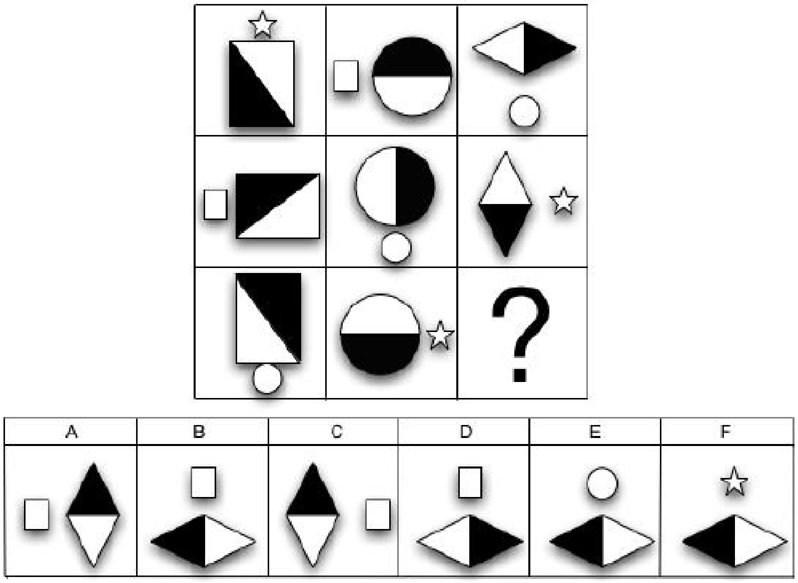


Figure C.2 MX46 Matrix Reasoning Item for the ICAR Sample Test

a. A

b. B

c. C

d. D

e. E

f. F

11. Which of the following completes the series?

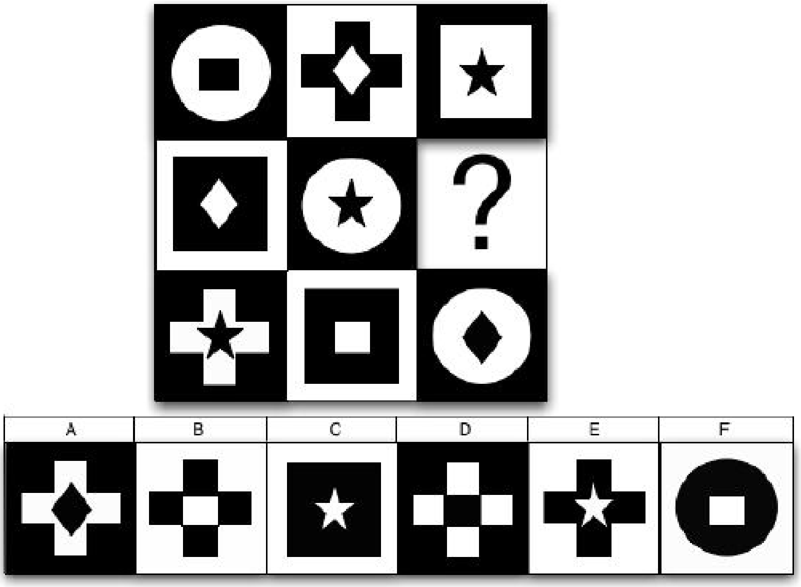


Figure C.3 MX47 Matrix Reasoning Item for the ICAR Sample Test

a. A

b. B

c. C

d. D

e. E

f. F

12. Which of the following completes the series?

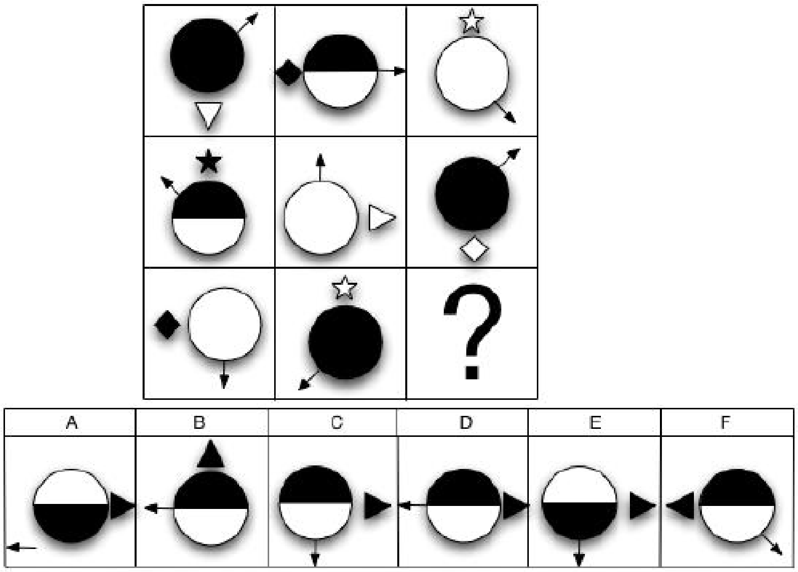


Figure C.4 MX55 Matrix Reasoning Item for the ICAR Sample Test

a. A

b. B

c. C

d. D

e. E

f. F

13. All the cubes below have a different image on each side. Select the choice that represents a rotation of the cube labeled X.

