A Typology Based on Self-Identity & Explanatory Factors of Cybercriminal Behavior

Master's Paper Submitted by

Ashley Ireson

Advised by

Dr. Sue Brown

Dr. Jesse Bockstedt

In Partial Fulfillment for the Degree of

Master of Science

Department of Management Information Systems

Eller College of Management

The University of Arizona

May 2017

Table of Contents

Acknowledgements

I would like to thank my research advisors, Dr. Sue Brown and Dr. Jesse Bockstedt, for all of their continued guidance, support, and time over the past two years. I want to thank all of my fellow SFS students and other friends who gave me suggestions and took my survey. I also want to thank everyone who helped me to disseminate my survey both to my knowledge and otherwise. A special thank you to Eric Case and Matt Heffelfinger for going above and beyond to help me get survey responses. Additional thanks are due to Lee Spitzley for answering all of my conceptual and R-related questions.

This material is based upon work supported by the National Science Foundation under Grants No. DUE-1303362 and No. SES-1314631.

List of Figures

List of Tables

Abstract

Cybercrime is a top national security threat, higher than terrorism, espionage, and weapons of mass destruction (Mickelberg 2014), but more research is necessary to further understand and define it. This study developed a theoretical model and survey instrument in an attempt to close some of the gaps in knowledge by discovering types of skilled technologists based on self-identity. Additional factors, attributes known to be correlated with cybercriminal propensity, were included to further differentiate these types. We expected to find groupings of individuals that have been described in previous literature, but with our innovative approach, the discovery of new types of technologists was possible. Following a clustering analysis, our respondents were grouped into four different types. We preliminarily named and defined each group: heroes, eccentrics, hacking professionals, and conservatives. A multinomial logistical regression was performed to provide additional explanatory factors for each type. Future research is suggested.

1. Introduction

Reliance on the Internet – by people and devices – has exploded, increasing opportunities for malicious activity along with it. Since 2000, the number of global internet users has increased by 934% and as of March 2017, there were almost 3.4 million users ("World…" 2017). The number of IoT devices on the Internet is expected to almost double from 15.4 billion in 2015 to 30.7 billion in 2020 (Columbus 2016). This expansion of the Internet has simultaneously augmented the attack surface for cybercriminals. In 2014, the US Director of National Intelligence ranked cybercrime as the top national security threat, higher than terrorism, espionage, and weapons of mass destruction (Mickelberg 2014). The number of and cost of cyber-attacks continue to rise, affecting individuals, businesses, and governments alike.

Although the ubiquitous nature of cybercrime has attracted substantial attention to the issue, there are many gaps in knowledge that remain, including about individuals who commit the offenses. This study seeks to contribute to cybercrime research by filling in some of these gaps. We seek to study differences between groups of skilled technologists in order to define those groups. Existing taxonomies (e.g. Rogers 2006) have almost exclusively relied on motivation, technique, and/or skillset for technologist categorizations. We expect to find the commonly described types of technologists emerge, such as IT professionals and hacktivists, but our approach using additional factors may discover a new type or method of categorization. Such a finding could have implications for government and industry, perhaps providing additional criteria to consider in hiring decisions.

The remainder of this paper is organized as follows: We first review the literature on cybercrime and hackers, noting the disparity in how these terms are defined and the lack of consensus whether hacktivism and hacktivist are subcategories. We also explore the relevant gaps in cybersecurity research in more detail. Next, we introduce our theoretical model, developed for this study. We then review our methodology, consisting of belief elicitation, survey development and survey implementation. Our results follow and then we present our next steps. Finally, we end this paper with our concluding thoughts.

2. Literature Review

Any study of cybercrime is immediately challenged by the lack of one, universal definition of cybercrime (e.g., Finklea and Theohary 2015) and the variety of interchangeable terms, which includes computer-related crime, digital crime, and internet crime (McQuade 2006). In academia, cybercrime is often defined very generally, such as "online deviance utilizing technology" (Donner et al. 2014, pp. 166), but studies that attempt to compartmentalize cybercrime do so in a variety of ways. Some separate the more technical offenses that require expertise, such as denial of service attacks, from the less technical acts like cyberstalking (Ghosh and Turrini 2010). Still others differentiate between crimes in which computers are purely incidental, crimes that have evolved with the introduction of computers and the internet, and crimes that would not exist without technology and often target the technology itself (e.g., Donner et al. 2014).

The same challenges exist for studies of the perpetrators of cybercrime. 'Hacker' is often used interchangeably with cybercriminal, both in public discourse (Bachmann 2010) and in academia (e.g., Lloyd 2015). Those taking the opposite approach, ignore the malicious side of hacking and only discuss the curious individuals who use their computer skills to explore, both solving problems and having fun (e.g., Sarma and Lam 2013). The latter view mirrors the connotation of the term when was first introduced, back in the 1960s. At that time, a 'hacker' was anyone who developed computer programs in efficient and creative ways. Ultimately, many researchers overlook the diversity and variation among people labeled as hackers. Today, 'hacker' can refer to computer literate people who vary widely in motivation, skill, and behavior (Bachmann 2010).

There are many researchers who do recognize the variation among hackers, cybercriminals, and other skilled technologists. One common categorization consists of 'black hats,' 'white hats,' and 'gray hats.' Black hats have malicious intentions and often hack out of a desire for revenge or profit. Gray hats usually have innocent intentions and are looking to fulfill a desire for curiosity or notoriety. White hats are often motivated by an opportunity to learn, and focus on alerting organizations of security weaknesses they have found (Xu et al. 2013). Another widely accepted taxonomy includes nine categories based on skill and motivation. For example, the least skilled category are the 'novices' who have limited computer and programming skills and are thrill-seekers, motivated by ego. (Rogers 2006). Many other classifications of skilled technologists exist as well (e.g., Coleman 2011).

Hacktivism and hacktivists only add to the dilemma of term ambiguity. Although hacktivism is frequently distinguished from cybercrime based on its social or political objectives (e.g., Hampson 2012), by action, it is almost indistinguishable. Statistics and reports on cybercrime rarely differentiate the two (e.g., Mickelberg 2014). Furthermore, like cybercrime, defining hacktivism raises the question of whether activities requiring little technical skill are within the scope. Some activist activities have shifted online (Denning 2001), which could arguably be said to be less technical than those performed by hacktivists. Another approach to separate activism from hacktivism might be to associate activism with legal activities while hacktivism is synonymized with cybercrime. However, some activist activities are illegal (Piven and Cloward 1991), so this is not an effective delineation.

Despite these challenges, many researchers have studied cybercrime from a variety of theoretical perspectives, including rational choice theory, routine activities theory, social learning theory, and the general theory of crime (e.g. Donner et al. 2014). However, several gaps in this research still exist. Most study populations only included college students or younger school-aged students (e.g. Holt et al. 2011), which is not a realistic sampling of cybercriminals. Many studies failed to incorporate activities requiring substantial technical ability (Holt et al. 2011; Moon et al. 2010). Most classification studies limited their criteria to motivation and skill level (e.g. Rogers 2006). This research seeks to address many of these gaps by creating a theoretical model composed of a variety of attributes that have been demonstrated to be predictors of cybercriminal behavior, that includes behaviors of a highly technical nature, and testing it on a more varied sample population.

3. Developing a Theoretical Model

Both the General Theory of Crime (GTC) and the Theory of Planned Behavior (TPB) have been widely tested, finding great support, including for explaining cybercriminal behaviors (e.g. Donner et al. 2014, Moon et al. 2010). However, many studies demonstrated that the addition of other constructs added to the predictive ability of these theories. For example, some have combined GTC with constructs from Social Learning Theory for an improved explanation of digital piracy (Higgins et al. 2006, Higgins and Makin 2004). Another study added multiple constructs to TPB, including moral judgement, to explain information technology ethnical behaviors (Leonard et al. 2004).

This study developed a theoretical model (*Figure 1*) that leveraged GTC and TPB and added additional constructs to improve its explanatory power. The additional constructs were those used in previous studies to explain cybercriminal behavior, as well as two constructs that were developed specifically for this study (social engineering self-efficacy and hacking self-efficacy), but were predicted to have a similar explanatory power. Our model was structured to discover types of skilled technologists. We expected to find types of individuals that have been described in previous cybercrime literature. Each type was to be predicated on a combination of self-identity and past behavior while the other constructs would further explain each type.

