2014

# Mr Hyde Or Dr. Jekyll? Characteristics Of The Information Systems Security Mindset

David Pumphrey
*University of Mississippi*

# MR. HYDE OR DR. JEKYLL? CHARACTERISTICS OF THE INFORMATION SYSTEMS SECURITY MINDSET

A Dissertation
Presented in partial fulfillment of requirements
for the degree of
Doctor of Philosophy in Business Administration
in the Department of Management Information Systems
The University of Mississippi

by

DAVID L PUMPHREY

October 2014

## ABSTRACT

Information security professionals have a unique challenge in today's connected world. They are charged with protecting digital assets from individuals, groups, and even foreign governments with little or no restrictions limiting their behavior. To be successful, security experts must have the mindset and skills of those who seek to harm their organization, but most are not allowed to retaliate, in kind. Instead, they must use these skills only to predict and to prevent future attacks; thus using their technical prowess for good and not for evil. In a survey of 330 information security professionals, the data reveals six mindsets of security experts through a latent class analysis. One class emerged containing approximately 52% of the respondents, which indicates that the information security field is consistent with social identity theory and contains significant homogeneity in mindset toward securing an organization's digital assets. Additionally, personality characteristics such as Creativity, Trait Competitiveness, and Morality influence membership in one of six information security mindsets.

## DEDICATION

This dissertation is dedicated to my children: Matthew, Karis, Joshua, and Hannah. Education, at every age, is worth pursuing with vigor. I just want to be an example to each of you – as a student, as a person, and as a dad. To my parents, Bobbye Brengard & Norman Pumphrey, because without the thirst for knowledge and drive to succeed they instilled in me as a child, I would have never had the determination to complete a doctoral program.

## LIST OF ABBREVIATIONS AND SYMBOLS

| | |
|---|---|
| DoS | Denial of Service |
| DDoS | Distributed Denial of Service |
| IP | Internet Protocol |
| TCP | Transmission Control Protocol |
| LCA | Latent Class Analysis |

## ACKNOWLEDGMENTS

I express my sincere gratitude to my advisor, Dr. Brian Reithel, and to my committee members, Drs. Tony Ammeter, John Bentley, and Bart Garner. Each of you has invested in me in ways I can never repay. Dr. Ammeter, for steering me through my first year of trying to think like a researcher, for setting an example for excellence in teaching, for motivating me, for mentoring me, and for simply being a friend. A special thanks to Dr. Bentley who instilled a love of statistics in me that is just not normal. A very special thanks to Dr. Reithel, who not only inspired me in my doctoral seminars but convinced me that over 20 years of practical experience is useful in both research and in teaching. And to Dr. Garner, who helped me to finally comprehend pattern recognition and machine learning. Additionally, a special thanks to Dr. Milrad Novicevic, who challenged me to think – a lot…every time he saw me before I saw him. For that, I will be forever grateful.

Finally, I thank my fellow doctoral students for their camaraderie and support. I offer a very special thanks to Clif Eason and Robert King of the Tuesday Night Pancake Society. Many weeks, you talked me off the ledge on those late night pancake outings, as we experienced the worst restaurant service in all of Oxford that was only surpassed by the inedible food.

# TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

# CHAPTER 1: INTRODUCTION

In recent years, the popular media has reported data breaches leading to stolen credit cards numbers (Rodriquez, 2013), theft of login credentials from major social networks (Vijayan, 2012), release of sensitive intelligence data by security analysts , and publication of classified movements of military personnel (Bumiller, 2010). Without regard for privacy or national security, computer savvy hackers and paid contractors break into networks as well as access sensitive information within a secure network with the intent to use or to publicize the sensitive information (Mackey, 2013). As self-appointed champions of full-disclosure in government, these infamous whistleblowers have, potentially, placed lives or national security in danger. Certainly, they have succeeded in bringing to light sensitive information of which they determined the public, through the national media, should be informed. In light of the much publicized events of hackers and security analysts absconding with financial data and national secrets, recent research has attempted to identify characteristics of hackers in an attempt to suggest reasons for their behavior (Xu, Hu, & Zhang, 2013). Xu, Hu, & Zhang (2013) proposed an integrative framework to explain the factors influencing young computer users to become hackers. Drawing on the criminal justice literature, their qualitative research shows the influence of Social Learning Theory, Routine Activity Theory and Situational Action Theory on young computer programmers turning to hacking. With so many young, intelligent computer enthusiasts looking for acceptance and challenge, it becomes even more important to identify equally intelligent and motivated computer experts of all ages to work for government and industry to secure national and corporate data. Although informative, Xu et al. (2013) focus on

the social learning perspective in their study. Social identity is equally relevant to how computer enthusiasts become hackers, and this study suggests that it, also, influences how security professionals are chosen to protect an organization.

Who better to occupy the ranks of information system security organizations than bright, curious computer enthusiasts who form their own in-groups and have spent much of their formative years experimenting with computers learning tricks and techniques designed to infiltrate computer networks. It is these computer users that have the background and knowledge to detect intrusions and to protect the assets of an organization. Although not all information systems security (ISS) professionals are former hackers, the purpose of this study is to classify types of security professionals and then to investigate their personality characteristics by showing how these personality characteristics influence membership in the specific classes. Once characteristics can be successfully identified, understanding how to motivate the young computer enthusiasts with an interest in hacking and redirecting their enthusiasm toward information security can begin.

This study draws on research into motivation for young computer enthusiasts and previous research into personality characteristics to determine a classification of security professionals. Further, the classification will help organizations identify the types of individuals that are responsible for securing their government and corporate networks from new and experienced hackers intent on doing them harm. The study, also, investigates the relationships between the classes of ISS professionals along with specific personality characteristics to determine whether the particular characteristics chosen for this study predict membership into a specific type of security professional.

## 1.1 Research Questions

In this study, the types of ISS professionals that span the continuum from aggressive anti-hacker to a passive IT security worker are explored. The goal of this study is to begin to develop a classification of ISS professional whose intent is to detect, stop, and, potentially, retaliate when a breach of network security is detected compared with an ISS professional that simply monitors the installed software and reports suspicious activity to management. The study suggests there are multiple conceptual groupings, or mindsets, of ISS professionals that span the entire continuum. Interesting findings such as the types of ISS personnel that exist in organizations today, discovering the characteristics of these ISS professionals, and to which classes these characteristics are assigned, is the focus of this study. The study seeks to answer two questions:

1) *What conceptual groups exist that distinctly categorize the types of ISS professionals that are prone to either avoid network security activity or to develop aggressive means to stop those intent on breaching them?*
2) *Which characteristics predict membership into ISS Professional's mindset classes?*

To address the first research question, the study uses latent class analysis, which identifies levels of a latent, categorical variable using observed categorical variables. In this instance, the observed variables will lead to the types of information security professionals found in organizations. After determining the classification of ISS professionals, the study investigates the influence of important personality characteristics on class membership. Those personality characteristics are covered in the following sections.

## 1.2 Creativity

This study investigates creativity of the security professional from the perspective of his or her ability to think like the person attempting to intrude on the network. To be an effective ISS professional, the influence of creativity on ISS classification was explored. Much work has been

done in the area of creativity but very little work has been done to assess the influence of creativity on information security workers. This study shows that the more creative the person is, the more effective he or she is in thinking like a person intent on breaching a network.

Within the domain of information systems security, creativity manifests itself in numerous ways. Hackers find ways to breach a network, such as social engineering techniques designed to acquire network credentials, brute force distributed denial of service attacks, and viruses that lie dormant for months or even years before activating and allowing access or damaging nodes on a network. A "creative" ISS professional must develop numerous ways to communicate to members of an organization to help prepare employees for social engineering attempts, but he or she must, also, know how to detect intrusion through the use of intrusion detection software as well as through use of detection algorithms that are unique to an organization. Therefore, the study draws information from the creativity literature related to domain specificity as much as from the traditional creativity literature to understand the influence of creativity on ISS classification. In addition to creativity, ISS professionals must possess the ability to "out-think" a hacker by identifying a vulnerability before a hacker has an opportunity to exploit it. After identifying the vulnerability, the ISS professional must mitigate the potential damage of the vulnerability before the hacker has an opportunity to access the network through the uncorrected vulnerability.

## 1.3 Trait Competitiveness

Competitive individuals possess an intrinsic desire for interpersonal competition from which they receive enjoyment that drives the desire to compete against others, and to win (Spence & Helmreich, 1983). This intrinsic competitiveness is referred to as a trait competitiveness (S. P. Brown, Cron, & Slocum, 1998). Unlike situational competitiveness in

which a person competes only for the duration of the competition, trait competitiveness spans situations. This study suggests that ISS professionals can be classified differently based on the measure of trait competitiveness. Highly competitive ISS workers may be motivated to detect a breach in the network, identify where and how it was breached, determine a plan to mitigate the damage, develop a strategy for prevention of future intrusions, and even trace the intrusion back to its originator. These competitive ISS workers are on one end of the spectrum, and on the other end is a passive security worker. Passive workers can be valuable by monitoring the detection software, but their level of competitiveness does not motivate them to take an intrusion personally, like the highly competitive ISS professional. Not only does the study suggest the influence of competitiveness on class membership, but differing degrees of deceptiveness predict membership, as well.

## 1.4 Deceptiveness

Deceptiveness involves actions that are not straightforward. In fact, dictionary.com defines deceptiveness as misleading "by a false appearance or statement" ("the definition of deceive," n.d.). Infamous hacker, Kevin Mitnick, became, arguably, the most well-known hacker by simply using the art of deception, which was the title of his book (Mitnick & Simon, 2003). Although Mitnick claims to have used social engineering, primarily to break into networks, other hackers use other forms of deception to mask their identity. To be able to stop a hacker from breaching a network, an effective information security person must possess some ability to think like a hacker – only sooner. To think like a hacker requires the ISS professional to possess similar deceptive ability as the person he or she is trying to stop.

To be effective in ISS, one must anticipate possible intrusions and direct the potential attack vector to one in which the hacker can be detected and stopped. In many ways, the ISS

professional must be more deceptive, or at least think more deceptively, than those he or she is trying to stop, because not only must the potential vector be identified, but the ISS worker must be able to draw the attacker into a trap that the attacker does not detect. This is a level of deceptiveness that requires careful thought and planning; otherwise, the ISS professional will be required to anticipate the uncaught hacker returning at a later time with additional information and, often, new resolve.

## 1.5 Distrust

Trust is defined as "the expectancy of positive (or nonnegative) outcomes that one can receive based on the expected action of another party in an interaction characterized by uncertainty" (Bhattacharya, Devinney, & Pillutla, 1998, p 462). Bhattacharya et al. (1998) describe this definition as an imprecise verbal definition of trust. However it is defined, security workers cannot afford to rely in the trustworthy behavior of others. Certainly, they possess a level of trust in their colleagues and fellow employees of an organization, but much like the police personality, ISS professionals have the potential of developing a level of distrust in people both external to and within an organization they support (Twersky-Glasner, 2005).

Further, Bhattacharya et al. (1998) describe, using set theory, the necessary scenarios under which trust and distrust can be directly determined as a binary decision. Over time, distrust of practically everyone develops in the mind of the ISS professional - at least everyone with the access to organizational digital assets or with the technical ability to attempt to gain access to them. Thus, in this study, ISS professionals' level of general distrust is of greater interest than his or her level of trust.

In contrast with trust, distrust occurs when there is an expectation of injurious action (Luhmann, 1979). Distrust manifests itself when an "other" displays incompetence, acts

irresponsibly, violates obligations, or acts in a manner that is harmful to the person exhibiting distrust (Lewicki, McAllister, & Bies, 1998). This study explores the impact of an ISS professional's level of distrust as a predictor of a specific ISS classification. . Finally, using all of these characteristics without a way to govern the behavior, the ISS professional may be as dangerous as the hacker; however, one characteristic is important to keep the ISS professional from "crossing the line" into the world of hacking.

## 1.6 Morality

Defining morality is a challenge with a multitude of "what-if" exceptions. It cannot simply be defined in terms of moral versus immoral, nor can morality be defined as the opposite of non-moral. Immorality and non-moral are two completely different ideas (Frankena, 1988). This study views morality in the simple context of private ownership of property and information. An organization owns the digital assets that it has accumulated in the normal course of its business and has acquired by legal means. This study is not intended to evaluate specific instances of data an organization or government has acquired in the determination of morality. In this study, the assets of an organization are assumed to belong to an organization and any access to the information by unauthorized persons is considered a violation of the legal right of ownership granted to the organization. Therefore, any attempted access to the information is considered a violation of an organization's right to protect it.

Thus, unauthorized attempts to access information are considered an immoral act. Although this is a very narrow definition of morality, it is somewhat universally accepted that organizations are well within their rights to protect assets of which they consider themselves the owners.

## 1.7 Latent Class Analysis

Latent class analysis (LCA) is a method of determining latent variables from categorical observed variables. A technique similar to factor analysis, LCA, however, produces a categorical construct, calculated without error. Factor analysis, on the other hand, produces a continuous factor from continuous observed variables (Collins & Lanza, 2010). The primary difference between the two approaches is that, where factor analysis identifies a latent continuous variable, LCA, on the other hand, produces a categorical latent variable whose distribution is multinomial. This study focuses on people who differ quantitatively along the continuum of types of information systems security professionals.

Latent class analysis has been used in many studies in the social and behavioral sciences to distinguish among characteristics of people (Mäkikangas, Hyvönen, Leskinen, Kinnunen, & Feldt, 2011; Morin, Morizot, Boudrias, & Madore, 2011; Qureshi & Fang, 2010). As described in the previous definition and brief description, it is useful to classify types of an entity using categorical observed variables and producing a categorical latent variable as a result. Woo & Allen (2013) used LCA to create a classification of stayers and seekers in an organization. Organizational research is rich with opportunity to use LCA to identify classifications of individuals at work (Wang & Hanges, 2010). Wang & Hanges (2010) point out the advantages of using latent class analysis as a clustering approach over traditional cluster analysis. One primary reason is that LCA produces a maximum likelihood (log-likelihood) estimate of the model parameters, similar to structural equation modeling, which uses statistically consistent criteria for allocating observations into latent classifications. A primary objective of this study is to identify classifications of ISS professionals, which makes LCA an attractive technique. Further, LCA is not restricted to normal distribution of the observed variables, which provides

flexibility in developing items used in the LCA. The estimate produced from a latent class analysis is a probabilistic classification, thus providing the probability of membership in each class determined. This allows the latent class model to be used with other observations within the population from which the model is developed to predict membership in the classes (Wang & Hanges, 2010).

LCA requires questions with categorical responses as input. To produce scientifically valid questions for use in the LCA, the study relies upon the Delphi technique to query a group of experts in information security to provide the questions. Therefore, this study presents the Delphi-Driven Latent Class Analysis Method as an approach to the analysis. It is not a statistical approach; rather, it is a set of steps, similar to a systems development methodology, to follow when conducting research similar to that used in this study. The nature of Delphi is such that when limited prior research is available in a subject area, the technique can be used to extract reliable information from a group of experts. The questions resulting from the Delphi study step are used to develop the questions asked in the LCA. In the situation where further analysis is desired to determine other factors influencing class membership, the remaining steps can be performed to assess the factors' influence on membership in one or more of the classes found in the LCA.

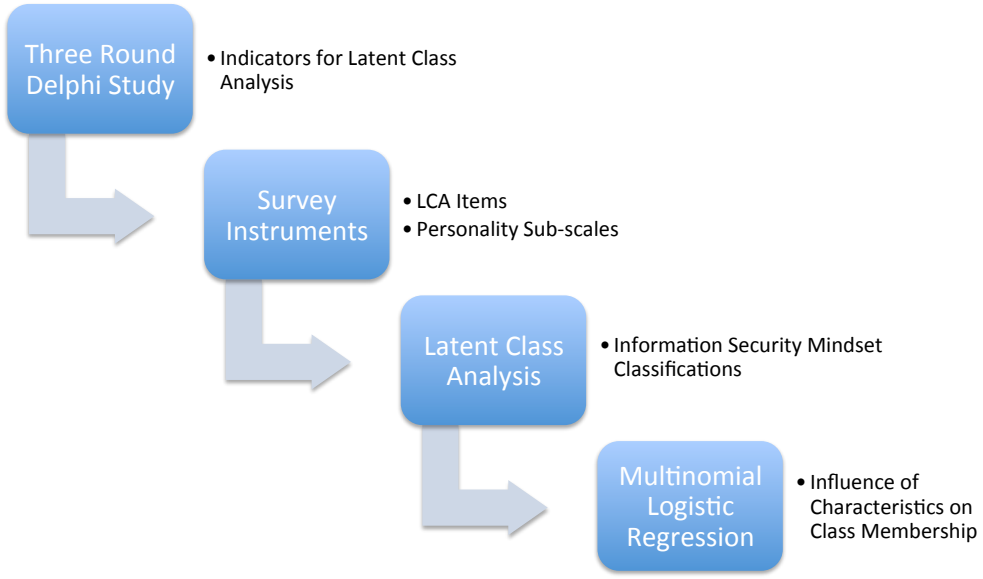



**Figure 1 - The Delphi-Driven Latent Class Analysis Method**

## 1.8 Next Steps

Chapter 2 contains a literature review of the theoretical foundation of the constructs under investigation and the methodological techniques employed in this study. Chapter 3 presents the methods used in gathering and analyzing the data upon which this study is based, while chapter 4 presents the study findings of the Delphi, the pilot, and the primary study. Chapter 5 discusses the findings, the of the study's impact on theory and management, and suggested future research, and chapter 6 contains concluding remarks on the study as a whole.

# CHAPTER 2: LITERATURE REVIEW

## 2.1 Research Model

Predicting the effectiveness of ISS professionals, as with any professional, is a combination of numerous constructs; however, there are constructs that are critical in determining the effectiveness of information security workers. They have many of the same skills common to application developers, system administrators, and other information technology workers; however, to be an effective ISS professional, this study investigates characteristics that, although possessed by all professionals in information technology, are particularly applicable to workers in ISS.

This study looks at the effect of trait competitiveness, distrust, creativity, deceptiveness and morality on membership in a specific class of information technology professional. The questions to ask, which are used to determine class memberships are developed through both a Delphi study to glean information from a group of information security experts and from the literature. In the study, it was initially planned to use Delphi solely to provide the questions, but the Delphi group focused almost exclusively on job interview questions and many of the responses from the panel were more general in nature, which did not allow for differentiation based on type of ISS professional. Thus, the Delphi questions are supplemented by ETSI's Information Security Incidents Taxonomy (Rennoch & Gaudin, 2013).

Information Systems Security type is the dependent variable of the study, and the design of the questions related to determining the type of ISS professional produced a binary or a ternary response. In other words, the responses to the questions, and thus the variables, were

categorical. Further, given the nature of classifications, the construct representing the type of ISS professional was a categorical variable, as well. This lends itself to the use of latent class analysis (LCA). LCA is described in more detail in a subsequent section of the literature review, but, in short, LCA is similar to factor analysis. However, where factor analysis uses continuous observed variables to determine continuous latent factors, LCA uses categorical observed variables to determine categorical latent variables.

After the types of ISS professionals are determined, the study investigates the influence that specific characteristics have on class membership in one of several classes. The characteristics of interest in this study are creativity, trait competitiveness, deceptiveness, distrust, and morality. These constructs are determined from the literature and are influential in the type of work performed by ISS professionals. Once all of the constructs are related, the following research model emerges:

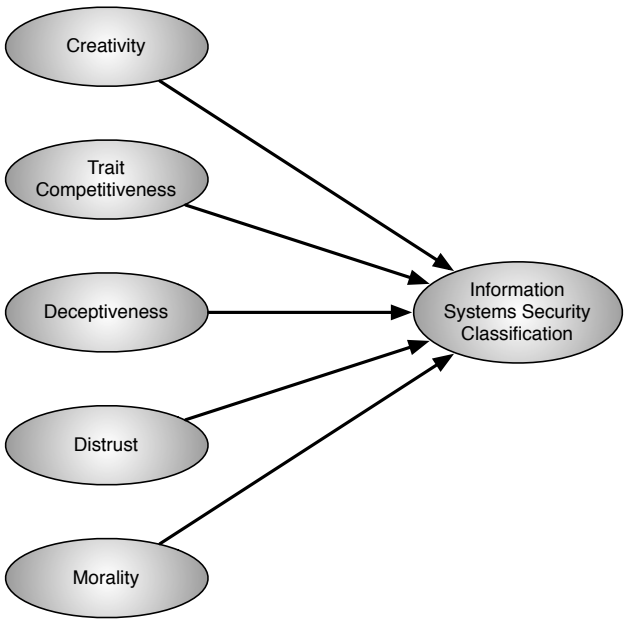



**Figure 2 – Research Model**

In this research, a Delphi study is performed and the resulting questions that are determined by experts are combined with questions based on the ISS literature to be used to determine the classification of ISS professionals. Finally, multinomial logistic regression is performed to determine the influence, on class membership, of each personality characteristic in Figure 2.

In the following sections, each technique and construct is described as determined from the literature. First, the Delphi technique is described, followed by the remaining methodological techniques. The constructs representing each personality characteristic are described from the relevant literature. As each construct is described, hypotheses are presented showing the expected findings of the theoretical relationships.

## 2.2 Delphi

The Delphi technique is a methodology that is useful when research describing the area of interest is limited and constructs are not identified are or unclear (Cegielski, 2008; Okoli & Pawlowski, 2004). Developed in the 1950's at the RAND Corporation, the Delphi technique is designed to elicit and refine group judgments (Dalkey, 1969). The primary objective is to obtain reliable consensus on a topic from a group of experts (Dalkey & Helmer, 1963).