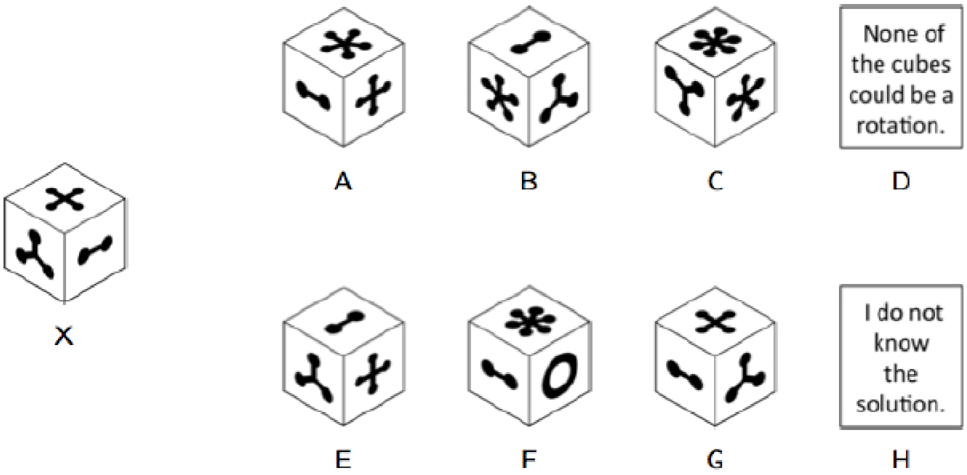

None of the cubes could be a rotation.
I do not know the solution.
A
B
C
D
X
E
F
G
H

Figure C.5 R3D3 Three-Dimensional Rotation Item for the ICAR Sample Test

a. A
b. B
c. C
d. D
e. E
f. F
g. G
h. H

14. All the cubes below have a different image on each side. Select the choice that represents a rotation of the cube labeled X.

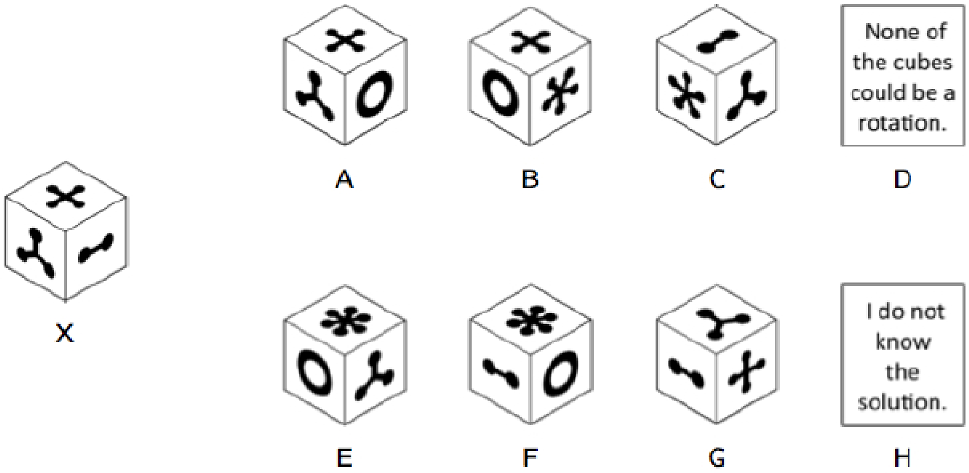

A
B
C
None of the cubes could be a rotation.
D
X
E
F
G
I do not know the solution.
H

Figure C.6 R3D4 Three-Dimensional Rotation Item for the ICAR Sample Test

a. A
b. B
c. C
d. D
e. E
f. F
g. G
h. H

15. All the cubes below have a different image on each side. Select the choice that represents a rotation of the cube labeled X.