3.1 Review of Model Constructs:

3.1.1 Self-Control

Self-control is the central concept behind the General Theory of Crime (GTC), which attempts to explain individual variations in the propensity to commit crime and deviant behaviors. More specifically, having low self-control increases the likelihood that one will commit crime (Gottfredson and Hirschi 1990). Most often, self-control is conceptualized as six dimensions: impulsivity, insensitivity, preference for simple tasks, preference for physical tasks, temper control, and risk taking (Grasmick et al. 1993). Despite a number of criticisms, the theory has been tested repeatedly in the decades since its conception and has found substantial support (e.g. Donner et al. 2016, Marcum et al. 2016). Early on, the theory was solely used to explain traditional crime, but today, it has been successfully applied to a variety of cybercrimes and online deviant behaviors (e.g. Bossler & Burruss 2011, Donner et al. 2014, Marcum et al. 2016, Moon et al. 2010).

3.1.2 Attitude, Subjective Norms & Moral Obligation

The Theory of Planned Behavior (TPB) predicts an individual's intention to engage in a specific behavior. The constructs of the standard model include attitude, subjective norms and perceived behavioral control. Attitude represents feelings or beliefs about performing a said behavior. Subjective norms account for beliefs about how people important in one’s life would feel about the performance of a said behavior. Perceived behavioral control (PBC) refers to perceptions about the ease or difficulty one would have performing said behavior (Ajzen 1991). PBC has been highly debated among researchers. In its initial conception, PBC was said to be comparable to self-efficacy as defined by Bandura (1982, 1977). However, one track of studies argued that measuring behavior and intentions involves two separate concepts – actual behavioral control and skills or abilities – and that self-efficacy is not the same as PBC (e.g. Conner and Armitage 1998, Terry and O’Leary 1995). Still, another track of studies implemented the model under the original assumption, even substituting measures of self-efficacy in place of PBC (e.g. Crawley and Black 1992, de Vries et al. 1988, Schwarzer and Fuchs 1996). This study took the latter approach, dropping PBC and including three types of self-efficacy (below) we believed could be significant to cybercrime.

TPB has been successfully applied to behaviors spanning a vast number of areas, such as business (Kautonen et al. 2013), family planning (Ajzen and Klobas 2013), and environmental activism (Fielding et al. 2008). A variation of this model was created specifically for dishonest actions, under the premise that there are additional factors at work when a behavior could have negative consequences for the actor. The primary change to the dishonesty model was the addition of moral obligation. Moral obligation is the feelings or beliefs about one's obligation or responsibility as it relates to performing a said behavior (Beck and Ajzen 1991). Many studies have since included moral obligation into their models for explaining a variety of dishonest behaviors (e.g. Conner and Armitage 1998, Sparks and Guthrie 1998).

3.1.3 Computer, Hacking, and Social Engineering Self-Efficacies

Self-efficacy is the perception of one's own ability to perform some action with a successful outcome (Bandura 1982). Computer self-efficacy specifically, has been of interest to a variety of researchers (e.g. Hsia et al. 2011, Compeau and Higgins 1995, Murphy et al. 1989). Generally, for studies of cybercrime and related behaviors, computer self-efficacy per se has not been included in research models, but computer skill, years of experience or frequency of use have been incorporated by some (e.g. Cronan et al. 2006). Cybercrime studies that test self-control, in particular, often include these measures as a proxy for the concept of criminal opportunity (e.g. Donner et al. 2014, Higgins and Makin 2004, Holt et al. 2012, Moon et al. 2010). Gottfredson and Hirshi (1990) noted that opportunity for crime was an important precondition of the predictive power of self-control and these studies have generally interpreted opportunity, in the cybercrime context, as access to and skill in using computers.

Many cybercrimes are inherently highly technical and others rely on the use of social engineering techniques to be successful. To address these qualities of some cybercrimes, we developed two additional measures of self-efficacy for our model: hacking self-efficacy and social engineering self-efficacy. Both of these constructs are theoretically based on the general concept of self-efficacy.

3.1.4 Motivation

Motivation is the drive or inclination to do something (Baumeister and Vohs 2007). It is a primary factor used to differentiate various types of cybercriminals and hackers (e.g. Coleman 2011, Rogers 2006, Xu et al. 2013). Motivation is especially key to the division of hacktivists and cybercriminals. Some delineations of hacktivism focus on unique behaviors (e.g. Denning 2001), but there have historically been plenty of examples of hacktivists taking credit for behaviors beyond the stereotypical activities like website take-downs (e.g. Bergal 2017). That leaves motivation as the only characteristic with which to distinguish hacktivist acts from cybercrime and, hence, was the primary reason for its inclusion in our model.

3.1.5 Self-Identity

Self-identity is one's self-perception (Sparks and Guthrie 1998) or the extent to which one sees him- or herself fulfilling criteria for a societal role (Conner and Armitage 1998). Self-identity has improved the predictive ability of TPB in many studies (e.g. Conner and Armitage 1998, Fielding et al. 2008, Sparks and Guthrie 1998, Terry et al. 1999). For this study, self-identity will serve as the initial factor with which to distinguish types of skilled technologists.

3.1.6 Past Behavior

Past behavior can include criminal or analogous activities, depending on the intent of the researcher. Some studies argued that past behavior is the best predictor of future behavior overall (e.g. Bagozzi and Kimmel 1995, Mullen et al. 1987). Often, past behavior has served as the dependent variable in the absence of longitudinal data to test theories of cybercrime (e.g. Holt et al. 2012). However, many studies that implemented behavioral measures of self-control either substituted analogous activities for crime or at least combined them with crime. This was to attempt to avoid the frequent tautological criticism of GTC based on measuring low self-control with the criminal activity that it was theorized to explain (e.g. Tittle et al. 2005). Past behavior has also been demonstrated to improve TPB and the Theory of Reasoned Action (an earlier version of TPB) models (e.g. Bagozzi and Kimmel 1995, Conner and Armitage 1998).

3.2 Construct Definitions:

- *Self-Control* – stable, individual differences in the propensity for criminal behavior (Gottfredson and Hirschi 1990)
- *Attitude* – feelings or beliefs about committing cybercrime (adapted from Ajzen 1991)
- *Moral Obligation* – "personal feelings of responsibility to perform, or refuse to perform…" cybercrime (adapted from Beck and Ajzen 1991, pp. 289)
- *Subjective Norms* (Normative Beliefs) – beliefs about how people important in one's life would view engagement in cybercrime (adapted from Ajzen 1991)
- *Computer Self-Efficacy* – perceptions of one's own abilities involving computers (adapted from Compeau and Higgins 1995)
- *Hacking Self-Efficacy* – perceptions of one's own ability to perform technically-advanced hacking activities with a successful outcome (adapted from Compeau and Higgins 1995)
- *Social Engineering Self-Efficacy* – perceptions of one's own ability to engage in social engineering with a successful outcome (developed for this study)
- *Motivation* – a drive or inclination to take action (adapted from Baumeister and Vohs 2007)

- *Self-Identity* – "the extent to which an individual sees him or herself fulfilling the criteria for a societal role," (Conner and Armitage 1998)
- *Past Behavior* – criminal or analogous (legally or morally ambiguous) behaviors (adapted from Arneklev et al. 2006)

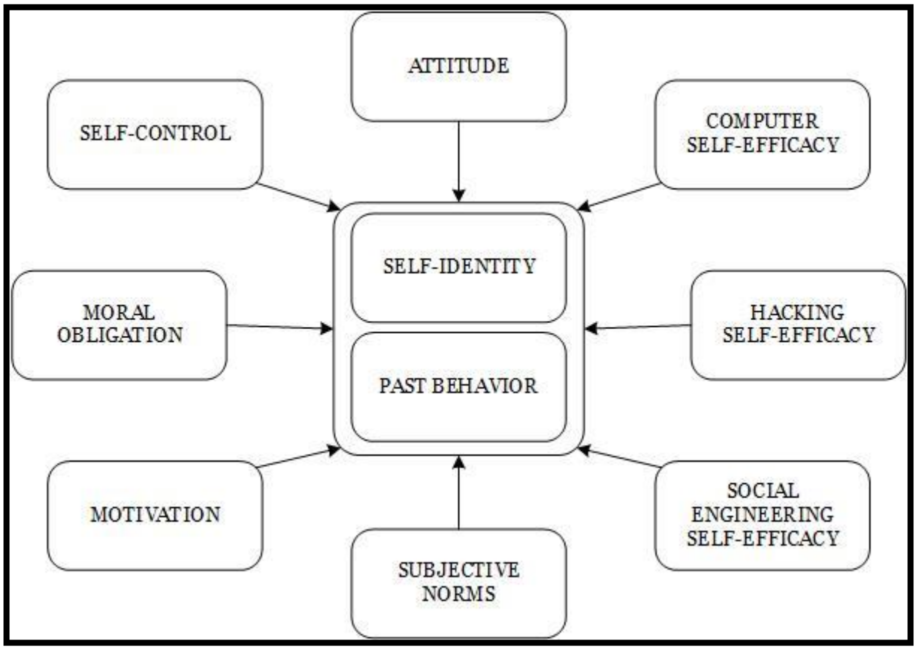

Figure 1: Proposed Theoretical Model

4 Research Methodology

This study consists of three phases: Phase I consists of belief elicitation, Phase II is survey development, and Phase III is survey implementation.