The methodology has three features that make it useful when seeking to discover information for which there is not a definitive source of authority. In the context of factors leading decision-makers to choose the use of virtual staffing firms over traditional methods, for instance, there have been studies looking at this issue; however, there are no sources of definitive authority (Kim, 2010; Lin, Viswanathan, & Agarwal, 2010). Therefore, the Delphi method is an adequate tool to elicit this information. The advantage this technique has over group interviews are: (1) anonymous response, (2) iteration and controlled feedback, and (3) statistical group

response. These advantages are important to group settings. The first advantage, anonymous response, is important to avoid the problems created when a single, prominent person dominates the conversation in a group setting. In certain settings, this can be the ranking member involved in the meeting. In other settings, it can simply be the person with the strongest personality or opinion. Anonymous responses in the Delphi technique, through the use of questionnaires, avoid the problems of respondent dominance in a group setting. Semantic noise can become a problem in a group setting where anonymity is absent, also. Semantic noise suggests the inevitability of group discussions losing focus of the purpose of the meeting. Semantic noise may appear focused on the problem, but often it is irrelevant or creates bias on the responses of the group as a whole (Dalkey, 1969). Finally, in face-to-face group communication, pressure to conform to the opinion of the group or of a dominant individual can influence the consensus of opinion.

**Table 1 – Characteristics of the Delphi Method**

(Cegielski, 2008, p. 35)

| Characteristics | Description |
|---|---|
| Anonymity | The administrator manages communication to and from all participants, which provides anonymity for all participants |
| Controlled Feedback | The administrator manages the flow of information to and from the participants |
| Group Response | Individual responses are gathered by the administrator and distributed back to the participants as a group response |
| Expert Opinion | Participants are selected for inclusion in the study based on knowledge of the topic |
| Reduced Time/Cost | Face-to-face meetings with a, potentially, widely distributed audience are rarely necessary |

The technique begins by asking experts open-ended questions related to the topic of the study. The number of questions asked is flexible, but should be concise. The purpose of the original questions is to elicit responses from the respondents in a manner much like a brainstorming session produces. The respondent answers each of the questions, which are asked in a free-form manner. The researcher then reviews the responses and, optimally, by at least two

additional coders, who review the free-form responses and develop a list of the responses to each question.

The researchers produce a second round of questionnaires with a list of the responses to each question. The respondents are asked to rank the responses from most appropriate to least appropriate response to the questions (from 1 to the number of items to rank). Upon receipt of the responses, the researcher calculates the ranking of the items for each question by calculating the average ranking for each item and ordering these responses in rank order. In the third round, questionnaires are sent to the respondent with the group rankings included. The respondents are asked to rank the items again or to confirm the existing rankings, given the order calculated by averaging the rankings from the previous round. This gives respondents an opportunity to reconsider their initial ranking. This process is repeated until group consensus is reached.

## 2.4 Social Identity Theory

People have a natural tendency to classify others and themselves into categories. Particularly within I.T., members of specific factions of the organization view their function and role in the organization as more important or as contributing more to the goals of the organization. This social identification is not unique to I.T.; rather it is common across human interaction and behavior (Brown, 2000).

This identification with others in similar roles in the organization is known as social identification, which is defined as "the perception of oneness with or belongingness to some human aggregate" (Ashforth & Mael, 1989). Within all aspects of an organization, and particularly within an I.T. organization, individuals identify with the goals of the group and project those group goals onto themselves as individual goals. Additionally, an individual may project his or her goals onto the group and thus perceive not only the group's goals as her own

but may view the congruence of individual and group goals without ability to distinguish between them.

Xu, Hu, and Zhang (2013) identified this behavior in their study investigating why young computer enthusiasts become hackers. Although they, likely, misconstrue the behavior as exclusively social learning, the behavior Xu et al. (2013) describes includes social learning and a social identification that contributes to hackers identification with like-minded enthusiasts. Much like the close-knit community of security professionals, hackers relate to and associate with other hackers (Xu et al., 2013). Many security professionals develop an interest in computers at a young age, like hackers do, and some have even actively hacked systems early in their association with computers (Kabay, 2008). Often, these young hackers experiment with increasingly deviant behavior, as defined by the majority of early computer enthusiasts, and many continue into less playful experimentation with hacking into an active "career" in hacking government or corporate computer systems (Xu et al., 2013). This identity with the hacking in-group may shape their behavior, leading some to continue into more questionable, and sometimes criminal behavior, while others adapt these skills for the sake of earning an income and become security professionals (Caldwell, 2011). This is not the usual path for a security worker, however.

Role conflict can become an issue for an I.T. person that has experience with, or certainly the intellectual capability to participate in hacking. Especially for those who move into the role of security professional (Ashforth & Mael, 1989). The majority of security professionals have, likely, never hacked into a computer system, but it is this close association between accessing a computer system without authorization and being charged with the responsibility of stopping those who want to access a system or network that underpins the characteristics assessed in this

study. It is not the assertion of this researcher nor the purpose of the study to suggest that all security professionals are former hackers or exhibit the tendency to hack networks. Rather, a primary reason the personality characteristics tested in this study were chosen was to suggest that to stop a hacker, a security professional must think like one.

## 2.3 Latent Class Analysis

Paul Lazarsfeld (1959) described the technique called latent structure analysis, which is now known as latent class analysis (LCA) (Henry, 1981). Lazarsfeld described the technique as the use of classical mathematical models in the study of attitudes, and it was developed for certain behavioral science studies to analyze discrete-valued data, which were assumed to be indicators of an underlying, latent construct. Often, a problem in sociological survey data is the necessity of gathering data for variables that are best designed to return ordinal or nominal values, instead of continuous variables. Factor analysis can be used to determine latent variables from variables represented by continuous data, but categorical data is often the best representation of an observed variable. Using LCA, latent classification variables measured as categorical data can be analyzed, much like factor analysis, to determine classes, thus, the development of latent class analysis. The technique was designed, specifically, for sociological survey analysis, as opposed to factor analysis, which was used to analyze continuous variables.

LCA's fundamental assumption is that the responses to each item are independent from selections made in other items, which describes local independence. The variables used in LCA are measured as either ordinal or nominal, and the objective in LCA is to define a latent variable within which the "manifest variables are locally independent" (McCutcheon, 1987, p. 17).

The goal of LCA is to determine discrete classes, which are mutually exclusive (have good class separation, entropy); in other words, a member of a class exists in one, and only one

class. Traditional LCA estimates both class membership probabilities and item-response probabilities (Lanza, Collins, Lemmon, & Schafer, 2007). LCA offers the advantage of not making any assumptions about how the data is distributed. Relative to factor analysis, which is a variable-oriented approach, LCA is a person-oriented approach (Collins & Lanza, 2010). In LCA, the person as a whole is the focus of the approach, which allows the study of individual characteristics related to the problem being studied (Bergman & Magnusson, 1997). LCA is appropriate when dichotomous or polytomous observed variables are available for use as input to the LCA. These categorical variables are used in the LCA to derive a latent categorical variable using the item-response probabilities of the observed variables. Similar to cluster analysis, LCA can be used to find clusters (or classes) of respondents to the observed variables, which, when analyzed by the investigator, result in distinct classifications.

Latent class analysis has been used in numerous studies to determine classifications of the respondents to the measures used. For example, Woo & Allen (2013) used LCA to investigate organizational employees intentions to leave a job and classified various type of seeking and staying behavior of employees. Other studies have been performed using LCA in psychology to assess depression (Mäkikangas et al., 2011), workplace affective commitment (Morin et al., 2011), and socialization process of open source software (Qureshi & Fang, 2010).

In the current study, LCA was used to determine the classification of the types of ISS professional. In practice, the study suggests that ISS professionals can be classified by a specific focus on one aspect of security over another. Further, the study posits that security workers range from aggressive to passive in terms of an individual's perception of a denial of service attack, for instance. In this scenario, one type of ISS professional monitors the output of particular security software systems and ensure that corrective action is taken to modify the

firewall when the monitoring software sends an attack alert. On the other extreme, a different type of security expert may frequently review the web server settings to determine ways to fine-tune the server to more quickly determine an attack is in-progress, while another type of ISS professional may develop a DoS program to run against a test server to validate and subsequently tweak settings to be modified before an attack is ever initiated against their organization. These different approaches are some of the many ways ISS professionals can be classified. This leads to the following hypothesis:

> H1: *Information Systems Security professionals can be categorized into classes ranging from passively-oriented (reactive) to aggressively oriented (proactive) mindsets toward information systems security.*

Whether passive versus aggressive is the name given to two of the classes, the intent of this hypothesis is to suggest that ISS professionals range from a more proactive approach to protecting digital assets to a more reactive stance.

Social identity theory, as discussed earlier, suggests that groups of people with similar characteristics tend to form homogenous groups, called in-groups. These groups seek people with similar characteristics and seek to consider others that do not possess these characteristics to be members of out-groups (Ashforth & Mael, 1989). Information security workers have a unique set of characteristics, even inside of I.T. They are directed to perform one of the most challenging jobs in an organization, which is to protect its digital assets. Performing this role can be taken very seriously and those who do it look for others that view security in much the same manner as they. One of the most influential tenets of in-group behavior is the tendency for a group member to view the successes and failures of the group as his or her own, which further drives the desire for association with like-minded security professionals. As part of their in-group, security experts see their roles as superior to other roles in the I.T. department, and in

many ways, they are, because a breakdown in security can have far-reaching, public impact, unlike a bug in a report program used by a middle manager (R. Brown, 2000). Because of the critical nature of the role played by ISS professionals, homogeneity of thought is very important, and the tendency to surround themselves with like-minded thinkers, likely, influences many security department staffing decisions. Therefore,

*H2: One class of the types of will be significantly larger than other types*

## 2.4 Creativity

Creative ISS professionals, this study suggests, are expected to possess the talent to anticipate the behavior of those intent to harm the security worker's organization from within or without. Creativity is necessary but not sufficient to anticipate security threats; however, without the ability to think like a hacker or like an internal employee who attempts to steal organizational secrets, the ISS professional will be not be considered a talented, aggressive information security expert. Creativity research has been conducted in various disciplines for decades. In fact, Baer (1998) reports that domain specificity of creativity, not generality of creativity is the relevant way to approach creative- and divergent-thinking (Baer, 1998). However, there is evidence that divergent thinkers exhibit creativity in cognitive process in various domains (Clapham, 2001; Guilford, 1959; Kim, 2006; 2008; Vincent, Decker, & Mumford, 2002), which has led to numerous scales used to measure creativity. Kim (2006) performed a review of the use of the TTCT and found that it is important, in Torrence's legacy, to enhance creativity among students. Measuring creativity is a challenging activity, compared to the use of creativity tests such as the TTCT in educational settings where the subject of the test is available and, given that it is most often used to test children for entry into gifted and talented programs, most parents readily agree to its use. In an adult setting, however, even an abbreviated version is, often, prohibitive.

This study suggests the necessity of aggressive information security professionals' high level of creativity enable them to anticipate hacking attempts, for instance, and to develop creative investigation and prevention techniques. Without high creativity, an ISS professional is reliant on the capabilities of the software installed for the organization and the alerts generated. This leads to the following hypothesis:

H3: *Creativity is related to class membership.*

## 2.5 Trait Competitiveness

Competitiveness involves the characteristic in a person in which he or she enjoys the desire to participate with the desire to win and to be better than others (Spence & Helmreich, 1983). This characteristic can manifest itself as a state in which a person is competitive in a particular situation but does not possess the competitive characteristic in other scenarios. Thus, from this perspective, competitiveness is situational rather than a trait of the individual's personality. However, even in situations in which people work independently, trait competitiveness is likely to set their expected level of performance higher to allow them to achieve favorable perception from their peers and lead to positive performance evaluations (S. P. Brown et al., 1998).

Competitiveness has been investigated at varying levels of analysis. For instance, competitiveness of the individual has been compared to the competitive climate of an organization using a person-environment framework to find that at the work group level, the competitive environment influenced the competitiveness of the individual (Fletcher, Major, & Davis, 2008). This indicates that in an environment where competition is encouraged, trait competiveness of the individual ISS professionals is, likely, higher, which suggests that in an environment such as an information security team where the constant threat of being out-

maneuvered by an intelligent foe is ever-present, the members of the organization, and certainly the top members of the information security team, will exhibit competitiveness for types of workers considered to be the top performers and the most aggressive. Further, in measures of interpersonal success, competitiveness has been shown to be a contributing factor to that success (Houston, Mcintire, Kinnie, & Terry, 2002). Houston et al. (2002) found that items of several popular competitiveness scales loaded on two factors: self-aggrandizement and interpersonal success. The scale used in this study is consistent with the self-aggrandizement factor, indicating that the definition presented in this study measures the competitive nature of the individual's desire to be noticed for their abilities to prevent "disaster" when faced with the seemingly insurmountable challenge of stopping threats from both inside and outside the organization. In short, whether the ISS professional competes with individuals or collectives whose goal is to defeat the security team for personal glory or for a sense of satisfaction due to successfully fending off a foe, the core behavior is competition, regardless of the underlying motivation. This competitiveness that is innate in the ISS professional is the construct under investigation.

ISS professionals have a significant responsibility to protect assets that belong to the organization for which they work. Adversaries are almost constantly attempting to break through the defenses set up by information security departments. A common competitor about whom an ISS professional must think is the computer hacker. Sometimes these hackers are bored, intelligent youth looking for a thrill or trying to test their computing abilities (Xu et al., 2013). Other times, competing organizations may use techniques like social engineering or even overt hacking of a company's network to gain competitive intelligence to use in the struggle to gain market share (Styles, 2013). In the worst case, organizations or governments must defend

networks against state-sponsored hackers whose financial backing and unlimited timeframe allow for seemingly never-ending and unstoppable attacks, called advanced persistent threats.

ISS professionals must face these challenges with unflinching determination and dedication to their profession. For those ISS workers who are devoted to their craft, the level of competitiveness in the face of insurmountable odds is staggering. In light of the types of ISS professionals in the study's classification, only those with a high level of competitiveness will meet this challenge with the levels of aggressive and highly competitive responses to fend off the most determined attackers. On the opposite extreme, a type of ISS professional whose low level of competitiveness will lead him or her to be satisfied with installation and monitoring of externally-facing intrusion detection software was anticipated, for instance. When an attack occurs, this latter type of ISS worker will rely solely on the alerts issued by the software and do only minimal investigation beyond the "canned" reports provided by the software vendor.

H4: *Trait competitiveness is related to class membership.*

## 2.6 Deceptiveness

We expect ISS professionals who aggressively protect his or her network from hackers, whose modus operandi relies largely on deceptive practices, to possess much the same, or higher, capability for deceptiveness. Kevin Mitnick (2003), one of the most notorious early hackers, describes the numerous instances of social engineering as a means to breach almost every network he admits to accessing. The role of ISS professional not only involves intrusion detection and log monitoring; it, also, requires preparing all employees for potential weaknesses in their organization's security scheme. Much to the chagrin of the ISS worker, their primary control of the "front door" is limited to adherence of all employees possessing security access to the digital assets to the security policy of the organization. With a little deceptive social

engineering, a hacker can convincingly gain access to security credentials with ease. To prepare the organization not to fall for phishing attacks, social engineering attempts, or even physical "tailgating" to gain physical access to sensitive data and areas of the company, the ISS professional must develop security policies and procedures to address all the varyingly deceptive means by which the security of the organization can be breached (Baskerville & Siponen, 2002).

Deceptive communication involves a message "purposely transmitted to foster a false belief or conclusion in a receiver" (Giordano & George, 2013, p. 211). Depending on the communication medium, deception can be difficult to detect and to prevent. In a group support systems context, Giordino & George (2013) found that groups participating in a complex task were more susceptible to deception. Serious deception in collaborative environments where electronic communication media is used at significant risk, and groups performing highly complex tasks are even more susceptible to deceptive communication (Giordano & George, 2013). This implies that in a highly complex environment of information system security, even the ISS professional is susceptible to deceptive communication. As the old adage goes, "you can't kid a kidder;" however, applies to information security workers, because the aggressively productive ISS professional will, this study suggests, have the ability to be highly deceptive, which will positively influence his or her ability to detect deception by others.

Charlton et al. (1997) performed a meta-analysis on people's judgment of their ability to detect deceptiveness and their confidence in the accuracy of their judgment. The researchers found that people were more confident in judgment of truth over judgment of lies (DePaulo et al., 1997). An ISS professional must confidently detect deception but not necessarily in statements made by individuals or organization threatening intrusion. Instead, they must think through the possible deceptive attack vectors, determine which are potentially accurate, develop

a prevention mechanism and monitor its success. They accomplish this through drawing hackers into scenarios too tempting for a hacker to resist, the honeypot (A. Gupta et al., 2010). This is a form of deceptiveness, which allows the ISS professional to detect deceptiveness in hackers. It is a difficult cycle of games of "chicken." ISS professionals have to either expose real digital assets to draw in a hacker or mask a benign digital asset in such a convincing manner that a hacker is drawn to it. The deceptiveness required to play this game indicates the level of deceptiveness necessary for ISS professionals. Since deceptiveness is a central characteristic of aggressively successful security workers, the following hypothesis is proposed:

H5: *Deceptiveness is related to class membership.*

## 2.7 Distrust

Distrust is used in this study, as opposed to trust, to indicate that the primary characteristic in use by ISS professionals is an inherent distrust for anyone capable of attempting to attack the ISS worker's organization's digital assets. Distrust is not an antonym of trust nor is it the absence of trust, regardless of how the word sounds. In information security, the digital assets of a company are of the utmost value to the success of that company, and the security worker is charged with protecting those assets. When the security worker trusts, he or she expects that unknown entities will not attempt to breach the network. This is simply a naïve way of looking at today's digital society. The literature on trust is both deep and broad. One aspect of trust is interpersonal trust and it is "an expectancy held by an individual or a group that the word, promise, verbal or written statement of another individual or group can be relied upon" (Rotter, 1967, p. 651). Non-negative outcomes are the expectation when an information security person trusts the actions of another party in an environment of uncertainty (Bhattacharya et al., 1998). Bhattacharya et al. provides a mathematical justification for the authors' definition of

trust. Further, in other studies, trust is defined in terms of an agency model (Shapiro, 1987). Within the framework of agency theory, trust is conveyed either formally or informally by a group or by an organization. This form of trust, however, is not the type of trust (or distrust) that is the subject of this study. Shapiro et al. (1987) focuses on impersonal trust, which occurs when, based on social convention or social ties, direct contact between two parties is unlikely. Distrust, this study contends, in many ways, is the opposite of this type of trust. An ISS professional cannot, specifically, scrutinize, or evaluate the performance of a person prior to a security attack. Therefore, rather than trusting that person, all unknown individuals are distrusted.

The distrust exhibited by ISS professionals suggested is similar to the distrust characteristics of the police personality, which states that a policeman develops a general distrust of everyone after seeing the side of humanity with which he or she must deal most often (Twersky-Glasner, 2005). A person who enters law enforcement, may enter with an idealistic notion of helping society, but over time and with experience, he or she sees the worst side of most everyone encountered. This exposure to the worst in many people can influence the attitude of the police officer toward everyone. This is a significant issue in law enforcement and has led to numerous studies and attempts to address what most law enforcement agencies consider a problem.

In many ways, the ISS professional is at risk of the same change in attitude toward other computer professionals and even internal employees. Distrust has been studied from many perspectives and in many disciplines. Cho (2006) suggested that trust and distrust are distinct concepts that affect the behavioral intentions of exchange relationships in B2C interactions. Distrust has been viewed as an expectation that the other party's actions will result in injury

(Luhmann, 1979). Further, colleagues are distrusted due to incompetence, irresponsible, or even harmful actions (Lewicki et al., 1998). In an organizational context, both Lewicki et al. (1998) and Kramer (1999) suggest distrust is correlated with other dispositional orientations such as belief about human nature. Distrust has been addressed in the management literature quite extensively, but distrust in technical fields has been primarily the focus of marketing and information systems

This study addresses distrust, not from the perspective of whether a person is trusted or not; rather, the study's interest is in the attitude of the ISS professional and the expectation he or she has on the behavior of other computer professionals or employees. The type of distrust exhibited by the ISS professional is not one focused on team members in an organizational context. This is not to imply that distrust as described by Lewicki et al. (1998) and Kramer (1999) is not present in an information security team; rather, the focus is on the distrust felt by the ISS professional similar to the distrust demonstrated in the police personality. Thus, the following hypothesis is offered:

H6: *Distrust is related to class membership.*

## 2.8 Morality

Early work on morals focused on moral development and reasoning as cognitive-development process in childhood through young adulthood (Piaget, 1932). Kohlberg (1958) continued along this line of research by describing the development of moral stages in children and young adults. The Defining Issues Test was developed to measure moral judgment and categorize them into stages of moral judgment development (Rest, 1975; Rest, Cooper, Coder, Masanz, & Anderson, 1974). As a person develops, he/she moves through moral stages of development, and Rest's (1973) research supported this by developing and validating principled

moral statements which indicate a person's moral development. Rest's P score correlated with education-level and not with age, which indicates moral judgment is more closely related with developmental stage rather than age (Rest et al., 1974). Further, it was determined that college students have higher moral judgment development than do students who do not continue their education beyond high school (Rest, 1975), and adults who do not continue their education into college measure moral judgment development equivalent to a college student. Therefore, research shows the moral judgment developmental level of college students is a valid indicator of the majority of adults.