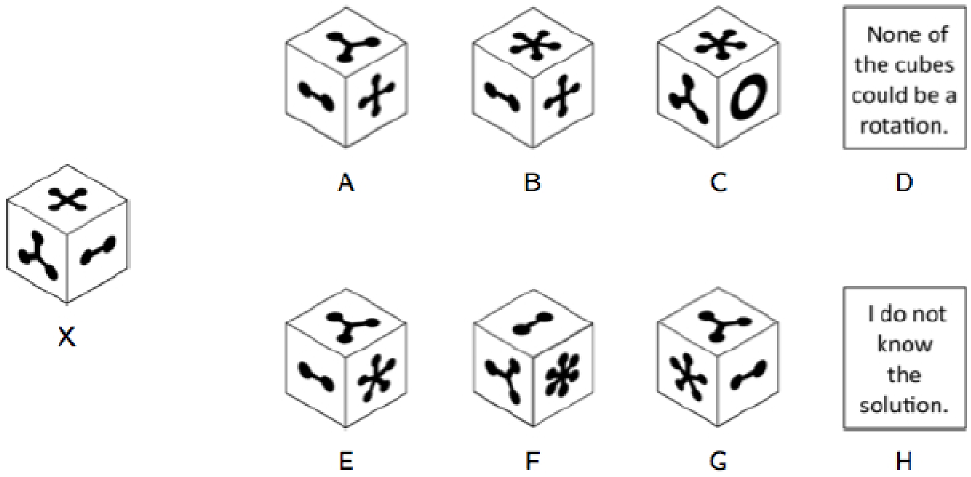

X
A
B
C
None of the cubes could be a rotation.
D
E
F
G
I do not know the solution.
H

Figure C.7 R3D6 Three-Dimensional Rotation Item for the ICAR Sample Test

a. A

b. B

c. C

d. D

e. E

f. F

g. G

h. H

16. All the cubes below have a different image on each side. Select the choice that represents a rotation of the cube labeled X.

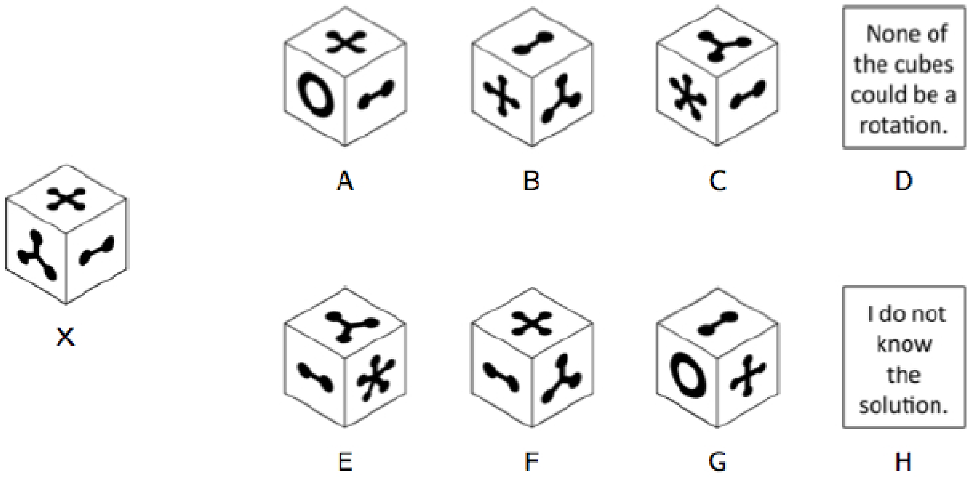

None of the cubes could be a rotation.
A
B
C
D
X
I do not know the solution.
E
F
G
H

*Figure C.*8 R3D8 Three-Dimensional Rotation Item for the ICAR Sample Test

a. A

b. B

c. C

d. D

e. E

f. F

g. G

h. H

APPENDIX D: COMPUTER CRIME INDEX – REVISED (CCI-R)

SECTION I

Using the following scale:

Never (1), within the past month (2), within the past year (3), 1-4 years ago (4), 5 or more years ago (5)

WHEN WAS THE LAST TIME THAT YOU:

1) Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold software?	1	2	3	4	5
2) Knowingly downloaded music, movies or other multimedia files that you did not legitimately purchase?	1	2	3	4	5
3) Tried to guess another's password to get into his/her computer account or files?	1	2	3	4	5
4) Accessed another person’s computer account or files without his/her knowledge or permission just to look at the information or files?	1	2	3	4	5
5) Accessed or used another person’s email account without their permission?	1	2	3	4	5
6) Added, deleted, changed or printed any information in another's computer account without their knowledge or permission?	1	2	3	4	5
7) Written or used a program that would destroy someone's data, infect a system or network or potentially cause problems (e.g., a virus, logic bomb or Trojan horse)?	1	2	3	4	5
8) Knowingly used or gave to another person someone else’s account password without the owner of the account’s knowledge or permission (e.g., facebook account, myspace account)?	1	2	3	4	5
9) Electronically obtained or possessed another person’s credit card number without his/her knowledge or permission?	1	2	3	4	5