4.1 Phase I: Belief Elicitation

The belief elicitation phase is important to ensure that the survey is built on the beliefs and attitudes of the actors (e.g., Ajzen and Fishbein 1980). Qualitative, open-ended questions were asked, including: In your opinion, what makes someone a hacktivist? What do you think are some, if any, circumstances in which it is ok for someone to conduct a hack illegally? These questions were posted in eight online hacking forums, and disseminated to two different student populations. A complete list of forums where we posted the open-ended questions can be found in *Appendix A*. All forums catered to participants interested in hacking and the hacker community. Examples include, isahackers.com and the subreddit 'hackers' on reddit.com. Out of nine total responses, seven were on topic and the remaining three responses were discarded. We also distributed the questions in paper form during a meeting of a college club that supports women in Computer Science. We received eleven responses from the meeting attendees. Finally, we created an electronic version of the questions using Survey Monkey. The link to the questions was emailed to eleven Cybersecurity graduate students, which gave us nine additional responses.

A review of the belief elicitation responses revealed several points worth discussing including general knowledge of the term of hacktivist and moral views of hacking. We were surprised to find that there was at least one person from each respondent type who was not familiar with the term hacktivist. We assumed, based on degree programs and/or social activities, that all respondents had an above-average interest or skill with technology and computers. Combined with the small size of the sample, we expected that all respondents would be well aware of hacking related labels. For respondents who did have a reasonable idea what a hacktivist is, they provided consistent descriptions using words or phrases like "altruistic", "against injustice", "don't pursue money", "political," and "to make a point." We also found that only one respondent noted whether hacktivist activities were illegal. In general, it was unclear from the context whether respondents considered hacktivist to be a negative or positive label.

In respect to beliefs about justifications for illegal hacking, the majority of respondents acknowledged that situations could arise when it might be necessary. Furthermore, there was a general difference in views of the student groups in comparison to the forum respondents. The students were more likely to limit the acceptability of illegal hacking to extreme situations, such as to prevent a death or protect national security. Three of them went so far as to say that it was never justified. In contrast, the hacker forum participants were more likely to see a difference between the law and morality, noting that laws can change or even be wrong. One forum respondent said that illegal hacking would be acceptable in any situation.

Respondent Type	No. Total Responses	Summary of Responses
Cybersecurity Graduate Students	9	-At least 1 respondent from each group type was not familiar with the term hacktivist -Most respondents left moral and ethical determinations out of their definitions of hacktivist -Both types of students were the less open to the idea that illegally hacking was sometimes a necessity and restricted justifications to extreme cases -Forum respondents were more likely to point out that legality and morality are not the same and that laws can change or be wrong
College Club Members Supporting Women in CS	11	
Hacker Forum Respondents	9	

Table 1: Summary of Belief Elicitation Responses

4.2 Phase II: Survey Development

In Phase II, we developed a 124-item survey instrument (see *Appendix F*) for testing our theoretical model, guided by Fowler (2009). The belief elicitation analysis from Phase I clarified our domain definition. Survey questions were adapted from previous studies that measured the same constructs, though possibly in a different context.

4.2.1 Construct Scale Development

4.2.1.1 Self-Control

Self-control can be measured using attitudinal or behavioral measures. The behavioral measures are often criticized as being tautological since the behavior that self-control is explaining, then becomes the measure of self-control itself (e.g. Akers 1991, Arneklev et al. 2006). One way studies have avoided this criticism is by using analogous behaviors that are not "force or fraud", but are still indicators of low self-control (Arneklev et al. 2006). Our study included past behavior in the form of both criminal and analogous behaviors, though for purposes beyond measuring self-control. The primary measure of self-control we chose to implement was the attitudinal measure. Although occasionally measured as a single construct (e.g. Higgins 2007), attitudinal measures more often encompass self-control's six dimensions - impulsivity, insensitivity, preference for simple tasks, preference for physical tasks, temper control, and risk taking. For this study, questions came directly from the Grasmick et al. scale (1993) that was developed to test self-control. We included three-to-four six-point scale items for each of the six dimensions of self-control.

4.2.1.2 Attitude, Normative Beliefs, and Moral Obligation

Attitude, normative beliefs, and moral obligation items were adapted from the seven-point semantic differential-scales Ajzen used to study dishonest behaviors (Beck and Ajzen 1991). Attitude toward cybercrime generally, was measured with five questions that each ranged from positive to negative sentiment (i.e. *Good–Bad*). Normative beliefs and moral obligation were each measured with three of the seven-point semantic scales.

4.2.1.3 Computer, Hacking, and Social Engineering Self-Efficacies

Each of the three computer self-efficacy (CSE) items used seven-point semantic differential scales. Items were modeled from the Compeau and Higgins (1995) study, but the behaviors were changed to reflect general computer abilities. Hacking self-efficacy (HSE) was developed specifically for this study. There were four seven-point scaled items and the questions were modeled similarly to CSE, but using behaviors that required a high technical prowess (i.e. penetrating an enterprise network system). Social engineering self-efficacy (SESE) was also developed for this study. Five items were designed to ask about personal qualities that been identified in studies of social engineering (e.g. Manske 2000). Due to the nature of these questions focusing on personality, they were merged into the survey with the 6-point attitudinal scale self-control questions.

4.2.1.4 Self-Identity, Motivation, and Past Behavior

Self-identity questions (14 items) were structured like those from the Fielding et al. (2008) study on environmental activism, but adjusted for our purposes. Item content was based on a high-level review of hacker (criminal non-criminal) literature that revealed hacker, hacktivist, cybercriminal, and IT professional to be the most general and encompassing categories. Fourteen questions targeted these identities using seven-point semantic differential scales. Motivation items (ten) were developed similarly by conducting a high-level review of hacker literature. Most item content was based on motivations identified in hacker taxonomies (e.g. Rogers 2006). These items also used seven-point semantic differential scales. There were 28 past behavior questions. For any behavior a respondent had ever performed, a second part of the question requested the number of times performing the behavior in the last 12 months. The cybercriminal behaviors were chosen particularly for this study, but the analogous behaviors were adapted from previous literature (e.g. Arneklev et al. 2006).

Construct	**No. of Items**	**Scale Measure**
Self-Control	23	Attitudinal 6-point scale (Grasmick et al. 1993)
Attitude	5	7-point semantic differential scale, adapted to cybercrime generally (Beck and Ajzen 1991)
Subjective Norms	3	7-point semantic differential scale, adapted to cybercrime generally (Beck and Ajzen 1991)
Moral Obligation	3	7-point semantic differential scale, adapted to cybercrime generally (Beck and Ajzen 1991)
Computer Self-Efficacy	4	7-point semantic differential scale (Compeau and Higgins 1995)
Hacking Self-Efficacy	3	7-point semantic differential scale, developed for this study (adapted: Compeau and Higgins 1995)
Social Engineering Self-Efficacy	5	6-point attitudinal scale (content: Manske 2000)
Motivation	10	7-point semantic differential scale, content from literature (e.g. Rogers 2006)
Self-Identity	14	7-point semantic differential scale (modeled after Fielding et al. 2008)
Past Behavior	28	Part 1: yes or no, Part 2: frequencies in past 12 months, developed for this study, analogous behaviors from literature (e.g. Arneklev et al. 2006)

Table 2: Survey Scale Design

4.2.2 Preparation for Deployment

The survey instrument was created to be anonymous. This was an attempt to avoid self-censorship or social desirability bias if the respondents were concerned their answers could be traced back to them. These phenomena could have impacted responses for the entire survey, but the past behavior section was the most likely to be affected since it requested intimate and crime-related details that could have negative consequences for a respondent, if publicly revealed. To preclude these unwanted effects and to meet the requirements for the Institutional Review Board (IRB) approval for human subjects research, no personally identifiable information was collected and the internet protocol (IP) address collection function of Qualtrics was deselected.

The survey instrument was pretested in paper form by five Cybersecurity graduate students. Field pretesting determines how the collection protocols and the survey instrument perform under realistic conditions (Fowler, 2009). Minor content adjustments were made based on the pretesting feedback. The electronic form of the survey was created using Qualtrics software, paying special attention to maintain design consistency with the paper version. The electronic version was also pretested by five Cybersecurity graduate students.

