MOTIVATION AND DEMOTIVATION OF HACKERS IN THE SELECTION OF A HACKING TASK – A CONTEXTUAL APPROACH

MOTIVATION AND DEMOTIVATION OF HACKERS IN THE SELECTION OF A HACKING TASK – A CONTEXTUAL APPROACH

By KENNETH DAUNE OWEN, BA, MMGT

A Thesis Submitted to the School of Graduate Studies in Partial Fulfilment of the Requirements for the Degree PhD in Business Administration

McMaster University © Copyright by Kenneth Daune Owen, March 2016

PhD in Business Administration (2016) Information Systems
McMaster University, Hamilton, Ontario

TITLE: Motivation and Demotivation of Hacker Activities – A Contextual Approach

AUTHOR: Kenneth Daune Owen, B.A. Geography (Lakehead University), M.M.G.T. Master of Management (Lakehead University)

SUPERVISOR: Dr. Milena Head

NUMBER OF PAGES: viii, 155

Abstract

This research explores hacker motivation, demotivation and task selection through the lenses of the Theory of Reasoned Action (TRA) and General Deterrence Theory (GDT). The research also explores how context surrounding individual and task characteristics affects a hacker's decision making process in selecting a hacking task. To build a solid foundation on which to understand and combat threats to information systems, researchers need to look past the technical issues of data security and explore why hackers do what they do. This research addresses this gap by understanding why hackers identify and assess hacking tasks. It is hoped that by investigating the motivations of these highly skilled Information Systems (IS) users, new insights into how to avoid becoming a hacker target might be developed.

Participants in this study were individuals who self-identify as hackers. They completed a survey to validate the proposed model and answered open-ended questions to provide further insights. The quantitative data was analysed using Structured Equation Modelling; classical content analysis was conducted to examine the qualitative data.

This research was successful in identifying the role of TRA and GDT in hacker task selection. The research confirmed the importance of mastery, curiosity, and task complexity in a hacker's evaluation process and provided enticing clues for further research into the role of task complexity in a hacker's task evaluation process. The research also confirmed that subjective norms play an important part in shaping behavioural intentions towards engaging in a hacking task. Additionally, a clear linkage was identified between perceived certainty of sanction and behavioural intention.

Contributions of this research to both academia and practice are outlined as well as potential limitations and areas for future research.

Table of Contents

Chapter 1: Introduction 1
Chapter 2: Theoretical Background 12
2.1 The Theory of Reasoned Action 12
2.2 Deterrence Theory 18
2.3 Integrating TRA and GDT 20
2.4 Context of Use 21
2.4.1 Individual Characteristics 24
2.4.2 Task Characteristics 26
2.4.3 Situational Characteristics 26
Chapter 3: Proposed Research Model and Hypothesis 28
3.1 Behavioural Intention 29
3.2 Contextual Considerations 31
3.2.1 Individual Characteristics 32
3.2.2 Task Characteristics 33
Chapter 4: Research Methodology 35
4.1 Procedure and Participant Recruitment 35
4.2 Research Stages 37
4.2.1 Pretest and Pilot Study 37
4.2.2 Main Study 38
4.3 Measurement Instrument 43
4.4 Model Validation 45
Chapter 5: Data Analysis and Results 49
5.1 Data Collection 49
5.2 Data Screening 50
5.2.1 Outliers and Missing Values 50
5.2.2 Multivariate Statistical Assumptions 51
5.3 Research model validation 53
5.3.1 Measurement model 54
5.3.2 Collinearity 60
5.3.3 Common method bias 61
5.3.4 Structural model 62

5.4 Post hoc analysis 66
5.5 Qualitative Analysis 67
5.5.1 Method 67
5.6 Findings 69
5.6.1 Question One: “What is it about hacking that you enjoy?” 69
5.6.2 Question 2: Outline some of the personality or character traits of a good hacker 73
5.6.3 Question 3: What would make a hack less desirable to you? 77
Chapter 6: Discussion and Conclusion 84
6.1 Summary of Findings 84
6.2 Contribution to Theory 90
6.3 Contributions to Practice 91
6.4 Limitations 93
6.5 Future Research 94
6.6 Conclusion 95
References 97
Appendix A: MREB Clearance Certificate 105
Appendix B: Letter of Consent to Group Organizer 106
Appendix C: Original Survey Questions with Consent 107
Appendix D: Modified Survey Questions with Consent 121
Appendix E: QQ Plots 138
Appendix F: Histograms 144
Appendix G: Scatter Plots 152

List of Figures

Figure 2.1: Theory of Reasoned Action (Madden et al., 1992) 15
Figure 2.2: Deterrence Theory adapted from D'Arcy, Hovav & Gallett (2009)..... 19
Figure 2.3: Integrating TRA and GDT 21
Figure 3.1: Integrated model for behavioural intention to engage in a hacking task..... 28
Figure 5.1: PLS Model Results..... 63
Figure 5.2: Codes for Question 1..... 70
Figure 5.3: Question 1 - Sub Codes for Personal Development..... 71
Figure 5.4: Codes for Question 2..... 74
Figure 5.5: Question 3 - Level One Codes 78
Figure 5.6: Questions 3 - Codes for Level 2 – Motivation (71% of Level 1)..... 79
Figure 5.7: Question 3 - Codes for Level 2 - External Constraint (22% of Level 1) 81
Figure 5.8: Questions 3 – Codes for Level 2 – Moral (7% of Level 1)..... 82

List of Tables

Table 4.1 Construct items used in the quantitative survey 43
Table 4.2: PLS Measurement Model Test Criteria for Reflective Constructs 46
Table 4.3: PLS Structural Model Test Criteria 47
Table 4.4: Collinearity Criteria 48
Table 4.5: Common Method Bias Criteria 48
Table 5.1: Jarque-Bera and robust Jarque-Bera tests normalcy tests 52
Table 5.2 Item Reliability Assessment 55
Table 5.3 Assessment of Construct Reliability 58
Table 5.4: Loadings and Crossloadings[1] 59
Table 5.5 Collinearity 60
Table 5.6: Summary of hypotheses results 64
Table 5.7 Results of the f^2 examination 65
Table 5.8 Krippendorf's Agreement Coefficient 69

Chapter 1: Introduction

Businesses lose billions of dollars every year because of the acts of computer criminals. Damages occur through a broad spectrum of incursions ranging from the covert theft of credit card information to the very public and overt defacement of corporate websites. Modern media is rife with stories of hackers both good and bad. Hackers are seen as stealing people's identities, defacing public websites and causing all kinds of computer mischief. A 2011 report by the Fiscal Times estimates that hackers cost the world economy more than 114 billion dollars annually (Serrano, 2011). More recently, McAfee researchers estimated the cost of cybercrimes to the global economy in 2013 to be as much as $575 billion (Intel Security, 2014). In 2010, Sony Corporation posted a 170 million dollar loss due to the actions of hackers interacting with their game system network (Yamaguchi, 2011). Citigroup reported losses of 2.7 million when hackers infiltrated their banking network (Naraine, 2011). In 2015, the adult lifestyle website "Ashley Madison" was hacked and its membership database was leaked to numerous websites (Hackett, 2015).

Hackers have also been at the center of some positive social projects. For example, the Raspberry Pi Foundation is a charity that turns its profits back into educational programs and developing new products. The Raspberry Pi has opened up opportunities for social good, such as computer training for girls in Afghanistan and children throughout Africa (Raspberry Pi Foundation, 2015b). The foundation offers this quote to explain their vision:

"*We don't claim to have all the answers. We don't think that the Raspberry*

> *Pi is a fix to all of the world's computing issues; we do believe that we can be a catalyst. We want to see affordable, programmable computers everywhere. We want to break the paradigm where without spending hundreds of pounds on a PC, families can't use the internet. We want owning a truly personal computer to be normal for children, and we're looking forward to what the future has in store.*"
>
> (Raspberry Pi Foundation, 2015a)

This foundation was developed by a group of technologically skilled individuals that saw an opportunity to contribute to their community. They used off-the-shelf technology and repurposed it to create credit card sized single board computers. This hack has now sold over 5 million copies making it the fastest selling microcomputer in the United Kingdom (Upton, 2015).

The Anonymous hacking movement is another example of hackers using their skills for a social purpose. They have been associated with campaigns targeting and/or identifying paedophiles, police brutality, Islamophobia, the KKK, the Charlie Hebdo shootings, Canadian Bill C-51 and the Church of Scientology (Wikipedia Contributors, 2016).

During the summer of 2015, Wired magazine published an article detailing the exploits of two hackers they hired to test the security of an Internet connected car. The hackers were able to manipulate several systems in the car including those responsible for the environment, windshield wipers, entertainment, and eventually the transmission and

breaks (Greenberg, 2015). The exercise was conducted in an attempt to explore the potential for new risks to personal and information security as once isolated cars were now becoming connected to a global data network. Following this exposure, in January of 2016, General Motors announced a partnership with HackerOne.com to identify bugs or vulnerabilities in their vehicles (Help Net Security, 2016). Hackerone.com is a portal service that acts as a mediator between hackers and product manufacturers to create a safe and open way for hackers to share and be rewarded for the vulnerabilities they find in commercial products.

Government agencies have also realized the potential of tapping into the hacker culture to better understand their vulnerabilities. For example, in 2011, NASA used ethical hackers to perform a comprehensive test of their network security. This led to 13 successful breaches (Conrad, 2012). These tests are more comprehensive than simple or automated vulnerability scans. Vulnerability scans can lead to many false positives and only provide a shallow understanding of the issues that might be of concern. However, the penetration test with hackers takes the vulnerability scan one step further and acts on found exploits to see what consequences might be had if the vulnerability is left unchecked (Conrad, 2012).

There is no doubt that hacking is an important issue for IS practitioners and thus should be an important issue for IS researchers. To build a solid foundation on which to understand threats and exploit opportunities, researchers need to look past the technical issues of data security and they need to explore why hackers do what they do. To date, very little rigorous research has been conducted to understand hacker motivations. This

research intends to develop an understanding of how hackers identify and assess hacking tasks. Whether seen as a positive force or a negative force, there is one thing that can be said for all hackers; their solution is to "break the rules" (Nikitina, 2012, p.134). While the media sometimes portrays hackers as cloistered evil geniuses with intentions of throwing the world into chaos, the reality is that hackers do plenty of good. They are innovators and novel thinkers. Hence, by exploring their motivations, academia and industry have much to gain.

The definition of a hacker used in this research is quite different than what one might expect based on popular media. Two complementary definitions of the term hacker include: "The true hacker can't just sit around all night; he must pursue some hobby with dedication and flair" (Harvey, 1985); as well as, "A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular." (Malkin & Parker, 1993, p.1). This definition comes from RFC 1392, "A Glossary of Internet Terms". RFCs are authoritative documents used to define the open standards that are used to operate the Internet. While some RFCs are completely technical in nature, others offer standardized glossaries.

Also included in RFC 1392, is a second salient definition, "A cracker is an individual who attempts to access computer systems without authorization. These individuals are often malicious, as opposed to hackers, and have many means at their disposal for breaking into a system." (Malkin & Parker, 1993, p.1). Contemporary definitions of hacker culture have absorbed the concept of the cracker as a subset of the hacker community. Certain distinctions as to the ethics of a hacker's/cracker's intentions

have been conceptualized via the colour of "hat" these individuals metaphorically wear. Contemporary hacker definitions present three ranges of hackers along an ethical continuum: White Hat, Grey Hat, and Black Hat (Bansal & Arora, 2012; Schumacher, n.d.). The term "White Hat" is meant to portray that the hacker only partakes in hacks that are ethical, while Black Hat hacker's works are characterized by a predacious and malevolent application of his or her skills. The Grey Hat hacker term is then used to pad this dichotomous view of hacker intentions and is essentially used to create a neutral space between the Black and the White. (Bansal & Arora, 2012; Schumacher, n.d.). The greatest concern for IS practitioners is the safety of their data, and as such, practitioners generally will focus on hacking activities that have negative consequences. The media labels these activities as "Black Hat". In a modern youthful digital culture hackers make complex social contributions. Hackers in many ways are like mythological trickster gods whose actions and social roles evolve and defy definition (Nikitina, 2012). The concept of categorizing hackers using hats to define the ethical impacts of their actions, while popularly used, is actually a distraction from the core issues surrounding what motivates a hacker to do the things he or she does. Mahmood, Siponen, Straub, Rao, & Raghu, (2010) make the argument that from a research perspective all hackers should be viewed the same, whereby the focus should be on their motivations and behaviour rather than the 'hats' they metaphorically wear. This is the view we adopt in the current research.

The key to understanding hackers does not lie in the ethics of their actions but rather in the aesthetics. "Hacking can involve the heartfelt conviction that beauty can be found in computers, that the fine aesthetic in a perfect program can liberate the mind and

spirit." (Sterling, 1994, p. 127). A hacker is someone who pursues his or her computer skills as a hobby and for fun, not necessarily out of a sense of duty or in the pursuit of money (Harvey, 1985). Sören Kierkegaard (1813-1855) posited that people live in the moment, they are moved by the artistry in their lives and not all actions follow ethical principles. Kierkegaard's idea of an aesthetic life superseding the motivation of living an ethical life is an important foundation to the understanding of the "Hacker Manifesto". The Hacker Manifesto was a short piece written in 1986 by a hacker named "The Mentor". The Hacker Manifesto outlines a number of key cultural affectations:

> *"...We seek after knowledge... We exist without skin color, without nationality, without religious bias... and you call us criminals.... Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.*" (The Mentor, 1986, p.1).

Kierkegaard's writing suggests that a hacker may choose a hack that may fail a certain ethical test but will still be compelled to attempt it based on its aesthetic value. Like an evaluation of a piece of art for its aesthetic value, a hacker seeks to ensure their endeavours hold some aesthetic merit. For a hacker, a hack is not valuable if it is not unique, original and complete (Jordan & Taylor, 1998; Turkle, 1984).

While the hat metaphor is the most common, there have been other attempts to construct a taxonomy for categorizing hackers using motivation of hackers and their argued skill levels (Raid & Pedersen, 2012; Rogers, 2006). The Rogers Hacker

Circumplex taxonomy (Rogers 2006) views motivation as a fixed component in the definition of the type of hacker being labelled. According to Rogers (2006), hackers are motivated either by, revenge, financial gain, curiosity or notoriety. They further define hackers by introducing skill as a variable for distinguishing between the definitions in their taxonomy. This approach illustrates the limitations of using nominal measures for classifying the fluid behaviours of hackers. For example, it seems artificially limiting that a "Cyber-punk" as describe in the Rogers taxonomy is only motivated by notoriety (Rogers, 2006). This would suggest that any one hacker is only interested in one outcome from their activities. If they focus on computer networks then social media will never interest them. This assertion seems implausible.

In another attempt to develop a taxonomy for hackers, the circumplex method proposed by Rogers (2006) was enhanced by adding additional categories and suggesting proximity to boundaries in their model indicated a blended motivation. This was to address, "the multifaceted nature of cyber malfeasance, including the rise in socially and ideologically motivated hacking..." (Seebruck, 2015, p.36). In Seebruck's (2015) article, he proposes that the value of his typology is that "classifying phenomena has many purposes that can benefit administrators of critical infrastructures like computer networks that are at risk of being attacked" (Seebruck, 2015, p.37). However, while his paper indicates that segments of the circular model are placed adjacent to one another, no explanation of the interconnectedness is given.

The work of Rogers (2006), Raid & Pederson (2012) and Seebruck (2015) demonstrate that while some efforts have been made to define what hackers are and how

they are motivated, these attempts have met only limited success as they lack testable scientific hypotheses and reference no primary data. The evolution of this approach shows that a need to move from ridged descriptors to more fluid and nuanced multidimensional classifications would be valuable. Hackers are not simple single-minded individuals. Such conceptualizations limit the diversity of the factors influencing a hacker's curiosity and other intrinsic drivers.

While the hacker cultural phenomenon in the computer world is not particularly new, it has seen limited quantitative and vigorous investigation. Hackers are often described as secretive, untrusting, using code names and shunning attention from people outside their close-knit communities (Voiskounsky & Smyslova, 2003; Rogers, n.d.). Much of the research into hacker motivation has used psychological and sociological theories of crime, and has focused on the criminal activities of a subset of the hacker culture. For example, Décary-Hétu, D. & Dupont, B. (2012) used Social Network Analysis (SNA) to explore the relationships between a group of cyber criminals using Internet Relay Chat to interact and operate their crime organization. In their paper, the authors make it clear that research into motivation has not received the same attention as technical developments.

As previously outlined a hacker "...delights in having an intimate understanding of the internal workings of a system..." (Malkin & Parker, 1993, p.1). Using this definition one can find that Free/Open Source software (F/OSS) developers can also be defined as part of the hacker community (Lakhani & Wolf, 2005). Those involved in F/OSS voluntarily develop valuable software, and freely share readily marketable skills.

They seem to be motivated less by commercial opportunities then by altruistic ones (Lakhani & Wolf, 2005). In the F/OSS group, it was found that enjoyment-based intrinsic motivation was a key element in motivation (Lakhani & Wolf, 2005). Furthermore, intellectual challenge and skill development were cited as important factors in creating engagement in a F/OSS project (Lakhani & Wolf, 2005). Participants who contribute to a F/OSS project often benefit from an intrinsic motivation caused by a sense of being fully involved in their work. This autotelic experience is referred to as flow (Nakamura, Jeanne, & Csikszentmihalyi, 2002). It is important to recognize that while F/OSS coders may be doing similar work in their occupation, they do not have as much choice in their task selection in their professional career. This freedom to choose leads to better matching of skills to challenges, which is a requirement for a good flow experience (Lakhani & Wolf, 2005). Malkin & Parker's (1993), Lakhani & Wolf's (2005) and Nakamura, Jeanne, & Csikszentmihalyi's (2002) work illustrates the importance of autotelic experiences, such as art and play, in a hacker's motivation. "Intrinsic motivation is the tendency to engage in tasks for their own sake because; one finds these tasks interesting or challenging. (Voiskounsky & Smyslova, 2003) The idea that F/OSS activities are autotelic and are done as an end on to itself shows the importance of intrinsic motivation to the hacker mindset.

This investigation proposes that hackers engage in their activities as a result of two forces working in opposition to one another. On the one hand, hackers experience a number of intrinsic and extrinsic motivations that drive them to pursue their hacking task. On the other hand, there is another set of countervailing forces that limit and mediate the

risks a hacker might expose him or herself to by engaging in a hack. These countervailing forces are seen as a hacker's perception of the likelihood he or she would be caught and the severity of any sanctions that may result. The goal of this research is to explore the interplay between the factors that both incite hacking behaviour and suppress it. Additionally this research seeks to understand the contextual factors (e.g., individual and task characteristics) that influence a hacker's attitude and aversion to a specific hacking task. Task characteristics are considered extrinsic contextual factors, which include the type of hacking task being considered as well as the complexity of the task. Thus, two research questions were established:

1. How is the intention of hackers to engage in a hacking task (hack) influenced by motivating and demotivating factors.
2. How may contextual factors of individual and task characteristics influence a hacker's attitude toward engaging in a hacking task.

Information security researchers struggle to develop a clear understanding of the motivations of so called "hackers". The goal of developing a clear accurate picture of the motivations for this seemingly aggressive, cloistered and untrusting subculture is fraught with many practical, ethical, and theoretical challenges (Mahmood et al., 2010). This research intends to develop insight into how hackers select their hacking tasks. First this research looks at motivation towards carrying out a hacking task using the Theory of Reasoned Action as a theoretical lens. Then it explores the factors that discourage the pursuit of a given hacking task through a General Deterrence Theory lens. Last, the research develops and validates a unified model to predict the desirability of pursuing a

specific hacking task.

Chapter 2: Theoretical Background

The purpose of this research is to develop an understanding of what motivates hackers to attempt a hacking task. This research views the intention to hack as a synthesis of attraction and detraction factors that combine to create a net intention from which a hacker acts. The foundation of this research is grounded in two well-established behavioural theories frequently used in IS research. The first theory, the Theory of Reasoned Action (TRA), describes adoption behaviour, i.e., what motivates a particular behaviour. The second theory, the General Deterrence Theory (GDT), presents a countervailing avoidance behavioural framework, i.e., what discourages a particular behaviour.

2.1 The Theory of Reasoned Action

The Theory of Reasoned Action (TRA) has been extensively used to study the relationship between attitudes and behaviours and where choices are of, "... appreciable personal or social significance" (Ajzen & Madden, 1986, p.454). The goal of this research is, in part, to explore the factors that entice an individual hacker to be interested in carrying out a specific task (hacking). TRA is very well suited to this objective. TRA posits that a person's Behavioural Intention (BI) is the immediate antecedent of behaviour (Madden, Ellen, & Ajzen, 1992). TRA further posits that BI can be considered a function of a person's behavioural beliefs and his or her normative beliefs. Behavioural believes are those believes that form an individual's attitudes towards a given action, while normative beliefs describe a person's perception of subjective norms (Ajzen & Madden, 1986). BI is defined as "the degree to which a person has formulated conscious

plans to perform or not perform some specified future behavior" (Warshaw & Davis, 1985, p.214). Within the IS domain, there are several theories and models that use BI as their endogenous variable of interest. Examples include the Theory of Reasoned Action (Fishbein, 1975), the Theory of Planned Behaviour (Ajzen, 1991), the Technology Acceptance Model (Davis, 1986), and the Unified Theory of Acceptance and Use of Technology (Venkatesh, Morris, Davis, & Davis, 2003). Attitude towards the specified behaviour is one construct that is seen to be informing BI. Attitude is a function of belief. In other words, if a person sees that an action leads to a favourable outcome, he or she will develop a positive attitude toward that action and other actions like it (Ajzen & Fishbein, 1980). Attitude is "...a learned predisposition to respond to an object in a consistently favorable or unfavorable manner" (Fishbein, 1975, p.41). As such, attitude evolves over time based on an accumulation of experiences.

TRA also uses subjective norm to capture a person's perception of how people who are important to them think they should or should not perform a specific behaviour (Fishbein, 1975; Venkatesh, 2012). Subjective Norm (SN) "... refers to the perceived social pressure to perform or not to perform the behavior." (Ajzen & Madden, 1986, p.43). SNs reflect the social environment (Ajzen & Fishbein, 1980) surrounding an individual's intentions and beliefs. In TRA, subjective norms differ from other sociological norms. Sociological norms are based on community expectations (Terry, Hogg, & White, 1999). In TRA, the focus is on what an individual believes influential others would expect of them (Ajzen & Fishbein, 1980). This means that what one person believes to be the expectations of others might not be an accurate reflection of what that

other person might actually believe. The distinction is important because other sociological norms are more clearly delineated and represent clear external pressure, while subjective norms represent an internal force that is specific to beliefs held by a person. Ajzen & Fishbein (1980) argue that subjective norms are also related to intention by means of two sub questions or elements within the construct. The first element addresses the question; would influential person X believe some action has value or merit? Secondly, would that influential person X want an individual to act on this belief or intention? These two elements can then be said to impact a behaviour in terms of action, target, context and time.

Hackers have been shown to develop their interests through the reinforcement and feedback of other hackers (McHugh & Deek, 2005). Subjective norm is used to capture a hackers perception of how people who are important to them think they should or should not perform a specific behaviour (Fishbein, 1975; Venkatesh, 2012). Social norms reflect the social environment (Ajzen & Fishbein, 1980) surrounding an individual's intentions and beliefs. In F/OSS projects, "we see a strong sense of community identification and adherence to norms of behavior. Participants in the F/OSS movement exhibit strong collective identities." (Lakhani & Wolf, 2005, p.5). As a result of this adherence to community values and a collective identity, socialized norms are established as part of the framework to identify a community participant. The resulting framework then becomes an additional motivator for hackers (Lindenberg, 2001). So, as a hacker becomes aware of a community and starts to act as the community's norms dictate, the hacker will become more satisfied with the experience of the community and will further

act to align with those norms.

Figure 2.1 illustrates the components of the TRA and its relationships between attitude toward behaviour, subjective norms and how they influence BI. The theory also posits that BI helps to predict action. However, while attitude influences intention, it cannot be said to directly influence action (Ajzen & Fishbein, 1980) but rather it is mediated through BI.

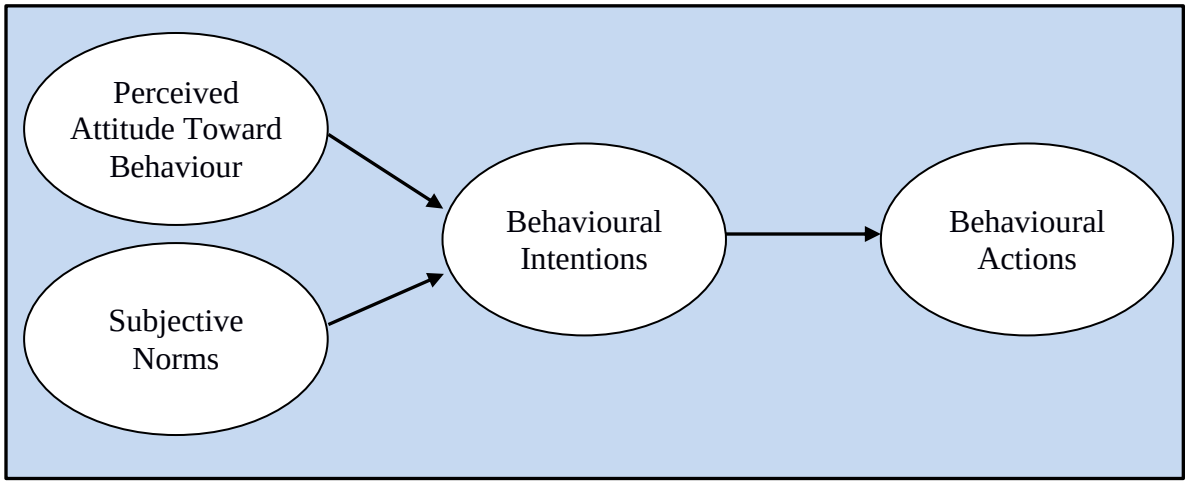


Figure 2.1: Theory of Reasoned Action (Madden et al., 1992)

Models that have stemmed from the TRA have operationalized such beliefs but have tended to focus on perceived benefits rather than perceived risks/concerns (Cazier, Medlin, & Wilson, 2007). For example, the Technology Acceptance Model (TAM), arguably the most dominant acceptance model of the past two decades of information systems research (which stemmed from the TRA), emphasizes utilitarian benefits such as perceived usefulness and perceived ease of use. While originally developed for mandatory organizational contexts, many authors have augmented or altered TAM to fit

various contexts. Through this augmentation and further development, TAM has been expanded to include the impacts of various hedonic perceptions, such as enjoyment (for example, Van der Heijden, Verhagen, & Creemers, 2003; Venkatesh, Brown, & Lee, 2001). However, the utilitarian and hedonic constructs examined to impact technology acceptance tend to focus on perceived benefits rather than perceived concerns.

There can be no denying the importance of perceived benefits, be they utilitarian or hedonic. However, when examining technology acceptance, the influence of perceived concerns cannot be overlooked (Kulviwat, Bruner, Kumar, Nasco, & Clark, 2007; Mick & Fournier, 1998). Relatively few adoption or acceptance models have explored both positive utility (benefits) and negative utility (concerns). Cazier, Medlin, & Wilson (2008) stress the significant and innovative contribution of examining both positive and negative utility for technology acceptance.

Increasingly, researchers are recognizing that the inclusion of negative utility factors in technology acceptance models can provide a more realistic and complete perspective (for example: Cazier et al., 2007, 2008). TRA specifically limits its scope to actions where the actor has volitional control (Madden et al., 1992). However, non-volitional factors have also been seen to influence decisions as in the case of the Theory of Planned Behaviour (TPB). TRA cannot contribute to understanding why a person selects to purchase a specific food item off a menu if that person is constrained by a limited cash reserve. TPB however, does address this constraint as it includes the additional construct of Perceived Behavioural Control. The Perceived Behavioural Control construct expresses motivational implications that items external to a person's

locus of control will have on behavioural intentions and the subsequent behaviour (Madden et al., 1992). This perceived behavioural control is different from a perceived locus of control, which is a stable character trait (Ajzen, 1991). A person with a strong internal locus of control sees themselves as being able to determine their own fate. However perceived behavioural control is contextual and varies from situation to situation. This means that a person who has a strong internal locus of control may simultaneously perceive their behavioural control as being low or high, given the context.

As an illustrative example, consider the case where a hacker has been experimenting with kiosk software in his or her home and has found a vulnerability. The hacker perceives a high degree of control over his or her locus of control. That is to say the hacker is confident the exploit is feasible. The hacker notices a kiosk that uses the same software at a local mall and decides that testing the exploit on a "live subject" would be an attractive proposition. The hacker then goes to the mall and upon approaching the kiosk notices an out of order sign on the kiosk. In this example the hacker maintains his or her intention as his or her locus of control is stable with the belief his or her skills are appropriate. However the hacker's control beliefs are significantly affected by a non-volitional condition, in this example, the out of order sign. This makes the concept of perceived behavioural control reflect a person's belief in how well they can perform to cope with a specific situation (Ajzen, 1991). TPB establishes the appropriateness of extending TRA to include non-volitional factors in effecting behaviour; however it does not have the granularity needed to explore the effects of socially constructed deterrents such as criminal law, corporate policies, etc. In this

research, the components of a non-volitional factor are also of interest, but need to be viewed through a research lens that will include social policies as deterrents. Some form of deterrence theory is needed to understand the demotivational contributions outside influences may have.

2.2 Deterrence Theory

In its simplest form, the knowledge of consequences will affect choices in such a way as to avoid infractions (Gibbs, 1986). Deterrence theories function "... when a potential offender refrains from or curtails criminal activity because he or she perceives some threat of a legal punishment for contrary behaviour and fears that punishment" (Gibbs, 1986, p.87). General deterrence theory is one of the most widely used criminology theories found in the IS research field (Young & Zhang, 2007). GDT has been used to explore both internal IS misuse and external IS misuse (D'Arcy, Hovav, & Galletta, 2009; Straub & Weike, 2008; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005; Young & Zhang, 2007). The effectiveness of deterrence theory relies on the perception of the certainty and severity of punishment given a planned action. For the sake of this research, we are going to assume that what is typically described in research literature as criminal activity will now encompass any undesirable behaviour that risks sanction from an authoritative body. For example, a "criminal activity" in context of a learning institution might include unauthorized access to student records in a computer system. The punishment being risked might include expulsion.

The presence of a deterrence stimulant in an environment can result in either restrictive or absolute deterrence. In the case of absolute deterrence a person is

completely dissuaded from a criminal act each time he or she contemplates carrying out an act. With restrictive deterrence, it is possible that a person is deterred only so far as to restrict the degree of criminal acts. For example a person may knowingly exceed the speed limit in an automobile but restricts the behaviour to five kilometers above the speed limit (Gibbs, 1975, 1986). In this way, he or she has committed an offence but have acted in some way to limit the risk of sanction he or she is exposed to. In the context of IS, General Deterrence Theory posits that the perceived certainty of detection and the severity of the consequence for a given action form one's perception of the perceived risk of that action, which in turn influences the behavioural intention to perform that action (D'Arcy, Hovav, & Galletta, 2009). Figure 2 illustrates the relationships between the key concepts of GDT. GDT does assume that criminals, or in this case hackers, are rational and are utility maximizers (Schulze, 2003).