10) Used another person’s cell phone number or cell phone without their permission?	1	2	3	4	5
11) Used someone else’s identity online (without their permission) to conduct a commercial transaction, apply for credit, or conduct any other financial transaction?	1	2	3	4	5
12) Used a wireless access point that you did not have permission or authorization to use?	1	2	3	4	5
13) Monitored network/Internet traffic without authorization or permission?	1	2	3	4	5
14) Accessed a computer system, network or website without permission or authorization?	1	2	3	4	5
15) Defaced/altered a website without authorization or permission?	1	2	3	4	5
16) Disclosed passwords, user IDs, or other account information without authorization or permission?	1	2	3	4	5
17) Viewed information on a business system or network that you did not have authorization or permission to see?	1	2	3	4	5
18) Harassed, annoyed or stalked someone through emails IM, Facebook or other web based technology?	1	2	3	4	5
19) Engaged in Internet activities (e.g., emails, web pages) designed to fraudulently obtain personal information, commonly known as phishing.	1	2	3	4	5
20) Sent unsolicited bulk emails?	1	2	3	4	5
21) Without authorization or permission, installed or used a device or software in order to obtain/sniff userids and/or passwords?	1	2	3	4	5
22) Without authorization or permission, installed software or a device on a network or system, that was designed to circumvent a security control?	1	2	3	4	5

SECTION II

Using the following scale:

Never (1), Once (2), 2-3 times (3), 4-5 times (4), 6+ times (5)

HOW OFTEN IN THE PAST 3 YEARS HAVE YOU:

1) Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold software?	1	2	3	4	5
2) Knowingly downloaded music, movies or other multimedia files that you did not legitimately purchase?	1	2	3	4	5
3) Tried to guess another's password to get into his/her computer account or files?	1	2	3	4	5
4) Accessed another person's computer account or files without his/her knowledge or permission just to look at the information or files?	1	2	3	4	5
5) Accessed or used another person's email account without their permission?	1	2	3	4	5
6) Added, deleted, changed or printed any information in another's computer account without their knowledge or permission?	1	2	3	4	5
7) Written or used a program that would destroy someone's data, infect a system or network or potentially cause problems (e.g., a virus, logic bomb or Trojan horse)?	1	2	3	4	5
8) Knowingly used or gave to another person someone else's account password without the owner of the account's knowledge or permission (e.g., facebook account, myspace account)?	1	2	3	4	5
9) Electronically obtained or possessed another person's credit card number without his/her knowledge or permission?	1	2	3	4	5
10) Used another person's cell phone number or cell phone without their permission?	1	2	3	4	5
11) Used someone else's identity online (without their permission) to conduct a	1	2	3	4	5

commercial transaction, apply for credit, or conduct any other financial transaction?					
12) Used a wireless access point that you did not have permission or authorization to use?	1	2	3	4	5
13) Monitored network/Internet traffic without authorization or permission?	1	2	3	4	5
14) Accessed a computer system, network or website without permission or authorization?	1	2	3	4	5
15) Defaced/altered a website without authorization or permission?	1	2	3	4	5
16) Disclosed passwords, user IDs, or other account information without authorization or permission?	1	2	3	4	5
17) Viewed information on a business system or network that you did not have authorization or permission to see?	1	2	3	4	5
18) Harassed, annoyed or stalked someone through emails IM, Facebook or other web based technology?	1	2	3	4	5
19) Engaged in Internet activities (e.g., emails, web pages) designed to fraudulently obtain personal information, commonly known as phishing.	1	2	3	4	5
20) Sent unsolicited bulk emails?	1	2	3	4	5
21) Without authorization or permission, installed or used a device or software in order to obtain/sniff userids and/or passwords?	1	2	3	4	5
22) Without authorization or permission, installed software or a device on a network or system, that was designed to circumvent a security control?	1	2	3	4	5

SECTION III

Using the following scale:

Does not apply to me (1), 16 or younger (2), 17-18 (3), 19-20 (4), 21 or older (5)

HOW OLD WERE YOU THE FIRST TIME YOU:

1) Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold software?	1	2	3	4	5
2) Knowingly downloaded music, movies or other multimedia files that you did not legitimately purchase?	1	2	3	4	5
3) Tried to guess another's password to get into his/her computer account or files?	1	2	3	4	5
4) Accessed another person’s computer account or files without his/her knowledge or permission just to look at the information or files?	1	2	3	4	5
5) Accessed or used another person’s email account without their permission?	1	2	3	4	5
6) Added, deleted, changed or printed any information in another's computer account without their knowledge or permission?	1	2	3	4	5
7) Written or used a program that would destroy someone's data, infect a system or network or potentially cause problems (e.g., a virus, logic bomb or Trojan horse)?	1	2	3	4	5
8) Knowingly used or gave to another person someone else’s account password without the owner of the account’s knowledge or permission (e.g., facebook account, myspace account)?	1	2	3	4	5
9) Electronically obtained or possessed another person’s credit card number without his/her knowledge or permission?	1	2	3	4	5
10) Used another person’s cell phone number or cell phone without their permission?	1	2	3	4	5
11) Used someone else’s identity online (without their permission) to conduct a commercial transaction, apply for credit, or conduct any other financial transaction?	1	2	3	4	5
12) Used a wireless access point that you did					

not have permission or authorization to use?	1	2	3	4	5
13) Monitored network/Internet traffic without authorization or permission?	1	2	3	4	5
14) Accessed a computer system, network or website without permission or authorization?	1	2	3	4	5
15) Defaced/altered a website without authorization or permission?	1	2	3	4	5
16) Disclosed passwords, user IDs, or other account information without authorization or permission?	1	2	3	4	5
17) Viewed information on a business system or network that you did not have authorization or permission to see?	1	2	3	4	5
18) Harassed, annoyed or stalked someone through emails IM, Facebook or other web based technology?	1	2	3	4	5
19) Engaged in Internet activities (e.g., emails, web pages) designed to fraudulently obtain personal information, commonly known as phishing.	1	2	3	4	5
20) Sent unsolicited bulk emails?	1	2	3	4	5
21) Without authorization or permission, installed or used a device or software in order to obtain/sniff userids and/or passwords?	1	2	3	4	5
22) Without authorization or permission, installed software or a device on a network or system, that was designed to circumvent a security control?	1	2	3	4	5

REFERENCES

Abrams, R. (2014, Aug.). Target puts data breach costs at $148 million and forecasts profit drops. *The New York Times*. Retrieved from http://www.nytimes.com.

Akers, R. (1977). *Deviant behavior: A social learning approach*. Belmont: Wadsworth.

Allen, I. E., & Seaman, J. (2013). *Changing Course: Ten Years of Tracking Online Education in the United States*. Sloan Consortium. PO Box 1238, Newburyport, MA 01950.

Anderson, M. (2015). The demographics of device ownership. *Pew Research Center*. Retrieved from www.pewinternet.org.

Bartels, J. M., Ryan, J. J., Urban, L. S., & Glass, L. A. (2010). Correlations between estimates of state IQ and FBI crime statistics. *Personality and Individual Differences, 48*, 579-583.

Beaver, K. M., & Wright, J. P. (2011). The association between county-level IQ and county-level crime rates. *Intelligence, 39*, 22-26.

Benson, M. L., & Moore, E. (1992). Are white-collar and common offenders the same? An empirical and theoretical critique of a recently proposed general theory of crime. *Journal of Research in Crime and Delinquency, 29*(3), 251-272.

Berinsky, A. J., Huber, G. A., & Lenz, G. S. (2012). Evaluating online labor markets for experimental research: Amazon.com's Mechanical Turk. *Political Analysis, 20*(3), 351-368.

Birnbaum, M. H. (2000). *Psychological experiments on the Internet.* M. H. Birnbaum (Ed.). San Diego, CA: Academic Press.

Bryman, A. (2012). *Social research methods* (4th ed.). Oxford: University Press.

Buhrmester, M., Kwang, T., & Gosling, S.D. (2011). Amazon’s Mechanical Turk: A new source of inexpensive, yet high-quality data? *Perspectives on Psychological Science*, *6*(1), 3-5.

Chiesa, R., Ducci, S., & Ciappi, S. (2009). *Profiling hackers: The science of criminal profiling as applied to the world of hacking.* Boca Raton, FL: Auerbach Publications.

Claycomb, W. R., Legg, P. A., & Gollmann, D. (2014). Guest editorial: Emerging trends in research for insider threat detection. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *5*(2), 1-6.

Coldwell, R. (1993). University students' attitudes towards computer crime: A research note. *Computers & Society*, *23*(1&2), 11-14.

Coldwell, R. (1994, March). Perceptions of Computer Crime. In *Conference Proceedings Crime against Business, Australian Institute of Criminology*.