The completed survey and additional documentation were submitted to the Institutional Review Board (IRB) for human subjects research approval. Additional documents included the application (F200), a statement regarding consent to participate in our research, an explanation of the consent notification process (Alteration/Waiver of Consent), a script for requesting listserv owner permission to email solicitations for survey participation, the resume/CV of each researcher, and proof of current Collaborative Institutional Training Initiative (CITI) certification for each researcher. The IRB approval number granted to this study was #1608817774.

4.3 Phase III: Implementation

The target population of this study included anyone skilled in technology and computers, whether they worked in technology as a career or simply participated as a hobby. The paper surveys were manually distributed and the electronic survey was shared via an anonymous link and QR code that were either emailed, posted online, or printed on cards to be handed out. A wide range of channels was used to elicit enough responses from our target population, including: discussion boards and forums, college classes, technology or hacker conferences, technology listservs, Amazon Mechanical Turk (Mturk), and personal networks. For specific distribution channels, see *Table 3*.

Channel Type	**Description**
Discussion Boards/Forums	LinkedIn, mturkgrind.com, Phoenix OWASP Meetup, reddit/hitsworthturkingfor, reddit/mturk, turkernation.com
Student Populations	Computer Science graduate & undergraduate students, MIS alumni, MIS online students
Technology Conferences	Black Hat, DEFCON, Grace Hopper, Hacker Halted
Technology Listservs	Bay Area LUG 'Talk', Boulder LUG, Corp Cyber Security Awareness, LV ISACA, LV ISC2, LV ISSA, Net Discuss, Phoenix LUG 'Discuss', Southern Nevada Cyber Alliance, UA General IT list
Other	Amazon's Mechanical Turk, friends (of friends) skilled in technology

Table 3: Survey Distribution Channels

We offered no incentives for respondents recruited through non-Mturk channels. In Mturk, survey responses were solicited in three separate batches, paying $1.00, $1.25, and $1.50, respectively. We also created a qualification test (*Appendix B*), using Mturk Command Line Tools, that asked prospective participants about their technical and computer skills and frequency of use. Only those rating themselves above average were permitted to continue to the survey. Successful participants were directed to our Qualtrics survey. Upon completion, they were returned to the Mturk site to enter a unique code, required to receive payment. A total of 73 Mturkers completed our survey.

5 Results & Analysis

This study collected a total of 208 survey responses. Two of the model constructs (SESE and HSE) were added to the survey after the onset of data collection and have 141 usable responses. Due to the anonymous nature of the survey and method of dissemination, the response rate is unknown, but any estimate would be small. Some of the listservs reached vast numbers of potential respondents (i.e. the Net Discuss listserv goes out to over 500 individuals), so it is not improbable that the survey request reached a couple of thousand people. The collection of just above 200 responses, would therefore suggest a low response rate.

Our data analysis was tested for reliability and validity, following the approaches laid out by Fowler (2009). We first tested the internal consistency (see *Table 4*) of our constructs. The constructs adapted from prior studies and HSE, developed for this study, all are internally consistent at an acceptable level above 0.6 (Nunnally 1967) or above 0.7 (Nunnally 1978). SESE is not acceptably internally consistent ($\alpha = 0.42$), so it may be a formative construct.

Our analyses included a principal components analysis, exploratory factor analysis, and a multinomial logistical regression. Additional analyses are necessary. A principal components analysis and an exploratory factor analysis of motivation and self-identity were performed. We reduced the dimensionality of self-identity from 14 items to six factors. A visual review confirmed that the factors represented logical groupings of the items (see *Appendix C*). Motivation dimensionality was reduced from ten items to four factors (see *Appendix D*). To achieve the four factors, the tenth item was dropped, appearing to perform as a double-loaded question. The factor scores replaced the original items for both self-identity and motivation.

	No. of Items	Cronbach's α	Mean	SD
Attitude	5	0.77	5.39	1.19
Subjective Norms	2	0.67	1.98	1.15
Moral Obligation	3	0.83	2.19	1.30
Self-Control				
Impulsivity	3	0.71	2.73	1.01
Temper	4	0.75	2.38	0.96
Simple Tasks	4	0.79	2.36	0.96
Risk Taking	4	0.79	2.96	1.00
Physical Activities	4	0.70	3.08	1.07
Self-Centered	4	0.75	2.52	1.01
Computer SE	3	0.80	5.80	1.03
Hacking SE	4	0.85	3.71	1.75
Social Engineering SE	5	0.42	2.62	1.90
Motivation				
(F1) Excitement	2	0.62	0.01	0.81
(F2) Enjoyment/Enrichment	3	0.60	0.02	0.70
(F3) Extrinsic	3	0.47	0.00	0.78
(F4) Patriotic	1	-	0.01	0.75
Self-Identity				
(F1) Problem solving, leveraging experience	4	0.76	0.00	0.90
(F2) Hacking	2	0.87	0.00	0.99
(F3) Ethics	3	0.62	0.00	0.80
(F4) Activism	1	-	0.00	0.98
(F5) Challenge the norm	2	0.56	0.00	0.76
(F6) Morality over ethics	1	-	0.00	0.96

*Motivation, self-identity, and past behavior data not expected to be internally consistent

Table 4: Summary Statistics & Internal Consistency

5.1 Cluster Analysis

We performed a cluster analysis on the self-identity factors using the K-means algorithm. Clustering is useful when grouping of the data is not previously known. In the case of this study, the types of skilled technologists that we would find were unknown, so clustering was an appropriate choice of analysis. We implemented three methods for determining the best number of clusters, including the elbow method, construction of a screeplot and NbClust (an R package). A four-cluster spread was found to be best for our data. The K-means (k=4) output revealed four clusters, sized 35, 58, 50, and 60, respectively. Based on a review of item responses within each cluster, we qualitatively described each cluster as follows:

- *Heroes* (Cluster 1) are most likely of the groups to consider themselves ethical or law-abiding and are the least likely to believe illegal activity is ever warranted. They are unlikely to identify as hackers.
- *Eccentrics* (Cluster 2) are the group that identifies the least as hackers and believe more than any other group that it is necessary at times to break the law. They are the most likely to describe themselves as unconventional and perhaps willing to take unorthodox or even extreme measures.
- *Hacking Professionals* (Cluster 3) identify as IT professionals who seek to use technology to solve problems, more than any other group. They also generally view themselves as unconventional, perhaps taking unorthodox or even extreme measures, though less so than cluster 2.
- *Conservatives* (Cluster 4) are the least likely to view themselves as an IT professional or be interested in solving problems with technology. They are most likely to feel a part of mainstream society, but they are also the least likely group to be concerned with contributing to a cause.

We calculated summary statistics of the other model constructs, broken down by cluster. The means and standard deviations can be found in *Table 4* below.

	Mean				Standard Deviation			
Cluster	C 1	C 2	C 3	C 4	C 1	C 2	C 3	C 4
Attitude	5.89	5.42	4.71	5.51	0.92	1.18	1.20	1.14
Subjective Norms	1.61	1.97	2.55	1.80	0.90	0.91	1.53	1.01
Moral Obligation	1.54	2.24	2.81	2.29	0.88	1.06	1.53	1.44
Self-Control								
Impulsivity	2.62	2.75	2.88	2.64	1.15	0.86	1.08	0.93
Temper	2.13	2.50	2.53	2.41	0.83	1.02	0.98	0.98
Simple Tasks	2.28	2.35	2.34	2.51	0.95	0.91	0.93	1.09
Risk Taking	2.71	3.04	3.29	2.81	0.93	0.97	1.00	1.05
Physical Activities	3.33	3.03	3.06	2.79	1.12	1.05	0.95	1.11
Self-Centered	2.38	2.54	2.63	2.57	0.99	0.94	1.06	1.07
Computer SE	5.74	5.77	6.18	5.41	0.92	1.04	0.71	1.38
Hacking SE	3.50	3.39	4.76	3.11	1.82	1.65	1.28	1.84
Motivation								
(F1) Excitement	-0.03	-0.02	0.10	0.01	0.86	0.62	0.85	0.94
(F2) Enjoyment/ Enrichment	0.03	-0.02	0.22	-0.24	0.72	0.69	0.62	0.75
(F3) Extrinsic	-0.25	0.18	0.22	-0.23	0.73	0.73	0.78	0.81
(F4) Patriotic	0.26	-0.20	-0.06	0.08	0.66	0.76	0.84	0.65

Table 5: Summary Statistics by Cluster (Type)

5.2 Multinomial Logistical Regression Analysis

We conducted a multinomial logistical regression (mlogit) that outputted regression coefficients and relative risk ratios (see *Appendix E*). Logistic regression is one of the most widely used methods for analysis of categorical outcome variables. Mlogit regression is specifically implemented when there are three or more categories, such as the clusters or types in this study. Self-identity cluster 1 was assigned as the reference and three regression models were generated, one for each of the other four clusters.