A person's "self-conception organized around a set of moral traits" defines a person's moral identity (Aquino & Reed, 2002). Characteristics of morality as described by moral identity may be identified by the following adjectives: caring, compassionate, fair, friendly, generous, helpful, hard-working, honest, and kind. A person's moral identity is comprised of outward actions in the person's environment and the person's self-concept of moral traits. These two components work together to form the moral identity, but they can be inconsistent when the actions in the world do not reflect the internal self-concept. For example, the person who backs into another car in a parking lot and leaves a note stating, "I am writing this note so the people who saw me hit your car and are watching me now think I am identifying myself and giving you my contact information" may not have an internalization component consistent with his/her symbolization component. The aspects of morality, within the context of moral identity, help define the important characteristics of his or her morality, which suggests:

H7: *Morality is related to class membership.*

**Table 2 – Hypotheses & Assessment Methods**

| | Hypothesis | Method of Assessment |
|---|---|---|
| H1 | Information Systems Security professionals can be categorized into classes ranging from passively-oriented (reactive) to aggressively-oriented (proactive) mindsets toward information systems security | Latent Class Analysis |
| H2 | One class of the types of will be significantly larger than other types | Latent Class Analysis |
| H3 | Creativity will predict class membership | Multinomial Logistic Regression |
| H4 | Trait Competitiveness will predict class membership | Multinomial Logistic Regression |
| H5 | Deceptiveness will predict class membership | Multinomial Logistic Regression |
| H6 | Distrust will predict class membership | Multinomial Logistic Regression |
| H7 | Morality will predict class membership | Multinomial Logistic Regression |

## CHAPTER 3: METHODS

The study consists of two stages of data gathering and analysis. First, to assist in determining the most informative questions to ask, which was used as input to the latent class analysis, a Delphi study was conducted. After the Delphi study was completed, a survey was developed to assess the characteristics in the research model. The information from the Delphi study and relevant information security literature were used to develop six questions for the survey that are used to classify the types of ISS professional is contained in the sample. In the pilot study, the questions were included in the survey and the survey was given to computer science and MIS students. In the primary study, practicing ISS professionals were the focus. The survey contains a total of 57 questions, including the six described above. In addition to the questions to aid in determining the classification, the remaining 51 questions measure creativity, trait competitiveness, deceptiveness, distrust, and morality using recently developed instruments that have shown to have good psychometric properties. A more detailed explanation of the instruments used is provided below. The data from the survey is first used to perform a latent class analysis to determine classes (or types) of ISS professional using the six questions influenced by the Delphi study. The primary researcher will review the classification and identify the number of classifications indicated and then will regress each of the classifications on the characteristics assessed in the other questions in the survey using multinomial logistic regression. The intent of the multinomial logistic regression is to determine which constructs best influence membership in each of the classes determined in the latent class analysis. A more detailed explanation of the logistic regression process is provided below.

## 3.1 Delphi Study

One of the challenges of the study's approach is to find scientifically valid questions to provide data to be used in the latent class analysis. The Delphi technique was chosen based on its long history and use in the information systems and social science fields (Landeta, 2006). The Delphi process is a repetitive process that seeks to build a common understanding and a consensus among experts in a specific area where theory is not developed or is conflicting. An advantage, in the context of information security, is the anonymity of the participant, which lends itself to more open input from participants. This openness is one of the greatest advantages of the Delphi technique, because it encourages honest and thorough input. Although it has its critics, the technique has shown benefits in situations where expert input into the method for determining ISS professional classification is required. The current study, uses the traditional form of the Delphi technique to guide the research to questions that practicing information security professionals find helpful when determining the effectiveness of other information security personnel. The study's use of Delphi was to provide information that can be used as a springboard to developing items for the survey instrument that will provide separation among ISS professionals as they respond to the survey. This will lead to a more effective classification and more applicable research.

### *3.1.1 Delphi Participants*

The researcher requested participation from chapter presidents listed on the Information Systems Security Association (ISSA). ISSA was chosen based on its stated purpose to "the community of choice for international cybersecurity professionals dedicated to advancing individual growth, managing technology risk and protecting critical information and infrastructure" (ISSA, n.d., p. 1). The stated goal of the ISSA is to promote information

management practices which achieve confidentiality, availability, and integrity of member organizations' digital assets. The association holds conferences and supports the education of its membership through training, through information availability on its website, and through information sharing between and within local chapters. Included on the page listing each chapter is the name of the local chapter president and an e-mail contact for the chapter. As the leader of each local chapter, the president directs the activities of the chapter, determines relevant security topics to discus, and schedules sessions to enhance the membership's professional development. To lead a group of ISS professionals, the president has prior experience of the topic of information systems security. In addition to personal expertise in ISS, the president serves as a conduit for information from the national organization, which further supports the president's recognition as a leader in the information systems security field to hold the position. It is for this reason that presidents of local ISSA chapters were a clear choice for a sample of information systems security experts.

### *3.1.2 Delphi Round 1 – Questions*

Participants were sent an e-mail explaining the importance of their participation in the study and the impact the study can have on the field of information system security. Another intent of the text of the e-mail was to establish credibility for the primary researcher and, hopefully, bypass the typical deletion of e-mails such as this when received by busy ISS experts. The primary researcher has experience in a role similar to the respondents and a significant challenge to gathering data from this population is simply getting possible participants to respond. Thus, the wording of the e-mail was carefully crafted. The question posed to the ISSA chapter presidents was:

*What question could you ask information systems security professionals (job candidate, colleague, etc.) to determine whether thy will be/are an effective information security worker? Not necessarily tool- or environment-specific questions.*

The first round of the Delphi study was sent, via e-mail, to the ISSA chapter presidents. The e-mail contained a brief introduction with a "thank you" statement for agreeing to participate, instructions explaining the use of a survey service to facilitate the capture of the participants' responses, a URL to the site, an explanation of the study, and instructions explaining how the participants can access the site. The URL was not a clickable link to avoid possible participants discarding the e-mail for security reasons. The participants were given ten days to respond to the questions before they received a reminder to respond. The e-mail sent is included in Appendix C as Initial Delphi Participation E-Mail.

ISSA chapter presidents choosing to participate in the Delphi study were presented with an instructional page explaining the context of the study and the process. The respondent was greeted with a "Thank you" message for participating in the study. The instructions explained the Delphi process as a three-round process in which they will provide data for the first stage of the research. Further, the instruction stated that the participant's e-mail address was needed to allow the researcher to compile the results from this questionnaire and to provide the respondent an opportunity to rank the questions provided by his or her peers. The third and final round of the Delphi study, stated in the instructions, was to allow the respondent to confirm the ranking of the questions, which were provided by their peers. Finally, a statement indicating that the study has been reviewed by the University of Mississippi's Institutional Review Board (IRB) was provided to the respondent.

After either confirming the e-mail address from the link provided in the e-mail address above, which was passed into the Qualtrics survey, or the respondent was allowed to provide an

alternative e-mail address, the respondent was taken to the next page of the questionnaire. The second page of the Qualtrics questionnaire asked the respondent to provide the following demographic information:

1. Age
2. Years in Information Systems (Information Technology, In the computer field, etc.)
3. Years in Information Systems Security (Information Security)
4. Sex
5. Job Title
6. Industry of [respondent's] current company

After the respondent provided information answering the question, the questionnaire thanked the respondent and states that "in about 5 business days, you will receive an e-mail at the address you provided above with instruction on the next step." The Qualtrics software then thanked the respondent for the time taken to complete the survey.

### *3.1.3 Delphi Round 2 – Ranking*

As responses were recorded by Qualtrics, the information provided by the respondents was downloaded, with the final download performed on the fifth business day after the initial e-mail was sent. The questions were extracted from the downloaded responses, duplicates were removed by the primary researcher and an independent researcher not involved in the study. The responses were compiled into a list and sorted on the 12$^{th}$ through 20$^{th}$ characters in the question provided. Although this did not randomly order the responses, the intent of sorting on an arbitrary string in the response is to re-sort the responses so that each participant's responses are not grouped together. This is to, as best as can be performed, mix the responses to prevent any individual respondent from recognizing his or her group of questions and rank them highest. As time had passed prior to the ranking, the hope was that a respondent would have forgotten the data provided by him or her, which served to reduce bias toward his or her own questions.

The respondents to Round 1 of the Delphi study were sent an e-mail with instructions and a link to a Qualtrics survey containing the list of questions provided by all of the participants in Round 1 in a format that allows each respondent to order the questions from 1 to 10. The e-mail is included in Appendix C – Communication as Delphi Ranking E-Mail.

The participants in the first round copied and pasted the URL in the e-mail into a browser, which took them to the opening statement for the second round. The statement displayed on the first page of the Qualtrics questionnaire is:

> Thank you for your responses to our question regarding identifying effective information security professionals. Please rank the questions presented on the next page in order of importance in determining effective information security workers, with the questions at the top best identifying effectiveness and, at the bottom, questions you feel provide the least information to determine information security effectiveness.
>
> Please provide your response by [date], and, again, this research is not possible without your input. So, please take a short time to assist in this research.
>
> *This study has been reviewed by The University of Mississippi's Institutional Review Board (IRB). The IRB has determined that this study fulfills the human research subject protections obligations required by state and federal law and University policies. If you have any questions, concerns, or reports regarding your rights as a participant of research, please contact the IRB at (662) 915-7482.*

Each respondent proceeded to a single page of a Qualtrics survey and rank the questions received in Round 1 in order of importance in assessing a person's effectiveness as an ISS professional.

### *3.1.4 Delphi Round 3 – Confirmation*

E-mail was sent to the respondents in Round 2, which enabled each participant to confirm the rankings and make any changes each felt necessary. After the confirmation was received, the questions and their rank were used to develop questions included in the survey of ISS professionals. The six questions were used in a latent class analysis to classify information security types.

## 3.2 Research Design

An emphasis of this study was to perform a person-centered approach to information system security. To that end, a Delphi study was conducted to determine questions that could formed the basis of the classification of ISS professionals. This classification is important to show the characteristics that make individuals effective in a wide array of security roles. Further, it demonstrates the diversity of responsibilities in information security and suggests that an aspect of information systems critical to both organizational and national security that cannot be simply populated with the best technically competent individual; rather, an emphasis on personality characteristics is necessary to keep digital assets secure. First, however, the researcher must determine the types of information security professionals that are currently practicing in the security field. To determine this classification of security professionals, latent class analysis (LCA) was used. The class indicators were developed from the ETSI Information Security Incident taxonomy based on the Delphi survey items resulting from the Delphi study that was perfumed in stage 1 of the study (Rennoch & Gaudin, 2013). The survey items used in the LCA contained multiple categories per item in the first four items, and the last two questions had dichotomous responses. The four multi-category items were pooled to make them dichotomous items for use in the latent class analysis. Menard (2010) suggests pooling multi-category items when use of binary items helps in the analysis without loss of meaning.

## 3.3 Measures

The current study has two distinct sets of measures that are included in the survey instrument. The results of the Delphi study were used as a basis for developing the first set of items to be included in the survey. Additionally, existing instruments to use in measuring the latent personality traits were included in the survey. The following section describes the survey

participants, the two sets of questions that were included on the survey, and two types of data analysis approaches to analyze the resulting data.

### *3.3.1 Delphi/ETSI ISI Taxonomy Integration*

The Delphi study respondents provided many useful questions to guide the development of questions used in the latent class analysis. Additionally, the ETSI ISI taxonomy provides very specific attributes and categories of incidents and vulnerabilities, which can be used to determine the breadth of work an information security professional is expected to perform (Rennoch & Gaudin, 2013). By using the specificity of the ETSI ISI taxonomy in classifying the types of incidents and vulnerabilities and the general nature of the questions provided by the Delphi respondents, the researcher developed questions that covered the breadth of the Delphi responses. For example, a highly ranked Delphi response was "what is the biggest challenge you have faced in securing your past or current employer." The ETSI ISI taxonomy describes an Origin attribute that details corresponding Categories such as Accident, Unintentional act, Careless act, and Malicious act. These categories of the attribute Origin in the ETSI ISI taxonomy represent four threats or challenges to a network. Thus, by combining the Delphi respondents' questions with the ETSI ISI Origin list of categories, the researchers arrived at the following survey question:

> Which of the following presents the biggest threat to your network?
> 1. Accident
> 2. Unintentional act
> 3. Irresponsible/careless act by internal employee
> 4. Malicious act on a digital asset

The remaining five questions used in the LCA were developed in a manner similar to the process described above. Upon completing the questions used for the LCA, the list of questions were

sent to practicing information security professionals who were asked to confirm that the questions developed adequately interpreted the breadth of the Delphi respondents' questions.

### *3.3.2 Survey Items*

The survey consists of 51 questions that measure the type of ISS professional of the respondent as well as personality traits such as creativity, morality, deceptiveness, and distrust. The specific survey items for each of these constructs can be found in Appendix A, as can the items for the dependent variable, Information Systems Security Class. The personality items have been drawn from current studies where the instrument was either developed for the study or simply used as part of the recent study. To determine convergent and discriminant validity, a confirmatory factor analysis (CFA) was performed and the factor loadings were assessed.

## 3.4 Pilot Study

A pilot study was conducted using computer science and information systems students from a mid-sized southern university. The pilot study involved a survey of fifty-one questions. Five of the questions were adapted from the Delphi study with the remaining pilot questions comprised of instruments from measuring creativity, trait competitiveness, deceptiveness, distrust, and morality. Following the pilot study, the original IPIP questions were replaced with more recent survey scales for use in in the main study.

### *3.4.1 Pilot Study Participants*

Students were invited to participate in the study through the use of bonus points offered by the professor or through the opportunity to be selected to receive a $20 gift card from a local business. If the gift card approach was used by the professor of a class asked to participate, the gift card was awarded through the use of a sign-in sheet where the participants wrote only their

students IDs and no other identifying information as they left the survey. The list of student IDs were delivered to the professor along with a gift card. The professor randomly chose a participant in the class to receive the gift card using a method determined by the professor.

Two hundred students were given the opportunity to participate with the expectation of having 75 student participants. A total of 106 responses to the pilot study were received.

## 3.5 Main Study

The Phase II study for this project involved a survey given to practicing information systems security professionals. These respondents provided the basis for security professional classification and for the analysis of the influence of the personality characteristics on class membership.

### *3.5.1 Main Study Participants*

Participants for the main study included working adults in the information technology and security industry. A variety of sources were used to achieve 330 respondents from 23 different industries with a median age range of 29 to 33. Respondents were contacted through personal LinkedIn connections and LinkedIn information security groups. The potential respondents were asked to forward the link to the survey to colleagues working in the security field. A large number of respondents forwarded the Qualtrics survey link to five or more personal business contacts. Furthermore, additional respondents were attained from regional and national information security groups on LinkedIn. Almost 500 participants responded to the survey but a large number of the respondents abandoned the survey without answering more than 10 of the questions assessing characteristics of the respondent. These surveys were removed from the study.

The participants were provided a link to a Qualtrics survey containing the questions resulting form Stage 1 of this study, forty-four questions assessing personality traits of the participants, and three questions used to control for age, education, and sex. The average length to respond to the survey was approximately 12 minutes. All respondents answered the questions between April 21 and June 5, 2014. The surveys were closed on June 5, 2014 and no additional responses were allowed.

### *3.5.2 Latent Class Analysis*

One of the issues in LCA is the sparseness of the contingency table (Collins & Lanza, 2010). If a study does not contain an adequate number of observations, the table against which all of the analysis is performed can contain too few observations, leading to empty cells when viewed as a grid. Sparseness of the contingency table is a function of the number of observations (N), specifically, the number of observations divided by the number of possible cells in the table (W). The recommended minimum number of observations is $\frac{N}{W} > 5$, where W is calculated, for binary class indicators used in this study, as $2^q$. The exponent, $q$ is the number of binary questions. Thus, the formula used in this study to calculate the minimum number of participants for a questionnaire containing six binary class indicator questions was $\left(\frac{N}{2^6}\right) > 5$. Solving for N gives $N > 5(2^6) > 320$. Therefore, the minimum number of usable observations, to provide the recommended minimum for LCA use, was 320 usable observations.

Traditionally, researchers employing latent class analysis have used a single-step approach in which the covariates are included in the analysis in the same process in which the latent classes are determined (Clark & Bengt, 2009). Although this method avoids the problem

of incorrect estimates and standard errors by allowing the individual observations to be fractional members of all classes, it is computationally intensive due to the number of variables in the analysis. Additionally, the auxiliary variables may influence class membership, which may change how the latent classes are interpreted.

A three-step process has been proposed that involves first determining class membership prior to including auxiliary variables (Asparouhov & Muthen, 2013) to analyze only the classification identified in the LCA. To confirm the classification, the entropy of the latent class model was calculated to find values higher than 0.6 which indicates better classification of individuals (Asparouhov & Bengt, 2013). Performing a multinomial logistic regression using the most likely classes saved as a result of the LCA can be performed if the entropy value of the LCA is close to 0.8 (B. O. Muthén, n.d.). After the LCA, a multinomial logistic regression is performed; so, to remain consistent with the suggestions of Asparouhov & Muthen (2013) and include all of the predictor variables in the analysis to estimate the multinomial model, the covariates are listed as auxiliary variables in the LCA.

### *3.5.3 Confirmatory Factor Analysis*

A confirmatory factor analysis (CFA) was run on the items measuring the personality characteristics creativity, trait competitiveness, deceptiveness, distrust, and morality. Reliability was calculated on each latent variable. When the CFA did not provide adequate model fit, the advice of Byrne (2012) was used to achieve adequate model fit of CFI > 0.9, RMSEA < 0.7, according to Hair etal. (2010).

### *3.5.3 Multinomial Logistic Regression*

Multinomial logistic regression was used as the third step of the 3-step analysis, as suggested by Asparouhov & Muthen (2013). Following the technique offered by Hosemer and

Lemeshow (2013). The fit of the individual variables was assessed prior to performing the multivariable multinomial logistic regression. Colinearity was assessed and offending variables removed, and, finally, multivariable multinomial logistic regression was performed with all variables (Hosmer, Lemeshow, & Sturdivant, 2013). Following the first round of multinomial logistic regression, likelihood ratio tests were used to assess the fit of each variables (B. O. Muthén & Muthén, n.d.). Additionally, the likelihood ratio tests were confirmed with Wald tests. After the model fit was assessed and confirmed, a final multinomial logistic regression was performed with the three remaining factors and covariates serving as control variables (Hosmer et al., 2013).

Figure 3 contains a graphic representation of the research methodology used in the study.

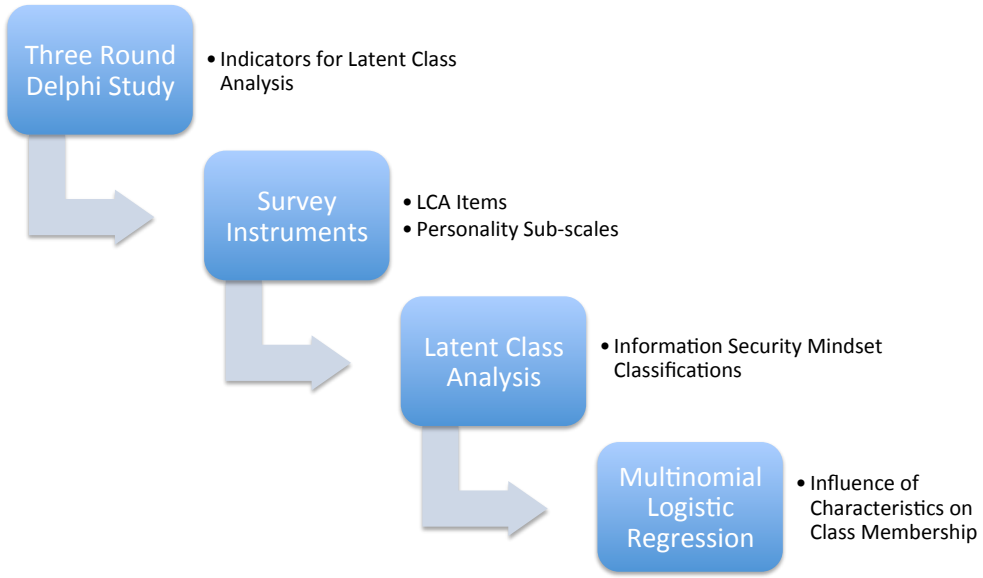



**Figure 3 – The Delphi-Driven Latent Class Analysis Method**

# CHAPTER 4: RESULTS

## 4.1 Delphi Study Results

The study utilized the Delphi technique as a way to determine questions to use during phase 2 of the study, which involves determining the types of ISS professionals, which will lead to a classification of ISS professionals. The goal was a set of four to ten questions that result in categorical responses that are added to a survey of ISS workers. The responses to these questions were used in a latent class analysis, which is described in the methods section of this paper. To arrive at a list of questions that results in a practical classification of ISS professionals, the investigators chose the Delphi method on which to base questions used to calculate the classification to leverage security experts' opinions. Structured interviews are a valid means to extract information from expert security professionals; however, without subsequent, independent confirmation of their opinions, the questions could be less reliable than Delphi-based questions. Therefore, Delphi was chosen due to the four tenets of a Delphi study: anonymity, controlled feedback, group response, and reduced time involved in identifying, convincing to participate, and then interviewing numerous security experts.

The best approach to a Delphi study is to contact potential participants through direct means of communication such as face-to-face or by telephone. In the case of this study with the population of information security professionals, data indicating name, address, and/or telephone contact information was not readily available. The best source of information found by the researchers was the Information Systems Security Association (ISSA) list of chapters (ISSA, n.d.). The chapter page on the ISSA site listed the name of each chapter, the name of the

president of each chapter and the chapter's official e-mail address. Most of the e-mail addresses were of the form president@issa-location.org, where 'location' is the chapter name or an abbreviation of the chapter name. This inhibited the investigator's attempts to adhere to the "high-touch" nature of a traditional Delphi study. The Delphi study returned somewhat useful results, but were different responses than anticipated. Although the results led to useful questions added to the survey, the process of the Delphi study went unexpectedly, too.

The process of the Delphi study did not run as smoothly as originally designed, and the results reflected an understanding of the questions asked during the Delphi process that was different than the original intent of the researcher. However, the broad understanding of the primary focus of the Delphi question provided a better foundation upon which to build the survey instrument. After a brief period of trying to recover from the "lemons" the researchers were dealt, lemonade was the result. This led to a better set of questions to use for the classification of ISS professional and to a better study, overall. Below, the results of the Delphi study are presented and the ultimate questions developed from the results are presented.