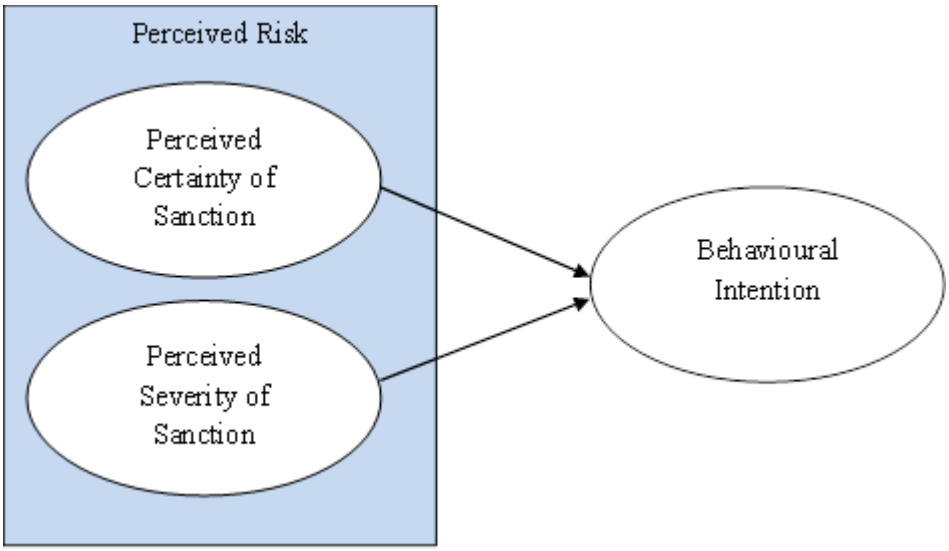


Figure 2.2: Deterrence Theory adapted from D'Arcy, Hovav & Gallett (2009)

2.3 Integrating TRA and GDT

Thus far the theoretical discussion of hacker motivation has exclusively looked at well-situated motivation theories that are used in their natural form without extension. However, as shown in the development of the TPB (Madden et al., 1992) and the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003), it is sometimes both necessary and desirable to combine theories and to extend them with new constructs. As previously discussed, to understand hacker motivation, both the attractor elements and the detractor elements need to be considered together. In this research, the attraction elements originate in TRA whereas GDT provides the appropriate constructs to evaluate the detractor elements. This integration of TRA and GDT is illustrated in Figure 2.3.

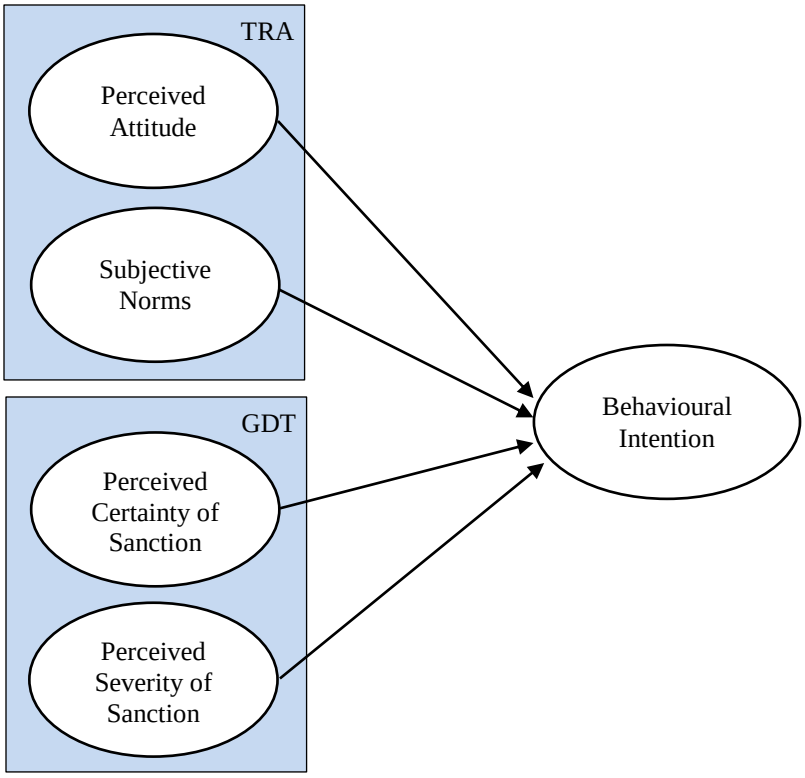


Figure 2.3: Integrating TRA and GDT

2.4 Context of Use

While combining TRA and GDT is expected to give insight into the motivation/demotivation process for hackers, it is of value to consider the unique contextual characteristics (e.g., individual and task characteristics) that may influence this process (Hong, Chan, Thong, Chasalow, & Dhillon, 2014). The development of context specific theory is important in IS research (Brown, Dennis, & Venkatesh, 2010). When a model is focused on the specific contextual constraints of a given IS artifact, it will have more explanatory power than a theory meant to explain the same phenomenon over a broader spectrum of technologies (Brown et al., 2010). In the case of hackers, context may influence how they perceive any motivators and demotivators (Hong et al., 2014).

For example, Brown et al identify four categories of contextual factors that can be used as antecedents, i) technology characteristics, ii) individual or group characteristics, iii) task characteristics, and iv) situational characteristics (Brown et al., 2010). While Whetten (2009) describes context as "the set of factors surrounding a phenomenon that exert some direct or indirect influence on it" (p. 31), Rousseau and Fried (2001) posit that "contextualization entails linking observations to a set of relevant facts, events, or points of view that make possible research and theory than form part of a larger whole" (p. 1). Without context, an important part of the hacker story cannot be told and a hacker's interactions with a given situation cannot be understood (Johns 2006). This will lead to findings that are incomplete or possibly inconclusive (Whetten, 2009). In response, this dissertation uses the "Single Context Theory Contextualization" approach outlined by Hong et al. (2014). This method allows for well-established theories such as TRA or GDT to act as a foundation on which constructs are added or removed. This is done by first separating core constructs from TRA and GDT, then combining them with relevant contextual factors as antecedents. Examples of these contextual factors include individual context, situational context and task context.

The word context comes from a Latin root that means "to knit together". By knitting ideas together, researchers apply a more focused research lens to a specific topic and, by doing so, create a clearer, more effective understanding of the phenomenon they are scrutinizing. "Contextualizing entails linking observations to a set of relevant facts, events, or points of view that make possible research and theory that form part of a larger whole" (Rousseau & Fried, 2001, p.4). Context can play many roles in shaping a

research investigation. It does so by clarifying both opportunities and constraints (Johns, 2006; Hong et al., 2014). It draws attention to the importance of specific situational features that "heightens our sensitivity to potential contextual impacts" (Johns, 2006, p.387). For example, the context would be different if comparing a specific task being undertaken in a lab setting rather than in a production environment. "A set of factors, when considered together, can sometimes yield a more interpretable and theoretically interesting pattern than any of the factors would show in isolation" (Rousseau & Fried, 2001, p.4). Context also allows a researcher to bundle stimuli together to allow for a clearer examination of interactions between discreet constructs that may not have been observable without a contextual filter being in place.

Brown et al., (2010) suggest there are four contextual factors that influence the intention to use certain types of collaboration technology. These broad contextual factors are: i) technology characteristics, ii) individual or group characteristics, iii) task characteristics, and iv) situational characteristics (Brown et al., 2010). In the case of exploring TRA and GDT and their impact on hacker intentions, the contextual factors of technology characteristics from the Brown et al. (2010) list that could be set aside. The volume of alternative tools identified in constraining technology characteristics left no meaningful limitation on this research. Therefore this research focuses on the intrinsic motivations of a hacker and not the choice of technology he or she uses. For example, evaluating a writer's choice of pen when trying to discern what drives that writer's topic selection is analogous to understanding why technology is not an important contextual concern in this research. When TRA and GDT are used as lenses, only the internal and

external pressures of an individual's motivations are what become important. Those motivations come from how the hacker perceives the hacking task in terms of social merit and risk, as well as the challenge it creates for the hacker. This leaves three of Brown et al. (2010) factors relevant to this course of research. First, there are the individual characteristics of the hacker that act as drivers to motivate them to attempt a hacking task. Second, there are the characteristics of the intended task itself. Last, there is the situational context that influences a hacker's actions based of the visibility of the intended hacking task.

2.4.1 Individual Characteristics

Attitude evolves over time and is based on the accumulation of experiences (Ajzen & Fishbein, 1980). A good hacking task always contains components of mastery over the intended target (Jordan & Taylor, 1998). From a hacker perspective, there are two individual characteristics or intrinsic drivers that seem to be consistently described in the extant literature: curiosity and mastery (Lakhani et al., 2002). Curiosity and intellectual challenges associated with mastery increase a hacker's sense of control and power (Lindenberg, 2001). They also build an association with other hackers, giving the individual a greater sense of belonging (McHugh & Deek, 2005).

Curiosity is regarded as a fundamental personality trait that is defined as "[implying] a high degree of receptivity and willingness to engage with novel stimuli."(Kashdan et al., 2009, p.988). Curiosity is described as one of the fundamental character traits studied by psychologists (Kashdan, 2004; Kashdan et al., 2009; Reiss, 2004). According to Kashdan (2004), "curiosity involves the active recognition, pursuit

and regulation of one's experience in response to challenging opportunities". While most researchers of intrinsic motivation associate curiosity with intellectual pleasure, this is not always the case (Kashdan et al., 2009; Reiss, 2004). Ultimately the acquisition of knowledge is the intended end result of curiosity (Reiss, 2004). For example, a student preparing a paper may not be interested in the topic but still requires curiosity to guide his or her knowledge collection and to find novel viewpoints. It is curiosity that drives hackers to try novel approaches to problems just to see how their knowledge of a situation changes. For example, it is curiosity that drives a hacker to vary data into a program and to monitor how the program responds. In the case of the 2014 Heart Bleed bug that compromised Open SSL, it is not difficult to imagine that a hacker might have read the specifications for Open SSL and asked out of curiosity "what would happen if I didn't follow the instructions" and "what if I feed Open SSL some bad data?" In the case of Open SSL, this curiosity led to compromising tens of thousands of web servers around the world.

Mastery is the second key personality trait associated with hackers (Jordan & Taylor, 1998). For hackers to be effective with their time, they need to know that the steps they take and the methods they use are appropriate and are reasonable to use given the goals they seek. This means that while curiosity answers the hacker's subconscious questions of "what" and "where", mastery answers the question of "how". By seeking to master a specific skill or technology hackers are improving the odds of knowing what tool to use and in what way.

2.4.2 Task Characteristics

Research has attempted to classify hackers and hacking tasks into various categories based on technology, exploits, intention, social relevance, skill, etc. (Jordan, 2009; Lakhani & Wolf, 2005). The "task-qua-task" or task-as-a-task approach allows for actual aspects of the task to be considered by strictly looking at the instance of a given task (Zigurs & Buckland, 1998). This task-qua-task strategy is ideal when studying hacker motivation because hackers have vast and varying skill sets. What is difficult for one hacker might be simple for another. Under the task-qua-task approach, task characteristics such as complexity can be explored and used as a baseline to compare hackers' interests and challenges.

Through the task-qua-task lens, Zigurs & Buckland, (1998) and Cambell (1988) view task complexity as an important feature in the understanding of a task. Cambell (1988) proposes that a task is complex if it has multiple paths to a desired end state, the presence of multiple outcomes, the presence of conflicting interdependence between paths and outcomes, and the presence of uncertain probabilistic links among the pathways and the outcomes.

2.4.3 Situational Characteristics

Situational characteristics represent the social environment around a hacker. It describes the peer and organizational pressures the hacker perceives from his or her social environment (Brown et al., 2010). Situational context is therefore tantamount to subjective norms in the TRA model (Taylor & Todd, 1995). A subjective norm reflects what individuals believe the people they respect and include in their peer groups like to

see them do. So if a hacker believes that the people in his or her peer group were to think that he or she should carry out a specific action then that hacker is going to believe that he or she should do that action. Since situational characteristics are embodied in SN (as part of TRA), they are not included as separate contextual factors in this research.

Chapter 3: Proposed Research Model and Hypothesis

To better understand the behavioural intentions of a hacker in engaging in a specific hack, a model outlining the theoretical foundations for this research was developed and is shown in Figure 3.1. The constructs and hypotheses development of this model are described below. It is important to note that the relationships found in TRA and GDT are well understood and have been repeatedly validated across various contexts. Thus, only a selection of representative work is cited to support each relationship.

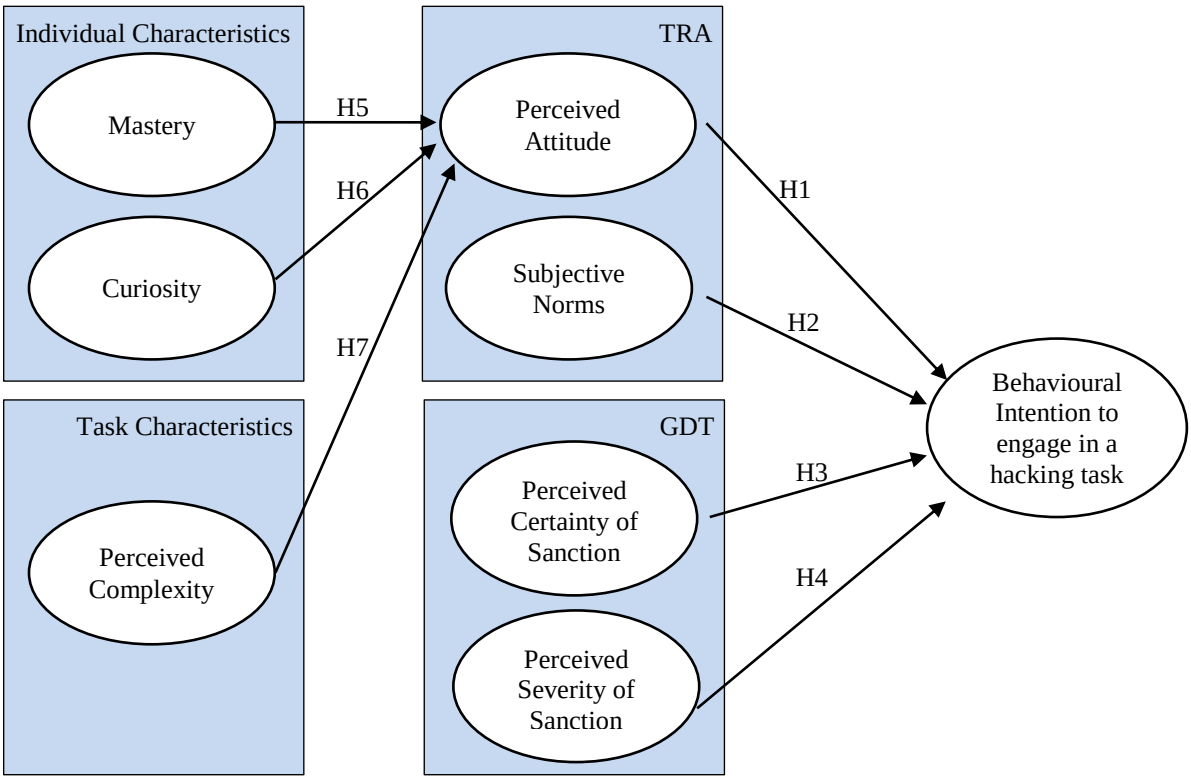


Figure 3.1: Integrated model for behavioural intention to engage in a hacking task

This model posits that Behavioural Intentions (BI) for a hacker are consistent with

the Theory of Reasoned Action (Ajzen & Fishbein, 1980) and General Deterrence Theory (Gibbs, 1975, 1986). Thus the model proposes that BI is informed both by motivating factors (attitude; social norms) and demotivating factors (risk assessment of the perceived certainty and severity of sanction for engaging in a hacking task). Furthermore, this model proposes that an individual's perceived attitudes are influenced by the context in which a task is being undertaken.

3.1 Behavioural Intention

Behavioural Intention (BI) has been well established through TRA as a direct antecedent of behaviour (Ajzen, Fishbein, & Wicker, 1973). In accordance with TRA research, BI has been demonstrated to be influenced by Perceived Attitude and Subjective Norms (Madden et al., 1992). Subjective Norms reflect how a person sees his or her relationship with their broader community. It holds the key to a hacker's collective identity (Lakhani et al., 2002; Lakhani & Wolf, 2005; Voiskounsky & Smyslova, 2003; Rogers, n.d.). From a GDT perspective, BI has also been shown to be influenced by perceived risk (operationalized as the assessment of perceived certainty and severity of sanction for performing an action) in a variety of contexts (D'Arcy et al., 2009). Based on the extant literature, we posit that a hacker's behavioural intention will increase if he or she has developed a positive attitude towards carrying out a given hack. The hacker's intention to carry out a hack will also increase if he or she were to believe that those people who make up his or her social network believe that he or she should carry out the intended hack.

Thus, it is hypothesized that

H1: *Perceived Attitude will have a positive impact on Behavioural Intention to engage in a hacking task.*

H2: *Subjective Norms will have a positive impact on Behavioural Intention to engage in a hacking task.*

While hackers' intention to engaging in a hacking task was hypothesized to increase based on a positive evaluation of their attitude and perceived social support for the hack, a third, external factor, would be acting as a deterrent to carrying out the hacking task. This third factor is perceived risk for engaging in the hacking task. As the hacker assesses the hacking task, his or her intention to do the hack will decrease as his or her perception of perceived risk increases. Perceived risk is the degree to which an individual believes that engaging in a specific action will result in an unfavourable outcome. General Deterrence Theory posits that the perceived certainty of detection and the severity of the consequences for a given action are the key elements in perceived risk and influence Behavioural Intention negatively (D'Arcy et al., 2009). It hypothesized that when a hacker assesses the degree of risk a specific hack carries with it, he or she would consider what he or she believes is the certainty of a sanction and how severe the sanction might be. The more likely the hacker perceives that his or her actions would result in a sanction, the more risk they will associate with the specific hack. Furthermore GDT hypothesizes that the severity of the sanction will also positively correlate with the perceived risk associated with the hacking task (D'Arcy & Herath, 2011). Imagine a hacker is interested in exploring the latest security flaw in a web server. He or she decides to build a server using his or her own equipment. As the activity is completely

contained to his or her own server, the hacker would perceive the risk of sanctions to be low. However if this same scenario were carried out with a slightly different context, for example the computer being tested on was a surplus machine at the hacker's place of employment, the hacker might expect that his or her actions would have a greater chance of being noticed by his or her supervisor who might verbally chastise the hacker for misusing his or her time. In this case, there is an elevation in both perceived likelihood of discovery and perceived severity of sanction. Now consider a third scenario where the hacker chooses to explore the latest security flaw in a web server associated with federal income tax processing. In this case, the hacker may believe that federal authorities would likely observe this activity and that if caught he or she would be incarcerated. To the hacker this might represent extreme risk motivating strong avoidance to conduct such a hacking task.

Thus, it is hypothesized that

H3: *Perceived Certainty of Sanction will have a negative impact on Behavioural Intention to engage in a hacking task.*

H4: *Perceived Severity of Sanction will have a negative impact on Behavioural Intention to engage in a hacking task.*

3.2 Contextual Considerations

As previously discussed, contextualization can help provide valuable research insights into specific domains of investigation. In the case of hackers, there were three relevant categories of context identified: individual characteristics; task characteristics; and situational characteristics. Subjective norms were identified as the situational

characteristic that influences the behaviour of hackers. Given that subjective norms are included within TRA and already hypothesized within the above discussion of behavioural intentions, here we focus on the contextual characteristics of the individual and the task.

3.2.1 Individual Characteristics

Hackers seek gratification through skill development and challenge (Lakhani & Wolf, 2005). Research shows that hackers have certain character traits that can influence their attitudes towards a hacking task. These character traits include curiosity (Holt, 2007) and mastery (Jordan & Taylor, 1998). What is the point of hacking a computer system? Why not just use it for the job it was intended for, and in the ways that are prescribed for that task? For some, this is a reasonable assertion. However for hackers, they derive their satisfaction by pushing the boundaries of expected use. For example, imagine a hacker is looking at a website that contains lists of valuable data that he or she was hoping to collect and use in his or her PhD dissertation. Unfortunately the data does not come formatted in a way that can be readily used. The hacker knows about a hacker craft called "screen scraping" where data is collected from a source and reformatted. The desire to advance one's skills by learning screen scrapping is an incentive to develop and master a new skill. This desire of mastery is argued to increase interests in hacker tasks that offer a challenge (Holt, Burruss, & Bossler, 2010).

Curiosity has been defined as the "degree of receptivity and willingness to engage with novel stimuli." (Kashdan et al., 2009, p.988). This is an essential trait for a hacker to possess. The hacker is driven by curiosity to want to explore and better understand

technology in the first place. This also holds true for hackers when considering the individual traits of mastery. Mastery gives the hacker the skills and confidence to try something new. Curiosity encourages reflection and identification of new sources of mastery. As Jordan & Taylor (1998) attest, if a hacker sees a task as a challenge, the hacker will be drawn to it to test and develop his or her skills. This means that when a hacker's sense of mastery and or curiosity is aroused, his or her attitude towards the hacking task will become positive and heightened.

Thus, it is hypothesized that

H5: *Need for Mastery will have a positive impact on Perceived Attitude towards engaging in a hacking task.*

H6: *Need for Curiosity will have a positive impact on Perceived Attitude towards engaging in a hacking task.*

3.2.2 Task Characteristics

The tasks that make up a hack have their own qualities. These qualities encompass the specific nature of a task and the perceptions of the person carrying out the task. The key task trait being explored in this research is the complexity of the task (Campbell, 1988; Zigurs & Buckland, 1998).

Task complexity refers to the number of inputs, outputs and internal interactions within a task (Zigurs & Buckland, 1998). For example, a simple task for a hacker might be to disable a network switch. To do this there is only one outcome and one type of input. A more complex task for a hacker would be to extract passwords from a database

on a remote server. This task may include dealing with attack vectors, web injections, buffer attacks, social engineering, and worms. The outcome being sought is equally complex in that it might be delivered locally to the server through a core dump or remotely through a SQL query or Web response. To further complicate this task, the intermediary steps and interactions that need to occur on the server may be abundant.

Task complexity can be a double-edged sword for a hacker. If the task is too complex, the hacker's attitude towards the hacking task may not be positive. This is the case since with increased task complexity, the hacker is more likely at risk of failure, and with the increased likelihood of failure, an individual is less likely to be motivated to attempt the task (de Vries, Dijkstra, & Kuhlman, 1988; Mcgrath, 1983; Shanteau, 1992; Spence & Helmrelch, 1983). Conversely, a lack of complexity may also weaken a hacker's attitude toward doing a hacking task. This is the case since if perceived challenge compared to necessary skills in a computer task (a hacking task in this case) is too low, the users will lose interest in performing that task and the task is deemed boring (Ghani & Deshpande, 1994).

Thus, it is hypothesized that

H7: *Perceived Complexity will have a positive impact on Perceived Attitude.*

Chapter 4: Research Methodology

This chapter details the process by which this dissertation's research questions were answered. The details of the procedure and participant recruitment are explained followed by the procedure used for data collection, and a review of the research process from pretest, to pilot test, to main study. This chapter also reviews the measurement instrument and how it was validated. A survey was used as it is a common approach in IS studies (Sivo, Saunders, Chang, & Jiang, 2006). An experimental model was considered but ultimately rejected as it would have introduced biases between varied hacker skill levels that could not be easily accounted for.

4.1 Procedure and Participant Recruitment

Participants in this study were adults over the age of 18 that self identify as computer hackers. To confirm that every participant understood the term "hacker" to mean the same thing, all participants were shown the following statement and asked to agree that it matched their understanding of the word "hacker":

> *"To participate in this survey you must see yourself as a hacker. This research defines a hacker as a person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The true hacker can't just sit around all night; s/he must pursue some hobby with dedication and flair."*

This definition is based on both the Harvey (1985) definition and the Malkin & Parker (1993) definition. The data were collected from October of 2014 through May of 2015.

Participants were contacted though twitter solicitations using hash tags associated with the hacker culture, postings on message boards that were used by hackers, through communications with hacker spaces (organized clubs) located all over the world, and through direct contact at conferences and hacker group events. Potential participants contacted via the internet were directed to a web page that contained a working definition of who a hacker is, and explained the purpose of the research. In the case of face to face interactions, potential participants were given a paper copy of the survey that included all the same information/questions as the website. Participants receiving a paper copy of the survey were informed of a drop box location to deposit their survey if they chose to complete it. The paper version of the survey included a web address should the participants prefer to submit their answers online.

Upon filling out the survey, participants were asked to reflect on a hacking task that they had considered doing but have not yet tried to execute. Participants were asked to think about a hacking task they had not attempted yet so as to ensure that when they responded to the survey questions, they would be speaking of their expectations and not previously established experiences. This distinction was important since TRA and GDT are both theories that use expectations as predictors of behaviour as opposed to actual experience.

The survey was designed in three parts. The first section asked for responses on a five point and a three point Likert scale, as per the operationalization of the construct items from the extant literature. The second section contained open-ended questions and the third section collected demographic information. The first part of the survey was

focused on testing the theoretical model outlined previously while the second section contained open ended questions with the intention of both understanding the respondents answers as well as broadening the exploration of the general concepts under investigation.

4.2 Research Stages

This research investigation involved three stages: a pretest; a pilot study; and the main study. The pretest was used to test the understanding of the questions and verify the smoothness of the data collection process to ensure that the main study worked flawlessly. The pilot study was a 'dress rehearsal' for the main study where participants were contacted from the intended research population and the process was carried out as it would be done for the main study. The final stage was the main study that collected data from the sample population in order to validate the proposed research model.

4.2.1 Pretest and Pilot Study

For the pretest, 11 graduate students from the DeGroote School of Business at McMaster University were recruited. The purpose of the pretest was to test the clarity of the survey questions and the flow of the survey process in order to resolve any issues that arose. Issues like confusing instructions, confusing questions and software reliability were of greatest concern. The data collected from the pretest was only used for the pretest and was not used in subsequent analysis. Aside from one or two minor spelling and language clarification issues, the pretest revealed no major issues with the flow or understanding of the survey instrument.

A pilot study was then conducted using the same online sources that were used to

solicit participants for the full study. Twelve individuals participated in the pilot test. The participants in this study were self identified hackers and were recruited in exactly the same way the main study was designed to collect data. The pilot study acted like a dry run to ensure the smooth operation of the full survey and to address any potential misunderstanding or confusion caused by the survey questions.

The pilot study revealed that gaining trust of the hacker groups over the Internet presented several unexpected challenges. Assurances over personal motivation for the research were particularly difficult to address. The questionnaire had to be reorganized twice before the concerns of the hackers were suitably addressed. In its final form, the survey had questions relating to General Deterrence Theory moved to the end of the quantitative questions section. In the questionnaires' original layout some participants were interpreting the GDT questions to be an attack on their character and objected hostilely to those questions. In the first change, The GDT questions were moved deeper into the questionnaire and this resulted in a reduction in negative feedback. These concerns were then diminished further by placing the GDT questions after the majority of other questions had been presented. The data collected from the pilot test was only used for the pilot and was not used in subsequent analysis.

4.2.2 Main Study

Following the pretest and pilot test, the main study was conducted. In total, 107 individuals participated in the main study. A minimum sample size for the study was determined following Barclay et al.'s (1995) guideline for reflective constructs who recommend a minimum participant size of ten times the number of structural paths

directed towards a dependent variable in the research model. The largest number of structural paths pointing at any dependent variable was four for the BI construct with paths coming from attitude, social norms, perceived certainty of sanction and perceived severity of sanction constructs. Thus this study required 40 participants. A more conservative approach to identifying the minimum suggested sample size for PLS modelling is the greater of: (i) ten times the number of items in the most complex construct in the model, or (ii) ten times the number of paths leading to the dependent variable in the model with the most independent variables (Chin, 1998; Gefen et al., 2000). The most complex construct in this research study is curiosity with ten items. Thus, utilizing this more conservative approach, the minimum sample size was determined to be 100 (the greater of 100 and 40).

Popular media has frequently mislabelled the term "hacker" to represent criminal endeavours involving computers so it was expected that there would be a low response rate from any cold call strategy for finding participants. Even after acknowledging this hurdle, this research struggled with the following two significant challenges related to enticing hackers to participate in the research: (i) locating hackers and getting them to consider participating in the study; and (ii) getting participant hackers to share their thoughts and ideas with others. While both these issues had been anticipated and planned for, the magnitude of these challenges was greater than expected.

To identify hackers the researcher consulted several former colleagues that were self-identified hackers for advice on where hackers were likely to mingle and associate. From these discussions, five avenues were identified for contacting hackers: (i) "Hacker

Spaces": physical locations where hackers meet to share ideas and to collaborate on projects; (ii) hacking groups: organized groups of hackers that share ideas and occasionally meet. Hacker groups do not own dedicated spaces of their own but could be associated with a hacker space. An analogy would be a book clubs relationship with a library; (iii) mailing list admins for hacker related discussions: similar to a hacking club only a much looser association of individuals. Hackers may or may not know each other in these mailing lists and they use the mailing list to share ideas with their community; (iv) Internet Relay Chat (IRC) channels: much like a mailing list except communications are synchronous and transient. An analogy for this technology is a conversation in public where if you are not present you do not benefit from the information shared; and (v) web forums: these tools work exactly like a mailing list except all content is maintained online instead of via e-mail.

IRC channels are community discussion spaces that facilitate like-minded individuals to virtually come together and participate in one-on-one as well as group discussions. IRC uses its own servers and application software but is quite often also tied to some form of web interface. Communications is in real time and is synchronous in nature. Many of the participants in IRC channels have been present for an extended period of time and have developed relationships with others within the IRC environment. The use of pseudonyms is common and pervasive. New participants are generally viewed with some suspicion within these groups and are expected to observe the IRC traffic to develop an understanding of the culture and social order within the channel. Upon further review of this platform it was felt that effective use of this channel would be

problematic, as a personality would have to be inserted and maintained in the environment for some time to gain trust. This had the potential to bias the research and to compromise ethical considerations. As a result, this approach was abandoned.

Contacting hacker groups seemed like the method that would lead to the most fruitful responses. This belief was in part because the contact strategy called for negotiating permission with administrators of these groups to gain authorization to communicate with members. The hope was that if the administrator vetted the researchers request it would lend credibility to communications with its members. A number of web searches were undertaken to locate hacker groups. It was felt that if these groups were willing to advertise their existence they would also be willing to receive communications. Several lists were identified, which included the DEF CON groups list. DEF CON is an annual conference for hackers that is held each year in Las Vegas. Over 200 groups associated with DEF CON were identified for contact in this study. An additional 150 groups were identified through Wikipedia and other online resources. When contacting each of these groups' administrators, a clear explanation of the goals of the research as well as an outline of how the researchers would communicate with their members was provided (as per the protocol approved by McMaster University's Research Ethics Board). It was made clear that the researchers did not want direct access to their membership lists and that several steps had been taken to ensure the anonymity of all participants. After contacting 350 hacker groups, there were over 230 responses to the survey within a time frame of eight months. However, from these responses, only 8 were properly completed. The improperly completed surveys were incomplete surveys that had

a significant majority of their questions left blank. While this completion rate seemed unusual, a further unexpected circumstance arose when the researcher began receiving direct communications from several participants. Several of the participants who started but did not complete the survey spent considerable time and effort providing feedback and commentary on the survey instrument itself and its presumed motives. Essentially, these hackers were attempting to "hack" the survey. Some demanded to know who funded the research and what relationship McMaster University had with the NSA. Clearly this group of people found the questionnaire format challenging both to trust and to convey their thoughts.