Condon, D. M., & Revelle, W. (2014). The international cognitive ability resource: Development and initial validation of a public-domain measure. *Intelligence* (preprint).

Cullen, F. T., Gendreau, P., Jarjoura, G. R., & Wright, J. P. (1997). Crime and the bell curve: Lessons from intelligent criminology. *Crime and Delinquency*, *43*(4), 387-411.

Cummings, A., Lewellen, T., McIntire, D., Moore, A. P., & Trzeciak, R. (2012). *Insider threat study: Illicit cyber activity involving fraud in the US financial services sector* (No. CMU/SEI-2012-SR-004). Carnegie-Mellon University.

Field, A. (2013). *Discovering statistics using IBM SPSS Statistics* (4th ed.). London: SAGE.

Fitzpatrick, A. (Dec. 2014). Sony pulls *The Interview* after threats. *TIME*. Retrieved from http://www.time.com.

Flanagan, W. G., & McMenamin, B. (1992, Aug. 3). For whom the bell tolls. *Forbes*.

Fletcher, R. B., & Hattie, J. (2011). *Intelligence and Intelligence Testing.* Retrieved from http://www.purdue.eblib.com.ezproxy.lib.purdue.edu/patron/

Fötinger, C., & Ziegler, W. (1993). Understanding a hacker’s mind: A psychological insight into the hijacking of identities. *RSA Security*.

Furnell, S. (2002). *Cybercrime: Vandalizing the information society*. London: Addison-Wesley.

Gelbstein, E., Wuest, M., & Fridakis, S. (2012). Economic, political, and social threats in the information age. In P. C. Reich & E. Gelbstein (Eds.), *Law, policy, and technology: Cyberterrorism, information warfare, and internet immobilization* (pp. 17-30). Hershey, PA: IGI-Global.

Gelbstein, E. (2014). Attackers: Internal and external. In P. C. Reich & E. Gelbstein (Eds.), *Law, policy, and technology: Cyberterrorism, information warfare, and internet immobilization* (pp. 41-58). Hershey, PA: IGI-Global.

Goddard, H. H. (1914). *Feeblemindedness: Its causes and consequences*. New York, NY: Macmillan.

Goldberg, L. R. (2012). International personality item pool: A scientific collaboratory for the development of advanced measures of personality traits and other individual differences. Retrieved from http://ipip.ori.org/.

Gunter, W. D., Higgins, G. E., & Gealt, R. E. (2010). Pirating youth: Examining the correlates of digital music piracy among adolescents. *International Journal of Cyber Criminology, 4*(1&2), 657-671.

Heaven, P. C. L., Mak, A., Barry, J., & Ciarrochi, J. (2002). Self-Rated Academic Performance Measure [Database record]. Retrieved from PsycTESTS. doi: 10.1037/t12925-000.

Herrnstein, R. J., & Murray, C. (1994). *The bell curve: Intelligence and class structure in American life.* New York: Free Press.

Hirschi, T., & Hindelang, M. J. (1977). Intelligence and delinquency: A revisionist review. *American Sociological Review, 42*(4), 571–587.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). *Cybercrime and digital forensics: An introduction*. New York: Routledge.

Internet Crime Complaint Center. (2014). *IC3 2014 Internet Crime Report*. [Online]. Retrieved from http://www.ic3.gov/media/annualreport/2014_IC3Report.pdf.

Internet Movie Database. (n.d.). Most popular “hacker” titles. Retrieved from http://www.imdb.com.

Jennings, K. (2014). *Who are computer criminals?* (Doctoral dissertation, Texas State University). Retrieved from https://digital.library.txstate.edu/handle/10877/5258.

Keelog.com. (2017, January 18). KeyGrabber USB. *Keelog*. Retrieved from www.keelog.com.

Kirwan, G., & Power, A. (2012). *The psychology of cyber crime*. Hershey, PA: Information Science Reference.

Krebs, B. (2017). All about skimmers. *Krebs on Security*. Retrieved from www.krebsonsecurity.com.

Kumparak, G. (Nov. 2014). United States Postal Service hacked. *TechCrunch*. Retrieved from http://www.techcrunch.com.

Levy, S. (2001). *Hackers: Heroes of the computer revolution.* New York: Penguin.

Lochner, L. (2004). Education, work, and crime: A human capitalist approach. *International Economic Review, 45*(3), 811-843.

Lochner, L., & Moretti, E. (2004). The effect of education on crime: Evidence from prison inmates, arrests, and self-reports. *American Economic Review, 94*.