Moral obligation was the most interesting of all our constructs. The coefficients and relative risk ratios were significant (0.05 threshold) in two of the regression models (cluster 3 and cluster 4), more than any other construct. For a one-unit increase in moral obligation, the multinomial log-odds of that individual being in cluster 3 relative to cluster 1, would be expected to increase by 0.87 (coefficient). For a one-unit increase in moral obligation, the relative risk of an individual being in cluster 3 relative to cluster 1, with the other variables constant, would increase by a factor of 2.38 (risk ratio). In more comprehensible terms, when a skilled technologist has higher moral obligation (cybercrime is more compatible with his or her morals), the relative risk of being in cluster 3 is 2.88 times more likely than being in cluster 1. Therefore, we would expect that technologist to be in cluster 3 rather than cluster 1. From the cluster 4 regression model, we can see that the likelihood of being in cluster 4 for the same one-unit increase in moral obligation is a factor of 2.85, so we would expect the technologist to be in cluster 4, rather than cluster 1.

Five of our other constructs had coefficients and risk ratios that were significant (0.05 threshold) for one of the regression models. These constructs included physical activities, attitude, hacking self-efficacy, and motivation factors 3 (extrinsic) and 4 (patriotism). The models for which they were significant include, cluster 4, cluster 3, cluster 3, cluster 2, and cluster 2, respectively. A skilled technologist with a higher preference for physical activities would be expected to in cluster 1 over cluster 4 (RRR= 0.42). Someone with a more negative attitude towards cybercrime would be expected to be part of cluster 1 rather than cluster 3 (RRR=0.51). A technologist who rates him- or herself highly in terms of hacking ability would be more likely to be in cluster 2 relative to cluster 1 (RRR= 1.63). Someone who is more motivated by money or revenge or politics would be expected to be in cluster 2 rather than cluster 1 (RRR=2.63). Finally, a skilled technologist who is most motivated by patriotism would be expected to be in cluster 1, rather than cluster 2 (RRR=0.46).

6 Limitations

Although one of the research gaps that this study sought to address was the non-representative sample populations used in so many studies, we cannot say for sure that our own sample population included a true spectrum of skilled technologists. Our survey dissemination channels varied widely from students to technology listserv members to hacker conference attendees. However, these may not be the best channels to reach the most extreme characters. As discussed in a moment, even with some respondents admitting to criminal past behavior, there are always questions to the legitimacy and accuracy of self-reported data.

Another potential challenge of this research is the survey method itself. All of the data collected is self-reported and beyond checking for congruency in respondent answers, there is no way to check for correctness, especially in light of the anonymity of this survey. Social desirability bias could have caused respondents to answer questions in a way they thought was socially expected or, alternatively, they could have had a personal agenda and intentionally answered dishonestly. Many of the questions revealed personal details, even about illegal behavior, so a distrust that the survey is truly anonymous could also have tainted the results, especially the past behavior responses.

The length of the survey instrument was another potential limitation to this study. At 7 pages, 124 items, the survey took between 10-15 minutes or perhaps longer for respondents who took their time to think through each question. Qualtrics recorded any attempt at completing the survey, as long as the individual proceeded past the consent page. We believe at least some of the cases where the survey was opened, but not attempted, could be explained with the following scenario: an individual paged through the survey and decided not to participate upon realization of its length and the potential time to completion. Further impacts of the survey length could have included a change in responses as frustration with completing the survey rose or a decreased comprehension of questions as the speed of progress increased in order to accelerate task completion. There was at least one subjective norms question that we believed was misinterpreted by a substantial portion of the respondents based on the disparity of responses compared to the other items and the fact that it was negatively phrased, unlike those other related items.

The last potential limitation to be discussed at this time is that of term interpretations. This paper has already addressed in detail the disagreement in definitions for cybercrime and related terms. Many of our constructs related to beliefs and values, so we formed questions that asked about cybercrime generally, without providing a standard definition. We assumed that respondents would use whatever understanding of cybercrime they had come to accept, as the basis for answering our survey. On the one hand, this assures that responses are based on the underlying beliefs and values of the respondents without biases that could result from providing our own definitions. However, this also could mean that the respondents all had different concepts and definitions in their minds when they answered the survey.

7 Future Additions to This Research

Several additional analyses need to be conducted. We have identified types of skilled technologists based on self-identity clusters, but through additional analyses we will refine our labels and descriptions of those types. We will extend the explanatory power of our multinomial logistical regression (mlogit) analysis by calculating construct marginal effects. Additionally, we will compute an mlogit analysis a second time, treating self-control as a single dimension, as described in some past studies (e.g. Arneklev et al. 1999). Only one of the regression models found one (physical activities) of the self-control dimensions to be significant in terms of regression coefficients and relative risk ratios. We may have more success treating self-control as one dimension.

Another adjustment to our mlogit regression would incorporate social engineering self-efficacy (SESE) and past behavior. We have yet to include SESE or past behavior in our analyses. SESE question items were added after the start of the data collection process, so it may only be a useable construct for a smaller data set that begins when SESE was added to the survey. Therefore, we will repeat our analyses with a smaller (141-response) data set. The smaller data set would also allow us to use all the hacking self-efficacy (HSE) items, the majority of which were added at the same time as the SESE items. Such a computation would function as a robustness check. Finally, the past behavior data is unique from the other constructs, so a different method of analysis will be required. We may choose to group the past behaviors by behaviors that are never illegal, behaviors that can be illegal depending on circumstances, and behaviors that are always illegal. At that point, we would have a categorical variable like self-identity and could perform an mlogit regression. There would still be the issue of the second part of the past behavior question that asked for frequencies of each behavior in the last 12 months. This section of the survey had the lowest response rate, so it is unclear at present how useable that data will be.

One final potential addition to this research that will be discussed in this paper, is the incorporation of a scientific measure for assessing hacking skill level. One proposed study is attempting to design such a measure. At present, no such measure exists and all prior research, this study included, has relied on self-reporting to determine skill level. The study of interest has proposed a methodology for creating an 18-scenario scale that will "(1) more accurately discriminate between categories of hackers, (2) more accurately quantify who is a hacker and who is not, and (3) provide evidence that their findings are indeed generalizable to the population of interest," (Giboney et al. 2015, pp. 124). Including a scientific measure for hacking ability as opposed to self-reported self-efficacy, would improve the accuracy of our model.

Lastly, this measure could be redesigned to replace other measures of self-efficacy, such as social engineering self-efficacy, which would further improve the accuracy of our model.

8 References

Ajzen, I. 1991. “The Theory of Planned Behavior,” Organizational Behavior and Human Decision Processes (50), pp. 179-211.

Ajzen, I., and Fishbein, M. 1980. Understanding attitudes and predicting social behavior, Englewood Cliffs, NJ: Prentice-Hall.

Ajzen, I., and Klobas, J. 2013. “Fertility intentions: An approach based on the theory of planned behavior,” *Demographic Research* (29:8), July-December, pp. 203-232.

Akers, R.L. 1991. “Self-Control as a General Theory of Crime,” *Journal of Quantitative Criminology* (7:2), June, pp. 201-211.

Arneklev, B.J., Elis, L., and Medlicott, S. 2006. “Testing the General Theory of Crime: Comparing the Effects of ‘Imprudent Behavior’ and an Attitudinal Indicator of ‘Low Self-Control’,” Western Criminology Review (7:3), pp. 41-55.

Bachmann, M. 2010. “The Risk Propensity and Rationality of Computer Hackers,” International Journal of Cyber Criminology (4:1&2), January-July, July-December, pp. 643-656.

Bagozzi, R.P., and Kimmel, S.K. 1995. “A Comparison of Leading Theories for the Prediction of Goal-Directed Behaviours,” *British Journal of Social Psychology* (34:4), December, pp. 437-461.

Bandura, A. 1982. “Self-Efficacy Mechanism in Human Agency,” *American Psychologist* (37), pp. 122-147.

Bandura, A. 1977. *Social Learning Theory*, Englewood Cliffs, NJ: Prentice-Hall.

Baumeister, R.F., and Vohs, K.D. 2007. “Self-Regulation, Ego Depletion, and Motivation,” *Social and Personality Psychology Compass* (1:1), November, pp. 115-128.

Beck, L., and Ajzen, I. 1991. “Predicting Dishonest Actions Using the Theory of Planned Behavior,” Journal of Research in Personality (25:3), September, pp. 285–301.

Bergal, J. 2017. “‘Hacktivists’ Increasingly Target Local and State Government Computers,” The Pew Charitable Trusts: Stateline, 10 January, (http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2017/01/10/hacktivists-increasingly-target-local-and-state-government-computers).