After finding the e-mail solicitations to yield few completed surveys, the solicitation strategy was re-evaluated. It was decided that the impersonal nature of e-mails was not effective or trusted with this target population. As such, a face-to-face solicitation strategy was employed through hacker meetings/events. The same protocol was followed where permission had to be granted from the administrators of the events. One major event that was identified was the "Delta Hack" event at McMaster University. Delta Hack is an annual hacking event where students from all fields of study join in a 24-hour competition to use existing technology and create something new and of societal benefit. Organizers were contacted and they agreed to make space available to solicit participants during the 3-day event via a display table. In total, 100 surveys were given out and returned during this event where only 6 lacked sufficient data to be used in the analysis. Participants were invited to complete the paper-based survey and return it anonymously in a secured box. No identifying information was collected on the surveys.

An additional 13 surveys were collected via smaller hacker events/meeting.

This face-to-face strategy was remarkably different from the online interactions with this target population. Participants were very curious about the research and many wanted to share their own anecdotes about being a hacker and the positive contributions they sought to make to society. This resulted in a significantly higher response and completion rate than online interactions.

4.3 Measurement Instrument

The survey used previously validated instruments to help ensure content validity. Table 4.1 below lists the questions that were used in this research. The questions were adapted from validated sources and were appropriately contextualized for the subject of this research. They were measured using a combination of 3-point and 5-point Likert scales as per the original validated constructs.

Table 4.1 Construct items used in the quantitative survey

Construct (Source)	Items
Behavioural Intention (Venkatesh, Morris, Davis, & Davis, 2003)	1. I intend to do this hack in the next 6 months 2. I predict I would do this hack in the next 6 months 3. I plan to do this hack in the next 6 months
Attitude (Venkatesh, Morris, Davis, & Davis, 2003)	1. Doing this hack is a good idea. 2. I like the idea of doing this hack. 3. Doing this hack will be pleasant.
Subjective Norm (Venkatesh, Morris, Davis, & Davis, 2003)	1. People who influence my behaviour think that I should do this hack. 2. People who are important to me think that I should do this hack.
Mastery (Spence & Helmrelch, 1983)	1. I would rather do something at which I feel confident and relaxed then something which is challenging and difficult 2. When a group I belong to plans an activity, I would rather direct it myself than just help out and have someone else organize

	it. 3. I would rather learn easy fun games that difficult thought games. 4. If I am not good at something, I would rather keep struggling to master it than move on to something I may be good at. 5. Once I undertake a task I persist. 6. I prefer to work in situations that require a high level of skill. 7. I more often attempt tasks that I am not sure I can do that tasks that I believe I can do. 8. I like to be busy all the time.
Curiosity (Kashdan et al., 2009)	1. I actively seek as much information as I can in new situations 2. I am the type of person who really enjoys the uncertainty of everyday life 3. I am at my best when doing something that is complex or challenging 4. Everywhere I go, I am out looking for new things or experiences 5. I view challenging situations as an opportunity to grow and learn 6. I like to do things that are a little frightening 7. I am always looking for experiences that challenge how I think about myself and the world 8. I prefer jobs that are excitingly unpredictable 9. I frequently seek out opportunities to challenge myself and grow as a person 10. I am the kind of person who embraces unfamiliar people, events, and places
Perceived certainty of discovery (D'Arcy, Hovav, & Galletta, 2009)	If I did this hack I would probably get caught
Perceived sanction severity (D'Arcy, Hovav, & Galletta, 2009)	If I get caught doing this hack I will be severely reprimanded
Perceived Complexity (Jarupathirun,Zahedi, 2007)	This task is: Very simple vs. Very complex Very straight forward vs. Very complicated

Open-ended questions were also included in the survey instrument. These

additional questions sought to bring to light additional nuances in the understanding of the constructs under scrutiny that a quantitative approach would not capture. The open-ended questions asked of the participants were as follows:

1. What is it about hacking that you enjoy? How does it make you feel to hack something?
2. Outline some of the personality or character traits you believe are important to becoming a good hacker.
3. What would make a hack less desirable to you?

The final part of the survey instrument focused on demographical information about the hackers, which collected age, gender, education and nationality. The complete survey is shown in Appendix D.

4.4 Model Validation

Structural Equation Modeling (SEM) was used to validate the proposed research model. SEM techniques are extensively used in Information System research (Kock & Lynn, 2012) and are the preferred method because they combine the theoretical model's measurement model with its structural model (Meyers, Gamst, & Guarino, 2006). PLS is the specific SEM technique that has been chosen for this study. PLS is ideal because of its small sample size requirements and because PLS can be used in research that may be both confirmatory and/or exploratory in nature (Hair, Ringle, & Sarstedt, 2011). Additionally PLS imposes a minimal demand on data distribution and residual

distribution (Chin, 1998) and is more tolerant of small one or two item constructs than covarience-based SEM approaches (Hair et al., 2011). The PLS software used in this research was Warp PLS. Warp PLS was selected because of the possibility that the data collected may not satisfy the linearity assumptions of standard PLS software packages. Warp PLS is designed to analyze and test for both linear and nonlinear relationships (e.g., U-shaped and S-shaped functions) (Guo, Yuan, Archer, & Connelly, 2011). Upon examining the relationships in the data collected, a number of nonlinear relationships were detected, validating the use of Warp PLS.

Following Hair et al. (2011) recommendations, a two-step process was followed in evaluating the PLS results. The first step involved evaluating the measurement model to assess the reliability and validity of the measures in the model (Chin, 2010). This step was then followed by the evaluation of the structural model to determine if there was evidence to support the proposed theoretical model (Chin, 2010). This approach is recommended because if the researcher is not confident in their measurement model then there is no reason to move on to the structural model (Hair et al., 2011). Additionally the model was further tested for collinearity and common method bias.

The criteria for evaluating the PLS measurement model are outlined in Table 4.2 and the criteria for evaluating the PLS structural model are outlined in Table 4.3.

Table 4.2: PLS Measurement Model Test Criteria for Reflective Constructs

Analysis	**Test**	**Acceptance Criteria**
Item Reliability	Corrected item-total Correlation	Value > 0.40 (Churchill Jr., 1979)
	Item Loading	Values > 0.50 (Gefen, Straub, & Boudreau, 2000)

Construct Reliability	Composite reliability	Composite reliability should be > 0.60 (Bagozzi &Yi, 1988; Hair et al., 2011) However indicators of 0.4 through 0.7 should only be considered for removal if deleting the item will increase the overall composite reliability. (Hair et al., 2011)
	Cronbach's alpha	Value > 0.70 (Bernstein & Nunnally, 1994) or > 0.9 – Excellent > 0.8 - Good > 0.7 – Acceptable > 0.6 – Questionable > 0.5 – Poor < 0.5 – Unacceptable. (Gliem, J., Gliem, R., 2003)
Convergent validity	Average Variance Extracted (AVE)	AVE > 0.50 (Au, Ngai, & Cheng, 2008; Hair et al., 2011)
Discriminant validity	Item Cross Loading	Follow the Fornell-Larcker Criterion with the AVE for latent constructs > the highest squared correlation with any other latent constructs Indicator loadings should be > all of its cross loadings. (Chin, 2010; Gefen & Straub, 2005; Hair et al., 2011; Fornell C., & Lacker, D., 1981)

Table 4.3: PLS Structural Model Test Criteria

Goodness of Fit	R^2 values of endogenous latent variables	0.75 = Substantial 0.50 = Moderate 0.25 = Weak (Hair et al., 2011)
	Tenenhaus Goodness of Fit Index (GoF)	$GoF_{Small} = 0.10$ $GoF_{Medium} = 0.25$ $GoF_{Large} = 0.36$ (Akter, D' Ambra, & Ray, 2013; Wetzels, Odekerken-Schröder, & van Oppen, 2009)

Effect Size	F^2	The magnitude of the effect sizes of each path was evaluated using the following criteria: $f^2_{Small} = 0.02$, $f^2_{Medium} = 0.15$, $f^2_{Large} = 0.35$, (Kock, 2015)
Predictive Validity	Stone-Geisser test Q^2	A model with a value of Q^2 > zero is considered to have predictive validity

Collinearity can cause inflationary issues within SEM results and should also be assessed (Hair et al., 2011; Kock & Lynn, 2012). Table 4.4 outlines the criteria used to assess collinearity.

Table 4.4: Collinearity Criteria

Vertical or Classic Collinearity	VIF <5
Lateral	VIF <5

Common method bias can also cause inflationary issues by injecting unplanned influence into the model and causing a uniform variation in the model that deviates from the true results. Table 4.5 outlines the criteria used to assess common method bias.

Table 4.5: Common Method Bias Criteria

Harman's single factor test.	<50% explanatory power
Full Collinearity VIFs	<3.3

Chapter 5: Data Analysis and Results

This chapter highlights how the research data were collected, how the research data were analyzed to ensure validity, and provides results of the analyses. The data screening process was intended to identify samples that were unusual when compared to other results. These results were examined using various statistical procedures to determine if they were outliers that need to be excluded or were acceptable data. The results were also examined to determine the quality and effectiveness of the research questions. Again, statistical methods were used to assess the validity of a question as well as its overall fit in the research model. Once the data and the structure of the questions were validated, the data were again assessed using the theoretic framework to further validate the data use. Last, once the researchers had developed confidence in the data and the model, the final loadings and results were assessed.

5.1 Data Collection

Participants in this study were individuals who self-identify as hackers. They were contacted though various message boards, general community twitter solicitations, through communications with hacker spaces located all over the world and directly contacted at conferences. However the majority of the data collected came from the Delta Hack conference where participants were engaged in a face-to-face interaction. These communications asked potential participants to decide if the hacker term suitably described their own perceptions of their interests and behaviour. If they agreed with the definition they were given access to the survey. If participants did not feel they fit the definition, they were thanked for their participation and the interaction ended. The same

procedure was used in both the conference/face-to-face interactions and the online interactions.

The survey asked participants to reflect on a hacking task they had considered doing but as of yet had not tried to execute. The survey consisted of three parts each using a series of questions with responses measured on Likert scales; open ended questions; and demographic questions. The Likert scale questions were used to quantitatively explore the proposed model via structured equation modelling, while an open coding strategy was used to assess the open ended questions that were exploratory in nature and designed to elicit themes that might have been missed in the Likert-based questions. Data collection occurred between October 2014 and May 2015.

5.2 Data Screening

5.2.1 Outliers and Missing Values

Outliers are cases in the collected data that have values that are different from the majority of the values in the rest of the data set. The presence of outliers in the data creates a risk that the resulting interpretation is biased and not accurate. A univariate outlier represents a single value from a single field in one case that is unreasonably different then the majority of the values for that variable in the data set (Meyers, Gamst, & Guarino, 2006). A multivariate outlier is a single case (participant) within the data set that has an unusual grouping of two or more of its fields (Meyers, Gamst, & Guarino, 2006). A value in a case might not be considered a univariate outlier but when in the presence of other values in different fields their combined presence may be considered unusual. The data were scrutinized for both univariate and multivariate outliers. To assess

univariate outliers, all fields were converted to a standardized Z-score and then any values scoring 2.5 or above were considered an outlier and were excluded (Meyers, Gamst, & Guarino, 2006). To assess cases for multivariate outliers their Mahalanobis D^2 values were calculated. Mahalanobis D^2 value represents the distance the case is from the data sets centroid. This value was reviewed using the chi-square distribution (alpha level = 0.001). If D^2 value matched or exceeded this threshold, it was considered a multivariate outlier (Meyers, Gamst, & Guarino, 2006) and was excluded. Using these two outlier techniques, 13 cases were excluded from the 107 completed responses, resulting in a sample size of 94.

5.2.2 Multivariate Statistical Assumptions

The data screening and validation process focuses on two aspects of the integrity of the data being assessed for analysis. When looking for outliers and missing values, the data are evaluated at a highly refined level: first individual fields within a case are reviewed, then the interplay between values within a case are examined. Once each case is evaluated, the next step is to evaluate how well the overall set of data fits the requirements of the tests that are intended to be used on the data set. There are three data set characteristics that are generally considered important for SEM analysis: normality, linearity and homoscedasticty (Meyers,Gamst, & Guarino, 2006).

A normal distribution or Gaussian distribution is easily recognized by its bell shape distribution curve, and having a mean, median and mode that are all equal. A standardized normal distribution has a mean of zero and a standard deviation of 1. Normal distributions are also symmetrical with a skewness of zero and a kurtosis or

peakedness of zero. When measuring skewness and kurtosis, a value that is ±1.0 is considered non-normal (George & Mallery, 2003). Six methods were used to assess the data set: (1) Shapiro-Wilk's test; (2) an analysis of skew and kurtoses; (3) an examination of histograms; (4) an examination of Q-Q plots; (5) the Jarque-Bera test; and (6) the robust Jarque-Bera test. The Shapiro-Wilk tests showed a significance smaller than 0.001 thus observing non-normality in the data set. Observing the histograms also supports the argument that the data-set is for the most part non-normal. The Q-Q plots showed close association with the normal trace suggesting there is normalcy. See Appendix A and B for Q-Q plots and Histograms. The examination of the Skew and Kurtosis also suggest that while not perfectly normal, the data is a reasonable approximation for all but two of the variables (Curiosity001 and ComplexityPCPX). Warp PLS has two additional built in tests for normality, the Jarque-Bera and robust Jarque-Bera tests. These tests use a samples skewness and kurtosis to provide a clear indicator of a sample's normality (Jarque & Bera, 1987; Gel & Gastwirth, 2008). Results from these last two tests are shown in Table 5.1.

Table 5.1: Jarque-Bera and robust Jarque-Bera tests normalcy tests

Normalcy Test	Construct								
	BI	Attitude	SN	Discovery	Punish	Mastery	Curiosity	Complexity	Difficulty
Jarque-Bera	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes
robust Jarque-Bera	No	Yes	Yes	Yes	No	Yes	Yes	No	Yes

Based on the findings of these tests it is reasonable to say that while the variables in the data set are not without their challenges for normalcy, they are also not

unreasonably abnormal for use in a PLS SEM examination.

The assumption of linearity requires that the relationship between two variables is constant through their entire range and will thus produce a straight line if plotted together. If this is not the case then any tool that assumes a linear relationship will either underestimate or fail to detect a relationship. To test for linearity, scatter plots of latent variables were produced and their visual correlation was assessed. Ideally the plots should form an oval distribution along one straight axis (Meyers, Gamst, & Guarino, 2006). The resulting charts were inconclusive.

The final assumption that must be assessed is the homoscedasticity of the data set. For a data set to be homoscedastic, the dependent variables must have equal levels of variability across a range of independent variables (Meyers, Gamst, & Guarino, 2006). To evaluate homoscedasticity for use in linear regressions, a plot is done between the residuals and their predicted values. Homoscedasticity is present if there is a constant spread of data points across the predicted values access (Fay, 2010).

Upon reviewing the normality, linearity and homoscedasticity of the data set collected, there appeared to be no strong reasons to reject any of the assumptions. However there are several indications that this data may be problematic to assess and will require careful tool selection for the PLS SEM phase of the data processing. As previously described, Warp PLS will be used to accommodate and minimize the challenges potentially presented in the data set's distribution.

5.3 Research model validation

All items for the constructs in this research have been previously validated

elsewhere. By using previously validated items, researchers are able to increase their confidence in their design work and have increased confidence that the tools they are planning to use will be effective. Having previously validated instruments also increases the researchers confidence that the questions they are asking are reflective of how participants understood the questions they were asked. However, having previously validated instruments is not sufficient in itself. These instruments are only valid in the original context they were asked. Adapted questions, situational context and any number of other factors can change how an instrument is received by a group of research participants. To ensure that the research being undertaken is an accurate reflection and analysis of the phenomena being investigated, three types of validation are required. These tests are used to confirm: the measurement model, common method bias, and the structural model.

5.3.1 Measurement model

The measurement model is also known as the outer model and refers to the measured variables and their relationship to the latent variables that are of interest to the researcher (Monecke & Leisch, 2012). The first step is to test the item reliability. As mentioned in the previous chapter, the composite reliability needs to be greater than 0.40 and preferably 0.70 or better. Additionally, item loadings greater than 0.50 are also preferred (Gefen, Straub, & Boudreau, 2000). As seen in Table 5.2 below, the majority of indicators met both criteria. However a selection of the indicators did not meet their thresholds and were dropped from the investigation.

Table 5.2 Item Reliability Assessment

Construct	Item	Item Loading	Corrected Item-Total Correlation
Behavioural Intentions	BI1	.908	.784
	BI2	.853	.704
	BI3	.936	.851
Attitude	Attitude1	.770	.437
	Attitude2	.777	.440
	Attitude3	.694	.363
Subjective Norm	SN1	.913	.667
	SN2	.913	.667
Mastery	Mastery1	Dropped	
	Mastery2	Dropped	
	Mastery3 R[1]	Dropped	
	Mastery4	.695	.407
	Mastery5	.734	.481
	Mastery6	.709	.435
	Mastery7	.642	.348
	Mastery8	Dropped	

Curiosity	Curiosity1	.583	.451
	Curiosity2	.619	.516
	Curiosity3	.542	.429
	Curiosity4	.602	.484
	Curiosity5	.658	.536
	Curiosity6	.721	.601
	Curiosity7	.649	.530
	Curiosity8	.700	.602
	Curiosity9	.771	.664
	Curiosity10	Dropped	
Complexity	Complexity1	.910	.655
	Complexity2	.910	.655
Perceived Certainty		Single Item	Single Item
Perceived Severity		Single Item	Single Item

[1] Items with the Suffix "R" were reverse coded for data collection but reversed for analysis

This research had eight constructs under investigation. For these constructs to be

valid they should have a composite reliability higher then 0.60 (Bagozzi &Yi, 1988; Hair et al., 2011). However indicators of 0.4 through 0.7 could be considered for removal if deleting the item will increase the overall composite reliability (Hair et al., 2011). Table 5.3 provides a summary of the composite reliabilities for the multi-item constructs used in this study, and shows that all exceeded the 0.7 threshold.

Typically, Cronbach's alpha values should be larger than 0.70 (Bernstein & Nunnally, 1994). However, the research instrument used in this project has a number of constructs with few items. According to Cortina (1993), Cronbach's Alpha is sensitive to the number of items in a construct and that constructs with 20 or more items can easily meet the .70 recommendation while smaller constructs will be less likely to achieve the same value. Gliem, and Gliem (2003) offer an alternative interpretation of Cronbach's alpha in which they expand the criteria for Cronbach's alpha assessment as follows:

> 0.9 – Excellent
> 0.8 – Good
> 0.7 – Acceptable
> 0.6 – Questionable
> 0.5 – Poor
<. 05 – Unacceptable.

Given the above, a threshold of 0.60 is being considered tolerable for this exploratory research. Table 5.3 provides a summary of the Cronbach’s alpha values for the multi-item constructs used in this study, showing all multi-item construct exceed the 0.6 threshold.

The average variance extracted (AVE) is used as an indicator of convergent validity. Values greater than 0.5 are desirable (Hair et al., 2011) as it suggests that,”...the

latent construct accounts for a majority of the variance in its indicators on average." (Mackenzie, Podsakoff, & Podsakoff, 2011, p. 313). In this research, the AVE scores for two constructs being explored (Attitude and Curiosity) fall slightly below the 0.5 threshold. However, they are both close to the threshold suggesting that while not ideal they still have explanatory power. Furthermore, since this research is exploring a novel phenomenon of hacker motivation, it is believed that these constructs will still be able to inform and provide insights in this study's context.

Table 5.3 Assessment of Construct Reliability

Construct[1]	**Composite Reliability**	**Cronbach's alpha**	**AVE**
Behavioural Intention	.927	.881	.809
Attitude	.792	.605	.559
Subjective Norm	.909	.800	.834
Mastery	.789	.644	.484
Curiosity	.869	.829	.426
Complexity	.905	.791	.827

[1] Perceived Certainty and Perceived severity not shown as they are single-item constructs

To ensure the reliability of the indicators loadings, their loading onto their constructs must meet or exceed 0.70 (Fornell & Larcker, 1981). Table 5.4 shows that this criterion is met for all indicators and their respective constructs. This table can also be used to test discriminant validity by verifying the indicators load the strongest on their intended construct and that they do not load within an order of magnitude on any other construct (Gefen & Straub, 2005). As shown in the table, the constructs have sufficient

discriminant validity.

Table 5.4: Loadings and Crossloadings[1]

	BI	Attitude	Mastery	Curiosity	Complex	SN
BI1	**0.908**	-0.058	-0.009	-0.049	0.057	0.015
BI2	**0.853**	0.099	0.090	-0.031	-0.041	0.047
BI3	**0.936**	-0.034	-0.073	0.076	-0.018	-0.058
Attitude1	0.254	**0.770**	-0.052	-0.169	0.022	0.042
Attitude2	-0.188	**0.777**	0.107	-0.107	0.107	0.240
Attitude3	-0.071	**0.694**	-0.062	0.308	-0.095	-0.315
Mastery4	-0.018	-0.315	**0.695**	-0.134	0.200	0.220
Mastery5	0.055	0.090	**0.734**	-0.125	0.146	0.130
Mastery6	-0.023	0.149	**0.709**	0.139	-0.237	-0.186
Mastery7	-0.018	0.074	**0.642**	0.134	0.121	-0.182
Curiosity1	0.157	0.046	0.030	**0.583**	0.027	0.049
Curiosity2	-0.009	-0.054	0.058	**0.619**	0.127	-0.103
Curiosity3	0.221	0.110	0.287	**0.542**	0.131	-0.132
Curiosity4	-0.001	-0.102	-0.264	**0.602**	0.012	-0.022
Curiosity5	0.024	0.062	0.088	**0.658**	-0.122	0.114
Curiosity6	-0.191	0.085	-0.199	**0.721**	-0.396	0.028
Curiosity7	0.261	0.048	-0.139	**0.649**	0.210	0.107
Curiosity8	-0.158	-0.048	0.200	**0.700**	-0.027	0.023
Curiosity9	-0.185	-0.013	-0.018	**0.771**	0.099	-0.080
Complexity1	0.095	-0.115	0.056	-0.028	**0.910**	0.076
Complexity2	-0.095	0.115	-0.056	0.028	**0.910**	-0.076
SN1	0.153	-0.027	0.158	-0.033	0.035	**0.913**
SN2	0.153	0.027	-0.158	0.033	-0.035	**0.913**

[1]Perceived Certainty and Perceived Severity not shown as they are single-item constructs

5.3.2 Collinearity

Collinearity is a phenomenon where two or more predictor variables in a model are highly correlated. If the predictor variables are highly correlated then it is likely that the variables are measuring the same thing. If this phenomenon is not addressed then the predictor variables are effectively causing inflation of effect sizes (Hair et al., 2011; Kock & Lynn, 2012). To test for the phenomenon, two strategies are used. Both methods use the models VIF score and both require a VIF score of less than 5 although 3.3 is recommended as a more conservative threshold by some researchers (Kock & Lynn, 2012). Traditionally collinearity was seen as only a vertical concern within a model. Essentially it was believed that only indicators at the same depth/level in the model could cause measurable differences in results. Kock & Lynn (2012) assert that the same effects may occur between model levels laterally. They also argued that current methodologies do not take into account this lateral risk and they provide a methodology to assess this potential lateral collinearity issue (Kock & Lynn, 2012). Warp PLS offers a test for both vertical and lateral collinearity. This test is referred to as a full VIF test (Kock & Lynn, 2012; Kock, 2010, 2014). The full VIF test scores for this study's data was 1.261, which is well below the recommended 3.3 threshold. As such, collinearity is not a concern in this data set. Results are shown in Table 5.5.

Table 5.5 Collinearity

Assessment	Finding	Criteria
Average block VIF (AVIF)	1.113	acceptable if <= 5, ideally <= 3.3

Average full collinearity VIF (AFVIF)	1.311	acceptable if <= 5, ideally <= 3.3

5.3.3 Common method bias

Common method bias occurs when data is collected using the same method, inadvertently introducing some unexpected biasing effect that changes how participant respond to the measurement instrument. Addressing common method bias requires two strategies. The first strategy is to anticipate biasing influences such as asking potentially identifying information or by inadvertently signalling an outcome bias to the participants. These types of issues are mitigated by providing assurances of steps to anonymize data and by reassuring participants that there are no right or wrong answers. In this study, some procedural remedies as recommended by Podsakoff, MacKenzie, Lee, and Podsakoff (2003) were used. The second strategy is to test for a biasing effect in the data collected after the data collection is complete.

During the development of the research instrument, a pilot study was conducted. It was very evident by the communications of those involved in the pilot study that an unintentional bias had formed in the research questions. Two questions related to General Deterrence Theory garnered a substantial amount of attention. This was corrected first by substituting the original word “punished” with the word “reprimanded” and then by reorganizing the questions to have the GDT questions appear later in the instrument. This had the effect of allowing participants better overall exposure to the nature of the research without touching on a hot topic before trust was developed. After these changes were

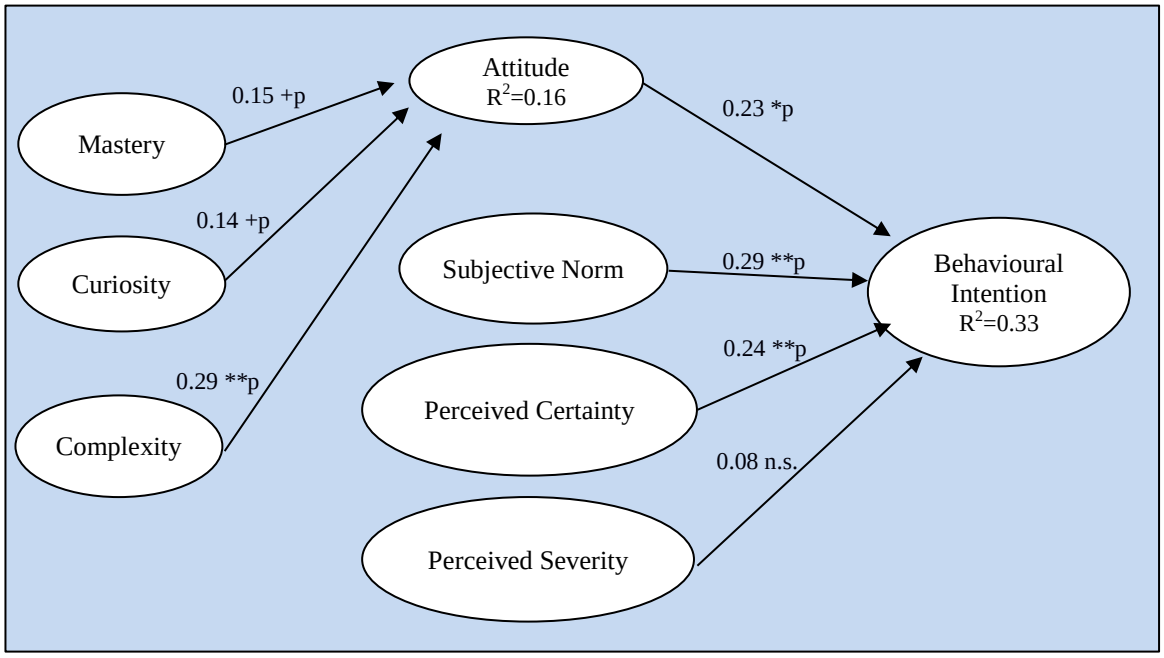
made no new comments were received.

To address the chance that a common method bias may still be present in the instrument, two statistical tests were undertaken. The first test was Harman's single factor test. The procedure for this test involves an unrotated exploratory factor analysis with the factors being constrained to one factor. If the single factor accounts for more than 50% of the variance then a common method bias is present. When this test was conducted on the research data only 17.768% of the variance was explained. This value supports the argument that no common method bias was present. A second analysis was conducted involving the examination of the full collinearity VIFs, where a score of 3.3 or lower suggest no common method bias (Kock & Lynn, 2012). The data in this research scored 1.261. Given the strong results from both tests, it can be concluded that common method bias did not impact this investigation.

5.3.4 Structural model

The structural model, which is also known as the inner model, maps the theoretical inter relationships of the latent or endogenous variables (Monecke & Leisch, 2012). To ensure the reliability of the structural model, 5000 samples were used in the bootstrapping process (Hair et al., 2011) as indicated in Table 5.6.

In order to evaluate the hypothesis proposed in this study the entire structural model was reviewed to establish if the proposed theoretical paths were significant and thus supported the proposed theory. Figure 5.1 shows the results of the structural model analysis of the proposed research model.



*p < .05; **p < .01; ***p < .001; +p<0.1; n.s.

Figure 5.1: PLS Model Results

The effect size of each path in the model was evaluated using Kock's f^2 statistic. The results of the f^2 examination showed all effects are small as illustrated in Table 5.6. The f^2 statistic was used to assess the effect size of a given relationship as it relates to the overall effect size of all the hypothesized paths leading to an endogenous variable. Kock's f^2 statistics are rated as f^2 small (.02), f^2 medium (.15), and f^2 large (.35) (Kock, 2015). The formula used to determine the effect sizes relative to other paths informing the endogenous variable is as follows:

$$f^2 = \frac{R^2_{AB} - R^2_A}{1 - R^2_{AB}}$$

Table 5.6: Summary of hypotheses results

Hypothesis	Path Coefficient	Significance	Supported (Yes/No)
H1: Perceived Attitude will have a positive impact on Behavioural Intention of engaging in a hacking task	0.23	p<0.01**	Yes
H2: Subjective Norms will have a positive impact on Behavioural Intention of engaging in a hacking task	0.29	p<0.01**	Yes
H3: Perceived Certainty of Sanction has a negative impact on Behavioural Intention in engaging in a hacking task	0.24	P<0.01**	Yes
H4: Perceived Severity of Sanction has a negative impact on Behavioural Intention in engaging in a hacking task	0.08	n.s.	No
H5: Need for Mastery will have a positive impact on Perceived Attitude towards engaging in a hacking task	0.15	$P<0.1^{+}$	Yes
H6: Need for Curiosity will have a positive impact on Perceived Attitude towards engaging in a hacking task	0.14	$P<0.1^{+}$	Yes
H7: Perceived complexity will have an impact on Perceived Attitude	0.29	p<0.01**	Yes

**p < .05; **p < .01; ***p < .001; +p<0.1; n.s.*

The Q^2 values for Attitude and Behavioural Intention this model are 0.174 and 0.325, respectively. Both values exceed the 0.00 threshold and thus indicate that the

model has predictive validity.

Of the seven hypothesis proposed, the structural model shows that there is sufficient evidence to support six of them, two being marginal. A summary of the hypotheses and their support is provided in Table 5.7. Attitude, Subjective Norm and Perceived Certainty of Sanction had a significant effect on Behavioural Intention ($p<.01$), whereas Perceived Severity of Sanction did not have a significant effect on BI. As antecedents of Attitude, Perceived Task Complexity had a significant impact ($p<.01$) and both Mastery and Curiosity individual traits marginally impacted Attitude at the 0.1 level (Dimoka et al., 2012).