### *4.1.1 Delphi Participant-Supplied Questions Results*

Participants for the Delphi study were chosen from the Information Systems Security Association (ISSA) web site, which contains a list of the names of each local chapter. The e-mail listed in the Delphi portion of the Methods section, above. The intent of the e-mail was to establish credibility for the primary researcher and, hopefully, bypass the typical deletion of e-mails such as this when received by busy ISS experts. See Appendix B – Tables for Delphi Rounds and Statistics for the information regarding respondents.

There were very few company e-mail addresses listed on the site. Most non-ISSA-related e-mails were personal GMail or other free e-mail services. In five attempts to follow a corporate

website to get a phone number and to make contact with the person listed on the ISSA site, the primary researcher was unsuccessful in multiple attempts for all five contacts for various reasons. Thus, the ISSA chapter e-mail addresses were used to send an e-mail requesting participation in the Delphi study. Additionally, many of the questions to ask that were provided by the Delphi experts were very good differentiating questions but many were simply focused on the binary selection decision with which ISS managers are concerned, and did not differentiate the differences among practicing ISS team members. The managers participating in the Delphi study were focused on providing questions they used to determine whether to hire an ISS person or not rather than on the questions to differentiate between the various types of ISS professionals.

The responses from the original e-mail to 82 participants did not yield as many responses as anticipated. In fact, only six people responded to the initial e-mail by filling out the Qualtrics questionnaire. It may be that the original e-mail tried too hard to show the primary investigator's experience in I.T. to warrant their cooperation in the study. Possibly, potential respondents felt that the e-mail "tried too hard" to convince them that the request was legitimate, or, the potential participants were simply unwilling to take yet another survey from an unknown person. Regardless of the reason, a low percentage responded to the initial request, which reinforced the knowledge that Delphi is a technique to be used in a setting where the potential respondents are available for contact. In the case of ISSA presidents, they were not. Therefore, a second attempt was necessary to get adequate response. This lead to a more direct e-mail with the requirements of the respondents even more clearly spelled out. Thus, a second e-mail was sent to the chapter presidents that had not responded to the initial request, approximately ten business days after the initial e-mail. The email is included in Appendix C – Communications as Delphi Second Request For Expert Participation.

The second e-mail resulted in an additional twelve respondents, which was not quite as high as the researcher had planned, but it was an acceptable number of responses. After removing responses with no e-mail addresses allowing the investigator to continue the Delphi technique with the participants, Round 1 of the Delphi study resulted in 22 questions, with two duplicates. After removing duplicated questions, twenty questions were sent back to the respondents for ranking. The questions resulting from Round 1 of the Delphi study can be found in Appendix B – Tables as Delphi Questions from Experts.

### *4.1.2 Delphi Ranking Results*

After closing the questionnaire to participants, the Delphi study finished with eight usable responses. Unfortunately, many of the questions they provided demonstrated a misunderstanding of the intent of the question asked in the Delphi study. The respondents appear to have interpreted the question as asking "what interview questions would you ask an information security job candidate?" The questionnaire did offer a job candidate as a "such as" example, but it also mentioned colleagues, as well. However, the results of the first round of the Delphi contained many questions that are irrelevant to this study. However, under the rules of Delphi, the respondents were sent a list of all questions and asked to rank them in order of effectiveness in assessing information security effectiveness. The e-mail to the respondents for the second round of the Delphi study is included in Appendix C – Communication as Delphi Second Request for Expert Participation.

Fortunately, the resulting ranking weeded out the uninformative interview questions received from Round 1. Of the 11 respondents from Round 1, eight sent back rankings. The respondents were asked to rank the questions relevance to assessing a person's information security effectiveness. At this point, the participants were apparently still considering them

interview questions, but, fortunately, the resulting ranking identified questions that could be easily adapted to a survey format. Others, however, were more difficult to adapt directly to a survey format, because they were too open-ended like interview questions can be.

To calculate the rankings, the top ten items provided by each of the eight information security experts were used. Then, the unranked questions were assigned a value of eleven. Some of the respondents ranked one through ten, another ranked one through twenty and a third, for example, ranked one through fourteen and left the remaining six questions blank. Since the instructions in the e-mail requesting ranking allowed for ranking the top ten, if needed, the researcher decided to keep the top ten items and assign the value 11 to the remaining, unranked questions. This decision introduced a level of consistency to all respondents' rankings. For instance, if one respondent ranked item E a rank of 2 and another assigned it a rank of 17 and another did not rank it in the top ten, taking the average of the rankings would calculate on average of 9.5. The third respondent, however, did not have question E in her top ten; so, without assigning a default value for unranked items, the results may be artificially high.

Further, to be consistent, any respondent that ranked questions beyond 10, their $11^{th}$ and greater ranking were all changed to 11. This gave all items with no ranking the same value; so, when the average ranking was calculated, no item ranked below 11, but many ranked higher than 10. It simply was not valid to either force an 11 through 20 ranking or to allow the average calculations to include 11 through 20 rankings, for those who did them. After the average rankings were calculate, the respondents were given an opportunity to confirm the ranking or make any changes. The respondents were not shown the actual average ranking calculations. They were simply shown the ordered list. None of the respondents offered any alternative order

to the questions. The final rankings can be found in Appendix B – Tables as Delphi Final Ranking of Expert's Questions.

### *4.1.3 Final Delphi Results*

Delphi studies are high-touch processes, and the context of information security presents an environment where high touch is extremely difficult. Optimally, 15 or more respondents in the final round of a Delphi study is best; however, the questions received by the eight respondents were adequate to use in developing scientifically valid questions to use in the survey for the classification analysis. To develop the questions to be added to phase II survey of information security professional, the ETSI information security incident taxonomy (Rennoch & Gaudin, 2013) was used. This taxonomy details and organizes the types of incidents that can occur in the context of information systems security. It identifies categories of the sources of the incident, the actions taken by the sources of the incident, the consequences of types of incidents, and many categories of events that occur when a digital asset is either attempted to be breached or is actually breached. By using the ETSI ISI Taxonomy, the study presents categorical responses to assess the type of information systems security person a participant in the Phase II survey.

Appendix A, Information Security Classification contains the questions derived from the results of the Delphi study as well as from the ETSI ISI Taxonomy. Where appropriate, the questions resulting from the Delphi study along with its proxy or re-wording are presented.

## 4.2 Main Study Results

### *4.2.1 Latent Class Analysis Results*

To test the existence of an information security classification, a latent class analysis was run on 330 respondents leading to an optimal model of six classes. To determine the optimal number of classes contained in the data, the researcher is responsible for evaluating the data using many different potential classes and determining which provides the best classification of the types, of information security professionals. The first test in determining the optimal model is a test of absolute fit. Collins & Lanza (2010) emphasize the importance of parsimony as a philosophical principle in research, which states that a simple model is preferred to a more elaborate one. Therefore, in this study, the goal is to find the model with the least number of classes that explains the data. To that end, the process of determining the number of classes began with a 2-class model and looked at absolute model fit, first. In LCA, the null hypothesis is a test of independence (Collins & Lanza, 2010). If the observed data are unlikely, then there is strong evidence to reject the null hypothesis. In LCA, to fail to reject the null hypothesis of independence indicates that the model being tested is the population model that produced the observed data. To assist in testing for absolute model fit, MPlus produces two chi-square test of model fit for the categorical outcomes, Pearson Chi-Square and Likelihood Ratio Chi-Square. As models are tested, starting with a 2-class model, the researcher first viewed these tests of absolute model fit before continuing to the tests for relative model fit. After determining the model had a good absolute fit, the relative fit was addressed to make the final decision regarding the number of classes that optimally explained the number of classes.

Nylund, Asporohov, & Muthen (2007) evaluated popular methods of determining an appropriate number of classes in a latent class model, often called class enumeration. A popular

statistical indicator for deciding the number of classes in a study's population is to rely on the lowest Bayesian Information Criterion (BIC) (Woo & Allen, 2013). Statistical software packages, such as MPlus, that contain latent class analysis modules provide a number of statistics to help the researcher discern the appropriate number of classes (Nylund et al., 2007). Nyland, et al. (2007) performed a simulation study that compared several common class enumeration techniques such as AIC, BIC, and the adjusted BIC with other, non-information-criterion (IC) techniques with other approaches such as Lo-Mendell-Rubin fit index and the Bootstrapped likelihood ratio test (BLRT). Further, the authors found that chi-square difference tests for determining the number of classes are not applicable in LCA due to regularity conditions not being met. The difference in likelihoods of a number of classes (k) compared to its k-1 model is not chi-square distributed.

Therefore, this study uses the BLRT as the primary statistic to assist in determining the appropriate number of classes found in the LCA (Nylund et al., 2007). Table 3 shows a comparison of the model with a different number of classes. Both the BIC & the BLRT are reported in this table, but the BLRT was the test that best identified the optimal model in conjunction with another very important statistic, entropy. Entropy indicates the level of class separation, with a higher number indicating more clearly identified clusters from which the classes are determined. For instance, Model 1, the 2-class model, has a significant BLRT p-value and the lowest BIC; however, entropy of this model is 0.546. Recall from a discussion in chapter 3 that .6 is the minimum value for entropy to adequately separate the observations into identifiable classes (Asparouhov & Muthen, 2013). Therefore, Model 1 was eliminated. Models 2 & 3 showed BLRT p-values of 0.065 & 0.092, respectively, which are significant at the $\alpha = 0.1$ level. Model 4, the 5-class model, does not have a significant BLRT p-value and is,

thus, eliminated, along with Model 6, the 7-class model for the same reason. Execution of the latent class analysis for Model 8 resulted in a local maxima and was eliminated due to inadequate calculation results.

**Table 3 – Comparison of Latent Class Models**

| Model | Number of Classes | Pearson $\chi^2$/ Likelihood Ratio $\chi^2$ p-values | Loglikelihood | BIC | # of free parameters | Entropy | Bootstrapped LRT (k vs. k-1 classes) p-value |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 0.005/0.001 | -1171.071 | 2417.5 | 13 | 0.546 | < 0.001* |
| 2 | 3 | 0.006/0.004 | -1162.619 | 2441.219 | 20 | 0.628 | 0.065** |
| 3 | 4 | 0.050/0.027 | -1154.093 | 2464.762 | 27 | 0.878 | 0.092** |
| 4 | 5 | 0.099/0.066 | -1147.623 | 2492.415 | 34 | 0.766 | 0.192 |
| **5** | **6** | **0.428/0.244** | **-1140.106** | **2517.976** | **41** | **0.785** | **0.040*** |
| 6 | 7 | 0.358/0.261 | -1136.028 | 2550.412 | 48 | 0.745 | 0.500 |

*Significant at $\alpha = 0.05$
**Significant at $\alpha = 0.10$

Thus, Model 5, the 6-class model, meets all of the criteria for the optimal model – non-significant Pearson & LRT, significant BLRT p-value and entropy greater than 0.6. In fact, the entropy value of Model 5 is adequate to enable the use of a particularly helpful technique in the subsequent multinomial logistic regression, which will be addressed later in this chapter.

Questions used for the latent indicators are listed in Appendix A. Questions 1, 2, 3, & 4 contained more than two options from which the respondent was required to select only a single response and were pooled to result in a binary response to the question. Question 5 & 6 included only two possibilities each. The questions used in the LCA were developed from the ETSI Information Security Incident Taxonomy guided by results of the Delphi study discussed earlier. Using the advice of Collins and Lanza (2010) to ensure adequate observations in the LCA and for parsimony, class indicator responses were pooled into responses that resulted in a binary decision, yet retained meaningful information.

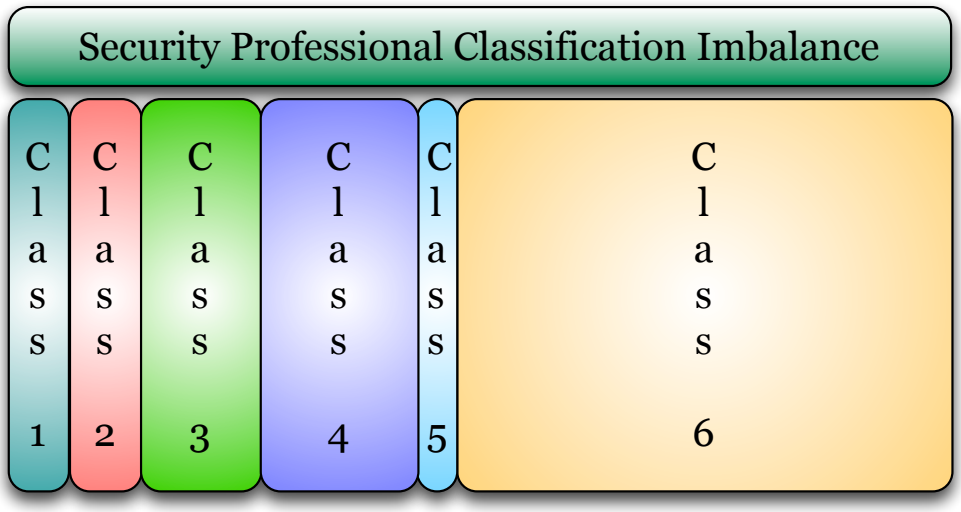



**Figure 4 – Security Professional Classification Imbalance**

**Table 4 – LCA Class Assignment**

| Class | Name | Count | Percentage |
|---|---|---|---|
| 1 | Passive Monitor | 21 | 6.40% |
| 2 | Active Planner | 25 | 7.60% |
| 3 | Manifest Technical Investigator | 42 | 12.70% |
| 4 | General Monitor | 55 | 16.70% |
| 5 | Active Investigator | 14 | 4.20% |
| 6 | General Protector | 173 | 52.40% |

Figure 4 highlights the imbalance that occurs in information security departments in even large organization. Consistent with social identity theory, security professionals gravitate toward other security workers with similar characteristics, and the figure illustrates the imbalance in mindsets that can occur. Table 4 shows the number and percentages of respondents placed in each of the six classes by the LCA. The items showing the most diversity in their ability to influence class membership are responses related to damage to the organization, challenge of security projects, level of commitment to security, and investigative skills. In Table 5, the probability of a respondent possessing skills to investigate a security event that is no longer an active exhibit the highest probability and members of Class 6 have a 67.7% probability of choosing this type of investigation compared to choosing to investigate a threat that is actively

underway. Members of Class 5 have a probability approaching 100% of selecting an inactive threat over an ongoing one. The other classes' probabilities fall between 67.7% and 100% probability. Thus, the status of a threat does not uniquely identify class membership. The same is true about the intent of the threat. Oddly, the probability a respondent will prefer to investigate a non-malicious threat is higher for all classes than the challenge of investigating malicious threats. The remaining four items influencing class membership show more diverse item-response probabilities.

**Table 5 - Item Response Probabilities**

| | Passive Monitor Class 1 (n=21) | Active Planner Class 2 (n=25) | Manifest Technical Investigator Class 3 (n=42) | General Monitor Class 4 (n=55) | Active Investigator Class 5 (n=14) | General Protector Class 6 (n=173) |
|---|---|---|---|---|---|---|
| **1. Completed Threat** | | | | | | |
| Threat no longer active | 0.798 | 0.720 | 0.871 | 0.790 | 1.000 | 0.677 |
| Threat actively underway | 0.202 | 0.280 | 0.129 | 0.210 | 0.000 | 0.323 |
| **2. Damage** | | | | | | |
| Loss of Reputation/Confidentiality | 0.315 | 0.000 | 1.000 | 0.607 | 0.000 | 1.000 |
| Loss of Asset | 0.685 | 1.000 | 0.000 | 0.393 | 1.000 | 0.000 |
| **3. Security Project Challenge** | | | | | | |
| Technical Project | 0.045 | 0.160 | 0.686 | 0.477 | 0.000 | 0.250 |
| Assessment/Planning Project | 0.955 | 0.840 | 0.314 | 0.523 | 1.000 | 0.750 |
| **4. Intent of Threat** | | | | | | |
| Non-Malicious | 1.000 | 1.000 | 0.623 | 0.827 | 0.571 | 0.645 |
| Malicious | 0.000 | 0.000 | 0.377 | 0.173 | 0.429 | 0.355 |
| **5. Level of Commitment** | | | | | | |
| Personal | 1.000 | 0.000 | 0.000 | 0.000 | 1.000 | 0.343 |
| Impersonal | 0.000 | 1.000 | 1.000 | 1.000 | 0.000 | 0.657 |
| **6. Investigative Skills** | | | | | | |
| Passive Monitoring | 1.000 | 0.000 | 0.000 | 1.000 | 0.000 | 0.624 |
| Active Searching | 0.000 | 1.000 | 1.000 | 0.000 | 1.000 | 0.376 |

A person placed into Class 1 is four times more likely (0.798 vs. 0.202) to prefer investigating completed security threats compared to threats underway, and is twice as likely to consider the loss of an organization asset more harmful to an organization than a loss of reputation when a security event is discussed (0.685 vs. 0.315). They consider threats accidental incidents and unintentional or irresponsible acts by employees to be far more important than malicious acts. They do, however, take security personally and consider incidents an affront to

their efforts. They are, also, heavily reliant on security detection software to make them aware of security incidents. A security professional placed into this class is considered to be a Passive Monitor.

Persons placed into Class 2 are 2.5 times more likely to prefer investigating security incidents after they are completed than while they are ongoing. They consider the loss of corporate assets more damaging than loss of reputation, and over five times more likely to feel challenged while assessing network security or while developing security plans than the technical aspects of security. They view security as simply a job in which they focus on non-malicious threats while actively searching for incidents, as opposed to relying on software alerts. The person placed in Class 2 is an Active Planner.

Characteristics of the Class 3 security professional demonstrate a more technical approach to securing organizations. These professionals actively search for security events that have occurred but are no longer in progress. Furthermore, they are concerned with the reputation and integrity of their organization when a security threat has occurred, but they do not take the threats personally. They are twice as likely to feel challenged by a technically oriented project like hardening a firewall or developing an intrusion detection algorithm. A person placed in this class is a Manifest Technical Investigator.

Class 4 respondents take a more general, passive approach to security by exclusively monitoring alert software rather than actively searching the network for breaches. They view their role as security professionals as simply a job, and view projects to assess and plan security as equally challenging to technical projects. Those in this class prefer investigating completed security incidents four times more than ongoing events and consider the loss of reputation of an organization after a security incident as moderately more damaging than the loss of assets. They

are more five times more likely to be motivated by investigating non-malicious incidents than malicious ones. Thus, a security professional placed in this class is called Active Investigator.

Security professionals placed into Class 5 are the smallest of the classes in this study, primarily because they view many aspects of security as cut-and-dry as their item response probabilities imply. They consider completed security incidents as the most challenging types of investigations; they consider the loss of organizational assets as the type of damage and event causes; and they prefer to assess and design security instead of develop algorithms or hard firewalls, for instance. They consider both malicious and non-malicious events as equally threatening, as well as take threats against their network as a personal attack on their security efforts. Finally, they actively search the network and logs for security incidents. Given the clear-cut views on security, a security worker placed into Class 5 is an Active Investigator.

Class 6 is the largest class in the current study, boasting 173 of the 330 respondents. Those security professionals placed into this class are generalists and the most common type of security person. Only one item-response probability is 100% and that involves the damage that a security event can have on the reputation of the organization for which they work. The other item-responses demonstrate that they consider actively occurring threats important but, like all other classes, they consider investigating events that are over to be more appropriate to their skillset. They are three times more likely to find an assessment project more challenging than a technical project, and they are almost twice as likely to consider non-malicious events a bigger threat to their network. They take their work personally, but they mostly look at it as a job to perform. Although actively monitoring the network through logs and other active mechanisms, they are more likely to rely on monitoring the security alert software. Thus, a person placed into this largest class of information security workers is a General Protector.

A six-class model emerged from the data that showed good absolute model fit and good relative fit using the BLRT; thus, *H1 is supported*. Class 6, the General Protector, contains over half the observations, which indicates that more than half of the respondents answered the questions in a similar manner. Thus, most of the respondents view security in much the same way. Thus, *H2 is supported.*

With over 50% of security professionals possessing a General Protector view of information security, organizations are faced with the issue of securing their digital assets with a balance in security skills. The following figure acts as a metaphor of the challenge introduced when such a large proportion of the staff views security issues in the same manner. Possible holes are exposed in the spectrum of digital asset protection, even with minimal overlap in skills.

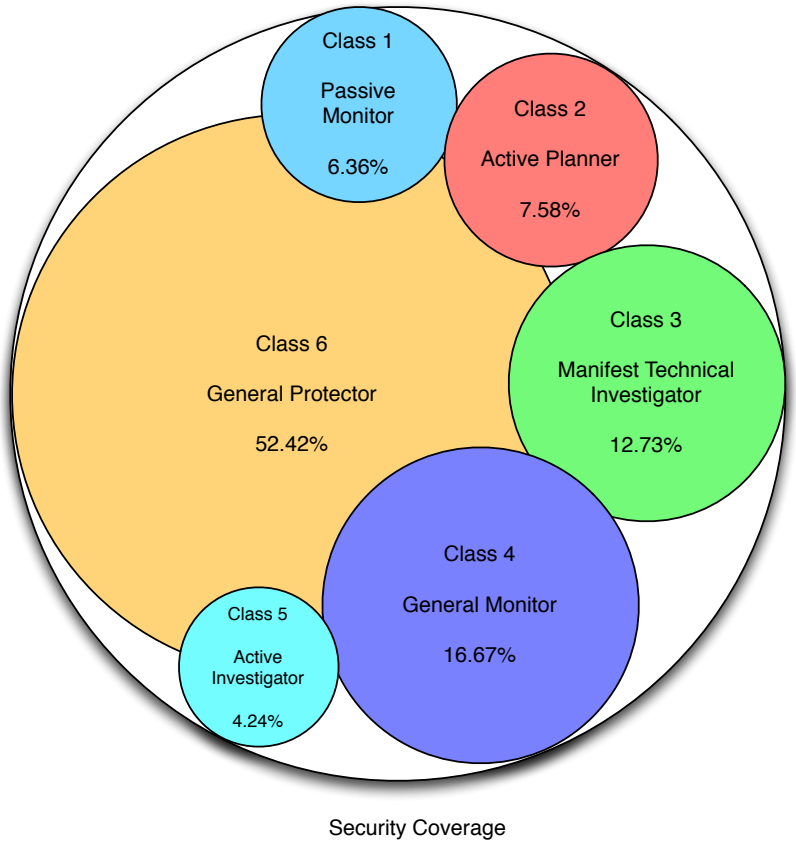



**Figure 5 – Security Coverage (Representative)**

### *4.2.2 Factor Analysis*

From the LCA, six classes emerged into which the information security respondents are placed. The next step of the analysis is to determine whether the latent factors of Creativity, Trait Competitiveness, Deceptiveness, Distrust, and Morality predict membership in the classes. Prior to performing the multinomial logistic regression to test whether the latent factors predict class membership, it is necessary to perform factor analysis to ensure the factor model is correct. The survey questions all originated from existing instruments, which were shown to load adequately in the studies in which they were used. However, it is important to confirm the loadings and fit of the measurement model prior to testing the structural model.