Bossler, A. M., and Burruss, G. W. 2011. "The General Theory of Crime and Computer Hacking: Low Self-Control Hackers?" in Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications, T. Holt and B. Schell (eds.), Hershey, PA: IGI Global, pp. 38-67.

Coleman, G. 2011. “Hacker Politics and Publics,” Public Culture (23:3), Durham, NC: Duke University Press, pp. 511-516.

Columbus, L. 2016. “Roundup of Internet of Things Forecasts and Market Estimates, 2016,” Forbes Contributor, Forbes.com, November 27 (available at https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#3e80eb92292d; retrieved May 11, 2017).

Compeau, D.R., and Higgins, C.A. 1995. “Computer Self-Efficacy: Development of a Measure and Initial Test,” *MIS Quarterly* (19:2), June, pp. 189-211.

Conner, M., and Armitage, M.C. 1998. “Extending the Theory of Planned Behavior: A Review and Avenues for Further Research,” *Journal of Applied Social Psychology* (28:15), pp. 1429-1464.

Crawley, F. E., and Black, C. B. 1992. “Causal modeling of secondary science students’ intentions to enroll in physics,” *Journal of Research in Science Teaching* (29), pp. 585-599.

Cronan, T.P., Foltz, C.B., and Jones, T.W. 2006. “Piracy, computer crime, and IS misuse at the University,” *Communications of the Association for Computing Machinery* (49:6), June, pp. 84–90.

de Vries, H., Backbier, E., Kok, G., and Dijkstra, M. 1995. “The Impact of Social Influences in the Context of Attitude, Self-Efficacy, Intention, and Previous Behavior as Predictors of Smoking Onset,” *Journal of Applied Social Psychology* (25), pp. 237-257.

Denning, D.E. 2001. “Chapter 8: Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy,” in Networks and Netwars: The Future of Terror, Crime, and Militancy, Arquilla, J. and Ronfeldt, D. (eds.), Santa Monica, CA: RAND, pp. 239-288.

Donner, C. M., Fridell, L. A., and Jennings, W.G. 2016. "The Relationship Between Self-Control and Police Misconduct: A Multi-Agency Study of First0Line Police Supervisors," Criminal Justice and Behavior (43:7), April, pp. 841-862.

Donner, C.M., Marcum, C.D., Jennings, W.G., Higgins, G.E., and Banfield, J. 2014. “Low Self-control and Cybercrime: Exploring the Utility of the General Theory of Crime Beyond Digital Piracy,” Computers in Human Behavior (34), pp. 165-172.

Fielding, K. S., McDonald, R., and Louis, W. R. 2008. “Theory of Planned Behaviour, Identity and Intentions to Engage in Environmental Activism,” *Journal of Environmental Psychology* (28), pp. 318-326.

Finklea, K., and Theohary C. A. 2015. “Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement,” in CSR Report No. R42547, Washington DC: Congressional Research Service, January 15, pp. 1-27.

Fowler, Jr., F.J. 2009. Survey Research Methods, 4th Edition, Thousand Oaks, CA: SAGE Publications, Inc.

Ghosh, S., and Turrini, E. 2010. “Chapter 1: A Pragmatic, Experiential Definition of Computer Crimes,” in *Cybercrimes: A multidisciplinary Analysis*, Heidelberg, Berlin: Springer-Verlag, pp. 3-23.

Giboney, J.S., Goel, S., Proudfoot, J.G., and Valacich, J.S. 2015. “Measuring Hacking Ability Using a Conceptual Expertise Task,” *2015 Proceedings on the Conference on Digital Forensics, Security, and Law*, May, pp. 123-134.

Gottfredson, M.R., and Hirschi, T. 1990. A General Theory of Crime, Stanford, CA: Stanford University Press.

Grasmick, H. G., Tittle, C. R., Bursik, Jr., R. J., and Arneklev, B. J. 1993. “Testing the Core Empirical Implications of Gottfredson and Hirschi's General Theory of Crime,” *Journal of Research in Crime and Delinquency* (30:1), February, pp. 5-29.

Hampson, N.C.N. 2012. “Hacktivism: A New Breed of Protest in a Networked World,” Boston College International & Comparative Law Review (35), pp. 511-542.

Higgins, G.E. 2007. “Examining the Original Grasmick Scale: A Rasch Model Approach,” *Criminal Justice and Behavior* (34:2), pp. 157-178.

Higgins, G.E., Fell, D.B. and Wilson, A.L. 2006. “Digital Piracy: Assessing the Contributions of an Integrated Self-Control Theory and Social Learning Theory Using Structural Equation Modeling,” *Criminal Justice Studies: A Critical Journal of Crime, Law and Society* (19:1), pp. 3-22.

Higgins, G.E., and Makin, D.A. 2004. “Does Social Learning Theory Condition the Effects of Low Self-Control on College Students’ Software Piracy?” *Journal of Economic Crime Management* (2:2), January, pp. 1-22.

Holt, T.J., Bossler, A.M., and May, D.C. 2012. “Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance,” *American Journal of Criminal Justice* (37:3), pp. 378-395.

Hsia, J., Chang, C., and Tseng, A. 2011. “Effects of individuals' locus of control and computer self-efficacy on their e-learning acceptance in high-tech companies,” *Behaviour & Information Technology* (33:1), pp. 51-64.

Kautonen, T., Gelderen, M.V. and Fink, M. 2013. “Robustness of the Theory of Planned Behavior in Predicting Entrepreneurial Intentions and Actions,” *Entrepreneurship: Theory and Practice* (39:3), pp. 655-674.

Lloyd, G. 2015. “The Need for Hacker Identification and Attribution,” Alexandria, VA: Lloyd Research Institute, pp. 1-6.

Manske, K. 2000. “An Introduction to Social Engineering,” *Information Systems Security* (9:5), pp. 1-7.

Marcum, C. D., Higgins, G. E., and Poff, B. 2016. "Exploratory investigation on theoretical predictors of the electronic leash," *Computers in Human Behavior* (61), pp. 213-218.

McQuade, III, S.C. 2006. *Understanding and Managing Cybercrime*, London, England: Pearson.

Mickelberg, K., Pollard, N., and Schive, L. 2014. “US Cybercrime: Rising Risks, Reduced Readiness: Key Findings from the 2014 US State of Cybercrime Survey,” PricewaterhouseCoopers LLP, pp. 1-19.

Moon, B., McCluskey, J.D., and McCluskey, C.P. 2010. “A General Theory of Crime and Computer Crime: An Empirical Test,” Journal of Criminal Justice (38), Joscelyn, K. (ed.), pp. 767-772.

Mullen, B., Johnson, D.A., and Drake, S.D. 1987. “Organizational Productivity as a Function of Group Composition: A Self-Attention Perspective,” *Journal of Social Psychology* (127), pp. 143-150.

Murphy, C.A., Coover, D., and Owen, S.V. 1989. “Development and Validation of the Computer Self-Efficacy Scale,” *Educational and Psychological Measurement* (49:4), pp. 893-899.

Nunnally, J.C. 1967. *Psychometric Theory*, New York: McGraw Hill.

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

Piven, F.F. and Cloward, R.A. 1991. “Collective Protest: A Critique of Resource Mobilization Theory,” International Journal of Politics, Culture and Society (4:4), Berlin, Germany: Springer, pp. 435-458.

Rogers, M.K. 2006. “A Two-dimensional Circumplex Approach to the Development of a Hacker Taxonomy,” in *Digital Investigations* (3), pp. 97-102.

Sarma, M., and Lam, A. 2013. “Knowledge creation and innovation in the virtual community – exploring structure, values and identity in hacker groups,” The 35th DRUID Celebration Conference 2013, 17-19 June, Barcelona, Spain.

Schwarzer, R., and Fuchs, R. 1996. “Self-Efficacy and Health Behaviors,” in *Predicting Health Behavior: Research and Practice with Social Cognition Models*, M. Conner and P. Norman (eds.), Buckingham, UK: Open University Press, pp. 163-196.

Sparks, P., and Guthrie, C.A. 1998. “Self-Identity and the Theory of Planned Behavior: A Useful Addition or an Unhelpful Artifice?” *Journal of Applied Social Psychology* (28:15), pp. 1393-1410.

Terry, D.J., and O’Leary, J.E. 1995. “The Theory of Planned Behaviour: The Effects of Perceived Behavioural Control and Self-Efficacy,” *British Journal of Social Psychology* (34), pp. 199-220.

Tittle, C.R., and Botchkovar, E.V. 2005. “Self-Control, Criminal Motivation and Deterrence: An Investigation Using Russian Respondents,” *Criminology* (43:2), pp. 307-354.