Table 5.7 Results of the f^2 examination

Dependent Construct	**Independent Construct**	**R^2**		**f^2**	**Effect Size**
		Included	**Excluded**		
Attitude	Mastery	0.16	0.02	0.023	Small
	Curiosity		0.02	0.023	Small
	Complexity		0.08	0.086	Small
Behavioural Intention	Attitude	0.33	0.01	0.014	Small
	Subjective Norm		0.06	0.082	Small
	Perceived Severity of Sanction		0.07	0.094	Small
	Perceived Certainty of Sanction		0.04	0.056	Small

[1] "Included" refers to R^2_{AB}

[2] "Excluded" refers to $R^2_{AB} - R^2_A$

The GoF is a measure of a model's explanatory power. The Tenenhaus GoF was

used for this measurement. Tenenhaus GoF is based on a communality index of the models latent variables and the Average R^2($Gof = \sqrt{\overline{AVE} * \overline{R^2}}$) (Kock, 2015; Wetzels, Odekerken-Schröder, & van Oppen, 2009). The resulting index takes into account both the structural and measurement models' performance (Henseler & Sarstedt, 2013). To assess the GoF, the following thresholds were used: GoF_{small} >= 0.1, GoF_{medium} >= 0.25, and GoF_{large} >=0.36 (Akter, D' Ambra, & Ray, 2013; Wetzels, Odekerken-Schröder, & van Oppen, 2009). The model under study in this research scored a GoF of 0.428, which associates it with "Large" explanatory power.

To evaluate the predictive power of the proposed model, R^2 values of the endogenous variables were examined (Gefen, Straub, & Boudreau, 2000). As can be seen in Figure 5.1 all R^2 values were in excess of 0.10, which is recommended by Falk and Miller (1992).

5.4 Post hoc analysis

In addition to the theorized model in this research project, a number of demographic questions were also included. The purpose of these additional questions was to provide a differentiating condition within the data set so as to compare groups.

The demographic data collected included age, gender, education and location. Unfortunately, since the majority of data came from the Delta Hack event, all the demographic variables had insufficient variability to identify meaningful subgroups.

A saturated model analysis was also conducted post hoc to explore if there were any additional significant relationships in the proposed model that were not hypothesized.

The saturated model identified two additional relationships. The first relationship is between Complexity and Perceived Certainty of Sanction and shows complexity influences perceived certainty of sanction with a Beta of 0.41, $p<.01$. The second discovered relationship is between Complexity and Perceived Severity of Sanction a Beta of 0.25, $p<.01$. These results indicate that task complexity also impacts how a hacker evaluated the risks associated with their activity.

5.5 Qualitative Analysis

5.5.1 Method

To examine the data collected in the open-ended question part of this study's survey instrument, a classical content analysis approach was used.

The process used for the qualitative analysis of this data followed the same classical content analysis method used by Detlor, Sproule, and Gupta (2003). The process was applied to the three open-ended questions asked of the participants at the end of the survey instrument:

1. What is it about hacking that you enjoy?
2. Outline some of the personality or character traits of a good hacker.
3. What would make a hack less desirable to you?

These questions were designed to broadly reflect the fundamental purpose of this study. They were intended to explore why hackers do what they do and what might disrupt their selection of activities. The first two questions were designed to have the hacker reflect on their internal motivations first by evaluating themselves then by having

them project their values on a hypothetical person ("a good hacker").

The third question was intended to illicit comments about deterrence and external influences. Instead the comments reflected personal interests and suggested introspective motivation.

To analyze the free form data that was collected, the lead researcher developed a code book. This code book was developed through an iterative process that started with *a priori* classifications derived from literature. These initial classifications were reviewed and expanded to include additional broad themes. Using this initial set of codes, the data were reviewed and classified to ensure a comprehensive fit. Once the first pass was completed, the individual items were reassessed within their initial codes and a second tier of codes was established. This was repeated for every root layer of codes establishing a complete second tier of codes and creating a hierarchical structure. The data were then sampled again and the same classification process was repeated to verify the fit with the codes was consistent between each review. After the iterative code building was completed, the code book was then reviewed by the lead researcher and where some codes had dubious clarity, a definition of the tag was provided and example language was added.

This code book was then used to train a second coder. The second coder was a peer that was familiar with the researcher's theories and expectations. The second coder received instruction from the primary researcher on how to use the code book and was given 15 examples to code. These example codes were compared to the primary researcher's coding and any variations were discussed. At this point it was clear that the

second coder understood their responsibilities and was capable of reviewing the data. The coders then s coded all the data for the three questions separately. Upon completing the coding, the results were tabulated and assessed for any disagreements. Using Krippendorf's agreement coefficient, the agreement between the two coders were evaluated and listed in Table 5.6 below. Any value greater than 0.80 is considered acceptable (Detlor, 2003).

Table 5.8 Krippendorf's Agreement Coefficient

Question	Krippendorf Agreement Coefficient
1	0.83
2	0.84
3	0.93

Using the Krippendorf agreement coefficient as an indicator that the coders were in basic agreement as to how the material was coded, the two coders then reviewed the dependencies and unified their assessment so that the codes were a 100% match. Having achieved agreement, the data was reviewed and interpreted as outlined in the below findings.

5.6 Findings

5.6.1 Question One: "What is it about hacking that you enjoy?"

For the first question ("What is it about hacking that you enjoy?"), there were 65 comments submitted by participants. Some examples and representative comments included:

"Building something and learning"

"Challenging self to be the best I can be"
"Creativity"
"Hacking is incredible. You can take anything you imagine or think up and build it. Possibilities are endless."
"It feels good to learn something new and to make something"
"Meeting new people"
"*The sense of accomplishment*"

Figure 5.2 below illustrates the distribution of answers to this question.

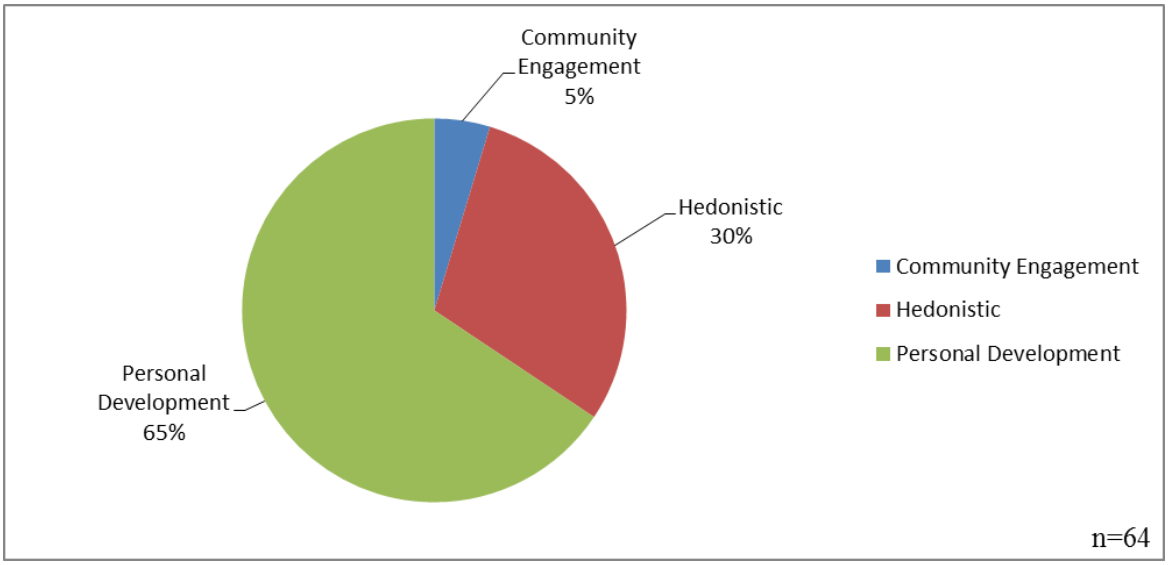


Figure 5.2: Codes for Question 1

Figure 5.2 illustrates that there were three themes identified by the participants: personal development, hedonistic, and community engagement. The personal development theme represented 63% of the responses and included references to this study's intrinsic motivators: mastery and curiosity. Because of the diversity of tags in this theme, it received a second tier of sub codes. Figure 5.3 shows the distributions of those codes.

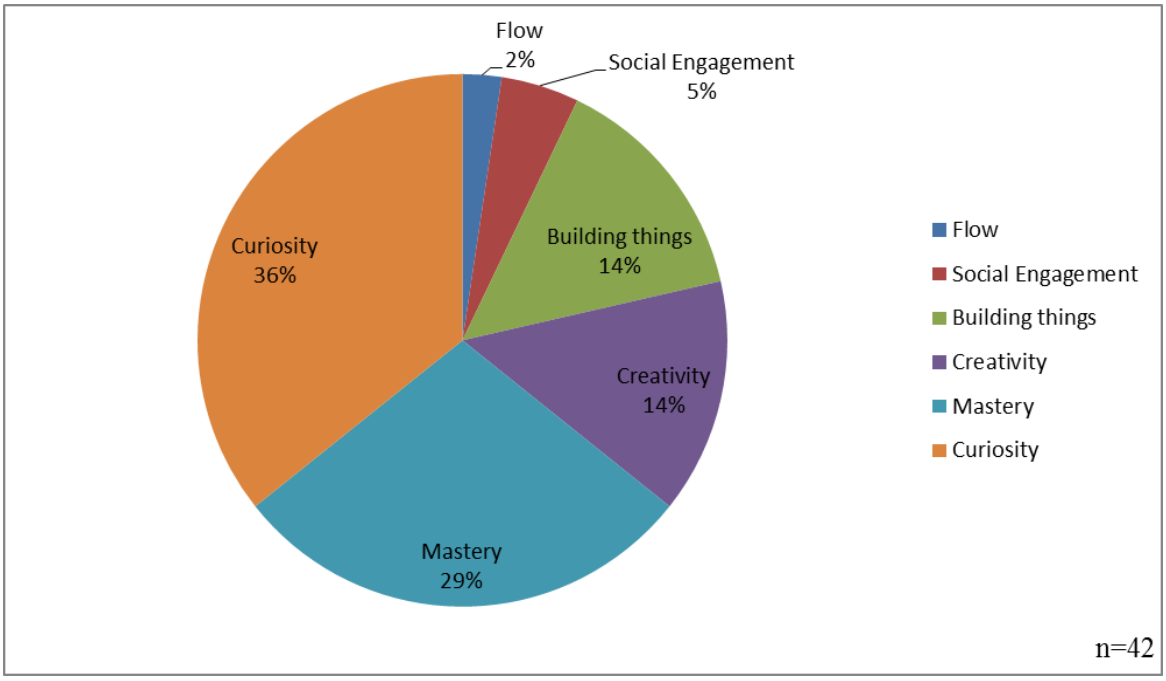


Figure 5.3: Question 1 - Sub Codes for Personal Development

The sub codes for the personal development section included curiosity (36%), mastery (29%), and creativity (14%), which were hypothesized to shape attitude. In addition to the expected results, the desire to build things (14%), social engagement (5%) and the desire to experience flow (2%) were also identified under the personal development theme through the qualitative analysis. The most prominent of these discovered themes was "building things", and was identified through comments such as:

"Make something new"
"End result"
"Building something and learning".

The social engagement (5%) sub code was identified with comments such as "meeting new people" and was likely a reflection of a participant at the Delta Hack conference where the technological experience was interwoven with a number of socialization opportunities such as food and games.

The flow (2%) sub code was distinct in its presentation, "Enjoy the focus only on the project without any other things to worry about", and while flow only captures a small segment of the personal development primary code, it was included because of how clearly the text spoke to the experience of the challenge. Flow is the "...means that an action freely follows the previous action, and the process is in a way unconscious; flow is accompanied by positive emotions and is self-rewarding" (Voiskounsky & Smyslova, 2003, p173). Flow was identified by Voiskounsky & Smyslova (2003) as a contributor to the motivations of hackers.

The hedonistic theme represented 28% of the answers and spoke directly to pleasure. It included comments such as:

"Feel Great"
"I feel excited and motivated"

The community engagement theme represented 5% of the comments and spoke to contributing in a positive way to the participant's community. This theme was driven by comments that addressed a desire to directly contribute to positive social changes and the hacker's responsibility to contribute to that goal. In the participants' comments on this point, usefulness to others as well as social responsibility and the ability to influence others were identified. Additionally, the need to belong and to have social interactions surfaced from the comments. This social awareness theme suggests that a hacker is concerned with factors associated with subjective norms, and supports the hypothesized role of subjective norms as predicted in the quantitative section of this research. There were a number of compelling quotes from the survey participants, such as:

"Meeting new people"
"Like I'm contributing to society. I like changing things."
"It's the same feeling you get when completing a difficult puzzle except that solved puzzle is useful for something"
"Design, problem solving, satisfied knowing people benefit from it"

By comparing the terms acquired in Question 1 of the open ended questions with the hypothesis that were theorized in the quantitative section of this research, there is clear support for the motivators/antecedents of curiosity and mastery. It is also evident that subjective norms play a role in how a hacker identifies tasks they might like to pursue. Additionally, a few new themes were identified in the qualitative data that were not originally hypothesized in our research model. For example, the need to be social, the need to learn and the need to contribute to the hacker's society or environment were all observed in the open-ended data.

5.6.2 Question 2: Outline some of the personality or character traits of a good hacker

The second question presented to the hackers asked that they identify what they felt were necessary personality traits to be a good hacker. Ninety-three participants provided comments for this question. Examples of some of the comments collected in this portion of the research included:

"A discontent of status quo"
"Attention to detail, patience, goo[d] teamwork skills"
"Attention to detail. Not getting discouraged easily (persistence)"
"Determination, creativity, good problem/puzzle solving skills"
"Motivation, passion, open-minded, creativity, patience"
"Problem solver, strong intake of new concepts, good listener, self-aware – know what helps me to learn"

Following the same procedures used in the first question, the second question was again reviewed by the same two coders. The coders determined the codes shown in Figure 5.4 below.

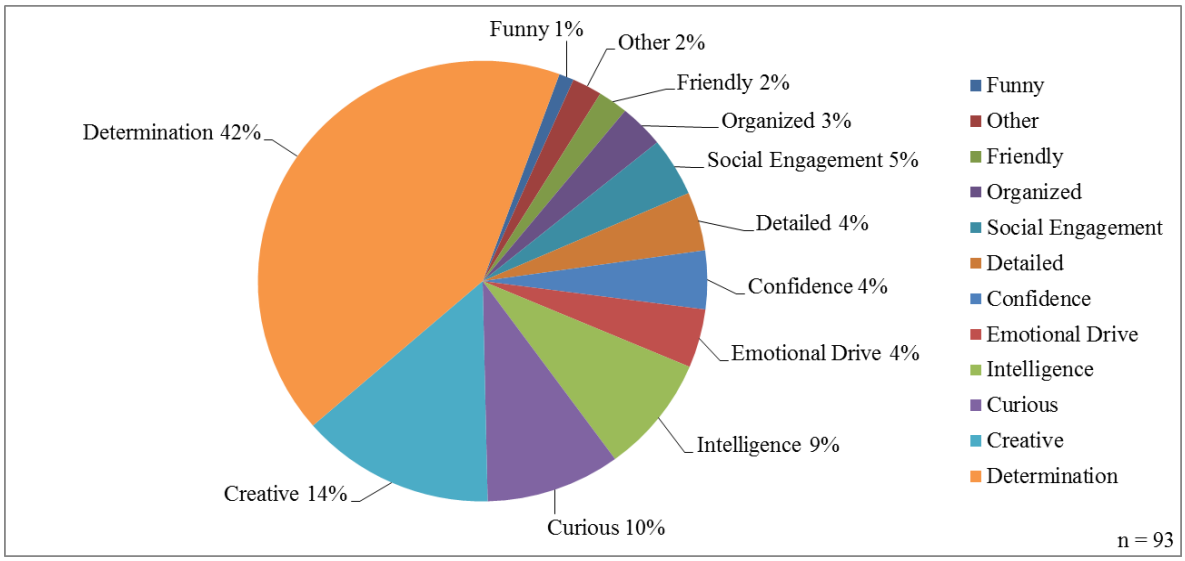


Figure 5.4: Codes for Question 2

The participants emphasized a great deal around the ability to stick with a challenge with 42% indicating determination as a key characteristic. Determination had numerous references to persistence, stubbornness, determination and tenacity. These themes line up well with the hypothesized personal traits of curiosity and mastery. A person trying to master a skill would have to be determined and patient to build his or her skills. Additionally the type of curiosity demonstrated by hackers is one that leads to a "intimate understanding" (Malkin & Parker, 1993). These stubborn and determined qualities are also an advantage to a hacker's creativity as it suggests the willingness to experiment and try things to achieve the best creative effect. These comments also give insight into the need for a hacker's tasks to be difficult and possibly complex. The

repeated references to tenacious behaviours suggest that hackers value being challenged and seek out opportunities to be exposed to difficult challenges. This theme of tenacious attitudes also supports the notion that a hacker values the opportunity to improve his or her skills and further advance his or her personal sense of mastery. Without determination, the concept of mastery would not manifest in a person as skills are only mastered through repeated and persistent effort. The participants also identified creativity at 14% and curiosity at 10%. Once again three key elements in the proposed theory are identified as key characteristics in a hacker's personality. The remaining traits that were felt to be important to a hacker's personality could be grouped into two groups: one for internal and one for external attributes. There was also one standalone code that did not fit well with any other code.

Those codes that related to intrinsic attributes or skills included:

- Organized (3%)
- Detailed (4%)
- Confident (4%)
- Emotionally driven (4%)
- Intelligent (9%)

These codes represent 24% of the comments received and clearly suggest that, while this research focused on three characteristics that could be tied to TRA, there are other personality characteristics that should be explored.

The codes that spoke to external attributes were friendly with 2%, and funny with 1%. These codes suggest that hackers are not necessarily the "lone wolf" personalities sometimes depicted in the media.

Other personality characteristics not represented were evident within the comments of questions 1 and 2. There were several references to learning and sharing with others within the comments of this second question that are consistent with the comments of the first question. Representative quotes from the second question included:

"... good teamwork skills..."
"Friendly"
"Funny"
"Good communication"
"Openness to collaborate"
"... good listener..."
"Willing to learn and teach others"
"... ask for help (collaborate)..."
"Willingness to learn from others..."

Another insight into the characteristics the hackers identified as being important was the repeated reference to cantankerous, stubborn and apparently anti-social behaviour. These comments were particularly surprising in the context of the already identified friendly or community oriented codes. This however is a false paradox. These more socially challenging codes, such as uncouth and disobedient, are reflective of the hacker's desire to not compromise on achieving his or her goals. These codes also suggest that hackers take pride in being unique and creative. The following is a list of examples from the responses to Question 2 that help support this argument:

"A discontent of status quo"
"Curiosity, stubbornness, introversion"
"Willing to try new things, ask for help (collaborate), excitement/positivity"
"Grit, drive, engineering mindset"

Social engagement/challenging was a standalone code with 5% of the responses

and identified that a portion of the respondents saw hacking as a way to engage in social change. This group saw that hacking was a way to challenge the status quo and to interact with their community.

The characteristics identified in this second question parallel the results from the first open ended question, but they also provide insight into the determination and focus on achieving a desirable end goal.

5.6.3 Question 3: What would make a hack less desirable to you?

The final open question in this research asked: "What would make a hack less desirable to you?". This question received 65 responses that included comments, such as:

"Hacking" seems to be trending and people who do it just to call themselves "hackers" to show-off/recognition."
"A trivial challenge or that you're not learning anything new"
"Being continuously put down or being made to feel that familiar projects I undertake are not important"
"Boring"
"Cockiness from the creators"
"Deadlines"
"Difficulty"
"Easy to implement"
"I find a good hack is beneficial to people. If a hack is detrimental to the world then it is less desirable to me."
"If it hurt people"

Once again, the same procedures used in the first and second question were used. The coders determined the codes shown in Figure 5.5. The answers to this question formed three codes that were identified at the highest level of a two level hierarchy. They were intrinsic motivation at 71%, external constraints at 22% and moral objections at 7%.

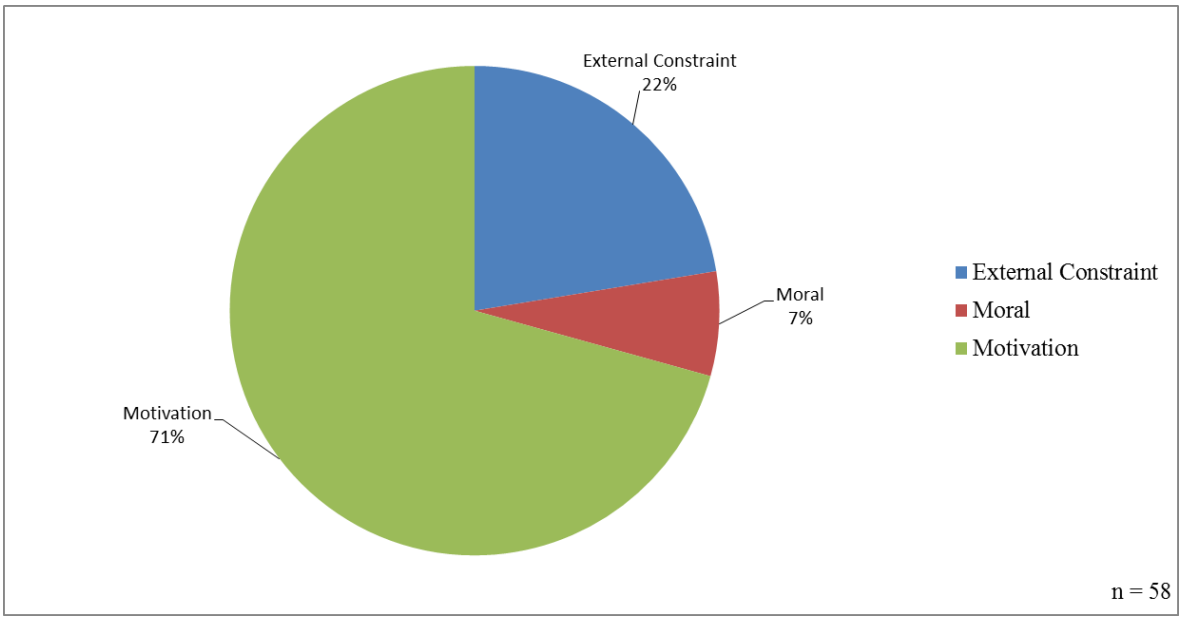


Figure 5.5: Question 3 - Level One Codes

Intrinsic motivations spoke to issues that limited the presence of key motivators. This theme is consistent with the role intrinsic motivators and subjective norms have in the TRA portion of the proposed theory. With 93% of the deterrent factors being identified as the absence of motivation, the remaining 7% relates to factors that, if present, will deter a hacker from taking on a certain task. These deterring factors are not as clearly linked to the specific elements of the GDT portion of the proposed theory, but they do indicate that a hacker may be dissuaded from a task if an argument is made that jeopardizes the hacker's perception of his or her own moral code.

To further understand the intrinsic motivation factors for discouraging hackers from a selected task, the motivation code (71% of Level 1 codes) was further subdivided as seen in Figure 5.6.

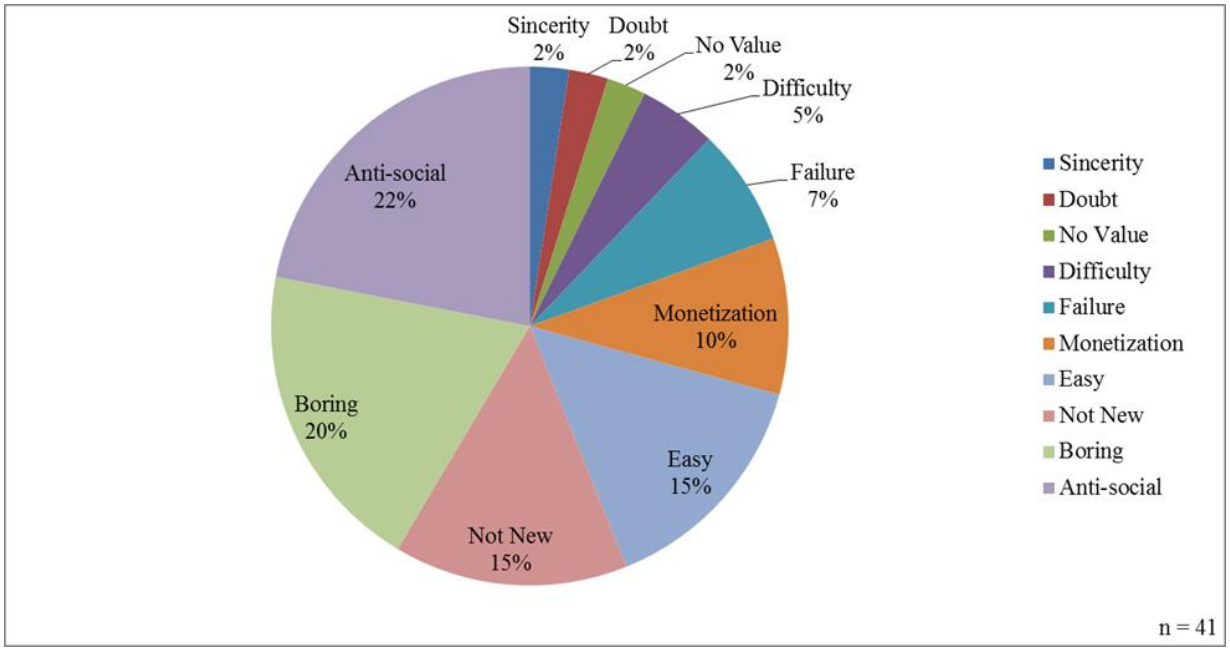


Figure 5.6: Questions 3 - Codes for Level 2 – Motivation (71% of Level 1)

As Figure 5.6 illustrates, 50% of the intrinsic motivation inhibitor was made up of codes that suggested a failure to challenge (boring, easy and not new). The proposed theory suggests that mastery and curiosity rely on challenge to give rise to the opportunities a hacker needs to express his/her intrinsic motivations. There is a 22% component of this code that reflected negative attacks on the hackers abilities or values (anti-social). For example, "Being continuously put down or being made to feel that familiar projects I undertake are not important". These comments and this sub code reflect how subjective norms are an important part of a hacker's motivation. This is consistent with the TRA component of the proposed theory.

The remaining barriers were as follows:

- Sincerity (2%) – persons involved were not genuinely interested in the challenges

of hacking. For example, "'Hacking' seems to be trending and people who do it just to call themselves 'hackers' to show-off/recognition."

- Doubt (2%) – fear of not being adequate for the challenge. For example "Intimidation – not thinking I'm skilled enough to be in it."
- No Value (2%) – the task has no meaning or purpose. For example, "No utility in it e.g. It won't improve me nor will it influence/help others".
- Difficulty (5%) – the task requires skills beyond the ability of the hacker. For example "Really hard to start e.g. hard tech"
- Failure (7%) – fear of failure. For example "Not making it work"
- Monetization (10%) – The proposed hacking project is seen as a commercial venture rather than a test of skill. For example "If Microsoft wants it"

External constraints (22% of Level 1 codes) also had a number of sub codes, as shown in Figure 5.7. The four sub codes identified were constrained challenge, time, cost and technology limitations.

The constrained challenge (46%) sub code speaks to factors that originate in the environment but place limitations on the freedom of the hacker to seek solutions. Examples of some of the participant's comments included:

"A structured problem"
"Closed system"
"It does not meet the requirements that we fought for"
"Large cost, no freedom to choose what to work on, overwhelming time commitment."
"Limiting what can be done"

"Restrictions to what can be done/heavily constrained problems"

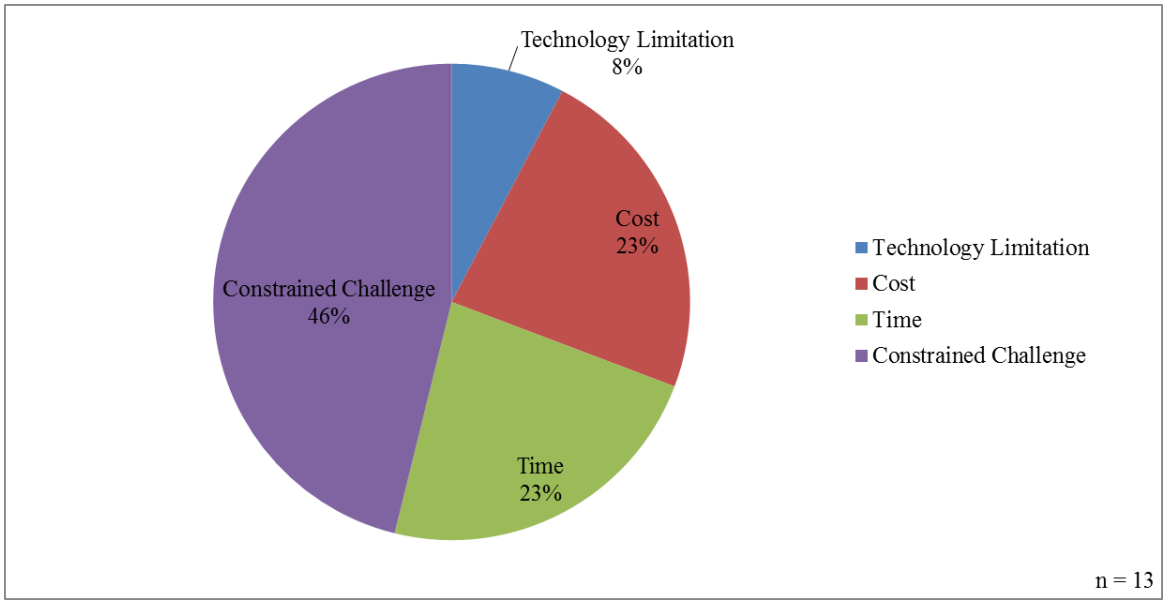


Figure 5.7: Question 3 - Codes for Level 2 - External Constraint (22% of Level 1)

Other external constraints that were identified included available time (23%), the cost of resources (23%) and technological limitations (8%).

The third of the three top-level codes for question three examines the sub codes associated with moral choices made by a hacker (7% of Level 1 codes). Figure 5.8 outlines issues that discouraged the undertaking of a hacking task based on a specific moral imperative.