According to Hair Jr., Black, Babin, & Anderson (2010), the $\chi^2$ goodness of fit test with n>250 will lead to a significant result, which is the case with the measurement model resulting from the study's factor analysis ($p < 0.001$). However, Hair et al. (2010) suggests using two tests of model fit to more confidently assess the fit of the model (Hair et al., 2010). Therefore, when the results of the confirmatory factor analysis (CFA) returned a significant $\chi^2$ p-value, the comparative fit index (CFI) and the root mean square error of approximation were not within the range suggested by Hair et al. (2010), it was necessary to address the badness of fit.

To address the issue with model fit using MPlus 7.2, the study relied on the advice given by Byrne (2012) to achieve an acceptable model fit. This exercise, admittedly, moves the analysis from a confirmatory one to an exploratory one, but it is necessary due to factor loadings and cross-loading of latent predictors (indicators). Using the modification indices section of the MPlus output, as suggested by Byrne (2012), the model was changed, based on the impact of the action suggested by the modification indices. Each action was taken one issue at a time with executions of MPlus between each change, the fit indices re-examined, and the modifications

reviewed before the next modification was performed. Variables with the highest MI value in the residual covariance (WITH statement) section were addressed first, followed by the possible cross-loadings. None of the suggested cross-loadings were added to the model. Instead, the variable that had a possible cross-loading were removed. Finally, variables that did not load on the factor at .5 or higher were removed.

Where the modification indices suggested freeing variance, in all cases, the reason was either a negatively worded item or an item that was worded similarly to another. When an item did not have an adequate loading or loaded markedly different than the other factors, and the modification indices recommended removal to achieve better model fit, it was removed.

The resulting model's $\chi^2$ p-value remained significant, but following the changes to the model, the CFI (0.924), the RMSEA (0.066), and the standardized root mean square residual (SRMR; 0.058) were at acceptable levels (Hair et al., 2010). Table 6 contains the correlation matrix of the factor predictors.

Table 7 contains the factor loadings of the items on the latent factors representing the constructs in the analysis. Hair et al. (2010) suggest a minimum factor loading of 0.5 with an optimal minimum of 0.7 loading on each factor. The reliability of the factors was assessed with factor determinacy and using Cronbach's alpha. Muthen (2008) suggests using factor determinacy because Cronbach's alpha "has to do with the correlation between the sum of items and a factor, where it is assumed that there is only 1 factor behind the items and the items have the same loadings and there are no residual correlations" (Muthen, Discussion post February 16, 2008). The factor determinacy of all five factors exceeds the minimum of 0.8 (Muthen, 2008). All but one of the Cronbach's alpha values exceeds to minimum value of 0.7, which

indicates reliability. Cronbach's alpha for Factor 4 (F4, Distrust) is lower than the required value of 0.7; however, the factor determinacy is significant.

Table 6 – Correlation Matrix

**Correlation Matrix**

| | Means | CREZG001 | CREZG004 | CREZG005 | CREZG007 | CREZG008 | TCJA001 | TCJA002 | TCHS003 | TCBCS004 |
|---|---|---|---|---|---|---|---|---|---|---|
| CREZG001 | 5.600 | 1.000 | | | | | | | | |
| CREZG004 | 5.506 | 0.679 | 1.000 | | | | | | | |
| CREZG005 | 5.452 | 0.644 | 0.596 | 1.000 | | | | | | |
| CREZG007 | 5.506 | 0.597 | 0.648 | 0.682 | 1.000 | | | | | |
| CREZG008 | 5.752 | 0.486 | 0.468 | 0.558 | 0.708 | 1.000 | | | | |
| TCJA001 | 5.073 | 0.075 | 0.064 | -0.046 | 0.038 | -0.009 | 1.000 | | | |
| TCJA002 | 5.039 | 0.152 | 0.133 | 0.033 | 0.108 | 0.112 | 0.788 | 1.000 | | |
| TCHS003 | 4.888 | 0.209 | 0.176 | 0.119 | 0.174 | 0.240 | 0.628 | 0.698 | 1.000 | |
| TCBCS004 | 5.079 | 0.105 | 0.163 | 0.000 | 0.031 | 0.043 | 0.593 | 0.562 | 0.440 | 1.000 |
| DEVDAH01 | 2.491 | -0.170 | -0.023 | -0.124 | -0.024 | -0.138 | 0.153 | 0.152 | 0.171 | 0.162 |
| DEVDAH02 | 2.633 | -0.184 | -0.086 | -0.167 | -0.101 | -0.180 | 0.137 | 0.114 | 0.100 | 0.132 |
| DEVDAH03 | 1.721 | -0.210 | -0.165 | -0.219 | -0.160 | -0.217 | 0.077 | 0.086 | 0.077 | 0.077 |
| DEVDAH04 | 2.424 | -0.181 | -0.093 | -0.139 | -0.085 | -0.184 | 0.112 | 0.128 | 0.076 | 0.152 |
| DEVDAH05 | 1.931 | -0.252 | -0.151 | -0.160 | -0.181 | -0.231 | 0.134 | 0.136 | 0.094 | 0.158 |
| DISTDAH1 | 3.721 | 0.030 | 0.005 | -0.094 | 0.005 | 0.016 | 0.188 | 0.183 | 0.090 | 0.087 |
| DISTDAH2 | 3.518 | -0.181 | -0.169 | -0.224 | -0.185 | -0.192 | 0.149 | 0.169 | 0.083 | 0.208 |
| DISTDAH3 | 2.864 | -0.103 | -0.039 | -0.179 | -0.123 | -0.078 | 0.154 | 0.152 | 0.246 | 0.261 |
| MORIDI01 | 5.879 | 0.201 | 0.124 | 0.103 | 0.160 | 0.197 | 0.080 | 0.040 | 0.052 | 0.107 |
| MORIDI02 | 5.982 | 0.297 | 0.183 | 0.079 | 0.146 | 0.143 | 0.182 | 0.142 | 0.190 | 0.256 |
| MORIDI04 | 5.776 | 0.279 | 0.163 | 0.163 | 0.238 | 0.283 | -0.025 | -0.071 | -0.002 | 0.023 |
| MORIDI05 | 5.330 | 0.108 | 0.114 | -0.013 | -0.006 | 0.067 | 0.149 | 0.058 | 0.015 | 0.157 |

**Table 6 - Correlation Matrix, Continued**

| | DEVDAH01 | DEVDAH02 | DEVDAH03 | DEVDAH04 | DEVDAH05 | DISTDAH1 | DISTDAH2 | DISTDAH3 | MORIDI01 |
|---|---|---|---|---|---|---|---|---|---|
| DEVDAH01 | 1.000 | | | | | | | | |
| DEVDAH02 | 0.530 | 1.000 | | | | | | | |
| DEVDAH03 | 0.499 | 0.518 | 1.000 | | | | | | |
| DEVDAH04 | 0.690 | 0.547 | 0.510 | 1.000 | | | | | |
| DEVDAH05 | 0.436 | 0.405 | 0.656 | 0.461 | 1.000 | | | | |
| DISTDAH1 | 0.243 | 0.356 | 0.287 | 0.257 | 0.158 | 1.000 | | | |
| DISTDAH2 | 0.342 | 0.295 | 0.349 | 0.259 | 0.276 | 0.221 | 1.000 | | |
| DISTDAH3 | 0.209 | 0.229 | 0.289 | 0.270 | 0.303 | 0.140 | 0.282 | 1.000 | |
| MORIDI01 | -0.352 | -0.366 | -0.346 | -0.413 | -0.281 | -0.109 | -0.119 | -0.130 | 1.000 |
| MORIDI02 | -0.214 | -0.287 | -0.272 | -0.248 | -0.241 | -0.033 | -0.167 | -0.032 | 0.463 |
| MORIDI04 | -0.359 | -0.383 | -0.375 | -0.384 | -0.408 | -0.146 | -0.251 | -0.120 | 0.676 |
| MORIDI05 | -0.450 | -0.284 | -0.335 | -0.440 | -0.212 | -0.077 | -0.192 | -0.135 | 0.566 |

**Table 6 - Correlation Matrix, Continued**

| | MORIDI02 | MORIDI04 | MORIDI05 |
|---|---|---|---|
| MORIDI02 | 1.000 | | |
| MORIDI04 | 0.393 | 1.000 | |
| MORIDI05 | 0.392 | 0.420 | 1.000 |

**Table 7 – Factor Loadings and Reliability**

| Factor Loadings | | Est. | S.E. | p-value | Reliability Cronbach's alpha | Reliability Factor Determinacy |
|---|---|---|---|---|---|---|
| F1 | CREZG001 | 0.804 | 0.026 | < 0.001* | 0.884 | 0.938 |
| | CREZG004 | 0.795 | 0.026 | < 0.001* | | |
| | CREZG005 | 0.802 | 0.026 | < 0.001* | | |
| | CREZG007 | 0.800 | 0.026 | < 0.001* | | |
| | CREZG008 | 0.617 | 0.040 | < 0.001* | | |
| F2 | TCJA001 | 0.874 | 0.019 | < 0.001* | 0.866 | 0.952 |
| | TCJA002 | 0.900 | 0.017 | < 0.001* | | |
| | TCHS003 | 0.746 | 0.028 | < 0.001* | | |
| | TCBCS004 | 0.647 | 0.035 | < 0.001* | | |
| F3 | DEVDAH01 | 0.723 | 0.035 | < 0.001* | 0.842 | 0.917 |
| | DEVDAH02 | 0.722 | 0.033 | < 0.001* | | |
| | DEVDAH03 | 0.709 | 0.035 | < 0.001* | | |
| | DEVDAH04 | 0.744 | 0.033 | < 0.001* | | |
| | DEVDAH05 | 0.576 | 0.044 | < 0.001* | | |
| F4 | DISTDAH1 | 0.422 | 0.058 | < 0.001* | 0.449 | 0.854 |
| | DISTDAH2 | 0.537 | 0.060 | < 0.001* | | |
| | DISTDAH3 | 0.452 | 0.058 | < 0.001* | | |
| F5 | MORIDI01 | 0.775 | 0.036 | < 0.001* | 0.785 | 0.894 |
| | MORIDI02 | 0.586 | 0.044 | < 0.001* | | |
| | MORIDI04 | 0.650 | 0.045 | < 0.001* | | |
| | MORIDI05 | 0.710 | 0.039 | < 0.001* | | |

*Significant at the $\alpha = 0.05$

### *4.2.3 Multinomial Logistic Regression*

The LCA performed determined most likely class membership for each observation using the six class indicators described in the Latent Class Analysis section, above. Asparouhov & Muthen (2013) demonstrate a 3-step method of determining class membership and then using a multinomial logistic regression procedure to regress the most likely class on covariates. The authors present both an automatic and manual method for performing this analysis (Asparouhov & Bengt, 2013). The automatic method can only be performed on observed auxiliary variables, or covariates. A more processing intensive, manual process is an option when latent factors are involved; however, the 3-step process is only suggested when entropy "goes much lower than 0.8" (B. O. Muthén, November 21, 2008 - 7:53am). The 6-class model chosen has an entropy

value of 0.785, which is sufficiently close to 0.8 to use the most-likely class approach to the multinomial logistic regression (Muthen, n.d.).

A multinomial logistic regression was performed by regressing the most-likely class of information security professional on latent factors representing Creativity, Trait Competitiveness, Deceptiveness, Distrust, and Morality while controlling for Age, Education, and Sex. Table 8 shows the results of a univariable multinomial logistic regression for each factor and control variable in the model. In the initial model-building stage of multinomial logistic regression, variables remain in the model at the $\alpha = 0.25$ level (Hosmer et al., 2013). Therefore, all factors and control variables remain in the model following the univariable, model-building step.

**Table 8 – Results of Univariable Multinomial Logistic Regression**

| | Wald $\chi^2$ | d.f | p-value |
|---|---|---|---|
| Creativity | 15.596 | 5 | 0.008* |
| Competitiveness | 9.526 | 5 | 0.088** |
| Deceptiveness | 32.264 | 5 | < 0.001* |
| Distrust | 34.715 | 5 | < 0.001* |
| Morality | 15.652 | 5 | 0.008* |
| Sex | 9.439 | 5 | 0.093** |
| Age Range | 10.991 | 5 | 0.052** |
| Education | 13.585 | 5 | 0.019* |

*Significant at the $\alpha = 0.05$
**Significant at the $\alpha = 0.10$

After determining that all factors should remain in the model, the most-likely class was regressed on all variables to further solidify model fit. Upon review of the initial results, a large odds ratio with an exceptionally "wide" odds ratio confidence interval was detected, which indicated a possible multicolinearity issue involving Deceptiveness (B. O. Muthén & Muthén, n.d.). Therefore, by regressing the latent factor representing Deceptiveness on all other predictors, the analysis indicated an $R^2$ value of 0.871, which leads to a tolerance value of 0.129.

Tolerance less than 0.2 indicates multicolinearity (Hair et al., 2010). Therefore, Deceptiveness was removed from the model, which results in *no support for H5*.

With Deceptiveness removed, the most-likely class was regressed on the remaining four factors and the control variables. Although the only significant p-values involving the control variables were seen in the logit of Class 6 vs. Class 3, it was determined to leave Age Range, Sex, & Education in the model throughout the analysis to control for these variables in the analysis. Also, some of the other factors were found to be non-significant for several of the logits, as can be seen in Table 9, which led to performing likelihood ratio tests to determine the inclusion of each of the remaining factors.

**Table 9 – Multinomial Logistic Regression for Model Building, STD Output**

| Table 9 Logit | Variable | Coeff. | S.E. | p-value | Odds Ratio | Odds Ratio 95% CI | |
|---|---|---|---|---|---|---|---|
| Class 1 vs Class 6 | F1 - Creativity | 0.064 | 0.365 | 0.861 | 1.054 | 0.643 | 1.727 |
| | F2 - Trait Competitiveness | 0.908 | 0.474 | 0.055 | 2.067 | 1.116 | 3.828 |
| | F4 - Distrust | -0.742 | 0.609 | 0.223 | 0.247 | 0.038 | 1.622 |
| | F5 - Morality | -0.764 | 0.563 | 0.175 | 0.460 | 0.183 | 1.156 |
| | Education | 0.911 | 0.435 | 0.036 | 2.488 | 1.216 | 5.092 |
| | Age Range | 0.241 | 0.224 | 0.283 | 1.272 | 0.880 | 1.840 |
| | Sex | -1.598 | 0.955 | 0.094 | 0.202 | 0.042 | 0.973 |
| | Intercept | -3.096 | 2.595 | 0.233 | | | |
| Class 2 vs Class 6 | F1 - Creativity | 0.624 | 0.421 | 0.138 | 1.670 | 0.947 | 2.946 |
| | F2 - Trait Competitiveness | 1.234 | 0.463 | 0.008 | 2.683 | 1.477 | 4.872 |
| | F4 - Distrust | -0.841 | 0.643 | 0.191 | 0.205 | 0.032 | 1.330 |
| | F5 - Morality | -0.713 | 0.545 | 0.191 | 0.484 | 0.194 | 1.210 |
| | Education | 0.809 | 0.372 | 0.030 | 2.245 | 1.217 | 4.139 |
| | Age Range | 0.308 | 0.231 | 0.182 | 1.360 | 0.931 | 1.988 |
| | Sex | -1.596 | 1.055 | 0.130 | 0.203 | 0.036 | 1.149 |
| | Intercept | -2.865 | 2.111 | 0.175 | | | |
| Class 3 vs Class 6 | F1 - Creativity | 1.277 | 0.442 | 0.004 | 2.857 | 1.587 | 5.145 |
| | F2 - Trait Competitiveness | 1.016 | 0.442 | 0.022 | 2.254 | 1.267 | 4.009 |
| | F4 - Distrust | -0.319 | 0.539 | 0.554 | 0.548 | 0.105 | 2.874 |
| | F5 - Morality | -1.453 | 0.567 | 0.010 | 0.228 | 0.088 | 0.588 |
| | Education | 0.610 | 0.365 | 0.095 | 1.841 | 1.009 | 3.358 |
| | Age Range | 0.291 | 0.216 | 0.178 | 1.337 | 0.938 | 1.908 |
| | Sex | 0.068 | 0.916 | 0.941 | 1.070 | 0.237 | 4.831 |
| | Intercept | -4.315 | 1.916 | 0.024 | | | |
| Class 4 vs Class 6 | F1 - Creativity | 0.659 | 0.355 | 0.063 | 1.719 | 1.060 | 2.787 |
| | F2 - Trait Competitiveness | 0.857 | 0.434 | 0.048 | 1.985 | 1.130 | 3.488 |
| | F4 - Distrust | -0.191 | 0.493 | 0.699 | 0.698 | 0.153 | 3.175 |

| Table 9 Logit | Variable | Coeff. | S.E. | p-value | Odds Ratio | Odds Ratio 95% CI | |
|---|---|---|---|---|---|---|---|
| | F5 - Morality | -1.281 | 0.532 | 0.016 | 0.272 | 0.114 | 0.645 |
| | Education | 0.415 | 0.349 | 0.235 | 1.514 | 0.852 | 2.689 |
| | Age Range | 0.393 | 0.215 | 0.067 | 1.482 | 1.041 | 2.110 |
| | Sex | -0.440 | 0.876 | 0.615 | 0.644 | 0.152 | 2.722 |
| | Intercept | -2.576 | 1.793 | 0.151 | | | |
| Class 5 vs Class 6 | F1 - Creativity | 0.404 | 0.319 | 0.206 | 1.394 | 0.908 | 2.139 |
| | F2 - Trait Competitiveness | 0.962 | 0.401 | 0.017 | 2.158 | 1.271 | 3.663 |
| | F4 - Distrust | -0.185 | 0.441 | 0.674 | 0.705 | 0.183 | 2.717 |
| | F5 - Morality | -0.967 | 0.483 | 0.045 | 0.374 | 0.166 | 0.842 |
| | Education | 0.656 | 0.339 | 0.053 | 1.926 | 1.102 | 3.366 |
| | Age Range | 0.318 | 0.203 | 0.117 | 1.374 | 0.984 | 1.919 |
| | Sex | -0.883 | 0.836 | 0.291 | 0.414 | 0.104 | 1.637 |
| | Intercept | -0.935 | 1.630 | 0.566 | | | |

Upon review of the results presented in Table 9, further investigation was warranted into the latent factors. By performing a likelihood ratio test for each variable against the model presented in Table 9, the factors to retain in the model were determined.

Comparison of loglikelihoods reported in the MPlus output between the baseline model and each nested model (setting the parameter of the factor of interest to zero) to which it was compared is not recommended when the maximum likelihood with robust errors (MLR) estimator is used in MPlus (B. O. Muthén & Muthén, n.d.). Instead, the following chi-square difference test is recommended:

$$cd = \frac{d_0 * c_0 - d_1 * c_1}{d_0 - d_1}$$

$$\chi^2\ Diff = -2 * \frac{T_0 - T_1}{cd}$$

where *cd* is the scaling correction, *d* represents the degrees of freedom, *c* is the scaling correction factor, and *T* is the $\chi^2$ values for the nested and comparison models.

Table 10 shows the results of the multivariable $\chi^2 Difference$ test on each factor and control variable. Additionally, a Wald test of each variable showed results consistent with the $\chi^2 Difference$ tests reported in Table 10. The results of the tests reported in Table 10 show that Distrust is not significant. Therefore, Distrust was removed from the model for all subsequent analyses. The decision to remove Distrust is also consistent with its less-than-desirable Cronbach's alpha value, as reported earlier in Table 7. Thus, there is *no support for H3*.

**Table 10 – Multivariable $\chi^2 Difference$ Tests**

| | |
|---|---|
| **Base Loglikelihood (L1)** | -8673.836 |
| **c1** | 1.3093 |
| **p1** | 103 |

| | L0 | c0 | p0 | cd | $\chi^2 Diff$ | d.f. | p-value | Decision for Variable |
|---|---|---|---|---|---|---|---|---|
| Creativity | -8637.92 | 1.2829 | 104 | 0.36076 | 36.8001 | 5 | < 0.001* | Keep |
| Trait Competitiveness | -8633.732 | 1.2732 | 104 | 0.56252 | 8.7108 | 5 | 0.121 | Keep per (Hosmer et al., 2013) |
| Distrust | -8632.253 | 1.2851 | 104 | 0.315 | 6.1651 | 5 | 0.291 | Remove Distrust |
| Morality | -8634.636 | 1.2854 | 104 | 0.30876 | 21.7256 | 5 | 0.001* | Keep |
| Education | -8635.302 | 1.2671 | 104 | 0.6894 | 11.6623 | 5 | 0.040* | Keep |
| Age Range | -8634.187 | 1.2514 | 104 | 1.01596 | 5.7187 | 5 | 0.335 | Keep as control variable |
| Sex | -8638.901 | 1.2684 | 104 | 0.66236 | 23.0056 | 5 | < 0.001* | Keep |

*Significant at the $\alpha = 0.05$
**Significant at the $\alpha = 0.10$

The final model is presented in Table 11 and includes the factors: Creativity, Trait Competitiveness, & Morality and the control variables Education, Age Range, & Sex. Age Range is a control variable and was kept in the model even though it was not significant in the $\chi^2$Difference test. Age range is coded as an ordinal number representing the age range, in increments of 5 years beginning at 21 to 25 and ending at 70+, selected by the respondent. In the analysis, the ordinal Age Range variable is treated as continuous due to the significant number of parameters estimated in the model.