“World Internet Users Statistics and 2017 World Population Stats.” 2017. Internet World Stats, Miniwatts Marketing Group, 30 March (http://www.internetworldstats.com/stats.htm; retrieved May 9, 2017).

Xu, Z., Hu, Q., and Zhang, C. 2013, April. “Why Computer Talents Become Hackers,” Communications of the AMC (56:4), Association of Computing Machinery, pp. 64-74.

Appendix A: Belief Elicitation Forums and Response Types

Forum Name	Website	Response Type
Askreddit	Reddit.com	1 relevant; 2 silly/off-topic
Community	Bitshacking.com	None
Comminity Talk	Defcon.org	3 relevant
Hacker_space	Reddit.com	None
Hack4good	Reddit.com	None
Hack	Reddit.com	2 relevant
Anarcho_hackers	Reddit.com	1 relevant
Hacker	Reddit.com	None

Table 6: Belief Elicitation Post Forum

Appendix B: Amazon Mechanical Turk Qualification Test Questions

1	How would you rate your ability to use technology in general? (1) Poor (2) Below Average (3) Average (4) Above Average (5) Excellent
2	How would you rate your ability to use a computer? (1) Poor (2) Below Average (3) Average (4) Above Average (5) Excellent
3	How often do you use technology? EXCLUDE basic uses, such as checking email, texting, or making phone calls. (1) All the time (2) Frequently (3) Occasionally (4) Rarely (5) Never
4	Where do you live? (1) China (2) Chile (3) England (4) India (5) United States (6) Other

Table 7: Mturk Qualification Test Questions

Appendix C: Self-Identity Factors and Respective Question Items

	Description	Question Items
Factor 1	Problem solving, leveraging experience	1. I am the type of person who uses computers and technology to solve or prevent problems. 2. I consider myself an IT professional. 3. Being knowledgeable about and skilled in using technology and computers is an important part of who I am. 4. Using computers and technology to make positive change is a priority for me.
Factor 2	Hacking	1. I consider myself a hacker. 2. Hacking is an important part of who I am.
Factor 3	Ethics	1. I think of myself as an ethical person. 2. I am not the type of person who would do something illegal. 3. I am not the type of person to worry about whether or not something is legal.
Factor 4	Activistism	1. Contributing to a cause is a key part of who I am.
Factor 5	Challenge the norm	1. I think of myself as someone outside of mainstream society. 2. I am the type of person who would go to extremes to further a cause I believe in.
Factor 6	Morality over ethics	1. I believe there are times when it is necessary to break the law.

Table 8: Self-Identity Factors

Appendix D: Motivation Factors and Respective Question Items

	Description	Items
Factor 1	Excitement	1. Often I do things because they are exciting. 2. Often I do things simply because I am able.
Factor 2	Enjoyment and enrichment	1. Often my actions are motivated by curiosity. 2. Often I am motivated by a chance to learn and grow my skills. 3. Often I do things because they are fun.
Factor 3	Extrinsic	1. Often I am motivated to act by money. 2. Often my actions are motivated by revenge. 3. Often my actions are motivated by political or social causes.
Factor 4	Patriotic	1. Often I am motivated to act by patriotism.

Table 9: Motivation Factors

Appendix E: Multinomial Logistical Regression – Coefficients & Risk Ratios (*Significant at a threshold of 0.05)

	(Intercept)	Self-Control						SN	MO	ATT	CSE	HSE	Motivation			
		I	T	ST	RT	PA	SC						F 1	F 2	F 3	F 4
C2	-1.32	0.07	0.23	-0.11	0.25	-0.46	-0.20	-0.15	0.56	-0.01	0.27	-0.04	-0.09	-0.23	0.97*	-0.78*
C3	-2.73	0.08	0.52	0.01	0.27	-0.31	-0.25	-0.30	0.87*	-0.66*	0.37	0.49*	-0.25	0.50	0.60	-0.11
C4	2.04	-0.10	0.10	0.23	0.24	-0.88*	-0.13	-0.54	1.05*	-0.10	-0.19	-0.08	0.72	-0.63	-0.03	0.25

Table 10: Regression Coefficients

	(Intercept)	Self-Control						SN	MO	ATT	CSE	HSE	Motivation			
		I	T	ST	RT	PA	SC						F 1	F 2	F 3	F 4
C2	0.27	1.08	1.26	0.90	1.28	0.63	0.82	0.86	1.75	0.99	1.31	0.96	0.92	0.79	2.63*	0.46*
C3	0.07	1.08	1.68	1.01	1.31	0.73	0.78	0.74	2.38*	0.51*	1.44	1.63*	0.78	1.65	1.81	0.90
C4	7.69	0.91	1.10	1.26	1.28	0.42*	0.88	0.58	2.85*	0.91	0.83	0.92	2.05	0.53	0.97	1.29

Table 11: Regression Relative Risk Ratios

	(Intercept)	Self-Control						SN	MO	ATT	CSE	HSE	Motivation			
		I	T	ST	RT	PA	SC						F 1	F 2	F 3	F 4
C2	0.62	0.80	0.49	0.73	0.40	0.07	0.49	0.64	0.10	0.96	0.30	0.78	0.81	0.52	0.01	0.02
C3	0.39	0.81	0.15	0.99	0.41	0.24	0.45	0.37	0.02	0.03	0.31	0.01	0.55	0.27	0.17	0.78
C4	0.48	0.76	0.80	0.50	0.47	0.00	0.69	0.14	0.00	0.74	0.50	0.64	0.08	0.12	0.95	0.53

Table 12: P-Values for Coefficients and Risk Ratios

Appendix F: The Survey Instrument

ARIZONA

Study Title*: Survey of Technology Enthusiasts*

Principal Investigator*: Ashley Ireson*

This is a University of Arizona consent form for research participation. *It contains important information about this study and details about participation. Please consider the information carefully. Feel free to discuss the study with friends and family and to ask questions before you decide whether or not to participate.*

Why is this study being done?

We are interested in learning about the behaviors and attitudes of hackers and IT professionals. We hope to see some patterns emerge that will prove useful to government and private industry to stay safe and perhaps make better hiring decisions.

What will happen if I take part in this study?

If you agree to participate, you will be asked to complete a survey about your attitudes and behaviors relating to online activities.

How long will I be in the study?

The survey will take approximately 10 minutes to complete.

What are the costs of taking part in this study?

There is no cost to you except for the roughly 10 minutes required to complete the survey.

How many people will take part in this study?

We hope to survey 200-300 people.

Can I stop being in the study?

You may withdraw from the study at any time without penalty. Simply notify the researcher and return the survey form to him or her.

What risks or benefits can I expect from being in the study?

There are no known risks from your participation.

Will my study-related information be kept confidential?

The survey is completely anonymous; your name will not be attached to the information that you provide. Only the researchers will have access to the data from this survey.

Who can answer my questions about the study?

For questions, concerns, or complaints about the study you may contact Ashley Ireson at airley@email.arizona.edu.

For questions about your rights as a participant in this study or to discuss other study-related concerns or complaints with someone who is not part of the research team, you may contact the Human Subjects Protection Program at 520-626-6721 or online at http://rgw.arizona.edu/compliance/human-subjects-protection-program.

If you are injured as a result of participating in this study or for questions about a study-related injury, you may contact Ashley Ireson at airley@email.arizona.edu.

An Institutional Review Board responsible for human subjects research at The University of Arizona reviewed this research project and found it to be acceptable, according to applicable state and federal regulations and University policies designed to protect the rights and welfare of participants in research.

By reading this document and taking this survey, I agree to participate in this study and have my anonymous responses analyzed.

HSPP Use Only:

Are you 18 years of age or older?