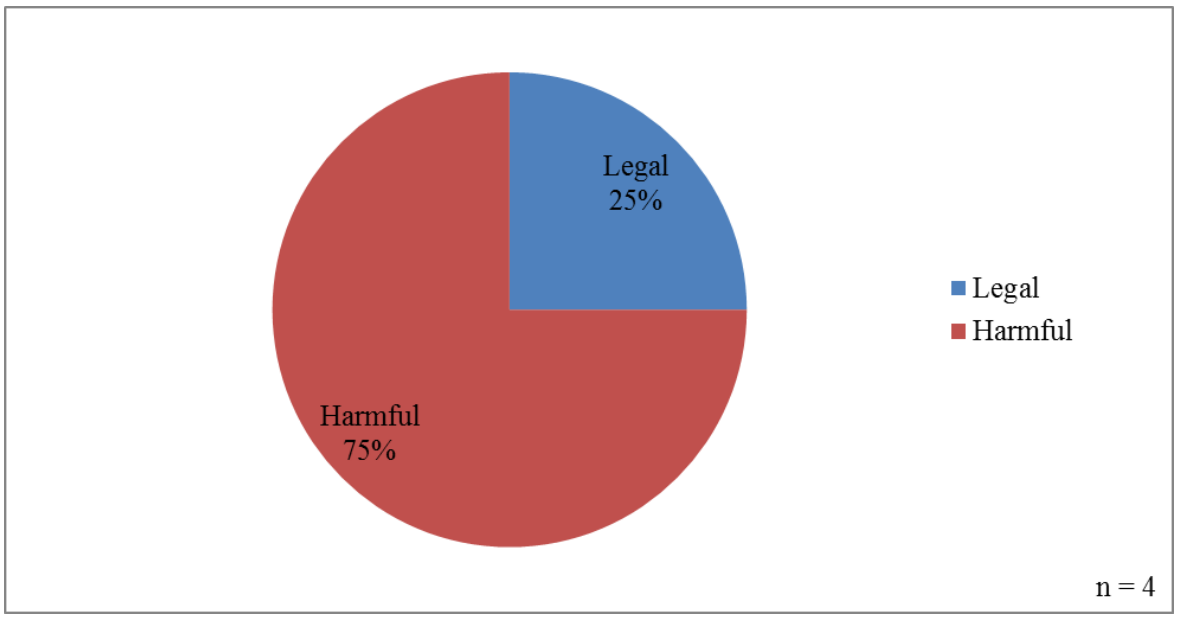


Figure 5.8: Questions 3 – Codes for Level 2 – Moral (7% of Level 1)

These two sub codes broke down easily into two groups. 75% said they would be dissuaded from a hacking task if it caused harm to others and the other 25% of respondents in this sub code indicated that they would be dissuaded if there were negative legal repercussions. In regards to the avoiding harm to others sub code, the respondents made the following comments:

> *"I find a good hack is beneficial to people. If a hack is detrimental to the world then it is less desirable to me."*
> *"If it hurt people"*
> *"Malicious intent"*

Comments directed towards legal implications included *"Legal issues"*

Using the classical content analysis method on the three open-ended questions, the goal was to both verify and enhance the quantitative contributions. In reviewing these three questions following the same classical content analysis used by Detlor, Sproule, and

Gupta (2003), the hypotheses investigated in the quantitative sections of this dissertation were both reflected and enhanced. These questions were designed to broadly reflect the fundamental purpose of this study. They were intended to explore why hackers do what they do and what might disrupt their selection of activities. Responses to these questions both identified key contributors to target selection and evaluation but also provided insight into characteristics of a hacking task that might diminish or discourage the selection of a particular task.

Chapter 6: Discussion and Conclusion

This chapter will examine the results reported in Chapter 5 in detail. Section 6.1 will summarize the findings for each of this dissertation's research questions. Section 6.2 will explore the contributions to theory and 6.3 will explore contributions to practice made by this dissertation. Section 6.4 will outline the limitations of this research while section 6.5 will provide direction for future development of this research area. The final section, 6.6 will summaries and conclude both the chapter and the dissertation.

6.1 Summary of Findings

This research was intended to explore hacker motivation and demotivation in regards to target selection through the lenses of the Theory of Reasoned Action (TRA) and General Deterrence Theory (GDT). The research also intended to explore how context affects a hacker's task selection. These intentions were expressed through two research goals:

Research Goal 1:

How is the intention of hackers to engage in a hacking task (hack) influenced by motivating and demotivating factors?

Related Hypothesis:

H1: Perceived Attitude will have a positive impact on Behavioural Intention of engaging in a hacking task.

H2: Subjective Norms will have a positive impact on Behavioural Intention of engaging in a hacking task.

H3: Perceived Certainty of Sanction has a negative impact on Behavioural Intention in engaging in a hacking task.

H4: Perceived Severity of Sanction has a negative impact on Behavioural Intention in engaging in a hacking task.

In hypothesis 1, the Perceived Attitude was predicted as an antecedent of BI. Which is to say that the more positive the attitude towards the hacking task, the more likely the hacker with have the intention to do the hack. Based on the findings in chapter five, the relationship under scrutiny had a beta of 0.23 (p-value <0.01) and exhibited a small effect size (f2=0.014). This leads to the conclusion that the evidence does support this hypothesis.

Hypothesis 2 argued that Subjective Norms were an antecedent of BI. Which is to say that the more the hacker believed his or her family, peers and other persons important to him or her thought the hacking task was a good idea, the more likely the hacker will have the intention to do the hack. Based on the findings in chapter five, the relationship under scrutiny had a beta of 0.29 (p-value <0.01) and exhibited a small effect size (f2=0.082). This leads to the conclusion that the evidence does support this hypothesis.

In Hypothesis 3, the Perceived Certainty of Sanction was predicted as an antecedent of BI. Which is to say that the more likely the hacker considered there to be repercussions for their behaviour, the more of an impact it would have on their desire to attempt the hacking task. Based on the findings in chapter five, the relationship under scrutiny had a beta of 0.24 (p-value <0.01) and exhibited a small effect size (f2=0.056).

This leads to the conclusion that the evidence does support this hypothesis.

Hypothesis 4 stipulated that Perceived Severity of Sanction were an antecedent of BI. Which is to say that the more sever the sanctions a hacker faced if discovered, the more of an impact it would have on BI. Based on the findings in chapter five the relationship under scrutiny had a beta of 0.08 (p-value >0.1) and exhibited a small effect size (f2=0.094). This leads to the conclusion that the evidence does not support this hypothesis.

Research Goal 2:

How may contextual factors of individual and task characteristics influence a hacker's attitude toward engaging in a hacking task?

H5: Need for Mastery will have a positive impact on Perceived Attitude towards engaging in a hacking task.

H6: Need for Curiosity will have a positive impact on Perceived Attitude towards engaging in a hacking task.

H7: Perceived Complexity will have a positive impact on Perceived Attitude.

In Hypothesis 5, the need for Mastery was predicted as an antecedent of Perceived Attitude. Which is to say that the more the hacking task was to challenge and press the hackers skills, the more Perceived Attitude would grow. Based on the findings in chapter five, the relationship under scrutiny had a beta of 0.15 (p-value >0.1) and exhibited a small effect size (f2=0.023). This leads to the conclusion that the evidence does marginally support this hypothesis.

Hypothesis 6 posited that the Need for Curiosity was an antecedent of Perceived Attitude. Which is to say that the more the hacking task tweeked the hackers Curiosity, the more Perceived Attitude would grow. Based on the findings in chapter five the relationship under scrutiny had a beta of 0.14 (p-value >0.1) and exhibited a small effect size (f2=0.023). This leads to the conclusion that the evidence does marginally support this hypothesis.

Hypothesis 7 posited that the Perceived Complexity of the hacking task was an antecedent of Perceived Attitude. Which is to say that the more the hacking task was seen to be technically complex to the hacker, the more Perceived Attitude would grow. Based on the findings in chapter five the relationship under scrutiny had a beta of 0.29 (p-value <0.01) and exhibited a small effect size (f2=0.086). This leads to the conclusion that the evidence does support this hypothesis.

To address the first goal of understanding how a hacker's intentions are molded by their intrinsic motivations as well as their social environment, two well established theories (TRA and GDT) were selected as a framework from which to expand and explore the hacker's motivation. TRA describes two sources for influencing behavioural intentions: attitude and subjective norms. Hypothesis 1 (Perceived Attitude will have a positive impact on Behavioural Intention of engaging in a hacking task) and Hypothesis 2 (Subjective Norms will have a positive impact on Behavioural Intention of engaging in a hack) tested the roles these element played in effecting Behavioural Intentions. The research results supported both hypotheses and thus supported the role of TRA as a framework from which to explore hacker motivations.

Based on the extant literature, two intrinsic motivators were identified as possible contributors to hacker's attitudes towards a hacking task. These motivations were mastery and curiosity. Based on the literature, these motivations were hypothesized to have a positive impact on a hacker's attitude. Hypothesis 5 (Need for Mastery will have a positive impact on Perceived Attitude towards engaging in a hacking task) was shown to be supported with a loading of 0.15 (p=.07) as was hypothesis 6 (Need for Curiosity will have a positive impact on Perceived Attitude towards engaging in a hacking task) with a loading of 0.14 (p=.09). These findings were further supported by the qualitative investigation that found 23% of respondents identifying curiosity and 19% identifying mastery as a critical element in their enjoyment of hacking. The extant literature also observed that a hacker has a need for novelty and challenge (Jordan & Taylor, 1998; Turkle, 1984; The Mentor, 1986).

In addition to the intrinsic motivations for a hacker to carry out his or her activities, it was hypothesized that certain characteristics of the activity itself may contribute to a hacker's attitude. To test this, the hackers were also asked about their perception of the complexity of a hacking task. It was hypothesized that the complexity of a task would contribute to attitude. This hypothesis listed as hypothesis 7 (Perceived complexity will have an impact on Perceived Attitude) and was supported by the research results (loading of 0.29, $p<0.01$). This further supports the assertion that hackers are motivated by novelty and challenge (Jordan & Taylor, 1998; Turkle, 1984; The Mentor, 1986). In terms of attitude, both the quantitative and qualitative data support that hackers are motivated by tasks that challenge their mastery of their skills, peak their curiosity

through novelty or learning and can maintain their interest by presenting complex processes.

Alongside attitude as an influence on behavioural intention, the TRA portion of this research model suggests that subjective norms are an important antecedent to behavioural intention. This argument seems to contradict the portrayal of hackers in modern commercial media where they are often depicted as loners and averse to socializing. This research hypothesized and has shown that close social association such as family and peer groups, represented by the subjective norm construct have a significant impact on a hacker's behavioural intentions. This was argued in hypothesis 2 and was supported with a loading of 0.29 ($p<.01$). This research showed that there is evidence to argue that if a hacker's social environment approves of his or her endeavours or sees his or her goals as valuable then the hacker's intentions to carry out a hacking task will increase. From a larger global perspective examples of this behaviour have been demonstrated by the Anonymous hacker operation "OpIceISIS", which targeted exposing terrorist recruitment activities on the web and in social media.

To the best of our knowledge, this research was the first study to utilize GDT to explore the hacker phenomena. In this study, it was determined that hackers do in fact consider the likelihood of being caught and sanctioned when they consider attempting a hacking task. Hypothesis 3 (Perceived Certainty of Sanction has a negative impact on Behavioural Intention in engaging in a hacking task) was supported with a loading of 0.24 ($p<0.01$). Interestingly the severity of punishment (Hypothesis 4 - Perceived Severity has a negative impact on Behavioural Intention in engaging in a hacking task)

was not supported in this research (p=0.23).

Post Hoc Discoveries

The post hoc analysis of the data collected identified two additional relationships in the deterrence portion of the model. The additional saturation tests showed that task complexity was an antecedent to both the perceived certainty of detection and the perception of the severity of sanction. While these relationships have not been identified in the extant literature, it appears reasonable that a hacker would perceive a highly complex hacking task would result in a higher perceived certainty of sanction. A highly complex hacking task may also imply importance of the target due to its extensive security measures. As such, it would be reasonable to assume that the sanction of being caught hacking a highly complex task would be severe due to its importance/sensitivity.

6.2 Contribution to Theory

This research makes several contributions to theory. It addresses the need to directly examine this unique population (Mahmood, Siponen, Straub, Rao, & Raghu, 2010) by surveying actual hackers that were active in a hacking task at the time of the research. The task also identifies curiosity and mastery as antecedents to attitude in TRA. This creates a new opportunity for researchers to recognize the role of internal motivation in the understanding of behavioural intention.

This dissertation also adopted a novel theoretical lens from which to observe the phenomena. This research used an aesthetic lens as an alternative to utilitarianism to view the phenomena. When this is combined with the intrinsic motivations explored in this dissertation, a new group of research questions form. For example, do all attitudes

towards actions come from the same logic or goal setting process, or could factors such as attitude be masked by other factors effecting decision making such as aesthetic goals instead of utilitarian goals. The use of an aesthetic lens introduces numerous opportunities to revisit old ideas and apply a fresh look. Sören Kierkegaard (1813-1855) posited that people live in the moment; they are moved by the artistry in their lives and not all actions follow ethical principles. Kierkegaard's idea of an aesthetic life superseding the motivation of living an ethical life has proven to be an important foundation for understanding the motivations of hackers. This thesis has shown that a research lens separated from the orthodoxy utilitarian rationales was an effective approach to investigate this novel population.

Finally this research also shows that GDT can be expanded to look at how external factors, such as the complexity of undesirable actions, may influence the degree to which an individual would be discouraged from engaging in a hacking task.

6.3 Contributions to Practice

The benefits of this research to the professional community are twofold. On one hand the research demonstrates key antecedents that attract hackers towards new tasks. On the other hand these same antecedents also hint at strategies to better engage these unique individuals and to leverage their skills in creative product development opportunities.

This research benefits cyber security professionals by providing a better understanding of the motivations of the people behind some of their threats. Based on these finding practitioners will be able to design strategies to better combat new or

developing threats by looking past the technical issues of data security and explore why hackers do what they do. Through the use of rigorous quantitative and qualitative methodologies this research introduced an understanding of how hackers identify and assess their tasks. It was hoped that by investigating the motivations of these highly skilled information systems users, new insights into how to avoid harmful actions could be ascertained.

By understanding the impacts that mastery, curiosity and complexity have on hackers' motivations, this research establishes opportunities to engage these IS gurus in fruitful economic activities. By leveraging the results of this dissertation, astute managers can create engaging work spaces replete with appropriate stimuli to attract and benefit from these highly skilled and creative individuals.

The key for industry to leverage this research is to understand that new innovations will attract hackers' attention. Whether it is illegally penetrating a network, messing with a traffic sign or modifying features in an Internet connected car, if it's new and looks like a challenge to hackers, then they will be drawn to it. While some of this type of attention is undesirable, there is an equally desirable side effect for industry. The characteristics that have been identified in this research would also make highly desirable characteristics for product designers. Given that the research has identified that novelty and social contributions are desirable to hackers, product developers like those seen on the kickstarter.com website would be ideal candidates to solicit hackers to contribute to their tasks and tap into the hackers unique skills.

6.4 Limitations

As with any study, this dissertation is constrained by certain limitations. The first limitation relates to generalizability and the second limitation relates to the sample size. While these issues are a concern, they also represent opportunities for the research community to verify and expand the results of this research.

For a research project to be generalizable there must be confidence that the research findings are repeatable across other samples. This project, while exceeding the recommended minimum sample size, did so only because of the contribution of participants at a youth oriented hacker conference. There were an additional 230 responses to the survey that were not completed that were sourced from hacker groups around the world. Given the enthusiastic adoption of the survey at the face to face conference, there might be a concern that the conference attendees were in some way bias and were differently engaged because of the environment they were in when they participated in the survey. Furthermore the hacking conference where the majority of results were obtained was targeted to younger people, generally university undergraduate students. This created an environment where variations in age, income, societal beliefs, etc., were likely diminished.

The second issue was the actual sample size. While the sample of 107 participants was sufficient for the research model to be tested, it would have been desirable to have a larger sample size. With a larger sample there would be less concern over the impact of erroneous and undetected outliers. This smaller sample size also presented impediments to post hoc analysis. Each of the group comparative analyses had insufficient sample

sizes to allow for statistically relevant results.

As a result of these limitations there is clearly an opportunity to return to this line of research and build on the foundations it has created. While the current investigation met all its required reliability and validity checks, it would still be desirable to find ways to support its generalizability claims and to increase the depth of the analysis through an expanded sample population. While these issues are a concern, they also represent opportunities for the research community to verify and expand our understanding of this emerging and important hacker phenomenon

6.5 Future Research

The first goal of this dissertation set out to establish the role of a select group of key intrinsic motivations and their role in how hackers identify the things that interest them and inspire them to discovery. The research made significant headway in establishing an understanding of the roles of mastery and curiosity in this process. Given the evidence provided in the qualitative research of this dissertation, future research should further explore the role of creativity in a hacker's decision making process. Given that the questions posed to the hackers in this research were to establish the roles these intrinsic drivers have in target selection, future research may also explore other ways creativity moulds the hacker psyche.

In parallel to the role of intrinsic motivation and hacker's task selection was the idea that the artifact also played a role in the hacker selection process. Task complexity was explored alongside the personality drivers and represented extrinsic motivation for a hacking task. How a hacker assesses task complexity was not clearly established in this

research. The role of this variable as well as task difficulty needs to be further investigated. According to Jordan & Taylor (1998) and Turkle (1984), a hacking task is not valuable if it is not unique, original and complete. How does complexity play into their definition of a hacking task. Throughout the open-ended questions, the concept of challenge was repeated over and over. This suggests that task characteristics of complexity in the hacker world have more depth to explore.

This research was novel in that it took two well-established theories (TRA and GDT) and placed them alongside each other to see if they were relevant to hackers and if there was any sort of interaction. The use of GDT in this research proved to be challenging as it created unnecessary and unproductive resistance among the participants due to their broader anxiety towards a negative public stereotype. While the connections discovered in this research relating to the roles and interactions of TRA and GDT are compelling, their might be benefit to studying these two concepts separately to enhance the scope of each theories' interaction with the broader hacker community.

6.6 Conclusion

This dissertation addressed an important gap in the research on hackers. It explored hacker motivation, demotivation and task selection. It did so by accessing actual hackers as Mahmood, Siponen, Straub, Rao, & Raghu, (2010) all identified as a gap in current security research. The study also used a novel research lens by looking at hacker motivation not as a function of utility but as a question of aesthetics. This novel lens approach opened opportunities to explore hacker behaviour by looking at the role context played in molding hackers' intentions. The study explored individual contextual

characteristics as well as task characteristics and situational characteristics. These all expanded the importance of context in IS research.

Ultimately this study did what it set out to do. It gave new insight into understanding how the intention of hackers to perform a hacking task is influenced by motivating and demotivating factors, and it added to the understanding how contextual factors of individual and task characteristics may influence the motivating and demotivating mediators of a hacker's intention to engaging in a hacking task.

References

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational behavior and human decision processes*, *50*(2), 179–211.

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, N.J.: Prentice-Hall.

Ajzen, I., Fishbein, M., & Wicker, A. W. (1973). Attitudinal and normative variables as predictors of specific behavior. *Journal of Personality and Social Psychology*, *27*(1), 41–57.

Ajzen, I., & Madden, T. (1986). Prediction of Goal-Directed Behavior : Attitudes , Intentions , and Perceived Behavioral Control. *Journal of Experimental Social Psychology*, *22*, 453–474.

Akter, S., Ambra, J. D., & Ray, P. (2013). Development and validation of an instrument to measure user perceived service quality of mHealth. *Information and Management*, *50*, 181–195.

Au, N., Ngai, E. W. T., & Cheng, T. C. E. (2008). Extending the Understanding of End User Information Systems Satisfaction Formation : An Equitable Needs Fulfillment Model Approach, *MIS Quarterly*, *32*(1), 43–66.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *16*(1), 74–94.

Bansal, A., & Arora, M. (2012). Ethical hacking and social security. *Radix international journal of reserch in social science*, *1*(11), 1–16.

Bernstein, I. H., & Nunnally, J. C. (1994). A catastrophe model for developing service satisfaction strategies. Journal of Marketing. In T. Oliva, R. Oliver, & I. MacMillan (Eds.), *Psychometric theory* (pp. 83–95). New York: McGraw-Hill.

Beveren, J. Van. (2001). A conceptual model of hacker development and motivations, *Journal of E-Business 1*(2), 1–9.

Brown, S., Dennis, A. R., & Venkatesh, V. (2010). Predicting Collaboration Technology Use: Integrating Technology Adoption and Collaboration Research. *Journal of Management Information Systems*, *27*(2), 9–54.

Campbell, D. J. (1988). Task Complexity: A Review and Analysis. *The Academy of Management Review*, *13*(1), 40.

Cazier, J. A., Medlin, B. D., & Wilson, E. V. (2007). The role of privacy risk in IT

acceptance: an empirical study. *International Journal of Information Security and Privacy.*, *1*(2), 61.

Chin, W. W. (1998). Issues and Opinion on Structural Equation Modeling. *MIS Quarterly*, *22*(1), 1.

Churchill Jr, G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research*, *16*(1), 64–73.

Conrad, J. (2012). Seeking help: The important role of ethical hackers. *Network Security*, *2012*(8), 5–8.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643–658.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, *20*(1), 79–98.

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems : theory and results* (Unpublished doctoral dissertation). Massachusetts Institute of Technology, Cambridge, MA

de Vries, H., Dijkstra, M., & Kuhlman, P. (1988). Self-efficacy: the third factor besides attitude and subjective norm as a predictor of behavioural intentions. *Health Education Research*, *3*(3), 273–282.

Detlor, B., Sproule, S., & Gupta, C. (2003). Pre-purchase online information seeking: Search versus browse. *J. Electron. Commerce Res.*, *4*(2), 72–84.

Dimoka, A., Hong, Y., & Pavlou, P. A. (2012). PHOS TAG PRoduct U Ncertainty in O Nline M Arkets :, *36*(X), 1–32.

Fay, K. (2010). *Encyclopedia of Research Design*. (N. J. Salkind, Ed.). Thousand Oaks: SAGE Publications, Inc.

Fishbein, M. (1975). *Belief, attitude, intention, and behavior : an introduction to theory and research*. (I. Ajzen, Ed.). Reading, Mass. ; Don Mills, Ontario: Addison-Wesley Pub. Co.

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equations with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, *18*(February), 39–50.

Gefen, D., & Straub, D. (2005). A Practical Guide to Factorial Validity Using Pls-Graph:

Tutorial and Annotated Example. *Communications of AIS*, *2005*(16), 91–109.

Gefen, D., Straub, D., & Boudreau, M.-C. (2000). Structural equation modeling and regression : guidelines for research practice, *Communications of the Association for Information Systems*, *4*(August).

Gel, Y. R., & Gastwirth, J. L. (2008). A robust modification of the Jarque-Bera test of normality. *Economics Letters*, *99*(1), 30–32.

George, D., & Mallery, P. (2003). *SPSS for Windows step by step: A simple guide and reference. 11.0 update* (4th ed.). Boston: Allyn & Bacon.

Ghani, J. a., & Deshpande, S. P. (1994). Task Characteristics and the Experience of Optimal Flow in Human—Computer Interaction. *Journal of Psychology*, *128*(4), 381–391.

Gibbs, J. P. (1975). *Crime, Punishment, and Deterrence*. New York: Elsevier Ltd.

Gibbs, J. P. (1986). Deterrence Theory and Research. In G.B. Melton (Ed.) *Nebraska Symposium on Motivation, 1985* (pp.87- 130). Lincoln: University of Nebraska Press.

Gliem, J. a, & Gliem, R. R. (2003). Calculating, Interpreting, and Reporting Cronbach's Alpha Reliability Coefficient for Likert-Type Scales,. *2003 Midwest Research to Practice Conference in Adult, Continuing, and Community Education*, 82–88.

Greenberg, A. (2015). Hackers Remotely Kill a Jeep on the Highway—With Me in It. Retrieved January 21, 2016, from http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems*, *28*(2), 203–236.

Hackett, R. (2015). What to know about the Ashley Madison hack. Retrieved from http://fortune.com/2015/08/26/ashley-madison-hack/

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. *The Journal of Marketing Theory and Practice*, *19*(2), 139–152.

Harvey, B. (1985). What is a Hacker ? Retrieved October 3, 2013, from http://www.cs.berkeley.edu/~bh/hacker.html

Help Net Security. (2016). General Motors invites hackers to report security flaws in their cars. Retrieved January 21, 2016, from http://www.netsecurity.org/secworld.php?id=19309

Help fund computing labs for girls in Afghanistan (2013, September 13). Retreived from https://www.raspberrypi.org/stories

Henseler, J., & Sarstedt, M. (2013). Goodness-of-fit indices for partial least squares path modeling. *Computational Statistics*, *28*(2), 565–580.

Holt, T. J. (2007). Subcultural Evolution? Examining the Influence of on- and Off-Line Experiences on Deviant Subcultures. *Deviant Behavior*, *28*(2), 171–198. http://doi.org/10.1080/01639620601131065

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2010). Social Learning and Cyber-Deviance: Examining the Importance of a Full Social Learning Model in the Virtual World. *Journal of Crime and Justice*, *33*(2), 31–61.

Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., & Dhillon, G. (2014). A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research*, *25*(1), 111–136.

Intel Security. (2014). *Net Losses: Estimating the Global Cost of Cybercrime*. Santa Clara: Unknown Author.

Jarupathirun, S., & Zahedi, F. (2007). Exploring the influence of perceptual factors in the success of web-based spatial DSS. *Decision Support Systems*, *43*(3), 933–951.

Jarque, C., & Bera, A. K. (1987). A Test for Normality of Observations and Regression Residuals. *International Statistical Review / Revue Internationale de Statistique*, *55*(2), 163–172.

Johns, G. (2006). The Essential Impact Of Context On Organizational Behavior. *Academy of Management Review*, *31*(2), 386–408.

Jordan, T. (2009). Hacking and Power: Social and technological determinism in the digital age. *First Monday*, *14*(7), 1–16.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *Sociological Review*, *46*(4), 757–780.

Kashdan, T. B. (2004). curiosity_VIA_chapter.pdf. In C. Peterson & M. E. P. Seligman (Eds.), *Character strengths and virtues: A handbook and classification* (pp. 125–141). Washington, D.C.: American Psychological Association.

Kashdan, T. B., Gallagher, M. W., Silvia, P. J., Winterstein, B. P., Breen, W. E., Terhar, D., & Steger, M. F. (2009). The Curiosity and Exploration Inventory-II: Development, Factor Structure, and Psychometrics. *Journal of Research in Personality*, *43*(6), 987–998.

Kock, N. (2010). Using WarpPLS in e-Collaboration Studies. *International Journal of E-Collaboration*, *7*(3), 1–13.

Kock, N. (2014). Advanced mediating effects tests, multi-group analyses, and measurement model assessments in PLS-based SEM. *International Journal of E-Collaboration*, *10*(1), 1–13.

Kock, N. (2015). *WarpPLS 5.0 User Manual* (5.0 ed., Vol. 1). Laredo, Texas: ScriptWarp Systems.

Kock, N., & Lynn, G. S. (2012). Lateral Collinearity and Misleading Results in Variance-Based SEM : An Illustration and Recommendations. *Journal of the Association for Information Systems*, *13*(7), 546–580.

Kulviwat, S., Bruner, G., Kumar, A., Nasco, S., & Clark, T. (2007). Toward a Unified Theory of Consumer Acceptance Technology. *Psychology & Marketing*, *24*(12), 1059–1084.

Lakhani, K. R., Wolf, B., Bates, J., & Dibona, C. (2002). The Boston Consulting Group Hacker Survey.

Lakhani, K. R., & Wolf, R. G. (2005). Why Hackers Do What They Do : Understanding Motivation and Effort in Free / Open Source Software Projects 1 By, 1–27.

Lindenberg, S. (2001). Intrinsic Motivation in a New Light, *54*(April), 317–342.

Mackenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral r esearch : Integrating new and existing techniques Summary of Steps for Scale Purification and Refinement. *MIS Quarterly*, *35*(2), 1–5.

Madden, T. j., Ellen, P. S., & Ajzen, I. (1992). A Comparison of the Theory of Planned Behavior and the Theory of Reasoned Action. *PSBP1*, *18*(1), 3 – 9.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. S. (2010). Moving toward black hat research in information systems security : An editorial introduction to the special issue. *MIS Quarterly*, *34*(3), 431–433.

Malkin, G., & Parker, T. L. (1993). *RFC 1392 - Internet Users Glossary*. Retrieved from http://tools.ietf.org/html/rfc1392

McGrath, J. E. (1983). G*roups : Interaction and performance (Vol.14)*. Englewood Cliffs, N.J.: Prentice-Hall.

McHugh, J. A. M., & Deek, F. P. (2005). An incentive system for reducing malware attacks. *Communications of the ACM*, *48*(6), 94-99.

Meyers, L. S., Gamst, G., & Guarino, A. J. (2006). *Applied Multivariate Research: Design and Interpretation*. Thousand Oaks, CA: Sage Publications.

Mick, D. G., & Fournier, S. (1998). Paradoxes of technology: consumer cognizance, emotions, and coping strategies. *Journal of Consumer Research*, *25*(2), 123–143.

Monecke, A., & Leisch, F. (2012). semPLS : Structural Equation Modeling Using Partial Least Squares. *Journal of Statistical Software*, *48*(3), 1–32.

Nakamura, Jeanne, & Csikszentmihalyi, M. (2002). The Concept of Flow. In C. R. Snyder & S. J. Lopez (Eds.), *Handbook of positive psychology* (pp. 89–105). New York, NY: Oxford University Press.

Naraine, R. (2011). Citigroup : Customer losses from hack attack reaches $2.7M. Retrieved August 26, 2012, from http://www.zdnet.com/blog/security/citigroup-customer-losses-from-hack-attack-reaches-2-7m/8921

Nikitina, S. (2012). Creativity in Hacker Culture. *The Journal of Popular Culture*, *45*(1), 133–153.

Novak, T., Hoffman, D., & Yung, Y. (2000). Measuring the customer experience in online environments: A structural modeling approach. *Marketing Science*, *19*(1), 22–42. Retrieved from http://philpapers.org/rec/WADCA

Raid, S. L. N., & Pedersen, J. M. (2012). An Updated Taxonomy for Characterizing Hackers According to Their Threat Properties, 81–86.

Reiss, S. (2004). Multifaceted Nature of Intrinsic Motivation : The Theory of 16 Basic Desires. *Review of General Psychology*, *8*(3), 179–193.

Rogers, M. (n.d.). A New Hacker Taxonomy.

Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation*, *3*(2), 97–102. http://doi.org/10.1016/j.diin.2006.03.001

Rousseau, D., & Fried, Y. (2001). Location , location , location : contextualizing organizational research Forces For and Against Contextualization. *Journal of Organizational Behavior*, *22*, 1–13.

Schulze, G. (2003). Deterrence versus intrinsic motivation : Experimental evidence on the determinants of corruptibility. *Economics of Governance*, 143–160.

Schumacher, T. (n.d.). White Hat Hacking.

Seebruck, R. (2015). A Typology of Hackers: Classifying Cyber Malfeasance using a

Weighted Arc Circumplex Model. *Digital Investigation*, *14*(14), 36–45.

Serrano, A. (2011). Cyber Crime Pays: A $114 Billion Industry. Retrieved August 26, 2012, from http://www.thefiscaltimes.com/Articles/2011/09/14/Cyber-Crime-Pays-A-114-Billion-Industry.aspx#page1

Shanteau, J. (1992). Competence in Experts : The Role of Task Characteristics. *Organizational Behavior and Human Decision Processes*, *53*(2), 252–266.

Sivo, S. a, Saunders, C., Chang, Q., & Jiang, J. J. (2006). How Low Should You Go? Low Response Rates and the Validity of Inference in IS Questionnaire Research. *Journal of the Association for Information Systems*, *7*(6), 351–413.

Spence, J. T., & Helmrelch, R. L. (1983). Achievement - Related Motives and Behaviors. In *Achievement and achievement motives: Psychological and sociological approaches* (pp. 7–74).

Sterling, B. (1994). *Law and Disorder on the Electronic Frontier* (ebook). Austin: Stuce Sterling. Retrieved from http://www.gutenberg.org/ebooks/101

Straub, D., & Weike, R. J. (2008). Coping With Systems Risk : Security Planning Models for Management Decision Making. *MIS Quarterly*, *22*(4), 441–469.

Taylor, S., & Todd, P. A. (1995). Understanding Information Technology Usage : A Test of Competing Models. *Information Systems Research*, *6*(2), 144–176.

Terry, D. J., Hogg, M. A., & White, K. M. (1999). The theory of planned behaviour : Self-identity , social identity and group norms. *The British Journal of Social Psychology*, *38*(Sep), 223-244.

The Making of Pi. Retreived from https://www.raspberrypi.org/about

The Mentor. (1986). Hacker's Manifesto. *Phrack Inc.*, *1*(7), 3 of 10. Retrieved from http://phrack.org/issues/7/3.html

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers and Security*, *24*, 472–484.