**Table 11 – Multinomial Logistic Regression Results for Final Model**

| Table 11 Logit | Variable | Coeff. | S.E. | p-value | Odds Ratio | 95% CI | |
|---|---|---|---|---|---|---|---|
| Class 1 vs Class 6 | F1 - Creativity | -0.187 | 0.302 | 0.535 | 0.858 | 0.572 | 1.286 |
| | F2 - Trait Competitiveness | -0.286 | 0.209 | 0.170 | 0.796 | 0.603 | 1.051 |
| | F5 - Morality | 0.385 | 0.342 | 0.260 | 1.461 | 0.823 | 2.594 |
| | Education | 0.282 | 0.276 | 0.307 | 1.325 | 0.842 | 2.086 |
| | Age Range | -0.064 | 0.105 | 0.539 | 0.938 | 0.789 | 1.114 |
| | Sex | -0.740 | 0.552 | 0.180 | 0.477 | 0.193 | 1.182 |
| | Intercept | -2.143 | 2.166 | 0.322 | | | |
| Class 2 vs Class 6 | F1 - Creativity | 0.366 | 0.263 | 0.164 | 1.350 | 0.946 | 1.927 |
| | F2 - Trait Competitiveness | -0.003 | 0.216 | 0.990 | 0.998 | 0.751 | 1.325 |
| | F5 - Morality | 0.540 | 0.262 | 0.039 | 1.702 | 1.120 | 2.586 |
| | Education | 0.194 | 0.165 | 0.239 | 1.214 | 0.926 | 1.592 |
| | Age Range | 0.005 | 0.102 | 0.962 | 1.005 | 0.849 | 1.189 |
| | Sex | -0.793 | 0.659 | 0.229 | 0.453 | 0.153 | 1.338 |
| | Intercept | -1.742 | 1.373 | 0.204 | | | |
| Class 3 vs Class 6 | F1 - Creativity | 0.906 | 0.305 | 0.003 | 2.101 | 1.392 | 3.173 |
| | F2 - Trait Competitiveness | -0.014 | 0.193 | 0.940 | 0.989 | 0.768 | 1.273 |
| | F5 - Morality | -0.433 | 0.247 | 0.079 | 0.653 | 0.439 | 0.971 |
| | Education | -0.033 | 0.170 | 0.846 | 0.967 | 0.731 | 1.280 |
| | Age Range | -0.024 | 0.078 | 0.762 | 0.977 | 0.860 | 1.110 |
| | Sex | 0.923 | 0.428 | 0.031 | 2.516 | 1.244 | 5.089 |
| | Intercept | -3.317 | 1.250 | 0.008 | | | |
| Class 4 vs Class 6 | F1 - Creativity | 0.254 | 0.211 | 0.230 | 1.231 | 0.922 | 1.644 |
| | F2 - Trait Competitiveness | -0.106 | 0.170 | 0.533 | 0.919 | 0.733 | 1.151 |
| | F5 - Morality | -0.319 | 0.222 | 0.152 | 0.731 | 0.517 | 1.033 |
| | Education | -0.240 | 0.154 | 0.120 | 0.787 | 0.610 | 1.014 |
| | Age Range | 0.077 | 0.077 | 0.323 | 1.080 | 0.950 | 1.226 |
| | Sex | 0.443 | 0.383 | 0.247 | 1.558 | 0.830 | 2.923 |
| | Intercept | -1.643 | 1.013 | 0.105 | | | |
| Class 5 vs Class 6 | F1 - Creativity | -0.461 | 0.298 | 0.122 | 0.685 | 0.463 | 1.015 |
| | F2 - Trait Competitiveness | -0.893 | 0.336 | 0.008 | 0.491 | 0.316 | 0.763 |
| | F5 - Morality | 0.935 | 0.522 | 0.073 | 2.511 | 1.092 | 5.777 |
| | Education | -0.672 | 0.340 | 0.048 | 0.511 | 0.292 | 0.894 |
| | Age Range | -0.319 | 0.200 | 0.112 | 0.727 | 0.523 | 1.011 |
| | Sex | 0.871 | 0.824 | 0.290 | 2.390 | 0.616 | 9.269 |
| | Intercept | 0.880 | 1.913 | 0.645 | | | |

Table 10 shows that each of the characteristics, taken individually, can be used to predict class membership. Creativity, Deceptiveness, Distrust, and Morality predict class membership at a 95% confidence level and Trait Competitiveness predicts class membership at a 90% confidence level, from Table 10, when assessed individually. Deceptiveness was removed because its inclusion created problems of multicolinearity, and Distrust was removed, because it

was not predictive when considered with the other variables in the model. This leaves Competitiveness, Trait Competitiveness, and Morality as predictors of class membership. Figure 6 shows the final research model containing Creativity, Trait Competitiveness, and Morality after Deceptiveness and Distrust have been removed as a result of the model building process. The multinomial logistic regression assesses the predictors' ability to influence class membership when comparing each class to a reference class.

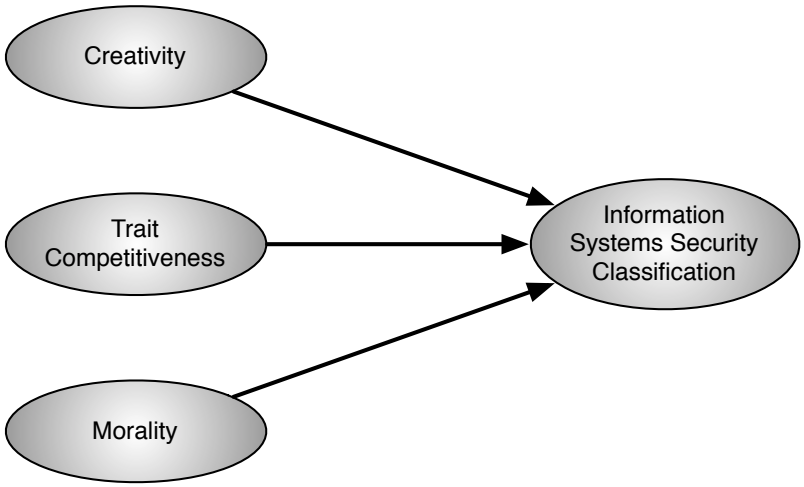



**Figure 6 – Final Model**

One of the six classes identified in the LCA must become the reference class (Hair et al., 2010; Hosmer et al., 2013; Menard, 2010; Tabachnick & Fidell, 2013). The largest class has 173 of the 330 observations, which seems to follow the earlier discussion about information security in organizations being staffed, primarily, with people who think similarly in their approach to security. The reference category for the multinomial logistic regression was the sixth and largest class and each of the five logits assesses the predictor variables' significance relative to the reference category (Menard, 2010).

When reviewing the logit comparing observations placed into Class 1 to observations placed into Class 6, none of the predictor variables are significant. Therefore, none of the variables in the model predict Class 1 membership. In the logit comparing membership in Class

2 to membership in Class 6, only Morality is significant ($\alpha = 0.05$). A significant predictor variable indicates that when Morality increases by one standard deviation, the odds of being classified into Class 2 is 1.7 times more likely than being classified into Class 6. The other characteristics are not significant, and no reliable information, other than Morality, can be used to predict Class 2 membership from the data used in this study. Creativity was significant ($\alpha = 0.05$) as was Morality ($\alpha = 0.10$) in the comparison between Class 3 and Class 6. For a one standard deviation increase in Creativity, the odds of being in Class 3 relative to Class 6 are 2.1-fold and are significant ($\alpha = 0.05$). Additionally, Morality is significant ($\alpha = 0.10$); so, for one standard deviation increase in Morality, odds of being in Class 3 are 0.65 times those of being in Class 6. The only other variable used to predict class membership that was significant was the control variable, Sex. All other variables used to predict membership in Class 3 relative to Class 6 were not significant.

Like the logit comparing Class 1 to Class 6, there were no significant predictors in the logit comparing Class 4 to Class 6. Given that the variables remaining in the model have been shown to be significant in predicting class membership, it is entirely likely that using a different reference class would yield a logit containing significant predictors; however, that is not of interest to this study. The logit comparing Class 5 to Class 6 indicates three variables that are significant in predicting class membership, Trait Competitiveness ($\alpha = 0.05$), Morality ($\alpha = 0.10$), and Education ($\alpha = 0.05$). Education is used in this study as a control variable; so only Trait Competitiveness and Morality are of interest to this study. A person with a one standard deviation higher measure of Trait Competitiveness is almost half as likely (0.49) to be in Class 5 than in Class 6. A person with a one standard deviation higher measure of Morality is

2.5 more likely to be in Class 5 than in Class 6. Creativity is not significant as a predictor of membership in Class 5 when compared to Class 6.

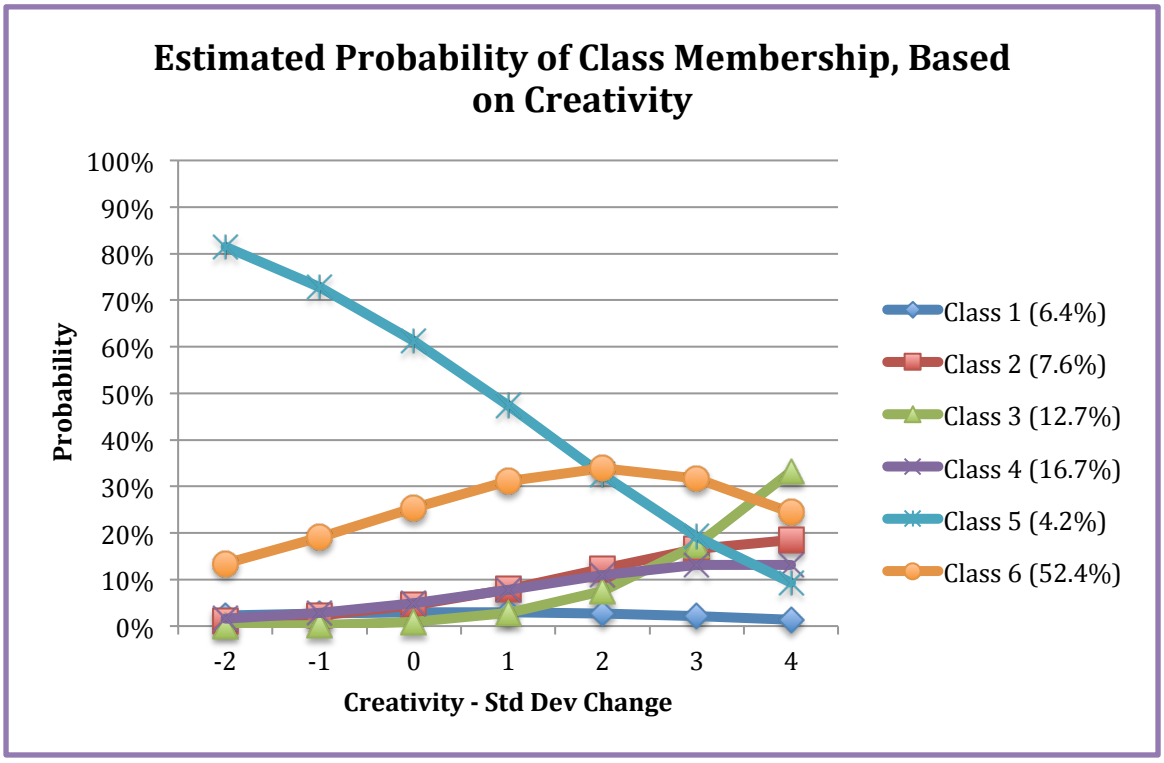
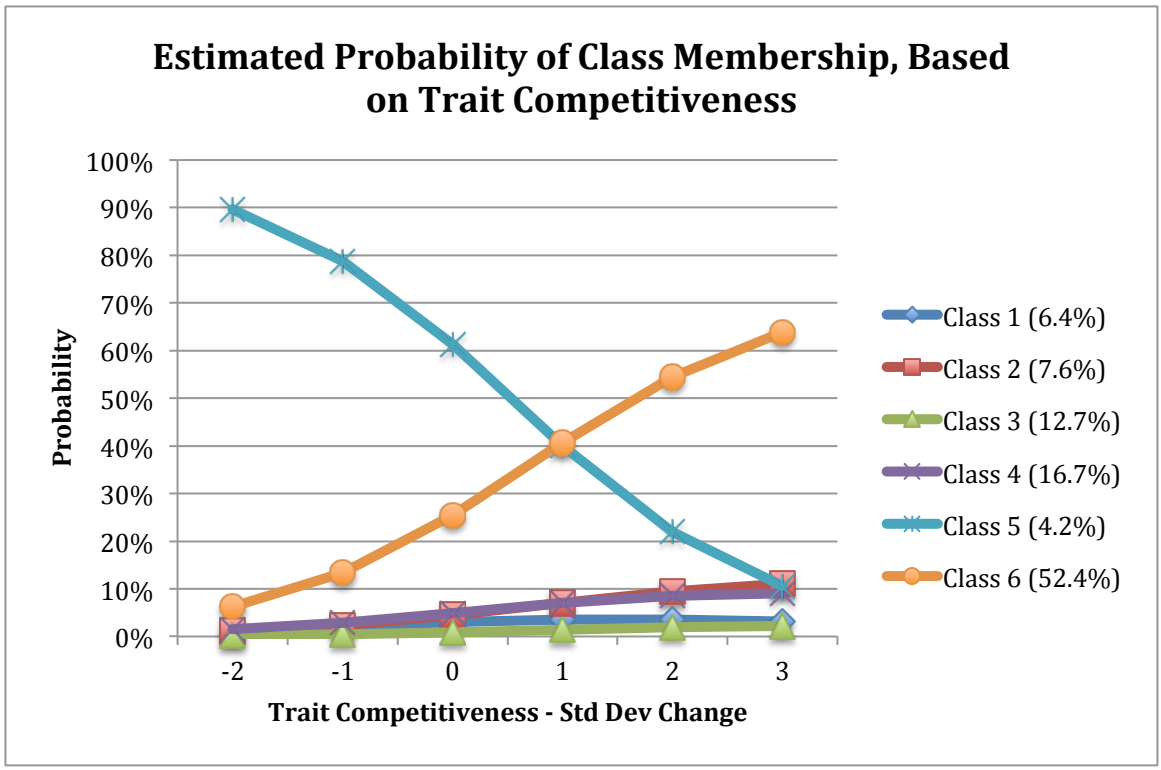



**Figure 7 – Estimated Probability of Class Membership based on Creativity**

Note: All values, other than Creativity, held to 0

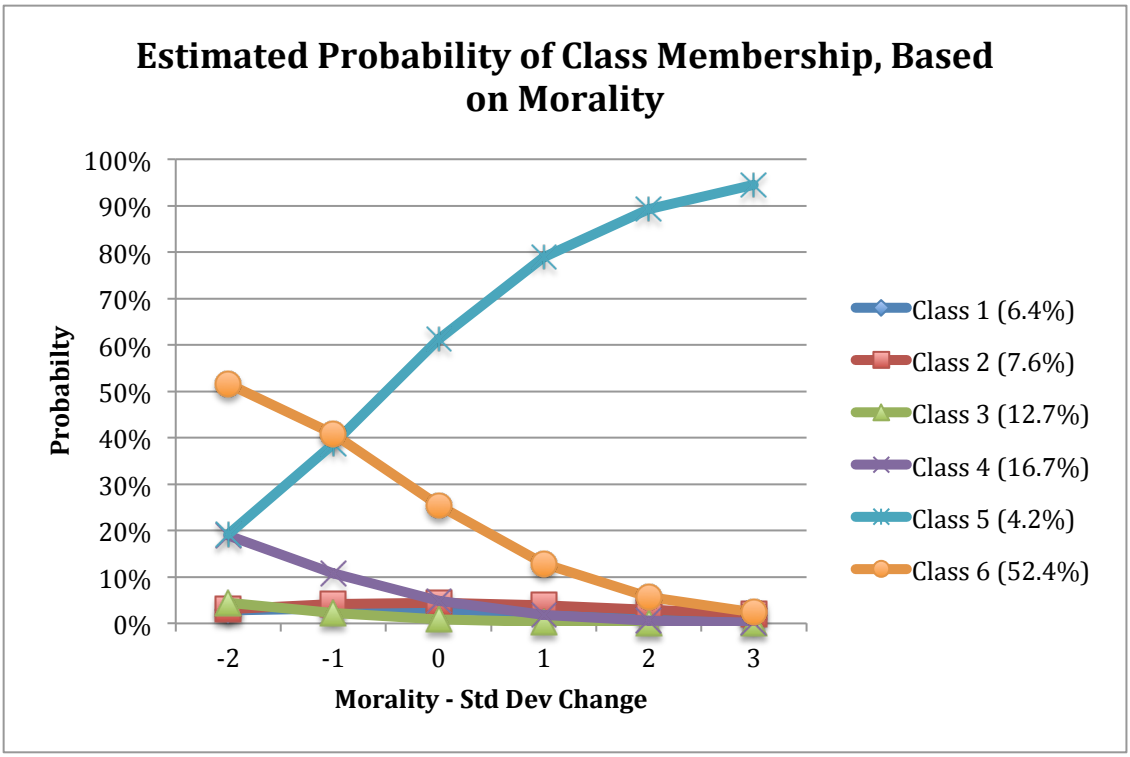
Figures 7, 8, & 9 tell an interesting story about the influence of each of the factors by demonstrating the impact of the factor on membership in each of the classes. The images seem to imply that each class has a dominant characteristic that drives respondents into these classes. For instance, Figure 7 shows that, a one standard deviation decrease in Creativity increases the probability of membership in Class 5. Whereas, after a two standard deviation increase in Creativity, a respondent has a higher probability of being placed in the General Protector (Class 6) group.




Note: All values, other than Trait Competitiveness, held to 0

**Figure 8 – Estimated Probability of Class Membership based on Trait Competitiveness**

Figure 8 shows that as Trait Competitiveness decreases by one standard deviation, the probability of membership in Class 5 compared to Class 6 increases, and continues to increase through a second decrease in standard deviation. Figure 9 paints a different picture when assessing class membership as Morality decreases one standard deviation. After a one standard deviation decrease in Morality, when compared to Class 6, the higher probability of membership changes from Class 5 to Class 6.




Note: All values, other than Morality, held to 0

**Figure 9 – Estimated Probability of Class Membership based on Morality**

## CHAPTER 5: DISCUSSION, IMPLICATIONS, AND FUTURE RESEARCH

As described earlier, Social Identity theory suggests that people tend to congregate into groups where the members are similar to themselves (Ashforth & Mael, 1989). The members of an in-group tend to seek homogeneity in many aspects of their professional lives. The results of this study seem to bear this out. Over half of the respondents to the survey used in this study were classified into one class. The overwhelming similarity of the majority of the respondents to this survey seems to indicate the homogeneity of workers in the information security field.

Latent Class Analysis (LCA) is a useful technique for classifying the respondents and using those classes to determine the predictive ability of the five personality characteristics on class membership. The skewed distribution toward Class 6 demonstrates an issue in the current method of staffing information security organizations. Like social identity theory suggests, people gravitate toward homogeneity; however, in a role as important as information security, doing so puts the organization at risk. A better solution is to identify information security workers who are best equipped to mitigate the risk to an organization. Rather than identifying one primary class of security expert, as this study indicates, an organization should staff the group that is charged with protecting its valuable digital assets in a manner that more evenly distributes the varying specialties across the security organization. This study is an important step toward helping organizations to move in the direction and to stop protecting only the most obvious of attack paths.

The many challenges found in information systems security is captured in the ETSI Information Security Indicator. This event model captures the breadth of knowledge a person

tasked to protect an organization's digital assets must possess (Rennock & Gaudin, 2013). With entries ranging from intrusions and externals attacks to malfunctions, internal deviant behavior and hardware/software vulnerabilities, the indicators cover a broad spectrum of scenarios that a typical information security professional must be well versed in and prepared to investigate an attack or mitigate as risk.

For this reason, this study used the ETSI ITI Taxonomy as a basis upon which to develop questions to classify the types of information security professional. The questions asked of security professionals were designed to tap the mindsets used in everyday security tasks within a variety of organizations. Because of the diversity of the tasks security experts are expected to perform, this study is important because it helps not only to understand the mindsets and types of security experts that are needed to fully protect an organization, but it takes a very important step in understanding the characteristics they should possess.

The results of the LCA were not surprising in some respects and telling in other respects. One surprising finding was that, although all groups were split between non-malicious and malicious threats as the most preferred type of threat to address, that in all classes, non-malicious was found to be most preferred. One view could be consistent with old I.T. adage, "once you feel you have your systems 'idiot proof,' the world seems to make a better idiot." Albeit a bit extreme, the statement does support the finding that protecting an organization's digital assets from accidents ranging from natural disasters, power failures, and the inevitable hard drive failure to inadvertent impact by an employee can be sufficiently challenging. Further, it may indicate that most organizations consider systems administrators their information security teams, which is not uncommon in mid-sized to some larger organizations. By splitting their time between managing the health and well-being of existing servers, implementing new servers,

other general systems administration tasks, and granting internal security access, they simply are unable to pay additional attention to the range of internal and external security issues that a full-time security professional would.

A large group of similarly oriented information security workers in one class was not unexpected, nor was it a shock to find that this group was more general in its views on information security. Although the item-response probabilities were not split directly down the middle on most categories, the fact that they were divided in five of the six questions for Class 6 demonstrates that the larger group of information security workers must be generalists. It also points to the possibility that the members of this class have been forced to become jacks-of-all-trades. There is certainly no data in the study to assert that members of this class of security workers are not good at protecting organizations from the multitude of threats, on the contrary, the study seems to indicate that the generalists should be fortified with specialists to help protect the weaker areas of the perimeters of their organization – the fringes.