Lynam, D., Moffitt, T., & Stouthamer-Loeber, M. (1993). Explaining the relation between IQ and delinquency: Class, race, test motivation, or self-control? *Journal of Abnormal Psychology, 102*(2), 187-196.

Lubin, G. (2013, September 26). These are the college majors with the smartest students. *Business Insider*. Retrieved from http://www.businessinsider.com.

McBrayer, J. (2014). *Exploiting the digital frontier: Hacker typology and motivation* (Doctoral dissertation, The University of Alabama).

McDaniel, M. A. (2006). Estimating state IQ: Measurement challenges and preliminary correlates. *Intelligence, 34*, 607–619.

Mears, D. P., & Cochran, J. C. (2013). What is the effect of IQ on offending? *Criminal Justice and Behavior, 40*(11), 1280-1300. doi: 10.1177/0093854813485736.

Mitchell, B. (2016, October 18). What is a keylogger and key logging software? *Lifewire*. Retrieved from https://www.lifewire.com.

Moffitt, T. E., & Silva, P. A. (1988). IQ and delinquency: A direct test of the differential detection hypothesis. *Journal of Abnormal Psychology*, *97*, 330-333.

Monk-Turner, E., Oleson, J., Cortez, P., Dean, D., Kracke, C., Harmon, J., … Trach, G. (2006). Gender disparity in criminal offenses among persons of high IQ. *International Journal of Offender Therapy and Comparative Criminology, 50*(5), 506-519.

Morris, I. (2015, January 20). Jimmy Kimmel exposes bad password security. *Forbes*. Retrieved from www.forbes.com.

Mueller, J. H., Jacobsen, D. M., & Schwarzer, R. (2000). What are computing experiences good for: A case study in on-line research. In M. H. Birnbaum (Ed.), *Psychological Experiments on the Internet* (195-216). San Diego, CA: Academic Press.

Murray, C. (1997). IQ and economic success. *The Public Interest*, 21-35.

Nairne, J. S. (2013). *Psychology* (6th ed.). Belmont, CA: Wadsworth.

Oleson, J. C., & Chappell, R. (2012). Self-reported violent offending among subjects with genius-level IQ scores. *Journal of Family Violence, 27*, 715-730. doi: 10.1007/s10896-012-9468-7.

Owen, S., & Sawhill, I. (2013, May). Should everyone go to college? *Center on Children and Families at Brookings*. Retrieved from http://www.brookings.edu.

Pagliery, J. (2014, May). Half of American adults hacked this year. *CNN Money*. Retrieved from http://money.cnn.com.

Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information.* New York: Wiley.

Porter, T. M., & Carson, J. (2009). The measure of merit: Talents, intelligence, and inequality in the French and American republics, 1750-1940. *Modern Intellectual History, 6*(3), 637-644.

Raine, A., Laufer, W. S., Yang, Y., Narr, K. L., Thompson, P., & Toga, A. W. (2012). Increased executive functioning, attention, and cortical thickness in white-collar criminals. *Human Brain Mapping, 33*, 2932-2940.

Randazzo, M.R., M. Keeney, E. Kowalski, D. Cappelli, and A. Moore. (2005). “Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector.” Technical Report CMU/SEI-2004-TR-021 Prepared by the U.S. Secret Service and CERT Coordination Center. Pittsburg, PA: Carnegie Mellon Software Engineering Institute Publication.

Riffkin, R. (Oct. 2014). Hacking tops list of crimes Americans worry about most. *Gallup*. Retrieved from http://www.gallup.com.

Robson, G. D. (2004). The origins of phreaking. *Blacklisted! 411, 6*(2), 17-23.

Rogers, M. (1999a). Psychology of hackers: Steps toward a new taxonomy. Retrieved May 5, 1999 from the World Wide Web: http://www.infowar.com.

Rogers, M. (1999b). Psychology of computer criminals. Paper presented at the annual Computer Security Institute Conference, St. Louis, Missouri.

Rogers, M. K. (2001). *A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study*. (Unpublished doctoral dissertation).

Rogers, M. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation, 3*(2), 97-102.

Rogers, M. (2010). The psyche of cybercriminals: A psycho-social perspective. *Cybercrimes: A Multidimensional Analysis, part 5*, 217-235. doi: 10.1007/978-3-642-13547-7_14.

Rogers, M., Seigfried, K., & Tidke, K. (2006a). Self-reported computer criminal behavior: A psychological analysis. *Digital Investigation, 3*, 116-120.

Rogers, M., Smoak, N., & Liu, J. (2006b). Self-reported deviant computer behavior: A big-5, moral choice, and manipulative exploitive behavior analysis. *Deviant Behavior, 27*(3), 245-268.