Turkle, S. (1984). *The Second Self* (Twentieth). Cambridge, MA: MIT Press.

Upton, L. (2015). Five Million Sold. Retrieved January 21, 2015, from https://www.raspberrypi.org/blog/five-million-sold/

Venkatesh, V. (2012). Consumer Acceptance and Use of Information Technology : Extending The Unified Theory. *MIS Quarterly*, *36*(1), 157–178.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: toward a unified view. *MIS Quarterly*, *27*(3), 425–478.

Vinzi, V. E., Chin, W. W., Henseler, J., & Wang, H. (2010). *Handbook of Partial Least Squares*. (W. W. Chin & H. Wang, Eds.). London: Springer.

Voiskounsky, A. E., & Smyslova, O. V. (2003). Flow-based model of computer hackers' motivation. *Cyberpsychology & Behavior : The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, *6*(2), 171–80.

Warshaw, P. R., & Davis, F. D. (1985). The Accuracy of Behavioral Intention Versus Behavioral Expectation for Predicting Behavioral Goals. *Journal of Psychology*, *119*(6), 599.

Wetzels, M., Odekerken-Schröder, G., & van Oppen, C. (2009). Using PLS Path Modeling For Assessing Hierarchical Construct Models : Guidelines and Empirical Illustration. *MIS Quarterly*, *33*(1), 177–195.

Whetten, David A. (2009). An examination of the interface between context and theory applied to the study of chinese organizations. *Management and Organization Review, 5(1), 29-55.*

Wikipedia Contributors. (2016). Anonymous (group). Retrieved January 21, 2016, from https://en.wikipedia.org/wiki/Anonymous_%28group%29

Yamaguchi, M. (2011). Sony PlayStation Network Hack To Cost $ 170 Million. Retrieved August 26, 2012, from http://www.huffingtonpost.com/2011/05/23/sony-playstation-network-hack-cost_n_865432.html

Young, R., & Zhang, L. (2007). Illegal computer hacking : An assessment of factors that encourage and deter the behavior. *Journal of Information Privacy & Security*, *3*, 33–52.

Zigurs, L., & Buckland, B. (1998). A Theory of Task/Technology Fit and Group Support Systems Effectiveness. *MIS Quarterly*, *22*(3), 313–334.

Appendix A: MREB Clearance Certificate

McMaster University

McMaster University Research Ethics Board (MREB)

c/o Research Office for Administrative Development and Support, MREB Secretariat, GH-305, e-mail: ethicsoffice@mcmaster.ca

CERTIFICATE OF ETHICS CLEARANCE TO INVOLVE HUMAN PARTICIPANTS IN RESEARCH

Application Status: New ☑ **Addendum** ☐ **Project Number:** 2014 169

TITLE OF RESEARCH PROJECT:

Motivation of Hacker Activities

Faculty Investigator(s)/ Supervisor(s)	Dept./Address	Phone	E-Mail
M. Head	Business	24435	headm@mcmaster.ca
Student Investigator(s)	**Dept./Address**	**Phone**	**E-Mail**
K. Owen	Business	26195	owenkd@mcmaster.ca

The application in support of the above research project has been reviewed by the MREB to ensure compliance with the Tri-Council Policy Statement and the McMaster University Policies and Guidelines for Research Involving Human Participants. The following ethics certification is provided by the MREB:

☐ The application protocol is cleared as presented without questions or requests for modification.

☑ The application protocol is cleared as revised without questions or requests for modification.

☐ The application protocol is cleared subject to clarification and/or modification as appended or identified below:

COMMENTS AND CONDITIONS: Ongoing clearance is contingent on completing the annual completed/status report. A "Change Request" or amendment must be made and cleared before any alterations are made to the research.

Reporting Frequency:	Annual: Sep-23-2015	Other:

Date: Sep-23-2014 **Vice Chair, C. Anderson:**

Appendix B: Letter of Consent to Group Organizer

Dear Sir/Madam,

My name is Kenneth Owen, a McMaster University PhD student, doing research to understand what motivates hackers. I found your organization through Google and I am hoping you and your members would assist me in my research by filling out a short survey.

A hacker is a person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The true hacker can't just sit around all night; he or she must pursue some hobby with dedication and flair.

The goal of this research is to gain insight into what stimuli may motivate a hacker in selecting a specific hack.

Please let me know if you are willing to send an invitation to your members to participate in my survey. It should take them no more than 10 to 15 minutes to complete. All the information is collected anonymously and is kept confidential.

If you are willing to participate I will send you an e-mail template and ask that you please forward the information to your members.

If you are interested in getting more information about taking part in this study please contact me at owenkd@mcmaster.ca **or by phone at 905-525-9140 Ext: 26195**

Ken and Dr. Head can be reached via the following methods:

Principal Investigator:
Kenneth D. Owen
DeGroote School of Business (DSB A211)
McMaster University
Hamilton, Ontario, Canada
(905) 525-9140 Ext.26195
E-mail: owenkd@mcmaster.ca

Faculty Supervisor:
Dr. Milena Head
DeGroote School of Business (DSB A206)
McMaster University
Hamilton, Ontario, Canada
(905) 525-9140 Ext.24435
E-mail: headm@mcmaster.ca

In addition, this study has been reviewed and cleared by the McMaster Research Ethics Board. If you have questions or concerns about your rights as a participant or about the way the study is being conducted you may contact:

McMaster Research Ethics Board Secretariat
Telephone: (905) 525-9140 ext. 23142
Gilmour Hall – Room 305 (ROADS)
E-mail: ethicsoffice@mcmaster.ca

Sincerely,

Ken Owen

Appendix C: Original Survey Questions with Consent

Test 1

There are 27 questions in this survey

Preamble and Consent

Preamble Statement

This survey is administered by Kenneth Owen At McMaster University. The purpose of the survey is to examine the relationship between intrinsic personal motivators and how task complexity effects how hackers select the projects they wish to work on. **Information gathered during this survey will be written up as a PhD dissertation.**

To learn more about the survey and the researcher's study, particularly in terms of any associated risks or harms associated with the survey, how confidentiality and anonymity will be handled, withdrawal procedures, or how to obtain information about the survey's results, please read the accompanying letter of information.

This survey should take approximately 10-15 minutes long to complete. People filling out this survey must be 18 years of age or older.

To participate in this survey you must see yourself as a hacker. This research defines a hacker as,

A hacker is a person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The true hacker can't just sit around all night; he must pursue some hobby with dedication and flair.

This survey is part of a study that has been reviewed and cleared by the McMaster Research Ethics Board (MREB). The MREB protocol number associated with this survey is [insert the MREB protocol number, e.g. MREB 2012 185].

You are free to complete this survey or not. If you have any concerns or questions about your rights as a participant or about the way the study is being conducted, please contact:

McMaster Research Ethics Secretariat
Telephone 1-(905)525-9140 ext. 23142
c/o Research Office for Administration, Development and Support (ROADS)
E-mail: ethicsoffice@mcmaster.ca

Consent to Participate

Having read the above, I understand that by clicking the "Yes" button below, I agree to take part in this study under the terms and conditions outlined in the accompanied letter of information.
*

Please choose only one of the following:

- ○ Yes, I agree to participate
- ○ No, I do not agree to participate

TRA

Take a moment to think of a recent hacking activity that you have considered doing but have not yet tried to execute

Please choose the appropriate response for each item:

	Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
I intend to do this hack in the next six months	○	○	○	○	○
I predict I would do this hack in the next six months	○	○	○	○	○
I plan to do this hack in the next six months	○	○	○	○	○

Please choose the appropriate response for each item:

	Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
Doing this hack is a good idea.	○	○	○	○	○
I like the idea of doing this hack.	○	○	○	○	○
Doing this hack will be pleasant.	○	○	○	○	○

Please choose the appropriate response for each item:

	Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
People who influence my behavior think that I should do this hack.	○	○	○	○	○
People who are important to me think that I should do this hack.	○	○	○	○	○

GDT

Continuue to think about that same recent potencial hacking activity

Pleas e choose the appropriate respons e for each item:

	Strongly Dis agree	Dis agree	Neither agree nor dis agree	Agree	Strongly Agree	
If I did this hack I would probably get caught	○	○	○	○	○	○
If I get caught doing this hack I will be s everely punis hed	○	○	○	○	○	○

TASK

Continuue to think about that same recent potencial hacking activity

Please choose the appropriate response for each item:

	Very Complex	Complex	Neither complex nor simple	Simple	Very Simple
This task is	○	○	○	○	○

Please choose the appropriate response for each item:

	Very complicated	Complicated	Neither Complecated nor straight forward	Straight forward	Very straight forward
This Task is	○	○	○	○	○

INTRINSIC

Please choose the appropriate response for each item:

	Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree			
I would rather do something at which I feel confident and relaxed then something which is challenging and difficult	○	○	○	○	○	○	○	○
When a group I belong to plans an activity, I would rather direct it myself than just help out and have someone else organize it.	○	○	○	○	○	○	○	○
I would rather learn easy fun games that difficult thought games.	○	○	○	○	○	○	○	○
If I am not good at something, I would rather keep struggling to master it than move on to something I may be good at.	○	○	○	○	○	○	○	○
Once I undertake a task I persist.	○	○	○	○	○	○	○	○
I prefer to work in situations that require a high level of skill.	○	○	○	○	○	○	○	○
I more often attempt tasks that I am not sure I can do than tasks that I believe I can do.	○	○	○	○	○	○	○	○
I like to be busy all the time.	○	○	○	○	○	○	○	○

Please choose the appropriate response for each item:

	Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
I actively seek as much information as I can in new situations	○	○	○	○	○
I am the type of person who really enjoys the uncertainty of everyday life	○	○	○	○	○
I am at my best when doing something that is complex or challenging	○	○	○	○	○
Everywhere I go, I am out looking for new things or experiences	○	○	○	○	○
I view challenging situations as an opportunity to grow and learn	○	○	○	○	○
I like to do things that are a little frightening	○	○	○	○	○
I am always looking for experiences that challenge how I think about myself and the world	○	○	○	○	○
I prefer jobs that are excitingly unpredictable	○	○	○	○	○
I frequently seek out opportunities to challenge myself and grow as a person	○	○	○	○	○
I am the kind of person who embraces unfamiliar people, events, and places	○	○	○	○	○

When you get interested in something, how much attention do you pay to the details?

Please choose only one of the following:

- ○ I do not pay much attention to the details.
- ○ I pay attention to some of the details.
- ○ I pay attention to all of the details.

How do you approach a complex task?

Please choose only one of the following:

- ○ I come up with a single approach.
- ○ I may be able to come up with a few approaches.
- ○ I will be able to come up with a variety of approaches.

How well do you express your ideas?

Please choose only one of the following:

- ○ I have difficulty expressing my ideas well.
- ○ I am able to express some of my ideas well.
- ○ I am able to express all of my ideas well.

What would you do if you were solving a difficult problem?

Please choose only one of the following:

- ○ I would ask an expert or someone else to help me.
- ○ I would read a book on the subject.
- ○ I would try a number of different ways to come up with my own answer.

Open Ended

The next few questions are open ended.

Please share as much detail and as many experiences as you can.

Remember, we want to protect your identity so avoid including any information that might identify you.

What is it about hacking that you enjoy? How does it make you feel to hack something?

Please write your answer here:

Outline some of the personality or character traits you believe are important to becoming a good hacker.

Please write your answer here:

To become a good hacker is it necessary to take risks?

What sorts of risks are important to learning to hack?

Please write your answer here:

What would make a hack less desireable to you?

Please write your answer here:

Demographics

Please take just a few more minutes to tell us a bit about yourself.

How old are you?

Please choose only one of the following:

- ○ 18 to 27
- ○ 28 to 37
- ○ 38 to 47
- ○ 48 to 57
- ○ 58 to 67
- ○ over 68

How much education have you completed

Please choose only one of the following:

- ○ Some highschool
- ○ Hichschool diploma
- ○ Some technicalschool
- ○ Technical School Diploma
- ○ Some Undergrad University
- ○ Undergrad University Degree
- ○ Some University Graduate Degree
- ○ A University Graduate Degree

How do you identify your gender?

Please choose only one of the following:

- ○ Male
- ○ Female
- ○ Trans-Gendered
- ○ prefer not to say

What country do you live in?

Please choose only one of the following:

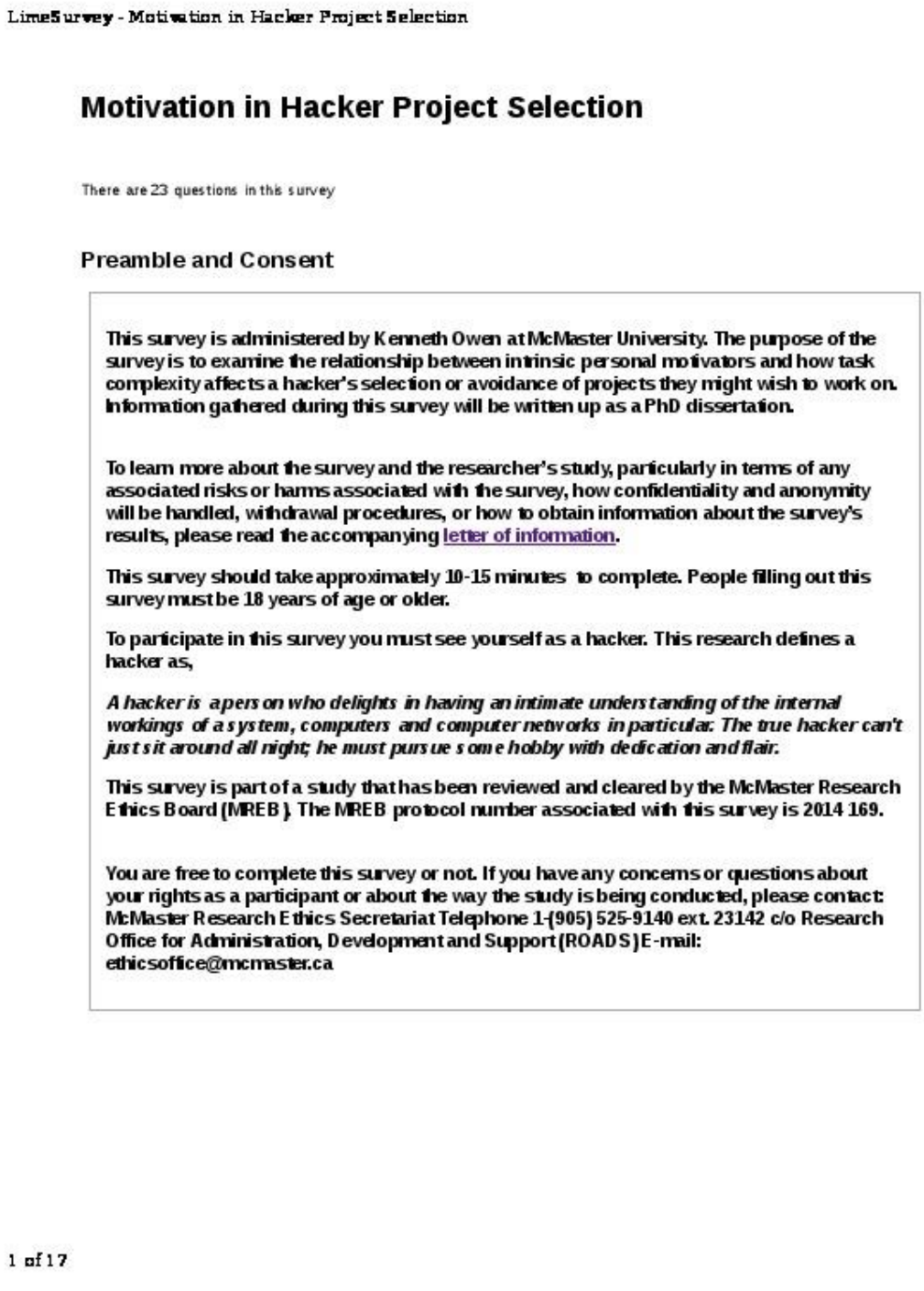
○ Predefined dropdown of countries

Thank you for taking this survey. Your answers are a valuable part of this research.

08-11-2014 – 00:11

Submit your survey.
Thank you for completing this survey.

Appendix D: Modified Survey Questions with Consent



LimeSurvey - Motivation in Hacker Project Selection

Motivation in Hacker Project Selection

There are 23 questions in this survey

Preamble and Consent

This survey is administered by Kenneth Owen at McMaster University. The purpose of the survey is to examine the relationship between intrinsic personal motivators and how task complexity affects a hacker's selection or avoidance of projects they might wish to work on. Information gathered during this survey will be written up as a PhD dissertation.

To learn more about the survey and the researcher's study, particularly in terms of any associated risks or harms associated with the survey, how confidentiality and anonymity will be handled, withdrawal procedures, or how to obtain information about the survey's results, please read the accompanying letter of information.

This survey should take approximately 10-15 minutes to complete. People filling out this survey must be 18 years of age or older.

To participate in this survey you must see yourself as a hacker. This research defines a hacker as,

A hacker is a person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The true hacker can't just sit around all night; he must pursue some hobby with dedication and flair.

This survey is part of a study that has been reviewed and cleared by the McMaster Research Ethics Board (MREB). The MREB protocol number associated with this survey is 2014 169.

You are free to complete this survey or not. If you have any concerns or questions about your rights as a participant or about the way the study is being conducted, please contact: McMaster Research Ethics Secretariat Telephone 1-(905) 525-9140 ext. 23142 c/o Research Office for Administration, Development and Support (ROADS) E-mail: ethicsoffice@mcmaster.ca

1 of 17

LimeSurvey - Motivation in Hacker Project Selection

Consent to Participate

Having read the above, I understand that by clicking the "Yes" button below, I agree to take part in this study under the terms and conditions outlined in the accompanied letter of information. I also understand that I may withdraw at any time by closing my browser window
*

Please choose only one of the following:

- ○ Yes, I agree to participate
- ○ No, I do not agree to participate

2 of 17

LimeSurvey - Motivation in Hacker Project Selection

INTRINSIC

Please choose the appropriate response for each item:

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I would rather do something at which I feel confident and relaxed then something which is challenging and difficult	○	○	○	○	○
When a group I belong to plans an activity, I would rather direct it myself than just help out and have someone else organize it.	○	○	○	○	○
I would rather learn easy fun games than difficult thought games.	○	○	○	○	○
If I am not good at something, I would rather keep struggling to master it than move on to something I may be good at.	○	○	○	○	○
Once I undertake a task I persist.	○	○	○	○	○
I prefer to work in situations that require a high level of skill.	○	○	○	○	○
I more often attempt tasks that I am not sure I can do than tasks that I believe I can do.	○	○	○	○	○
I like to be busy all the time.	○	○	○	○	○

3 of 17

LimeSurvey - Motivation in Hacker Project Selection

Please choose the appropriate response for each item:

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I actively seek as much information as I can in new situations	○	○	○	○	○
I am the type of person who really enjoys the uncertainty of everyday life	○	○	○	○	○
I am at my best when doing something that is complex or challenging	○	○	○	○	○
Everywhere I go, I am out looking for new things or experiences	○	○	○	○	○
I view challenging situations as an opportunity to grow and learn	○	○	○	○	○
I like to do things that are a little frightening	○	○	○	○	○
I am always looking for experiences that challenge how I think about myself and the world	○	○	○	○	○
I prefer jobs that are excitingly unpredictable	○	○	○	○	○
I frequently seek out opportunities to challenge myself and grow as a person	○	○	○	○	○
I am the kind of person who embraces unfamiliar people, events, and places	○	○	○	○	○

4 of 17

LimeSurvey - Motivation in Hacker Project Selection

When you get interested in something, how much attention do you pay to the details?

Please choose only one of the following:

- ○ I do not pay much attention to the details.
- ○ I pay attention to some of the details.
- ○ I pay attention to all of the details.

How do you approach a complex task?

Please choose only one of the following:

- ○ I come up with a single approach.
- ○ I may be able to come up with a few approaches.
- ○ I will be able to come up with a variety of approaches.

How well do you express your ideas?

Please choose only one of the following:

- ○ I have difficulty expressing my ideas well.
- ○ I am able to express some of my ideas well.
- ○ I am able to express all of my ideas well.

What would you do if you were solving a difficult problem?

Please choose only one of the following:

- ○ I would ask an expert or someone else to help me.
- ○ I would read a book on the subject.
- ○ I would try a number of different ways to come up with my own answer.

5 of 17

LimeSurvey - Motivation in Hacker Project Selection

TASK

Take a moment to think of a recent hacking activity that you have considered doing but have not yet tried to execute. Please indicate your assessment of each of the following statements.

Please choose the appropriate response for each item:

	Very complex	Complex	Neither complex nor simple	Simple	Very simple
Doing this task is	○	○	○	○	○

Please choose the appropriate response for each item:

	Very complicated	Complicated	Neither complicated nor straight forward	Straight forward	Very straight forward
This task is	○	○	○	○	○

6 of 17

LimeSurvey - Motivation in Hacker Project Selection

TRA

Take a moment to think of a recent hacking activity that you have considered doing but have not yet tried to execute.

Please indicate your agreement/disagreement to each of the following statements. Please note that some statements may seem very similar. This has been purposely done for validity checking or to capture some subtle nuances.

Please choose the appropriate response for each item:

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
I plan to do this hack in the next six months	○	○	○	○	○
I like the idea of doing this hack.	○	○	○	○	○
People who influence my behavior think that I should do this hack.	○	○	○	○	○
Doing this hack is a good idea.	○	○	○	○	○
If I did this hack I will probably be noticed / discovered	○	○	○	○	○
I predict I will do this hack in the next six months	○	○	○	○	○
Doing this hack will be pleasant.	○	○	○	○	○
People who are important to me think that I should do this hack.	○	○	○	○	○
I intend to do this hack in the next six months	○	○	○	○	○
If I am noticed doing this hack I will be reprimanded / punished	○	○	○	○	○

7 of 17

LimeSurvey - Motivation in Hacker Project Selection

Open Ended

The next few Questions are open ended.

Please share as much detail and as many experiences as you can.

Remember, we want to protect your identity s o avoid including any information that might identify you.

What is it about hacking that you enjoy? How does it make you feel to hack something?

Pleas e write your ans w er here:

Outline some of the personality or charactor traits you believe are important to becoming a good hacker.

Pleas e write your ans w er here:

8 of 17

LimeSurvey - Motivation in Hacker Project Selection

To become a good hacker is it necessary to take risks? What sorts of risks are important to learning to hack?

Please write your answer here:

What would make a hack less desireable to you?

Please write your answer here:

9 of 17

LimeSurvey - Motivation in Hacker Project Selection

Demographics

Please take just a few more minutes to tell us a bit about yourself.

How old are you?

Please choose only one of the following:

- 18 to 27
- 28 to 37
- 38 to 47
- 48 to 57
- 58 to 67
- over 68

How much education have you completed

Please choose only one of the following:

- Some highschool
- Highschool diploma
- Some technical school
- Technical School Diploma
- Some Undergrad University
- Undergrad University Degree
- Some University Graduate Degree
- A University Graduate Degree

How do you identify your gender?

Please choose only one of the following:

- Male
- Female
- Trans-Gender
- Prefer not to say

16 of 17

LimeSurvey - Motivation in Hacker Project Selection

What country do you live in?

Please choose only one of the following:

- Afghanistan
- Albania
- Algeria
- Andorra
- Angola
- Antigua & Deps
- Argentina
- Armenia
- Australia
- Austria
- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Belize
- Benin
- Bhutan
- Bolivia
- Bosnia Herzegovina
- Botswana
- Brazil
- Brunei
- Bulgaria
- Burkina
- Burundi
- Cambodia
- Cameroon
- Canada
- Cape Verde

11 of 17

- Central African Rep
- Chad
- Chile
- China
- Colombia
- Comoros
- Congo
- Congo
- Costa Rica
- Croatia
- Cuba
- Cyprus
- Czech Republic
- Denmark
- Djibouti
- Dominica
- Dominican Republic
- East Timor
- Ecuador
- Egypt
- El Salvador
- Equatorial Guinea
- Eritrea
- Estonia
- Ethiopia
- Fiji
- Finland
- France
- Gabon
- Gambia
- Georgia
- Germany
- Ghana
- Greece
- Grenada

- Guatemala
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Honduras
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Israel
- Italy
- Ivory Coast
- Jamaica
- Japan
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Korea North
- Korea South
- Kosovo
- Kuwait
- Kyrgyzstan
- Laos
- Latvia
- Lebanon
- Lesotho
- Liberia
- Libya
- Liechtenstein
- Lithuania

- Luxembourg
- Macedonia
- Madagascar
- Malawi
- Malaysia
- Maldives
- Mali
- Malta
- Marshall Islands
- Mauritania
- Mauritius
- Mexico
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Morocco
- Mozambique
- Myanmar
- Namibia
- Nauru
- Nepal
- Netherlands
- New Zealand
- Nicaragua
- Niger
- Nigeria
- Norway
- Oman
- Pakistan
- Palau
- Panama
- Papua New Guinea
- Paraguay

- Peru
- Philippines
- Poland
- Portugal
- Qatar
- Romania
- Russian Federation
- Rwanda
- St Kitts & Nevis
- St Lucia
- Saint Vincent & the Grenadines
- Samoa
- San Marino
- Sao Tome & Principe
- Saudi Arabia
- Senegal
- Serbia
- Seychelles
- Sierra Leone
- Singapore
- Slovakia
- Slovenia
- Solomon Islands
- Somalia
- South Africa
- South Sudan
- Spain
- Sri Lanka
- Sudan
- Suriname
- Swaziland
- Sweden
- Switzerland
- Syria
- Taiwan

- Tajikistan
- Tanzania
- Thailand
- Togo
- Tonga
- Trinidad & Tobago
- Tunisia
- Turkey
- Turkmenistan
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- United States
- Uruguay
- Uzbekistan
- Vanuatu
- Vatican City
- Venezuela
- Vietnam
- Yemen
- Zambia
- Zimbabwe
-

LimeSurvey - Motivation in Hacker Project Selection

Thank you for taking the time to fill out this survey.
Your answers are a valuable part of this research.

We are still a long way from having enough data.

If you can think on any one else who fits our definition of a hacker and might be willing tofill out the survey as well please forward this link to them and ask them to lend a hand and support this intresting research project.

https://surveys.mcmaster.ca/limesurvey/index.php/726651/lang-en

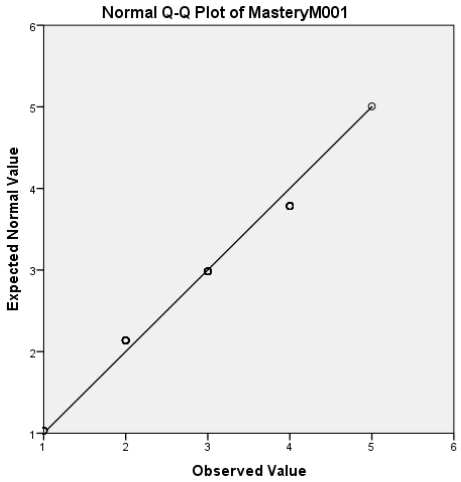
keep an eye out for the results of this research as a working paper will be posted on the McMaster eBusiness Research Centre (MeRC) website in the spring of 2015 once the dissertation is defended.
(http://merc.mcmaster.ca/working-papers/index.html

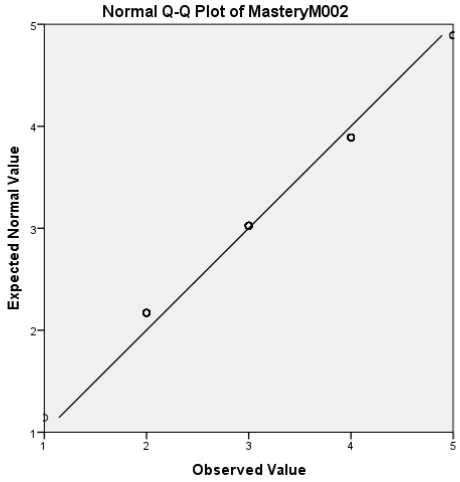
Once again thank you for your time and effort.

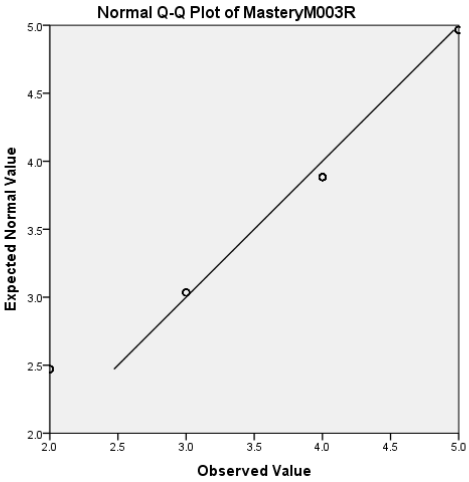
Submit your survey.
Thank you for completing this survey.