The other five classes identify various mindsets of security workers that are quite different from the General Protectors of Class 6. The respondents in Class 1, for example, consider an assessment/planning project more interesting than a technically oriented one. Further, they prefer waiting for security software to alert them to a threat rather than proactively protecting their network. Only a small percentage of the respondents were classified into this, Passive Monitors, class of information security professional. Another class that contained a small number of respondents was Class 2, the Active Assessors. The members of this class were a paradox as information security workers. Their investigation skills were best used actively investigating system logs and server file systems to investigate a threat, but these experts preferred to assess security and offer plans to strengthen an organization's security profile.

Actively monitoring system logs suggests a more technical approach but assessing and planning implies less hands-on work. Like Class 1, Class 2 is relatively small (25).

Classes 3, 4, & 5 are larger and demonstrate more expected characteristics than Classes 1 & 2. Class 3 members are clearly technical experts, based on the response patterns of members. Classes 3 & 4 prefer technical projects to assessments and planning, but Class 4 members are split almost 50-50 (48%-52%) on technical vs. assessment. Class 5 contains a very small but seemingly committed group of security workers. With only 14 respondents placed into Class 5, they are the smallest of the classes but the only item in the list of questions that they were not 100% on their chosen response to the binary question was the question assessing whether the respondent considered malicious or non-malicious threats a more serious threat to an organization. There were split 57% to 43% in favor of non-malicious. This is, likely, the group that would be more likely to investigate or stop an external hacker. Further, Figure 6 shows that just over one unit of an additional measure of morality compared to Class 6 increases the probability a security professional would be placed into Class 5. Therefore, it may be beneficial to assess potential security worker's personality characteristic, because Class 5 respondents likely see hacking as morally wrong, and would work to prevent external threats that seem to have such large, publicly reported impacts on organizations.

As Table 12 indicates, the data contains a classification of six measurable classes with of security experts helpful to solidify an organization's security efforts, which *supports Hypothesis 1*. As reported in the results of the data analysis, the entropy, a measure of class separation, indicated a good separation among classes. This indicates that the clusters for even the smaller classes were well defined. Class 6, the largest class, suggests a generalist approach, *which*

*supports Hypothesis 2* positing the existence of an in-group approach to staffing information security departments.

**Table 12 - Hypotheses, Assessment, and Support**

| | Hypothesis | Method of Assessment | Findings |
|---|---|---|---|
| H1 | Information Systems Security professionals can be categorized into classes ranging from passively-oriented (reactive) to aggressively-oriented (proactive) mindsets toward information systems security | Latent Class Analysis | Supported |
| H2 | One class of the types of will be significantly larger than other types | Latent Class Analysis | Supported |
| H3 | Creativity will predict class membership | Multinomial Logistic Regression | Supported |
| H4 | Trait Competitiveness will predict class membership | Multinomial Logistic Regression | Supported |
| H5 | Deceptiveness will predict class membership | Multinomial Logistic Regression | Not Supported |
| H6 | Distrust will predict class membership | Multinomial Logistic Regression | Not Supported |
| H7 | Morality will predict class membership | Multinomial Logistic Regression | Supported |

Figure 4 shows the probability of class membership of creativity with each one-unit (standard deviation) increase of Creativity relative to the level of creativeness of the members of Class 6. From this visualization of the data, as information security professionals are identified with greater levels of creativity, probability of placement into Class 3 increases significantly. However, with a one standard deviation change less creativity, the probability of class membership in Class 5 increases, and the probability of membership in Class 5 increases even more with a two standard deviation decrease. Thus, there is *support for Hypothesis 3*. A member of Class 3, as discussed previously, has a higher probability of favoring investigative work after a security threat is complete than members of all but members of Class 5. The label given to Class 3 is Manifest Technical Investigator. Members of this class of security expert are concerned about the organization's reputation, whose digital assets security experts protect, in a security incident. Most notably, however, the Manifest Technical Investigator considers technical ability the foremost skill as a security expert. This is in line with high levels of

creativity relative to investigating and preventing security incidents. For instance, intrusion detection algorithms and related systems have sophisticated software and hardware to detect and subsequently prevent a breach of the system. Professionals with high levels of creativity are essential in developing and supporting this type of activity. Finally, Manifest Technical Investigators favor searching through the detailed logs and other internals of networks and computer systems when performing an investigation rather than relying upon monitoring alerts to inform them of an issue. This clear indication of technical ability and prowess separates their creativity from other security experts.

**Table 13 – Summary of Information Security Mindsets (Classifications)**

| | Mindset Name | # of Respondents in Class (n=330) | % of Total | Influencing Characteristic Relative to Reference Class (Class 6) | Security Mindset Description |
|---|---|---|---|---|---|
| 1 | Passive Monitor | 21 | 6.36% | | Damage due to lost assets of greater value than loss of reputation, prefers planning over technical investigations, and responds to alerts instead of seeking breach evidence. |
| 2 | Active Planner | 25 | 7.58 | Creativity | Guards assets rather than org. reputation, plans security projects, and prefers to search for security issues instead of waiting for software to alert. |
| 3 | Manifest Technical Investigator | 42 | 12.73 | Creativity | Security is to guard reputation of organization. Seeks to technically investigate incidents, and actively searches for breaches. |
| 4 | General Monitor | 55 | 16.67 | Morality | Monitors alerts over actively searching for breaches, views loss of assets and reputation of equal value, as well as seeks challenging technical and assessment projects. |
| 5 | Active Investigator | 14 | 4.24 | Creativity<br>Trait Competitiveness<br>Morality | Loss of asset far outweighs loss of reputation to organization, takes breaches personally, and actively searches for cause of incident. |
| 6 | General Protector | 173 | 52.42 | Creativity<br>Trait Competitiveness<br>Morality | Loss of reputation because of an incident is of utmost importance, does not take incidents personally, and prefers alert monitoring more than searching for incidents that have occurred. |
| | | 330 | 100.00% | | |

Figure 5 contains a similar graph, but the focus of this graph is Trait Competitiveness. This graph does not single out a characteristic quite as dramatically, but it does show that competitiveness is a key indicator of the factors influencing membership in Class 6, the General Protectors. With slightly more than a one standard deviation change in Trait Competitiveness, the probability of membership in Class 5 becomes the dominant classification. Thus, *Hypothesis 4 is supported*. Although they are called General Protectors, the label in no way indicates less identification as a security expert. General Protectors, like Manifest Technical Investigators, are concerned with an organization's reputation in the event of a security incident, but General Protectors are more challenged by assessing and planning security and prefer to monitor software designed to alert security workers when an event is perceived to have occurred. They assess and plan as their means to compete with those who would attempt to access or harm an organization's digital access. Like most other security-minded professionals, General Protectors are involved in the interactive decision theory and conflict analysis upon which game theory elaborates (Manshaei, Zhu, Alpcan, Basar, & Hubaux, 2013; Myerson, 1991; Shiva, Roy, & Dasgupta, 2010). Although the study does not explore competitiveness from a game theoretic perspective in this paper, the competitiveness of hackers and security experts alike is well documented (Manshaei et al., 2013; Matusitz, 2009; Shiva et al., 2010; Tang, Zhao, & Zhou, 2011). The interest of this study is in classifying and understanding the characteristics of the information security professional.

Figure 6, like the others, shows a graph of a characteristic emerging in a manner that did not become evident in tabular form, such as the statistics presented earlier. The difference between this graph and either of the others is that it clearly shows an immediate impact of

Morality on membership into Class 5 after less than one standard deviation change, compared to Class 6, which indicates *support for Hypothesis 7.*

Early in the analysis, the issues with Deceptiveness became evident. Therefore, Deceptiveness was removed from the model, indicating *no support for Hypothesis 4*. Additionally, Distrust was not significant as the model building process continued when comparing Classes 1 through 5 to Class 6; however, it was shown to be a significant predictor of class membership in Table 8 (Hosmer et al., 2013). In multinomial logistic regression, a Wald test is performed to determine whether each variable is significant when comparing membership in a class compared to a reference class. A variable may show a p-value of less than 0.05 when comparing Class 1 to a reference class such as Class 2, for example, but it may not show a significant result when comparing Class 1 to a reference class such as Class 4. Since the purpose of this study was to determine membership in a class compared to Class 6 as the reference class, Distrust was removed from the model, but it may have been significant when comparing classes to a reference class other than Class 6. This is identified, because Table 8 shows Distrust as a significant predictor, which may be evident when a different reference class is used in the logistic regression. Because Distrust was removed from the model, even though it was shown to predict class membership, there was still *no support for Hypothesis 6.*

Although the purpose of the research was not to find the precise balance of skills across the entire security organization, the study suggests that over fifty percent of respondents being General Protectors, although beneficial, may not provide the most diverse thinking regarding how to prevent and stop security incidents. Furthermore, equal balance among all classes of security professional may not be the optimal mix for a security department. As figures 4 through 6 suggest, varying increases or decreases in Morality, Trait Competitiveness, and/or Creativity

may lead to a more balanced mix of security mindsets represented in the organization, as illustrated in Figure 10 and Figure 11.

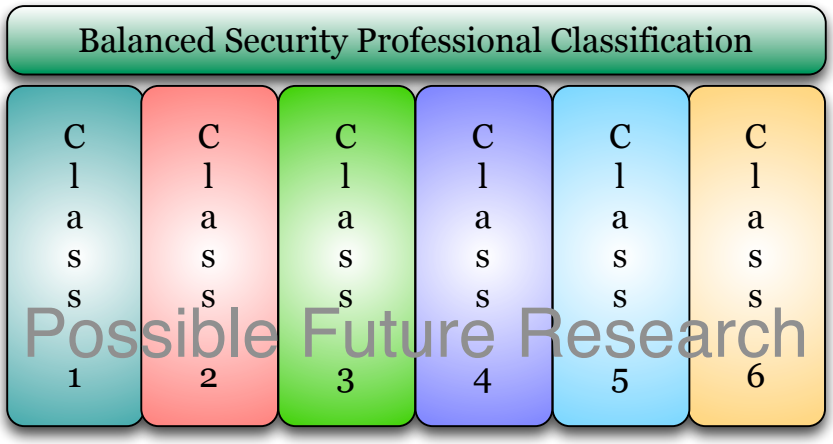



**Figure 10 – Balanced Security Professional Classification (Illustrative)**

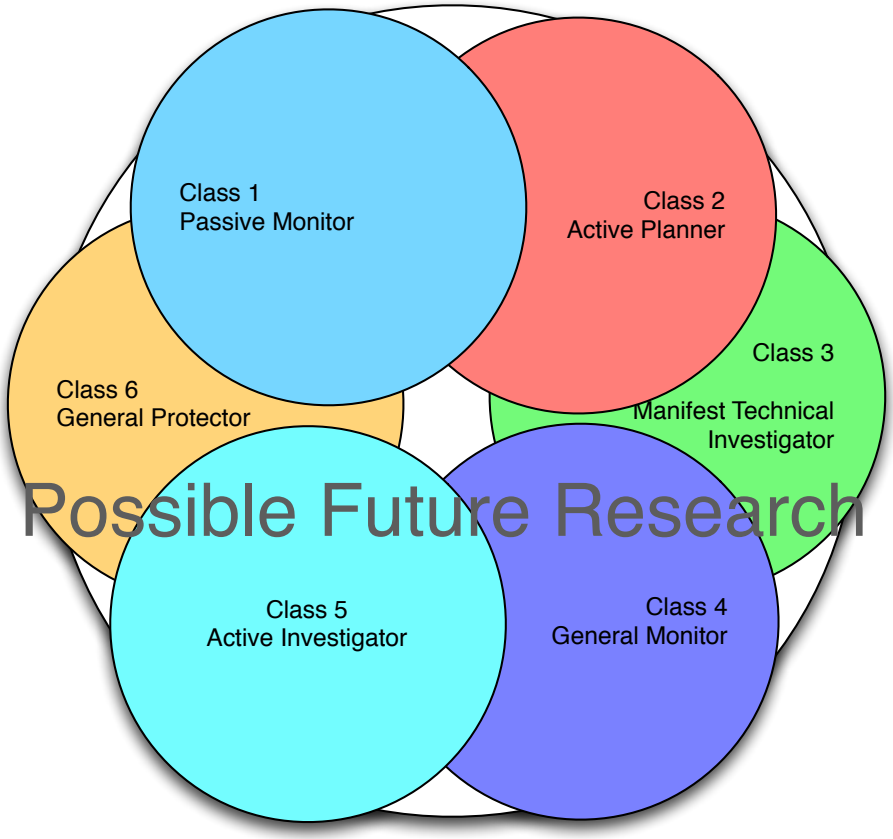



**Figure 11 – Possible Balanced Security Coverage**

## 5.1 Implications for Theory and Research

Determining the types of information security professionals advances the field of information security by providing the basis for the development of a more comprehensive taxonomy of information security activities. Future research should be conducted to determine any additional classification of security types.

As with any personality-oriented research, the volume of characteristics available to study seems endless, but this study chose five specific characteristics from literature suggesting characteristics of hackers. Instead of the Big Five or other popular comprehensive measures of personality, the study used sub-scales targeted at specific characteristics that could possibly help understand the relationship between hackers and those who are trying to stop them, in once sense. Demonstrating the importance of Morality, Competitiveness, and Creativity in information security work is a basis upon which the discipline can build.

Another important finding is that the characteristics that help define a hacker do not necessarily define the information security professional; however, some of the characteristics are consistent. Continuing this work to determine what leads a person to hack should continue (Xu et al., 2013). From this understanding, members of the information security field must continue this work to attempt to understand what may influence a hacker to turn toward security as a career. There is much anecdotal evidence of infamous hackers selling their abilities as consultants and to assist companies they formerly attacked; however, the information security field can greatly benefit by an extension of this research into the hacker community and then marrying the two research streams into one stream that attempts to understand and explain both sides, and the relationships among them, which may be two sides of the same coin.

The methodology used in this study is unique in the information systems and security discipline. Using Delphi to inform the selection of latent class indicators, as far as my research shows, has not been used. Determining the questions to ask by tapping into a small group of industry experts and then using their guidance to develop question adapted from a established security taxonomy provided a high level of relevance to the latent class analysis. Furthermore, with guidance from the management literature, the multinomial logistic regression method of determining class membership led to important probability information regarding the characteristics that will inform both the information systems discipline and practice. Thus, the Delphi-driven latent class analysis method is a research approach that could be used through information system as a guide to person-oriented studies.

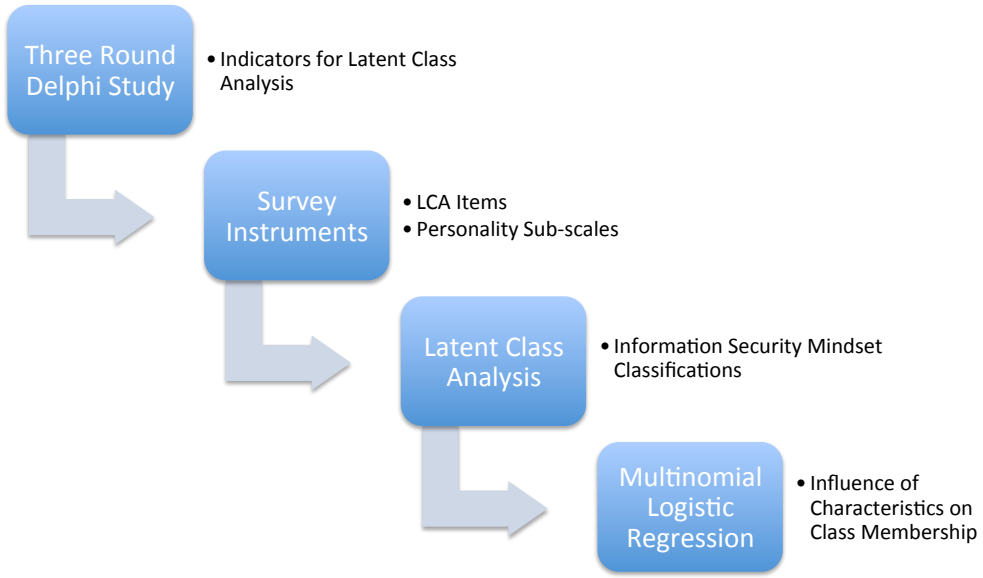



**Figure 12 - The Delphi-Driven Latent Class Analysis Method**

As with other person-oriented studies, this study not only helps provide an understanding of the underpinnings of information security behavior, but its most obvious implications are to practitioners in the field.

## 5.2 Implications for Management

Both I.T. management and Information security management can use these findings to further strengthen their ability to make organizations more secure. Identifying the classes of information security professionals is a very helpful finding, especially identifying and verifying the scenario that social identity theory has been suggesting in all aspects of human behavior for decades. Information security departments are in no better position than other parts of an organization when the group's thinking lacks diversity. If information security professionals all think alike, however, the impact to the organization can be damaging. External and internal threats can then, potentially, go undetected and an organization's digital assets become vulnerable. Simply knowing the risk of continuing the same practices that have allowed the field to skew the workforce in one particular direction can help management develop a plan to rectify the situation.

Fortunately, this study goes beyond merely identifying the classifications of information security workers. Instead, the study shows the characteristics that can be measured in existing staff and in potential new hires to more successfully staff the organization to protect it on many fronts. There is no doubt that an organization like Target, for instance, has the resources to hire a diverse group of information security workers. The results of this study suggest that, because the respondents span 23 different industries, it is likely that it is generalizable to the retail industry, as well. If so, then it is likely that many organizations', Target included, information security organization may be homogenous, as this study suggests, and it could benefit from diversity in mindsets to protect the assets Target has to protect. It is left to others to attempt to replicate these results to specific industries, like retail.

Because the study of specific characteristics is based in the literature that has attempted to identify the characteristics and motivation of hackers, the findings may begin the process of understanding ways in which to better prepare information security organizations to identify specific characteristics to help security workers think more like the people from whom they are trying to protect their organizations. As game theory suggests, knowing an adversary and how he or she thinks helps one make better decisions (Myerson, 1991).

## 5.3 Limitations

The study's multinomial logistic regression estimated a very large number of parameter estimates that came very close to the limitation for accurate estimates. The results may have been impacted by the sample size, because with all five factors in the model, convergence was sometimes an issue in the data analysis. Although the univariable tests of each factor and control variable showed all variables were significant, all but Trait Competitiveness and Sex at the $\alpha = 0.05$ level and Trait Competitiveness and Sex at the $\alpha = 0.10$ level, when comparing Class 6 to the other classes, Class 1 and Class 4 did not have any significant predictors. New characteristics could be added to the model to discover the other predictors of class membership, but this would add to the parameters to be estimated and would exacerbate the sample size problem. A larger sample, of course, would need to be acquired.

Similar to the problem predicting membership in Class 1 and Class 4, other predictors certainly contribute to prediction of class membership, but they were not identified in the literature and, thus, not include in the study. Although no study can include every variable and explain all of the variance, this study was not as predictive as the researcher had expected.

## 5.4 Future Research

Information systems security professionals are on the front lines protecting an organization's digital assets from threats, both internal and external; however, security workers are not solely responsible for an organizations security. A number of studies have been performed to assess end-user views of security through social engineering studies (Chantler & Broadhurst, 2006; M. Gupta & Sharman, 2006; Huber, Kowalski, Nohlberg, & Tjoa, 2009; Lauinger, Pankakoski, Balzarotti, & Kirda, 2010; Workman, 2007). However, little if any research has been performed to determine types of end users from the perspective of security.

Also, software developers are responsible for writing software that is not susceptible to exploitation by external hackers, as well as secure from unintended use within an organization. A study of the various types of software developers, relatively to how they address secure code would have implications for hiring and training software developers for a secure organization. It would, also, contribute to the information system body of knowledge by identifying tendencies of software developers that indicate potential lack of conscientiousness when developing forward-facing software containing sensitive corporate information.

An additional investigation with this study's data would be interesting to determine whether Morality moderates the relationship between any of this study's factors and class membership. Other studies have viewed the moderating effect of morality and the face validity of Morality moderating the relationship between Competitiveness, for example, and the type of information security professional a person is valid. Another study that may include the moderating and direct effects of Morality, using this study's data, would involve developing a full structural equation model testing the relationships between all of the factors included in this study after determining relationships among the constructs contained in the literature.

A related study may be to test the level of creativity demonstrated by I.T. professionals compared to the level of creativity in the general population. This study may show that creativity of I.T. personnel is higher than the general population, which may explain why the probability of moving to another class with an increase in Creativity only occurs after a two standard deviation increase due to an already high level of creativity in I.T.

Finally, a related stream of research that could easily follow this study is to perform this study on a sample of hackers to determine whether, first, that the hackers could be placed in the same classifications. Second, a study could determine whether empirical testing supports the literature showing that the five characteristics used in the current study that were reported to be characteristics of hackers truly were, when used in the same model.

# CHAPTER 6: CONCLUSION

This study identifies a significant trend in information security, which has gone mostly undetected from the time securing digital assets became an important part of an organization's infrastructure. True to the tenets of social identity theory, security organizations err when they staff in the manner they are currently hiring. Information security organizations are charged with a nearly impossible task of protecting everything in their organization that is stored or transmitted digitally. The studies showing characteristics of hackers and employees intent on doing harm to an organization, as discussed, exhibit the characteristics central to this study: creativity, competitiveness, deceptiveness, distrust, and morality at varying levels, which is why this study focused on these characteristics (Bachmann, 2010; Cavusoglu, Raghunathan, & Yue, 2008; Holt, Bossler, & May, 2012; Jordan & Taylor, 1998; Xu et al., 2013).