Rushe, D. (Feb. 2015). Most cars are vulnerable to ‘hacking or privacy intrusions’ – report. *The Guardian*. Retrieved from http://www.theguardian.com.

Rushton, J. P., & Templer, D. (2009). National differences in intelligence, crime, income, and skin color. *Intelligence, 37*(4), 341-346.

Schell, B., & Dodge, J. (2002). *The hacking of America: Who’s doing it, why, and how*. Westport, CT: Greenwood Publishing Group, Inc.

Schell, B. & Holt, T. (2009). A profile of the demographics, psychological predispositions, and social/behavioral patterns of computer hacker insiders and outsiders. In K. Chen & A. Fadlalla (Eds.), *Online Consumer Protection: Theories of Human Relativism* (190-213).

Schell, B. H., & Martin, C. (2004). *Cybercrime: A reference handbook*. Santa Barbara, CA: ABC-CLIO.

Seigfried-Spellar, K. & Rogers, M. (2010). Psychological analysis of computer criminal behavior: preliminary findings.

Seigfried-Spellar, K. C., O'Quinn, C., & Treadway, K. N. (2014). Assessing the relationship between autistic traits and cyberdeviancy in a sample of college students. *Behaviour and Information Technology*. doi: 10.1080/0144929X.2014.978377.

Seigfried-Spellar, K. C., & Treadway, K. N. (2014). Differentiating hackers, identity thieves, cyberbullies, and virus writers by college major and individual differences. *Deviant Behavior*, *35*(10), 782-803.

Selwyn, N. (2008). A safe haven for misbehaving?: An investigation of online misbehavior among university students. *Social Science Computer Review, 26*(4), 446-465.

Shaw, E., Post, J., & Ruby, K. (1999). Inside the mind of the insider. *Security Management*, *43*(12), 34-42.

Shipley, W. C., Gruber, C. P., Martin, T. A., & Klein, A. M. (2009). *Shipley-2.* Los Angeles, CA: Western Psychological Services

Shipley, W. C., Gruber, C., Martin, T., & Klein, A. M. (2010). *Shipley Institute of Living Scale* (3^{rd} ed.). Los Angeles, CA: Western Psychological Services

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.

Smith, J. L., Lewis, K. L., Hawthorne, L., & Hodges, S. D. (2013). Effort Expenditure Comparison Measure [Database record]. Retrieved from PsycTESTS. doi: 10.1037/t23899-000.

The College Board. (2013). *2013 SAT® report on college & career readiness*. Retrieved from http://media.collegeboard.com.

Thorndike, R. L., Hagen, E. P., & Sattler, J. M. (1986). *The Stanford–Binet Intelligence Scale* (4th ed.). Chicago: Riverside.

Treadway, K. N., & Seigfried-Spellar, K. C. (2015, March). *Influencing sensitivity levels toward victims of cyberbullying behaviors by manipulating sex of the victim & instigator*. Poster session presented at the meeting of the Academy of Criminal Justice Sciences, Orlando, FL.

Wall, D. S. (1998). Catching cybercriminals: Policing the Internet. *International Review of Law, Computers, & Technology*, *12*, 201-218.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the digital age.* Cambridge: Polity Press.

Walters, G. D., & Geyer, M. D. (2004). Criminal thinking and identity in male white-collar offenders. *Criminal Justice and Behavior, 31,* 263-281. doi:10.1177/0093854803262508.

Weschler, D. (1991). *The Wechsler Intelligence Scale for Children* (3rd ed.). San Antonio, TX: The Psychological Corporation.

Weise, E. (Feb. 2015). Millions of Anthem customers alerted to hack. *USA Today*. Retrieved from http://www.usatoday.com.

White, J. L., Moffitt, T. E., & Silva, P. A. (1989). A prospective replication of the protective effects of IQ in subjects at high risk for juvenile delinquency. *Journal of Consulting and Clinical Psychology*, *57*(6), 719-724. doi:10.1037/0022-006X.57.6.719.

Wilson, J. Q., & Herrnstein, R. (1985). Crime and human nature. *New York: Simon and Shuster*.

PUBLICATIONS

Seigfried-Spellar, K. C., O'Quinn, C., & Treadway, K. N. (2014). Assessing the relationship between autistic traits and cyberdeviancy in a sample of college students. *Behaviour and Information Technology*. doi: 10.1080/0144929X.2014.978377.

Seigfried-Spellar, K. C., & Treadway, K. N. (2014). Differentiating hackers, identity thieves, cyberbullies, and virus writers by college major and individual differences. *Deviant Behavior*, *35*(10), 782-803.