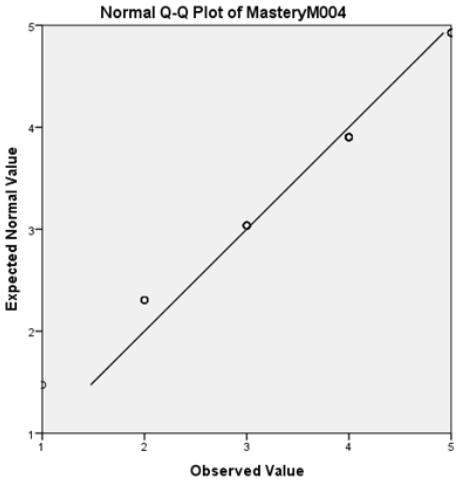
17 of 17

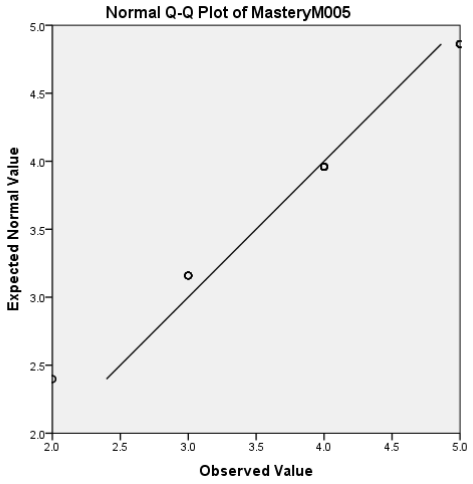
Appendix E: QQ Plots

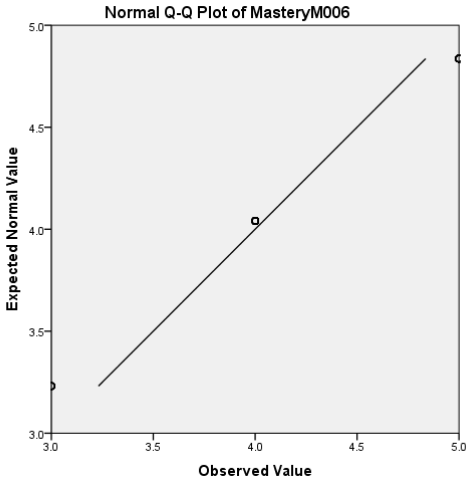


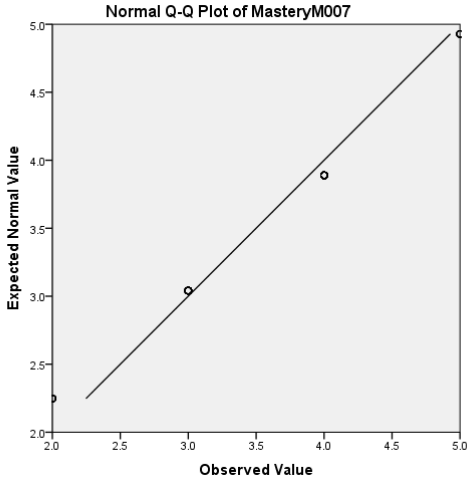


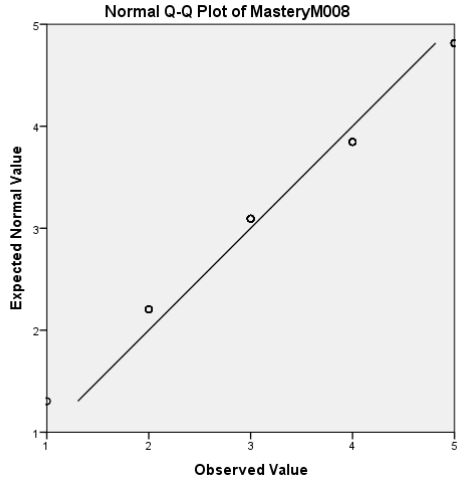


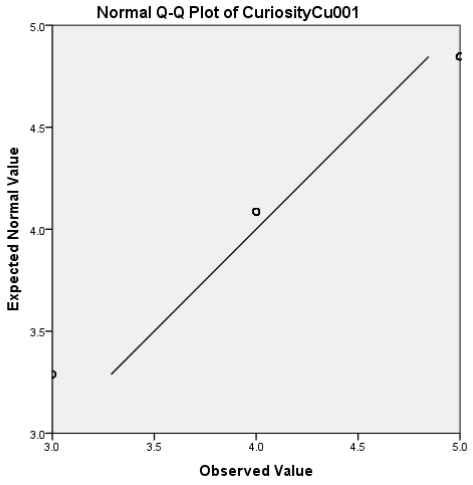


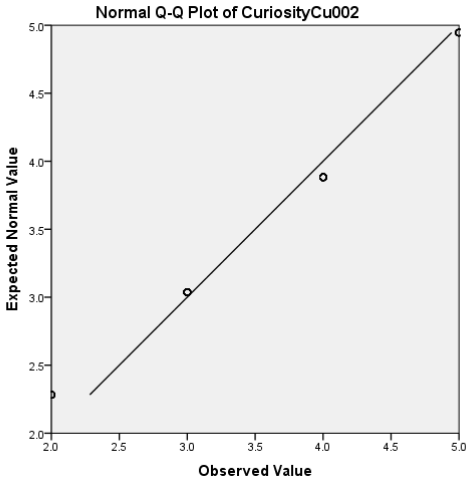

Normal Q-Q Plot of MasteryM005
Expected Normal Value
Observed Value

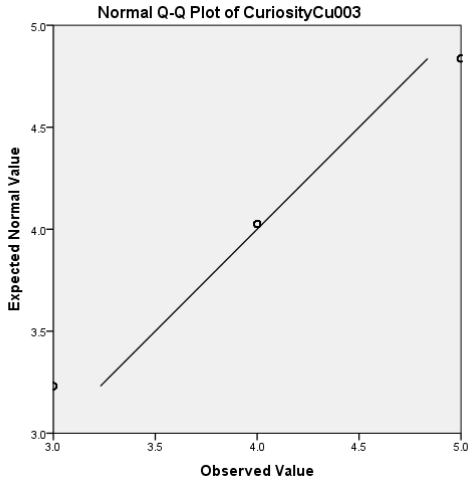

Normal Q-Q Plot of MasteryM006
Expected Normal Value
Observed Value

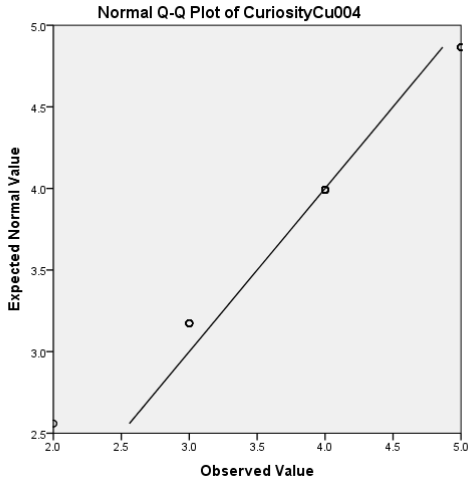

Normal Q-Q Plot of MasteryM007
Expected Normal Value
Observed Value

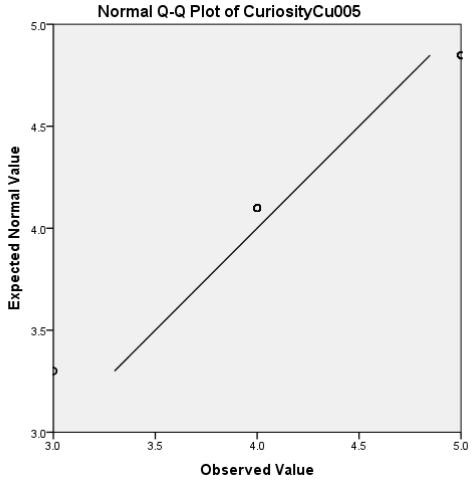

Normal Q-Q Plot of MasteryM008
Expected Normal Value
Observed Value

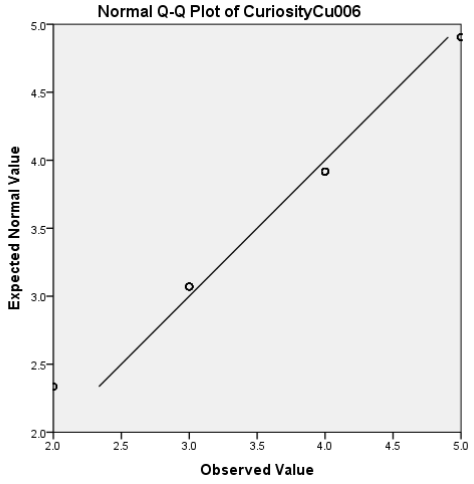

Normal Q-Q Plot of CuriosityCu001
Expected Normal Value
Observed Value

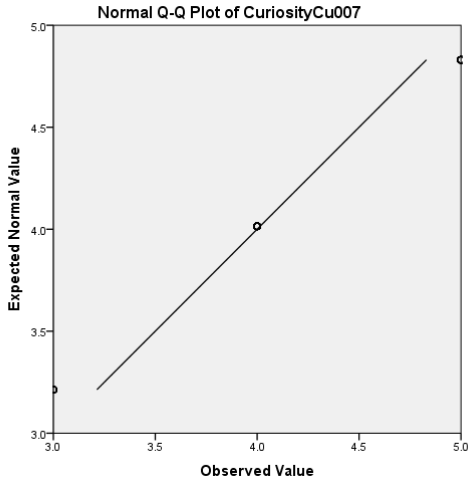

Normal Q-Q Plot of CuriosityCu002
Expected Normal Value
Observed Value

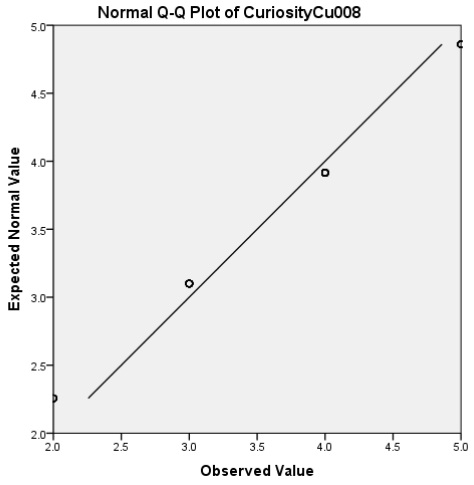

Normal Q-Q Plot of CuriosityCu003
Expected Normal Value
Observed Value
5.0
4.5
4.0
3.5
3.0

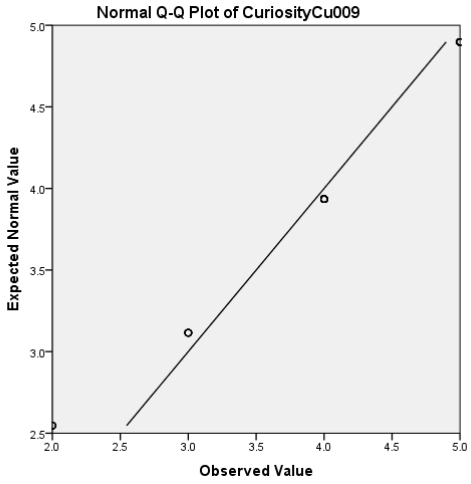

Normal Q-Q Plot of CuriosityCu004
Expected Normal Value
Observed Value
5.0
4.5
4.0
3.5
3.0
2.5
2.0

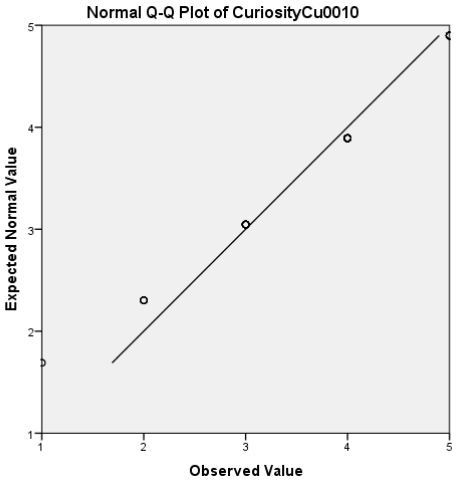

Normal Q-Q Plot of CuriosityCu005
Expected Normal Value
Observed Value
5.0
4.5
4.0
3.5
3.0

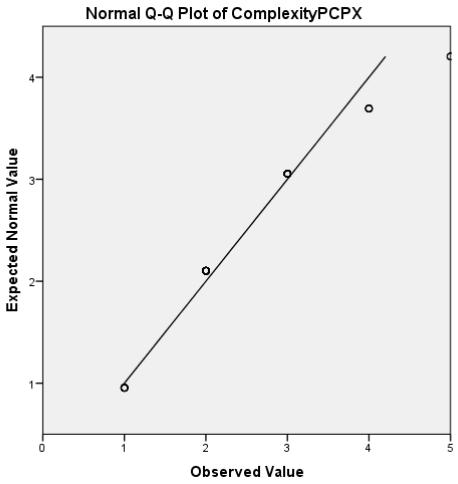

Normal Q-Q Plot of CuriosityCu006
Expected Normal Value
Observed Value
5.0
4.5
4.0
3.5
3.0
2.5
2.0

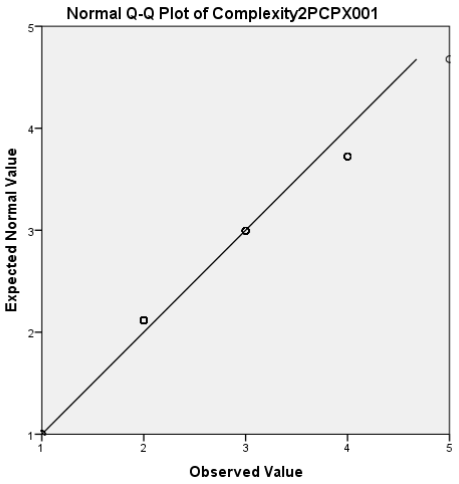

Normal Q-Q Plot of CuriosityCu007
Expected Normal Value
Observed Value
5.0
4.5
4.0
3.5
3.0

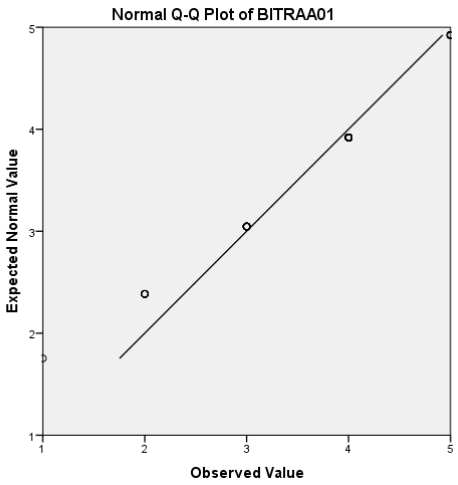

Normal Q-Q Plot of CuriosityCu008
Expected Normal Value
Observed Value
5.0
4.5
4.0
3.5
3.0
2.5
2.0

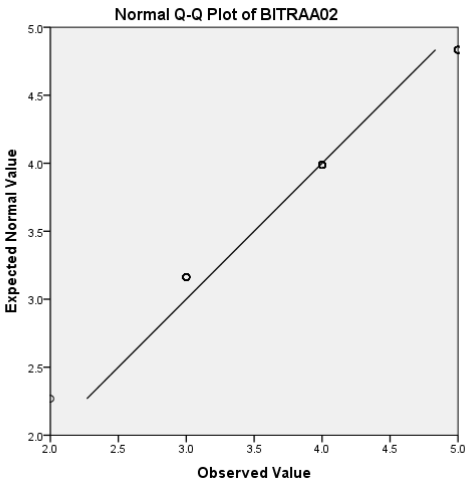

Normal Q-Q Plot of CuriosityCu009
Expected Normal Value
Observed Value

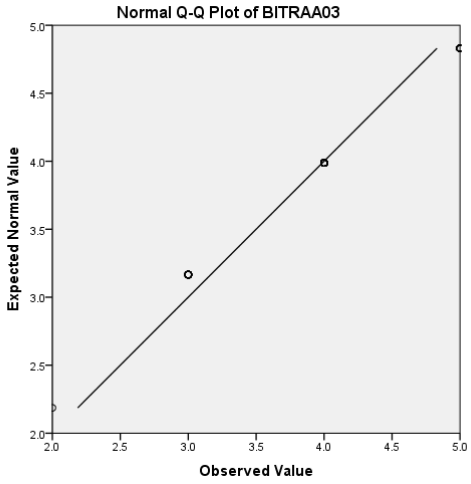

Normal Q-Q Plot of CuriosityCu0010
Expected Normal Value
Observed Value

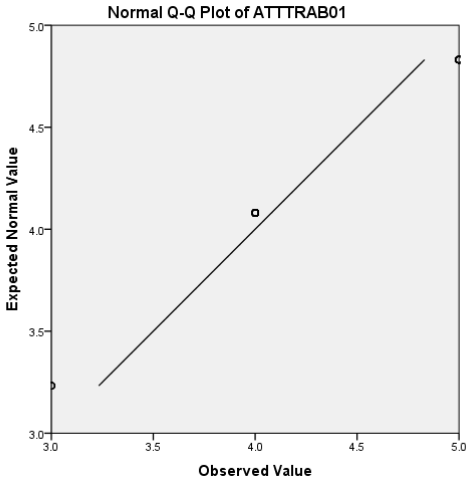

Normal Q-Q Plot of ComplexityPCPX
Expected Normal Value
Observed Value

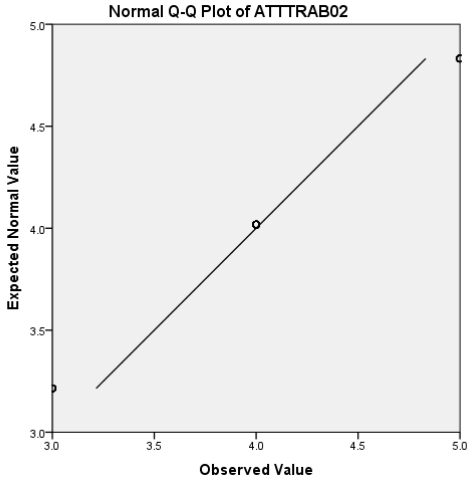

Normal Q-Q Plot of Complexity2PCPX001
Expected Normal Value
Observed Value

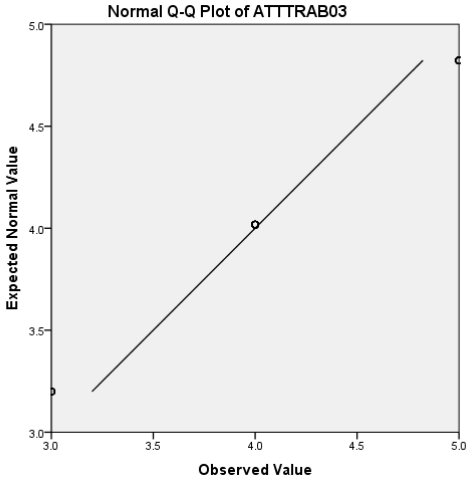

Normal Q-Q Plot of BITRAA01
Expected Normal Value
Observed Value

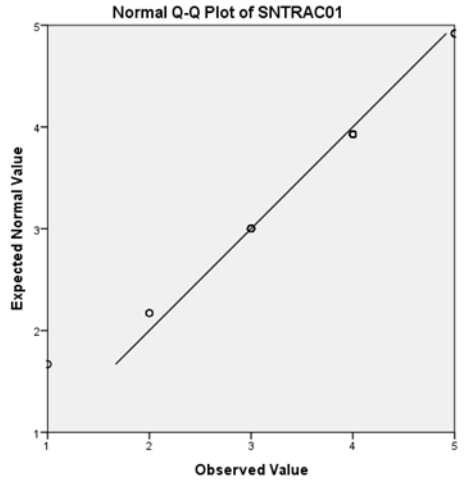

Normal Q-Q Plot of BITRAA02
Expected Normal Value
Observed Value

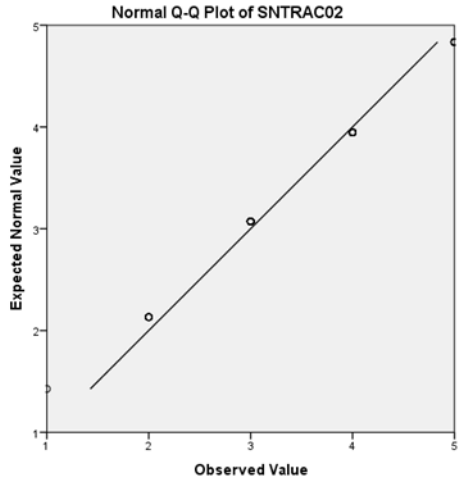

Normal Q-Q Plot of BITRAA03
Expected Normal Value
Observed Value
5.0
4.5
4.0
3.5
3.0
2.5
2.0

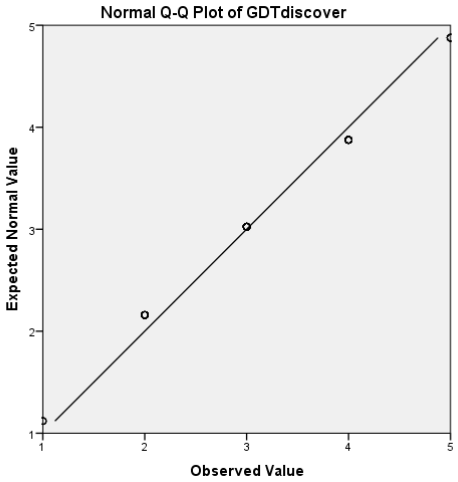

Normal Q-Q Plot of ATTTRAB01
Expected Normal Value
Observed Value
5.0
4.5
4.0
3.5
3.0

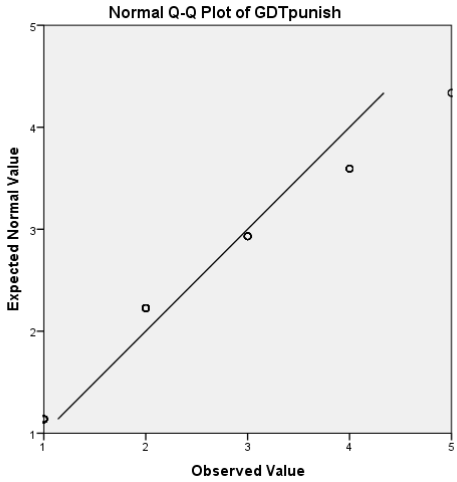

Normal Q-Q Plot of ATTTRAB02
Expected Normal Value
Observed Value
5.0
4.5
4.0
3.5
3.0


Normal Q-Q Plot of ATTTRAB03
Expected Normal Value
Observed Value
5.0
4.5
4.0
3.5
3.0