Yes

No

I. Please consider the extent to which the following statements apply to you and select your answer:

	Strongly disagree 1	Disagree 2	Mildly disagree 3	Mildly agree 4	Agree 5	Strongly agree 6
I don’t devote much thought and effort to preparing for the future.	○	○	○	○	○	○
I lose my temper easily.	○	○	○	○	○	○
I prefer doing things that pay off right away rather than in the future.	○	○	○	○	○	○
I try to get the things I want even when I know it’s causing problems for other people.	○	○	○	○	○	○

	Strongly disagree 1	Disagree 2	Mildly disagree 3	Mildly agree 4	Agree 5	Strongly agree 6
When things get complicated, I tend to quit or withdraw.	○	○	○	○	○	○
When I am really angry, other people better watch out.	○	○	○	○	○	○
I dislike hard tasks that stretch my abilities to the limit.	○	○	○	○	○	○
Unless I tell them, people don't know what I'm truly thinking or feeling.	○	○	○	○	○	○
I like to test myself every now and then by doing something a little risky.	○	○	○	○	○	○
I try to look out for myself first, even if it means making things difficult for other people.	○	○	○	○	○	○
I find it exciting to do things for which I might get in trouble.	○	○	○	○	○	○
I’m more concerned about what happens to me in the short run than in the long run.	○	○	○	○	○	○
I am good at figuring out people's weaknesses.	○	○	○	○	○	○
If I have a choice, I do something physical rather than something mental.	○	○	○	○	○	○
When I’m angry at people I feel more like hurting them than talking to them about why I am angry.	○	○	○	○	○	○

	Strongly disagree 1	Disagree 2	Mildly disagree 3	Mildly agree 4	Agree 5	Strongly agree 6
I'm not very sympathetic to other people when they are having problems.	○	○	○	○	○	○
I seem to have more energy and a greater need for activity than most other people my age.	○	○	○	○	○	○
I tend to take risks just for the fun of it.	○	○	○	○	○	○
I like to get out and do things more than I like to read or contemplate ideas.	○	○	○	○	○	○
If things I do upset people, it's their problem, not mine.	○	○	○	○	○	○
I know what questions to ask to get people talking.	○	○	○	○	○	○
I try to avoid things that I know will be difficult.	○	○	○	○	○	○
Excitement and adventure are more important to me than security.	○	○	○	○	○	○
I will exaggerate the truth if there is no other way to convince someone.	○	○	○	○	○	○
I feel better when I am on the move and active than when I am sitting and thinking.	○	○	○	○	○	○
People are comfortable telling me things.	○	○	○	○	○	○
The things in life that are easiest to do bring me the most pleasure.	○	○	○	○	○	○

	Strongly disagree 1	Disagree 2	Mildly disagree 3	Mildly agree 4	Agree 5	Strongly agree 6
When I have a serious disagreement with someone, it's hard for me to talk about it without getting upset.	○	○	○	○	○	○

II. What are your general views on or feelings towards cybercrime? Select the number that best reflects where your views fit on each spectrum below.

To me, cybercrime is...

Good 1						Bad 7
○	○	○	○	○	○	○
Pleasant 1						Unpleasant 7
○	○	○	○	○	○	○
Foolish 1						Wise 7
○	○	○	○	○	○	○
Useful 1						Useless 7
○	○	○	○	○	○	○
Unappealing 1						Appealing 7
○	○	○	○	○	○	○

III. Given your own understanding of or definition of cybercrime, consider whether or not the following statements would or do apply to you.

If I engaged in cybercrime, most of the people who are important to me would…	Strongly disapprove 1	Disapprove 2	Slightly disapprove 3	Not care 4	Slightly approve 5	Approve 6	Strongly approve 7
People who are	Strongly		Slightly		Slightly		Strongly

important to me do not think it is OK to commit cybercrime.	Strongly disagree 1	Disagree 2	Slightly disagree 3	Neutral 4	Slightly agree 5	Agree 6	Strongly agree 7
Most important people in my life would look down on me if I commit cybercrime.	Highly unlikely 1	Unlikely 2	Somewhat unlikely 3	Neutral 4	Somewhat likely 5	Likely 6	Highly likely 7
I would not feel guilty if I committed cybercrime.	Strongly disagree 1	Disagree 2	Slightly disagree 3	Neutral 4	Slightly agree 5	Agree 6	Strongly agree 7
Cybercrime goes against my principles.	Strongly disagree 1	Disagree 2	Slightly disagree 3	Neutral 4	Slightly agree 5	Agree 6	Strongly agree 7
It would be morally wrong for me to engage in cybercrime.	Strongly disagree 1	Disagree 2	Slightly disagree 3	Neutral 4	Slightly agree 5	Agree 5	Strongly agree 7

IV. The following statements are about your abilities related to computers and technology. Please circle the number that most accurately reflects your ability for each statement.

	Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neutral 4	Somewhat agree 5	Agree 6	Strongly agree 7
When I participate in computer, hacking or technology-related competitions, I have a good chance of winning.	○	○	○	○	○	○	○
I am able to do things with computers that most people cannot.	○	○	○	○	○	○	○
I am confident in my technical ability to penetrate a corporate network system.	○	○	○	○	○	○	○
I have been good with computers for as long as I can remember.	○	○	○	○	○	○	○

	Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neutral 4	Somewhat agree 5	Agree 6	Strongly agree 7
I have the skills to write an	○	○	○	○	○	○	○

exploit.	○	○	○	○	○	○	○
I can easily learn new computer skills on my own.	○	○	○	○	○	○	○
It would be easy for me to remotely take control of someone else's computer.	○	○	○	○	○	○	○

V. Please indicate whether or not you have <u>ever</u> engaged in the following activities and, if you have, how many times you have done so in the last 12 months.

	Have you ***ever*** engaged in any of the given activities?		If yes, how many times in the last 12 months?
	Yes	No	Times in last 12 months:
Written malware or a virus, etc.	○	○	□
Pretended to be someone else online	○	○	□
Attended a technology, hacker, cybersecurity, etc. conference	○	○	□
Bought a stolen credit card number	○	○	□
Obtained control of someone else’s computer without permission	○	○	□
Had unprotected sex	○	○	□
Stolen someone’s identity	○	○	□
Vandalized a website	○	○	□
Attempted to spoof someone via email	○	○	□
	Yes	No	Times in last 12 months:
Participated in a DDoS attack	○	○	□
Sent spam or a phishing email	○	○	□
Harassed someone online	○	○	□
Stalked someone online	○	○	□

	Have you ***ever*** engaged in any of the given activities?		If yes, how many times in the last 12 months?
	Yes	No	Times in last 12 months:
Distributed obscene material online	○	○	□
Used an illegal substance	○	○	□
Distributed pirated software	○	○	□
Created an exploit kit	○	○	□
Used an exploit kit	○	○	□
	Yes	No	Times in last 12 months:
Distributed malware or a virus, etc.	○	○	□
Obtained control of someone else's computer with permission	○	○	□
Been hired to find network or other vulnerabilities	○	○	□
Took advantage of a network or other vulnerability for personal gain	○	○	□
Been in an accident or injured yourself, requiring medical attention	○	○	□
Gambled or bet online	○	○	□
Not worn a seatbelt	○	○	□
Used a botnet	○	○	□
Sold illegal goods online	○	○	□

VI. The following statements relate to what drives you and encourages you to take action. Please rate how accurately each statement describes you.

	Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neutral 4	Somewhat agree 5	Agree 6	Strongly agree 7
Often I am motivated to act by patriotism.	○	○	○	○	○	○	○
Often I am motivated to act by money.	○	○	○	○	○	○	○

	Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neutral 4	Somewhat agree 5	Agree 6	Strongly agree 7
Often my actions are motivated by curiosity.	○	○	○	○	○	○	○
Often my actions are motivated by revenge.	○	○	○	○	○	○	○
Often my actions are motivated by political or social causes.	○	○	○	○	○	○	○
Often I do things because they are exciting.	○	○	○	○	○	○	○
Often I do things simply because I am able.	○	○	○	○	○	○	○
Often I am motivated by a chance to learn and grow my skills.	○	○	○	○	○	○	○
Often I do things because they are fun.	○	○	○	○	○	○	○
Often I do things to show others what I am capable of and gain respect.	○	○	○	○	○	○	○

VII. Reflecting on yourself and who you are, please consider each statement and rate how accurately it describes you.

	Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neutral 4	Somewhat agree 5	Agree 6	Strongly agree 7
I consider myself a hacker.	○	○	○	○	○	○	○

	Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neutral 4	Somewhat agree 5	Agree 6	Strongly agree 7

I think of myself as an ethical person.	○	○	○	○	○	○	○
Proving to people how skilled I am with computers and technology is important.	○	○	○	○	○	○	○
Contributing to a cause is a key part of who I am.	○	○	○	○	○	○	○
I think of myself as someone outside of mainstream society.	○	○	○	○	○	○	○
I am not the type of person who would do something illegal.	○	○	○	○	○	○	○
I am not the type of person to worry about whether or not something is legal.	○	○	○	○	○	○	○
I am the type of person who would go to extremes to further a cause I believe in.	○	○	○	○	○	○	○
I am the type of person who uses computers and technology to solve or prevent problems.	○	○	○	○	○	○	○
Hacking is an important part of who I am.	○	○	○	○	○	○	○
I consider myself an IT professional.	○	○	○	○	○	○	○
Being knowledgeable about and skilled in using technology and computers is an important part of who I am.	○	○	○	○	○	○	○
I believe there are times when it is necessary to break the law.	○	○	○	○	○	○	○
Using computers and technology to make positive change is a priority for me.	○	○	○	○	○	○	○