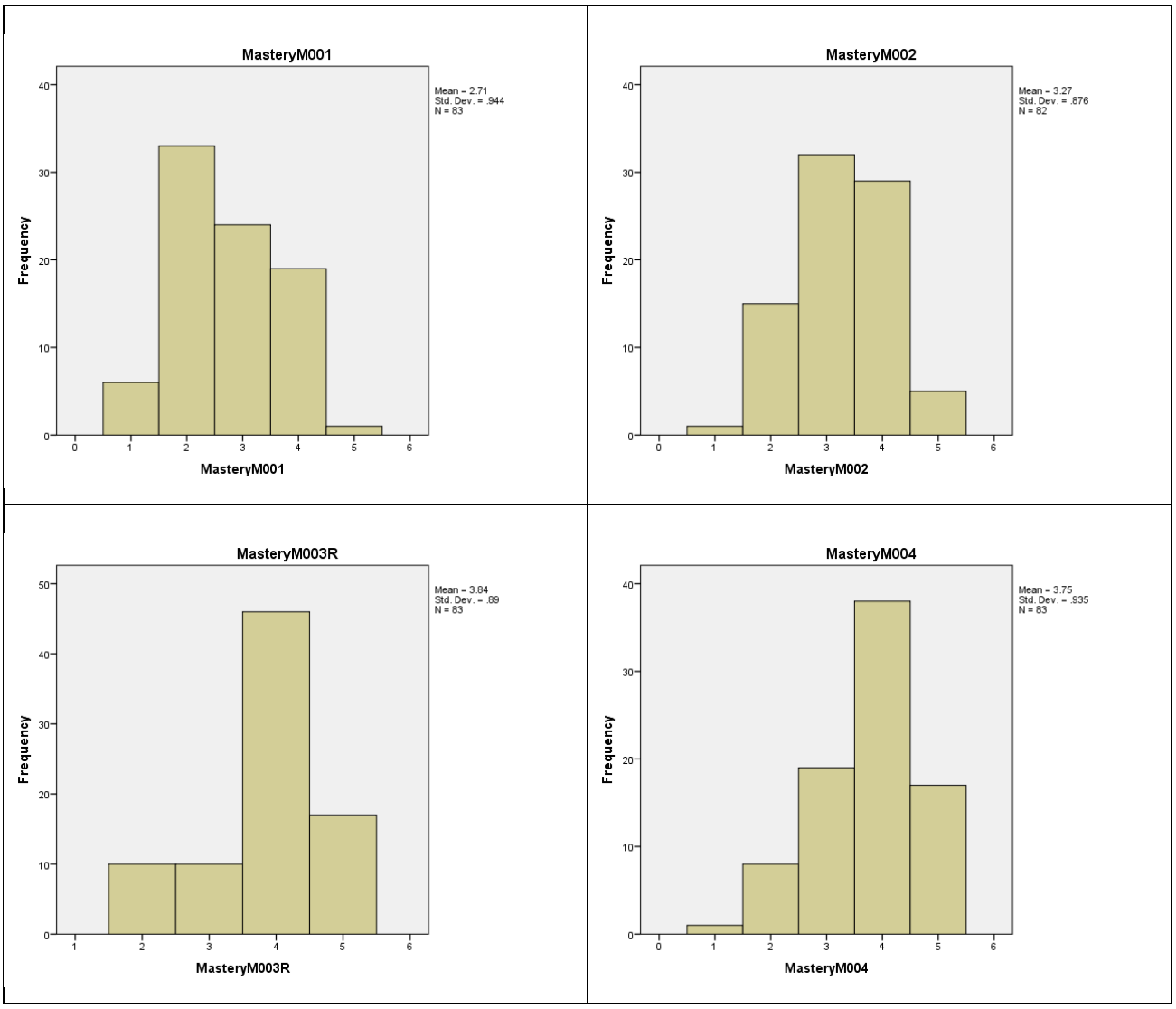

Normal Q-Q Plot of SNTRAC01
Expected Normal Value
Observed Value
5
4
3
2
1

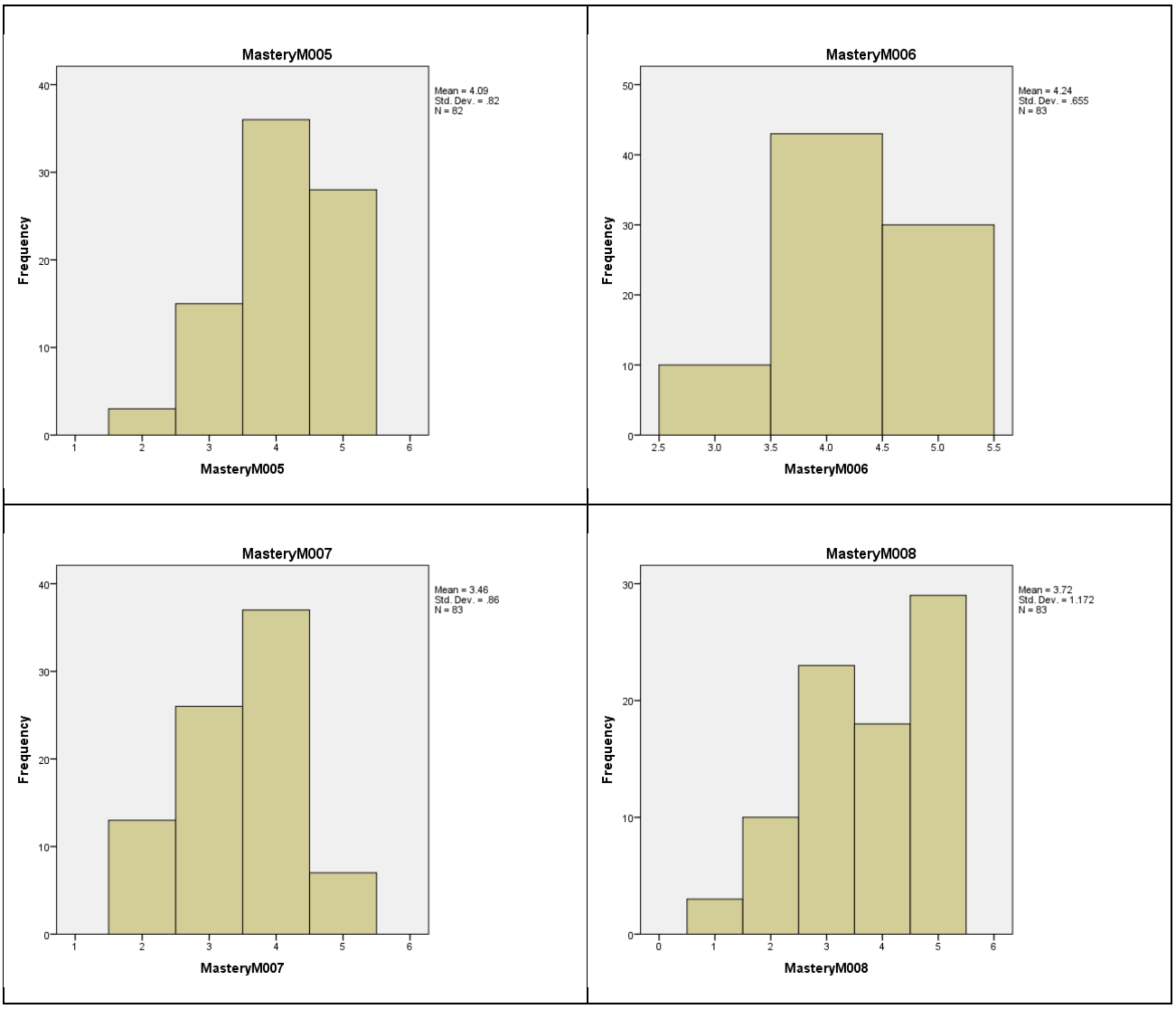

Normal Q-Q Plot of SNTRAC02
Expected Normal Value
Observed Value
5
4
3
2
1

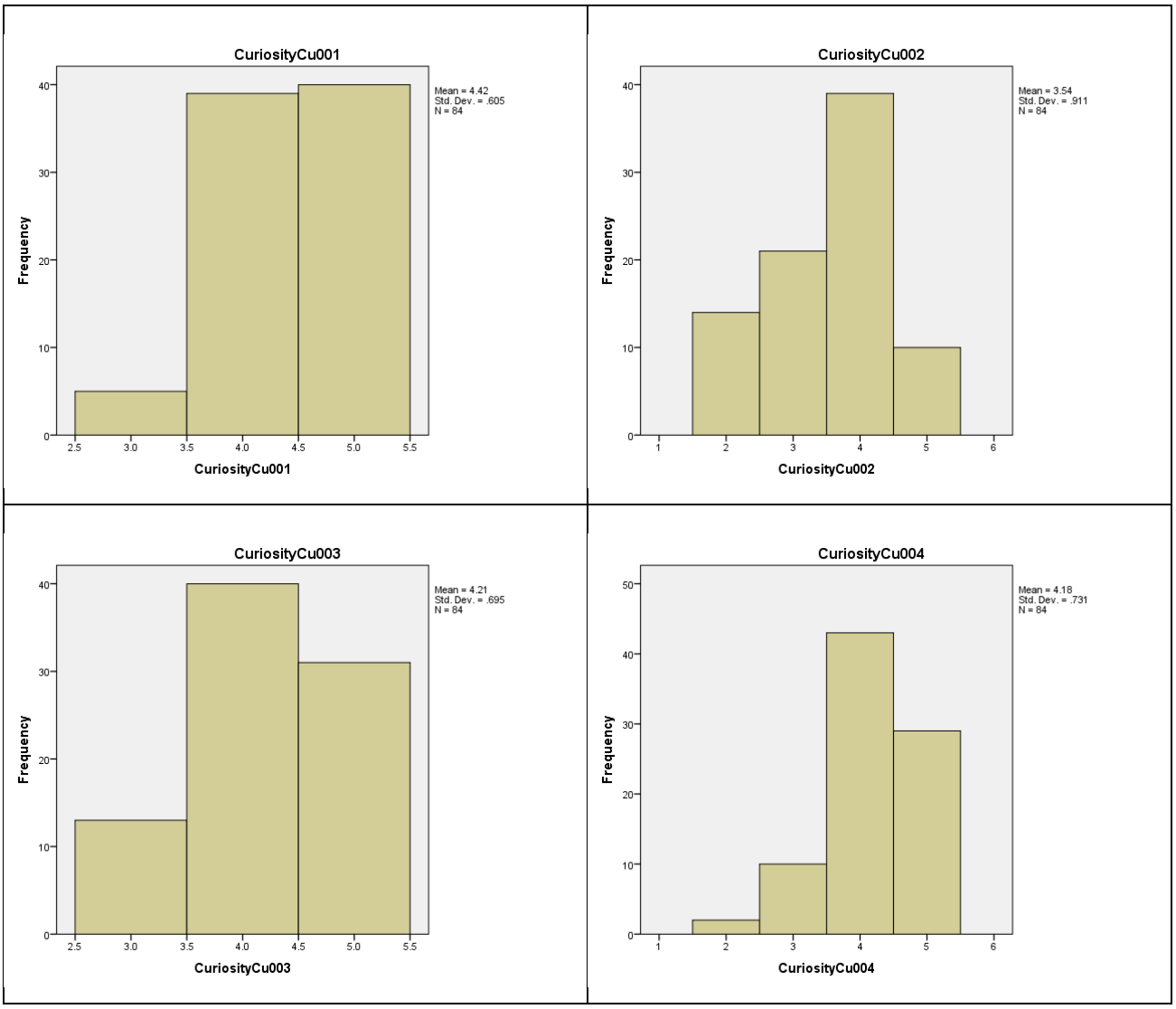

Normal Q-Q Plot of GDTdiscover
Expected Normal Value
Observed Value
1
2
3
4
5

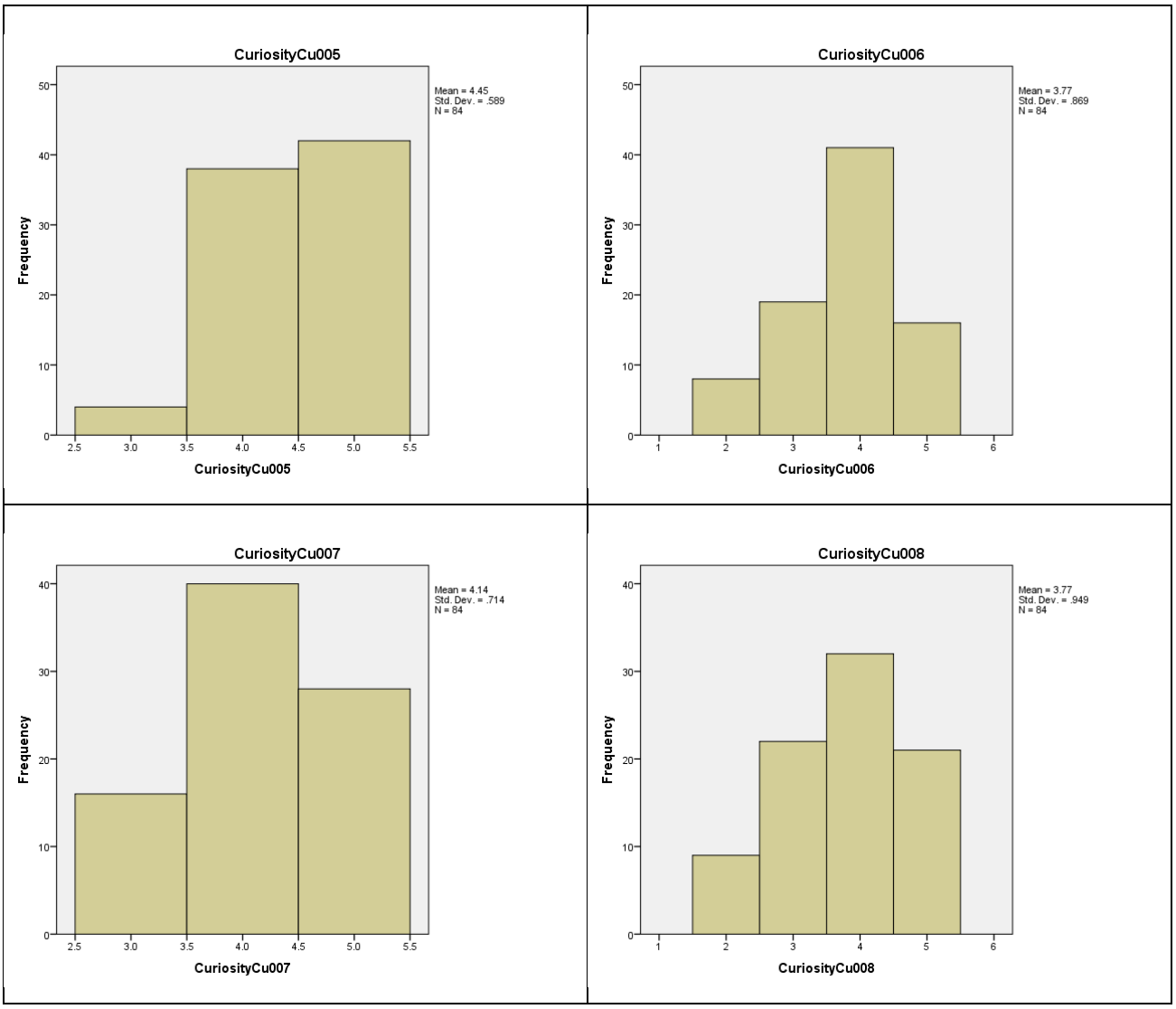

Normal Q-Q Plot of GDTpunish
Expected Normal Value
Observed Value
1
2
3
4
5

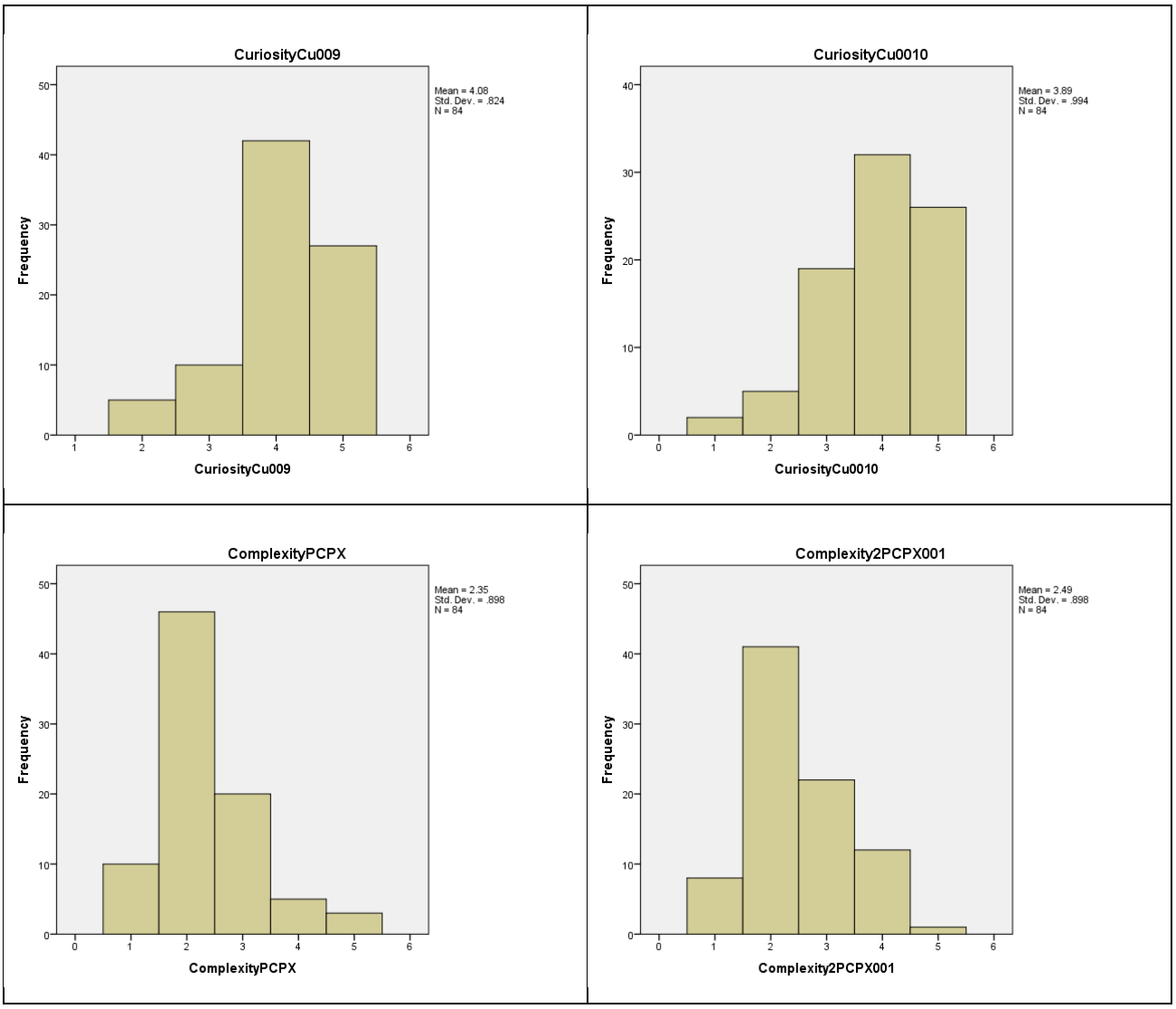
Appendix F: Histograms

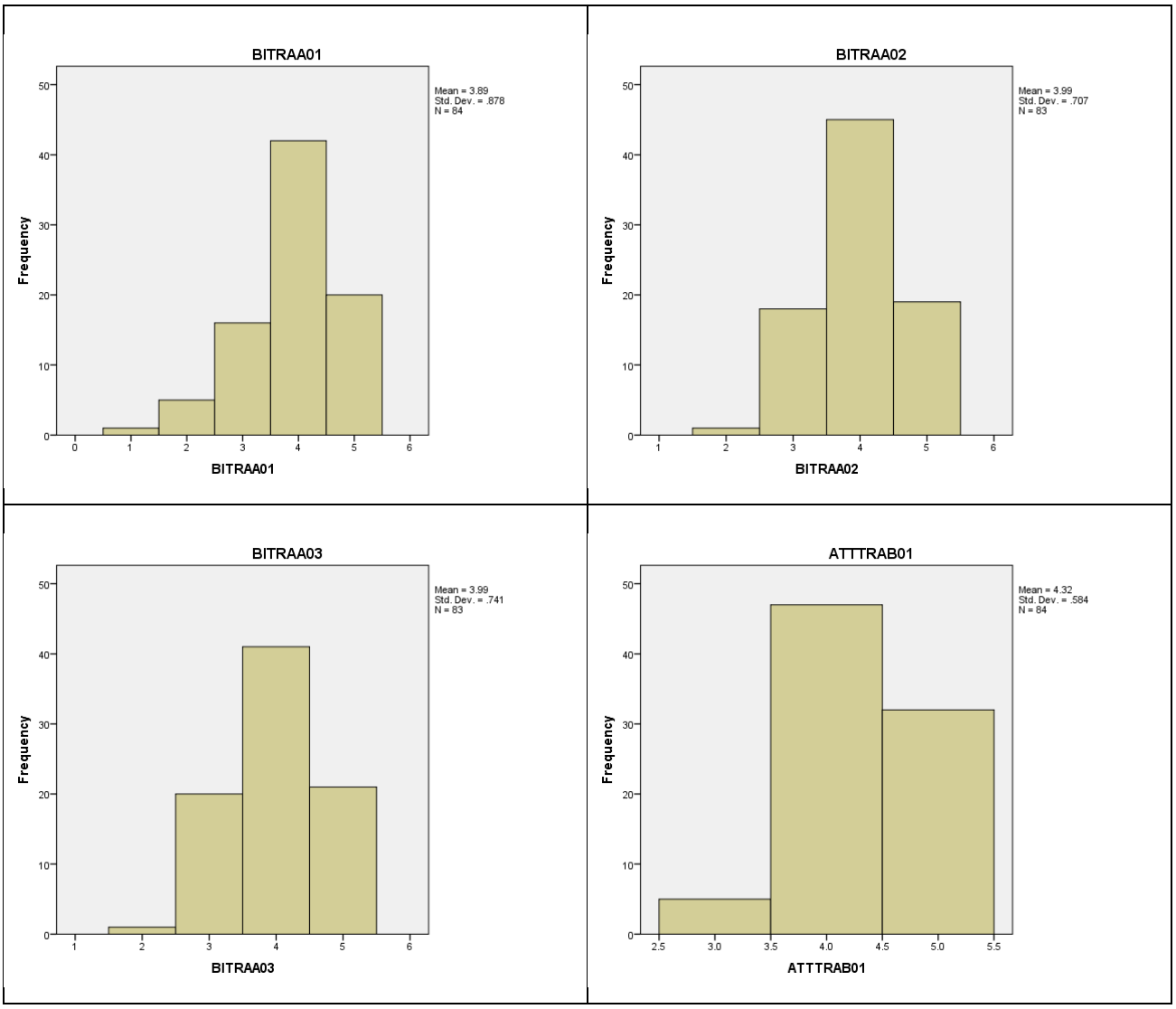


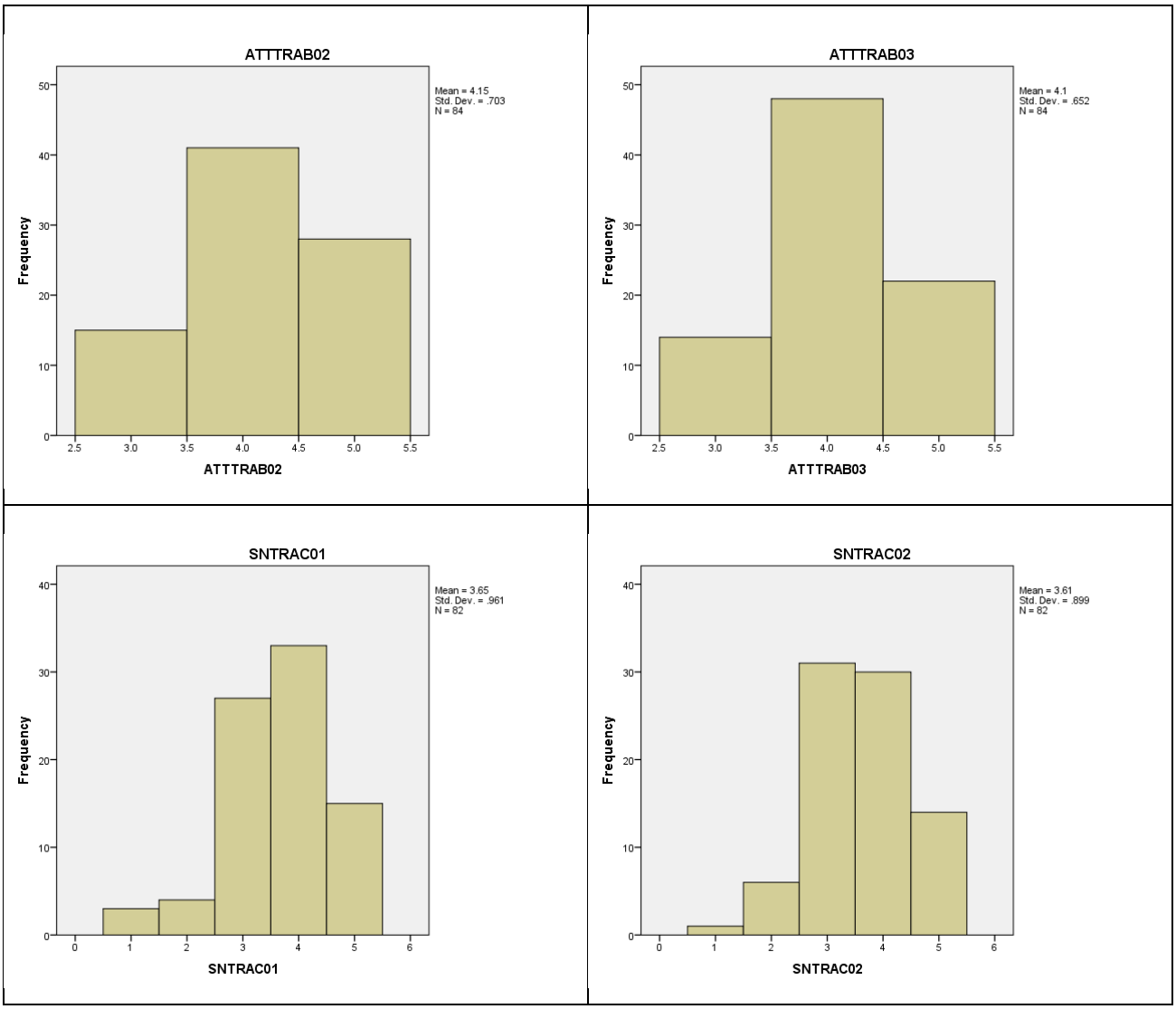

MasteryM005
Mean = 4.09
Std. Dev. = .82
N = 82
Frequency
MasteryM005
MasteryM006
Mean = 4.24
Std. Dev. = .655
N = 83
Frequency
MasteryM006
MasteryM007
Mean = 3.46
Std. Dev. = .86
N = 83
Frequency
MasteryM007
MasteryM008
Mean = 3.72
Std. Dev. = 1.172
N = 83
Frequency
MasteryM008

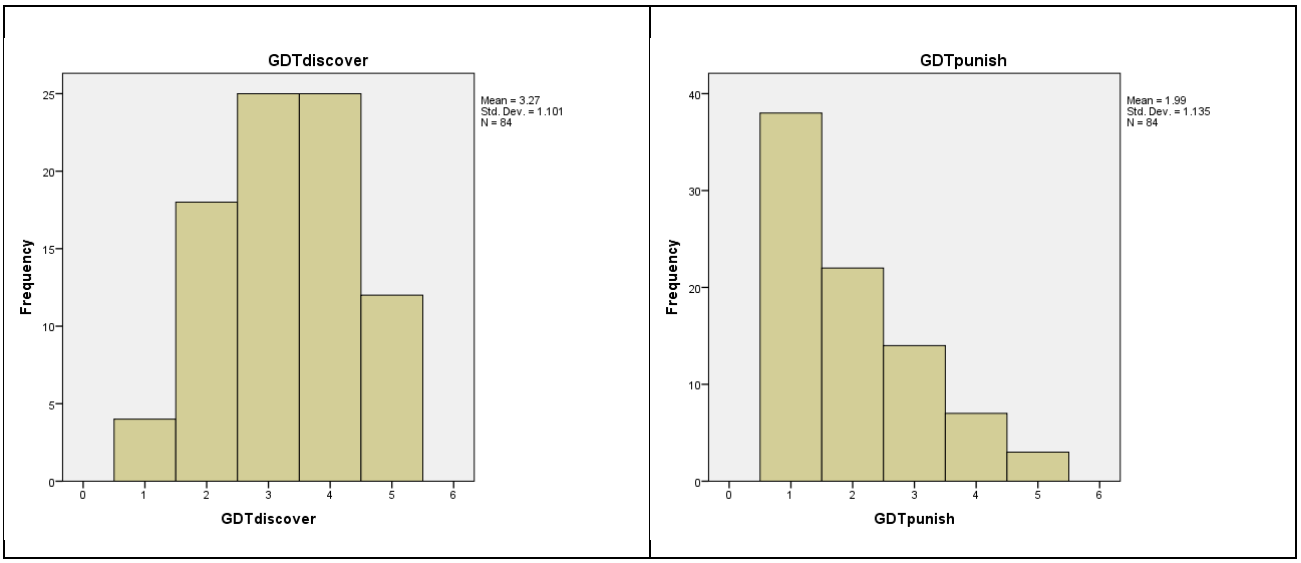

CuriosityCu001
Mean = 4.42
Std. Dev. = .605
N = 84
Frequency
CuriosityCu001
CuriosityCu002
Mean = 3.54
Std. Dev. = .911
N = 84
Frequency
CuriosityCu002
CuriosityCu003
Mean = 4.21
Std. Dev. = .695
N = 84
Frequency
CuriosityCu003
CuriosityCu004
Mean = 4.18
Std. Dev. = .731
N = 84
Frequency
CuriosityCu004


CuriosityCu005
Mean = 4.45
Std. Dev. = .589
N = 84
Frequency
CuriosityCu005
CuriosityCu006
Mean = 3.77
Std. Dev. = .869
N = 84
Frequency
CuriosityCu006
CuriosityCu007
Mean = 4.14
Std. Dev. = .714
N = 84
Frequency
CuriosityCu007
CuriosityCu008
Mean = 3.77
Std. Dev. = .949
N = 84
Frequency
CuriosityCu008

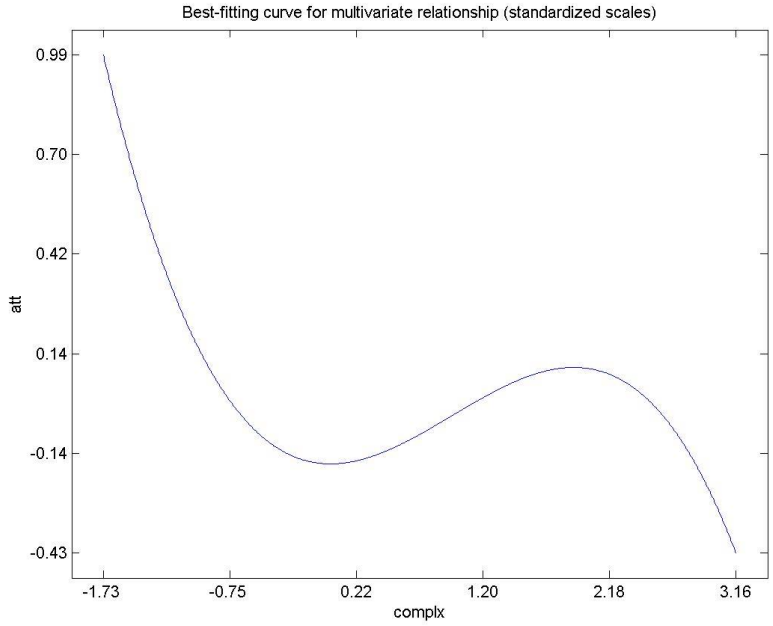

CuriosityCu009
Mean = 4.08
Std. Dev. = .824
N = 84
Frequency
CuriosityCu009
CuriosityCu0010
Mean = 3.89
Std. Dev. = .994
N = 84
Frequency
CuriosityCu0010
ComplexityPCPX
Mean = 2.35
Std. Dev. = .898
N = 84
Frequency
ComplexityPCPX
Complexity2PCPX001
Mean = 2.49
Std. Dev. = .898
N = 84
Frequency
Complexity2PCPX001

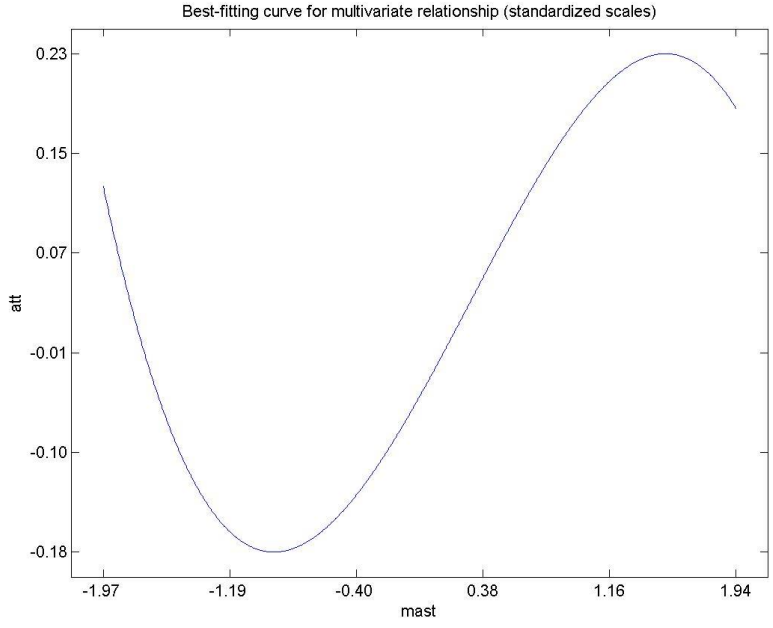

BITRAA01
Mean = 3.89
Std. Dev. = .878
N = 84
Frequency
BITRAA01
BITRAA02
Mean = 3.99
Std. Dev. = .707
N = 83
Frequency
BITRAA02
BITRAA03
Mean = 3.99
Std. Dev. = .741
N = 83
Frequency
BITRAA03
ATTTRAB01
Mean = 4.32
Std. Dev. = .584
N = 84
Frequency
ATTTRAB01

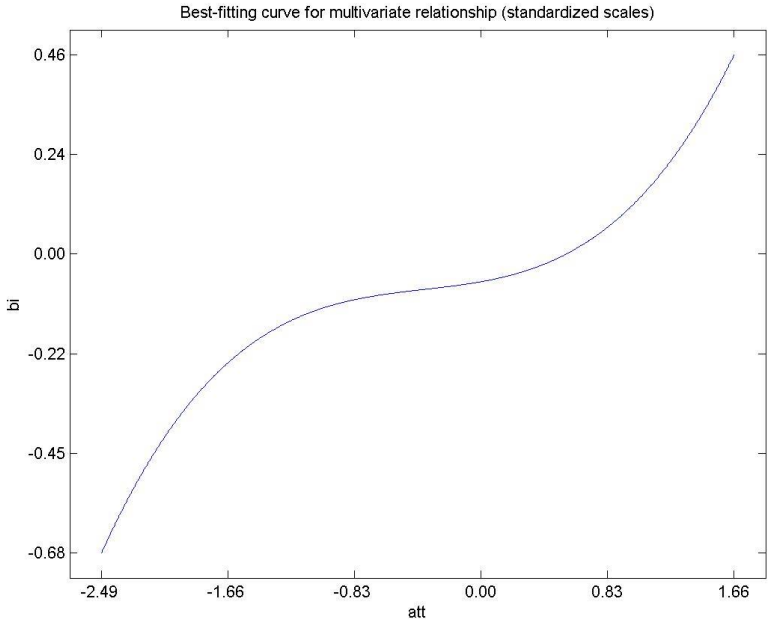

ATTTRAB02
Mean = 4.15
Std. Dev. = .703
N = 84
Frequency
ATTTRAB02
ATTTRAB03
Mean = 4.1
Std. Dev. = .652
N = 84
Frequency
ATTTRAB03
SNTRAC01
Mean = 3.65
Std. Dev. = .961
N = 82
Frequency
SNTRAC01
SNTRAC02
Mean = 3.61
Std. Dev. = .899
N = 82
Frequency
SNTRAC02

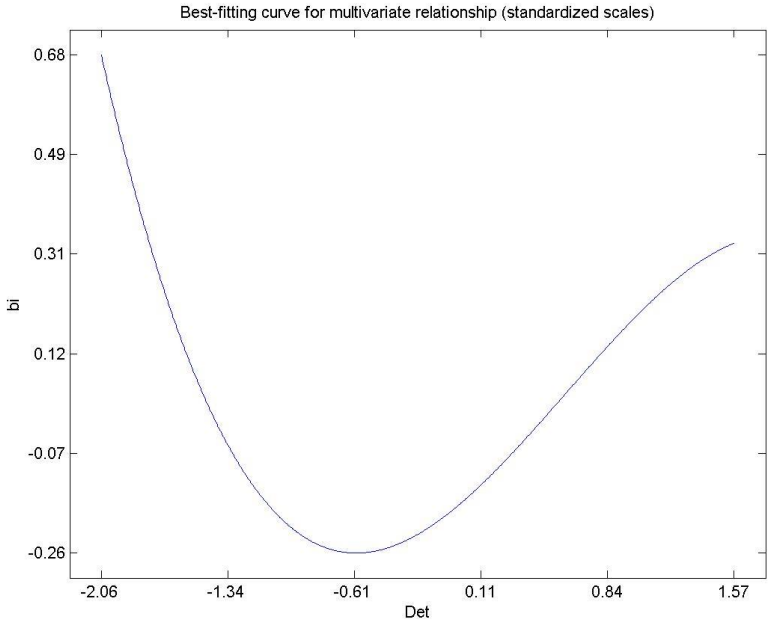

GDTdiscover
Mean = 3.27
Std. Dev. = 1.101
N = 84
Frequency
GDTdiscover
GDTpunish
Mean = 1.99
Std. Dev. = 1.135
N = 84
Frequency
GDTpunish

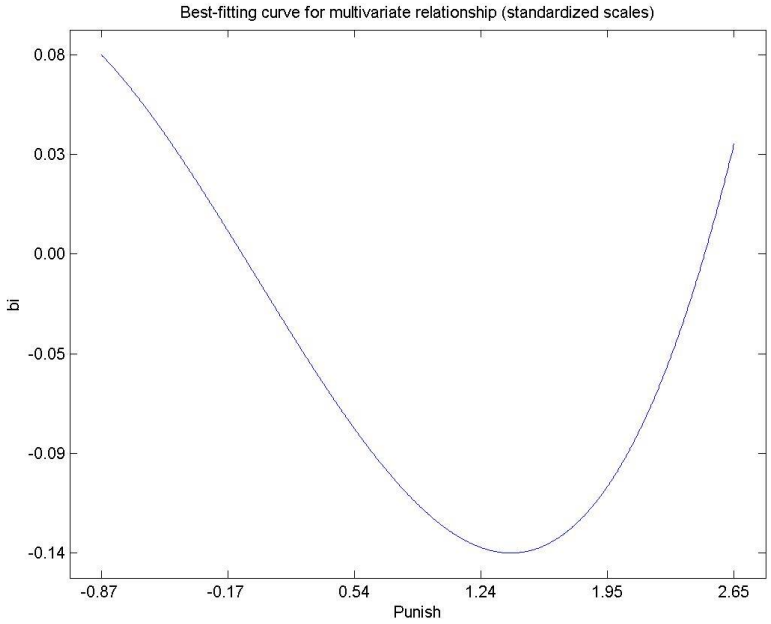
Appendix G: Scatter Plots

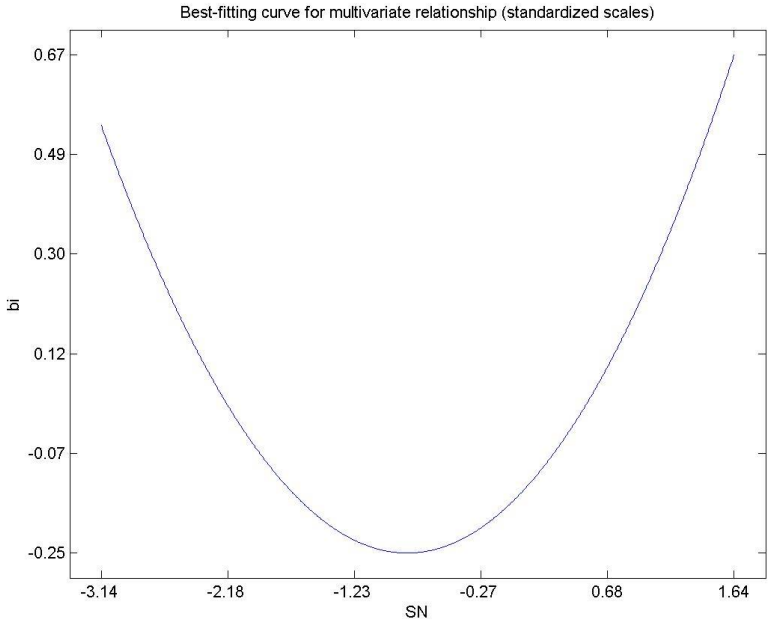





Best-fitting curve for multivariate relationship (standardized scales)
0.46
0.24
0.00
-0.22
-0.45
-0.68
bi
-2.49
-1.66
-0.83
0.00
0.83
1.66
att


Best-fitting curve for multivariate relationship (standardized scales)
0.68
0.49
0.31
0.12
-0.07
-0.26
bi
-2.06
-1.34
-0.61
0.11
0.84
1.57
Det


Best-fitting curve for multivariate relationship (standardized scales)
0.08
0.03
0.00
-0.05
-0.09
-0.14
bi
-0.87
-0.17
0.54
1.24
1.95
2.65
Punish


Best-fitting curve for multivariate relationship (standardized scales)
0.67
0.49
0.30
0.12
-0.07
-0.25
bi
-3.14
-2.18
-1.23
-0.27
0.68
1.64
SN

Key of Abbreviations

Abbreviation	Construct
att	Attitude
bi	Behavioural Intention
complx	Complexity
Det	Perceived Certainty
mast	Mastery
Punish	Perceived Severity
SN	Subjective Norm