Empirically studying these characteristics is a good starting point to help identify ways organizations can combat the same characteristics in the people they need to stop. To this point, organizations have found ways to improve their defenses and stop the vast majority of attacks through more sophisticated software and improved training of existing staff. However, identifying a well-rounded staff helps the security department better protect an organization and to anticipate attack vectors by both internal and external threats. This only strengthens the organization and increases the impact of the security function of an IT organization.

By understanding and implementing the findings in this study, organizations can take a positive step toward a more secure organization. Additionally, the study advances the information systems field by developing an understanding of the mindset of information systems

professionals. This allows academics to develop solid theory and techniques to guide a more comprehensive information security subset of the information security discipline.

This study is a step toward developing a more thorough understanding of the intangible characteristics and skills the information security field must develop to effectively combat the growing threat from hackers and deviant internal employees. Practitioners have anecdotal evidence of these characteristics and the behavior to which they lead, but the findings of this rigorous study involving empirical justification of why more diversity is needed in staffing security positions can lead to more secure organizations. Additionally, understanding the characteristics for which to look when hiring not only helps identify the right person for the role, but can help a hiring manager optimize hiring decisions.

**REFERENCE LIST**

Aquino, K., & Freeman, D. (2009). *Personality, Identity, and Character*. (D. Narvaez & D. K. Lapsley, Eds.) (pp. 375–395). Cambridge: Cambridge University Press.
Aquino, K., & Reed, A., II. (2002). The self-importance of moral identity. *Journal of Personality and Social Psychology*, *83*(6), 1423–1440. doi:10.1037/0022-3514.83.6.1423
Ashforth, B. E., & Mael, F. (1989). Social Identity Theory and the Organization. *The Academy of Management Review*, *14*(1), 20–39. doi:10.2307/258189?ref=search-gateway:671ca7e5c71e2bd594683234ec8127e2
Asparouhov, T., & Bengt, M. (2013). Auxiliary variables in mixture modeling: 3-step approaches using Mplus. *Retrieved From www.Statmodel.Com*.
Bachmann, M. (2010). The Risk Propensity and Rationality of Computer Hackers. *International Journal of Cyber Criminology*, *4*(1 & 2), 643–656.
Baer, J. (1998). The Case for Domain Specificity of Creativity. *Creative Research Journal*, *11*(2), 173–177. doi:10.1207/s15326934crj1102_7
Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15*(5/6), 337–346. doi:10.1108/09576050210447019
Bergman, L. R., & Magnusson, D. (1997). A person-oriented approach in research on developmental psychopathology. *Development and Psychopathology, 9*(2), 291–319. Retrieved from http://journals.cambridge.org/production/action/cjoGetFulltext?fulltextid=190386
Bhattacharya, R., Devinney, T. M., & Pillutla, M. M. (1998). A formal model of trust based on outcomes. *Academy of Management Review*, *23*(3), 459–472.
Brown, R. (2000). Social Identity Theory: past achievements, current problems and future challenges. *European Journal of Social Psychology*, *30*(6), 745–778.
Brown, S. P., Cron, W. L., & Slocum, J. W., Jr. (1998). Effects of trait competitiveness and perceived intraorganizational competition on salesperson goal setting and performance. *Journal of Marketing, 62*(4), 88–98. Retrieved from http://www.jstor.org/stable/10.2307/1252289
Bumiller, E. (2010, July 30). Army Broadens Inquiry Into WikiLeaks Disclosure. *New York Times*. Retrieved July 30, 2014, from http://www.nytimes.com/2010/07/31/world/31wiki.html
Caldwell, T. (2011). Ethical hackers: putting on the white hat. *Network Security*, *2011*(7), 10–13. doi:10.1016/S1353-4858(11)70075-7
Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems*, *25*(2), 281–304. doi:10.2753/MIS0742-1222250211
Chantler, A., & Broadhurst, R. (2006). Social engineering and crime prevention in cyberspace. (October 14, 2008). Available at SSRN: http://ssrn.com/abstract=2138714 or http://dx.doi.org/10.2139/ssrn.2138714
CHO, J. (2006). The mechanism of trust and distrust formation and their relational outcomes. *Journal of Retailing*, *82*(1), 25–35. doi:10.1016/j.jretai.2005.11.002
Clapham, M. M. (2001). The Effects of Affect Manipulation and Information Exposure on Divergent Thinking *Creativity Research Journal, 13*(3-4), 335–350. doi:10.1207/S15326934CRJ1334_11
Clark, S., & Bengt, M. (2009, April 6). Relating Latent Class Analysis Results to Variables not Included in the Analysis. Retrieved from

http://www.statmodel.com/download/relatinglca.pdf.
Collins, L. M., & Lanza, S. T. (2010). *Latent Class and Latent Transition Analysis: With Applications in the Social, Behavioral, and Health Sciences* (1st ed.). Hoboken, NJ: John Wiley & Sons.
Dahling, J. J., Whitaker, B. G., & Levy, P. E. (2008). The Development and Validation of a New Machiavellianism Scale. *Journal of Management*, *35*(2), 219–257. doi:10.1177/0149206308318618
DePaulo, B. M., Charlton, K., Cooper, H., Lindsay, J. J., & Muhlenbruck, L. (1997). The accuracy-confidence correlation in the detection of deception. *Personality and Social Psychology Review*, *1*(4), 346–357.
Fletcher, T. D., Major, D. A., & Davis, D. D. (2008). The interactive relationship of competitive climate and trait competitiveness with workplace attitudes, stress, and performance. *Journal of Organizational Behavior, 29*(7), 899–922. doi:10.1002/job.503
Frankena, W. (1988). Hare on moral weakness and the definition of morality. *Ethics, 98*(4), 779–792. Retrieved from http://www.jstor.org/stable/10.2307/2380897
Giordano, G., & George, J. F. (2013). The Effects of Task Complexity and Group Member Experience on Computer-Mediated Groups Facing Deception. *IEEE Transactions on Professional Communication, 56*(3), 210–225. doi:10.1109/TPC.2013.2273817
Guilford, J. P. (1959). Three faces of intellect. *American Psychologist, 14*(8), 469. Retrieved from http://psycnet.apa.org/journals/amp/14/8/469/
Gupta, A., Gupta, S. K., Ganesh, I. M., Gupta, P., Goyal, V., & Sabharwal, S. (2010). Opaqueness Characteristic of a Context Honeypot System. *Information Security Journal: a Global Perspective*, *19*(3), 142–152. doi:Article
Gupta, M., & Sharman, R. (2006). Social Network Theoretic Framework for Organizational Social Engineering Susceptibility Index (pp. 3383–3393). Presented at the Proceedings of the 2006 Americas Conference on Information Systems, Acapulco, Mexico.
Hair, J. F., Jr, Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis* (7 ed.). Upper Saddle River, NJ: Pearson Education, Inc.
Henry, N. (1981). Latent Structure Analysis. In S. Kotz & N. L. Johnson (Eds.), *Encyclopedia of Statistical Sciences* (1st ed., Vol. 4, pp. 497–504). New York: Wiley & Sons.
Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance. *American Journal of Criminal Justice*, *37*(3), 378–395. doi:10.1007/s12103-011-9117-3
Hosmer, D. W., Jr, Lemeshow, S., & Sturdivant, R. X. (2013). *Applied Logistic Regression* (3rd ed.). Hoboken, NJ: John Wiley & Sons.
Houston, J. M., Mcintire, S. A., Kinnie, J., & Terry, C. (2002). A factorial analysis of scales measuring competitiveness. *Educational and Psychological Measurement, 62*(2), 284–298. Retrieved from http://epm.sagepub.com/content/62/2/284.short
Huber, M., Kowalski, S., Nohlberg, M., & Tjoa, S. (2009). Towards automating social engineering using social networking sites. *International Conference on Computational Science and Engineering, 2009. CSE'09.*, *3*, 117–124.
ISSA. (n.d.). About the Information Systems Security Association. Retrieved July 30, 2014, from http://www.issa.org/?page=AboutISSA
Jelinek, R., & Ahearne, M. (2010). Be careful what you look for: The effect of trait competitiveness and long hours on salesperson deviance and whether meaningfulness of work matters. *The Journal of Marketing Theory and Practice*, 18(4), 303-321.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*(4), 757–780.
Kabay, M. E. (2008). *A Brief History of Computer Crime: An Introduction for Students* (pp. 1–51). Norwich University.
Kim, K. H. (2006). Can We Trust Creativity Tests? A Review of the Torrance Tests of Creative Thinking (TTCT). *Creativity Research Journal*, *18*(1), 3–14. doi:10.1207/s15326934crj1801_2
Kim, K. H. (2008). Meta-Analyses of the Relationship of Creative Achievement to Both IQ and Divergent Thinking Test Scores. *The Journal of Creative Behavior, 42*(2), 106–130. Retrieved from http://onlinelibrary.wiley.com/doi/10.1002/j.2162-6057.2008.tb01290.x/abstract
Kohlberg, L. (1958). *The development of modes of moral thinking and choice in the years 10 to 16*. University of Chicago, Chicago.
Kramer, R. M. (1999). Trust and distrust in organizations: Emerging perspectives, enduring questions, *Annual Review of Psychology, 50*(1), 569–598. Retrieved from http://www.annualreviews.org/doi/abs/10.1146/annurev.psych.50.1.569
Landeta, J. (2006). Current validity of the Delphi method in social sciences. *Technological Forecasting and Social Change, 73*(5), 467–482. doi:10.1016/j.techfore.2005.09.002
Lanza, S. T., Collins, L. M., Lemmon, D. R., & Schafer, J. L. (2007). PROC LCA: A SAS procedure for latent class analysis, *Structural Equation Modeling: A Multidisciplinary Journal, 14*(4), 671–694. Retrieved from http://www.tandfonline.com/doi/abs/10.1080/10705510701575602
Lauinger, T., Pankakoski, V., Balzarotti, D., & Kirda, E. (2010). Honeybot, your man in the middle for automated social engineering. *LEET'10, 3rd USENIX Workshop on Large-Scale Exploits and Emergent Threats*.
Lazarsfeld, P. F. (1959). *Latent Structure Analysis*. New York, NY. McGraw-Hill, Inc.
Lewicki, R. J., McAllister, D. J., & Bies, R. J. (1998). Trust and distrust: New relationships and realities. *Academy of Management Review*, *23*(3), 438–458.
Luhmann, N. (1979). *Trust and Power*. John Wiley & Sons.
Mackey, R. (2013, June 10). N.S.A. Whistle-Blower Revealed in Video. *New York Times.* Retrieved July 30, 2014, from http://thelede.blogs.nytimes.com/2013/06/10/n-s-a-whistle-blower-revealed-in-video/?_r=0
Manshaei, M. H., Zhu, Q., Alpcan, T., Basar, T., & Hubaux, J. P. (2013). Game theory meets network security and privacy. *ACM Computing Surveys*, *45*(3), 25:1–25:39.
Matusitz, J. (2009). A Postmodern Theory of Cyberterrorism: Game Theory. *Information Security Journal: a Global Perspective*, *18*(6), 273–281. doi:10.1080/19393550903200474
Mäkikangas, A., Hyvönen, K., Leskinen, E., Kinnunen, U., & Feldt, T. (2011). A person-centred approach to investigate the development trajectories of job-related affective well-being: A 10-year follow-up study. *Journal of Occupational and Organizational Psychology*, *84*(2), 327–346. doi:10.1111/j.2044-8325.2011.02025.x
McCutcheon, A. L. (1987). *Latent Class Analysis*. Newbury Park, CA: Sage Publications.
Menard, S. (2010). *Logistic Regression: From Introductory to Advanced Concepts and Applications* (Vol. 1). Sage Publications, Inc.
Mitnick, K. D., & Simon, W. L. (2003). *The art of deception – controlling the human element of security*. Indianapolis, IN: John Wiley & Sons.
Morin, A. J. S., Morizot, J., Boudrias, J.-S., & Madore, I. (2011). A Multifoci Person-Centered

Perspective on Workplace Affective Commitment: A Latent Profile/Factor Mixture Analysis. *Organizational Research Methods*, *14*(1), 58–90. doi:10.1177/1094428109356476
Muthén, B. O. (n.d.). What is a good value of entropy. Retrieved July 14, 2014, from http://www.statmodel.com/discussion/messages/13/2562.html?1237580237
Muthén, B. O., & Muthén, L. (n.d.). Chi-Square Difference Testing Using the Satorra-Bentler Scaled Chi-Square. *Statmodel.com*. Retrieved July 3, 2014, from http://statmodel.com/chidiff.shtml
Muthén, B. O., & Muthén, L. (n.d.). Correlation of exogenousvariables in SEM. *Statmodel.com*. Retrieved July 16, 2014, from http://www.statmodel.com/discussion/messages/11/7833.html?1379640552
Myerson, R. B. (1991). *Game Theory: Analysis of Conflict* (1st ed.). Cambridge, MA: Harvard University Press.
Nylund, K. L., Asparouhov, T., & Muthén, B. O. (2007). Deciding on the number of classes in latent class analysis and growth mixture modeling: A Monte Carlo simulation study. *Structural Equation Modeling*, *14*(4), 535–569.
Piaget, J. (1932). *The moral judgment of the child*. New York: The Free Press.
Qureshi, I., & Fang, Y. (2010). Socialization in Open Source Software Projects: A Growth Mixture Modeling Approach. *Organizational Research Methods*, *14*(1), 208–238. doi:10.1177/1094428110375002
Rennoch, A., & Gaudin, G. (2013). *ETSI Information Security Indicator Quick Reference Card (v0.1.0)*. Retrieved from http://www.fokus.fraunhofer.de/en/sqc/_docs/_docsmotion/isiQRC.pdf
Rennoch, A., & Gaudin, G. (2013). *ETSI Group Specification: Information Security Indicators Event Model* (No. ETSI GS ISI 002) (1st ed.). Sophia Antiipolis Cedex.
Rest, J. R. (1973). The hierarchical nature of moral judgment: A study of patterns of comprehension and preference of moral stages. *Journal of Personality*, *41*(1), 86–109.
Rest, J. R. (1975). Longitudinal study of the Defining Issues Test of moral judgment: A strategy for analyzing developmental change. *Developmental Psychology*, *11*(6), 738–748.
Rest, J., Cooper, D., Coder, R., Masanz, J., & Anderson, D. (1974). Judging the important issues in moral dilemmas: An objective measure of development. *Developmental Psychology*, *10*(4), 491–501.
Riggs, W. E. (1983). The Delphi technique: An experimental evaluation. *Technological Forecasting and Social Change*, *23*(1), 89–94. doi:10.1016/0040-1625(83)90073-2
Rodriquez, S. (2013, October 3). Data, credit card numbers for 2.9 million Adobe users stolen. *Los Angeles Times*. Retrieved from http://www.latimes.com/business/technology/la-fi-tn-adobe-hack-20131003,0,4679524.story
Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality*, *35*(4), 651–665.
Shapiro, S. P. (1987). The social control of impersonal trust. *American Journal of Sociology*, *93*(3), 623–658.
Shiva, S., Roy, S., & Dasgupta, D. (2010). Game theory for cyber security (pp. 1–4). Presented at the CSIIRW '10: Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, ACM Request Permissions. doi:10.1145/1852666.1852704
Spence, J. T., & Helmreich, R. L. (1983). Achievement-related motives and behaviors. In J. T. Spence (Ed.), *Achievement and Achievement Motives* (1st ed., pp. 7–74). W.H. Freeman and

Company.
Styles, M. (2013). Constructing Positive Influences for User Security Decisions to Counter Corporate or State Sponsored Computer Espionage Threats. In L. Marinos & I. Askoxylakis (Eds.), *Human Aspects of Information Security, Privacy, and Trust* (Vol. 8030, pp. 197–206). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-39345-7_21
Tabachnick, B. G., & Fidell, L. S. (2013). *Using Multivariate Statistics*. (J. Mosher, Ed.) (6 ed.). Pearson Education, Inc.
Tang, K., Zhao, M., & Zhou, M. (2011). Cyber Insider Threats Situation Awareness Using Game Theory and Information Fusion-based User Behavior Predicting Algorithm. *Journal of Information & Computational Science*, *8*(3), 529–545.
the definition of deceive. (n.d.). the definition of deceive. Retrieved from http://dictionary.reference.com/browse/deceive
Tuominen-Soini, H., Salmela-Aro, K., & Niemivirta, M. (2011). Contemporary Educational Psychology. *Contemporary Educational Psychology*, *36*(2), 82–100. doi:10.1016/j.cedpsych.2010.08.002
Twersky-Glasner, A. (2005). Police personality: what is it and why are they like that? *Journal of Police and Criminal Psychology, 20*(1), 56–67. Retrieved from http://link.springer.com/article/10.1007/BF02806707
Vijayan, J. (2012, June 6). LinkedIn probing reports of massive breach. Retrieved July 30, 2014, from http://www.computerworld.com/s/article/9227816/Update_LinkedIn_probing_reports_of_massive_breach
Vincent, A. S., Decker, B. P., & Mumford, M. D. (2002). Divergent Thinking, Intelligence, and Expertise: A Test of Alternative Models. *Creativity Research Journal, 14*(2), 163–178. doi:10.1207/S15326934CRJ1402_4
Wang, M., & Hanges, P. J. (2010). Latent Class Procedures: Applications to Organizational Research. *Organizational Research Methods*, *14*(1), 24–31. doi:10.1177/1094428110383988
Woo, S. E., & Allen, D. G. (2013). Toward an Inductive Theory of Stayers and Seekers in the Organization. *Journal of Business and Psychology*. doi:10.1007/s10869-013-9303-z
Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Systems Security*, *16*(6), 315–331. doi:10.1080/10658980701788165
Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM*, *56*(4), 64. doi:10.1145/2436256.2436272

## LIST OF APPENDICES

# APPENDIX A: MEASUREMENT INSTRUMENTS

## *A.1 Information Security Classification*

(Emphasis added to demonstrate coding)

**In which of the following situations are you most effective?** (*completed security events coded 0,* events underway coded 1*)*

*1. A failed security event*
2. Security event attempt underway
*3. Security event succeeded*

**When/if an incident occurs, which of the following consequences damages your organization the most?** (*loss of reputation coded 0,* loss of asset coded 1)

*1. Loss of confidentiality*
*2. Loss of integrity (defacement, financial fraud, etc.)*
3. Loss of availability of the asset

**On which of the following information security projects do you prefer to work?** (*technical projects coded 0,* assessment/planning project coded 1)

1. Risk assessment of your corporate network
*2. Hardening your forward-facing firewalls*
3. Training end-users in how to detect and avoid social engineering threats
4. Developing a digital asset risk management strategy
*5. Developing an automated intrusion detection algorithm*

**Which of the following presents the biggest threat to your network?** (*non-malicious event coded 0,* malicious attack coded 1)

*1. Accident (natural disaster, physical failure, software malfunction)*
*2. Unintentional act (i.e. error by internal employee/service provider)*
*3. Irresponsible/careless act by internal employee*
4. Malicious act on a digital asset

**If a security event occurred in an area (network device, program, etc.) for which you were primarily responsible, would you consider this even an affront to your efforts to keep your organization safe from threats?**

*0. No. "It's just another day at the office."*
1. Yes. "How dare someone break into my network!"

**Which of the following two scenarios would most stimulate your investigative skills?**

*0. Intrusion detection software issues an alert that a security event has been detected*
1. You discover a security event on your network as you look through the server logs.

### *A.2 Creativity Scale*

Respondents are presented with the following instructions and respond on a 7-point Likert-like scale:

Please use the rating scale below to indicate how accurately each statement describes you. (1 – Very Inaccurate to 7 – Very Accurate)

1 Suggest new ways to achieve goals and objectives
2 Come up with practical ideas to improve security
3 Search out new technologies, processes, techniques, and/or product ideas.
4 Suggest new ways to increase quality.
5 Is a good source of creative ideas.
6 Is not afraid to take risks.
7 Promotes and champions ideas to others.
8 Exhibits creativity on the job when given the opportunity to
9 Develops adequate plans and schedules for the implementation of new ideas
10 Often has new and innovative ideas.
11 Comes up with creative solutions to problems.
12 Often has a fresh approach to problems.
13 Suggests new ways of performing work tasks.

(Zhang and Bartol, 2010; Zhou and George, 2001)

### *A.3 Trait Competitiveness Scale*

Respondents are presented with the following instructions and respond on a 7-point Likert-like scale:

Please use the rating scale below to indicate how accurately each statement describes you. (1 – Very Inaccurate to 7 – Very Accurate)

1. I am a competitive person
2. I like to compete against others
3. I enjoy working in situations involving competiton with others
4. It is important to me to perform better than others on a task

Jelinek and Ahearne (2010)

### *A.4 Deceptiveness Scale*

Respondents are presented with the following instructions and respond on a 7-point Likert-like scale:

Please use the rating scale below to indicate how accurately each statement describes you. (1 – Very Inaccurate to 7 – Very Accurate)

1 I believe that lying is necessary to maintain a competitive advantage over others.
2 The only good reason to talk to others is to get information that I can use to my benefit
3 I am willing to be unethical if I believe it will help me succeed
4 I am willing to sabotage the efforts of other people if they threaten my own goals
5 I would cheat if there was a low chance of getting caught

Dahling et al. (2008)

### *A.5 Distrust Scale*

Respondents are presented with the following instructions and respond on a 7-point Likert-like scale:

Please use the rating scale below to indicate how accurately each statement describes you. (1 – Very Inaccurate to 7 – Very Accurate)

1 People are only motivated by personal gain.
2 I dislike committing to groups because I don't trust others.
3 Team members backstab each other all the time to get ahead.
4 If I show any weakness at work, other people will take advantage of it.
5 Other people are always planning ways to take advantage of the situation at my expense.

Dahling et al. (2008)

### *A.6 Morality Scale*

Respondents are presented with the following instructions and respond on a 7-point Likert-like scale:

Please use the rating scale below to indicate how accurately each statement describes you. (1 – Very Inaccurate to 7 – Very Accurate)

| | |
|---|---|
| 1 | It would make me feel good to be a person who has these characteristics. |
| 2 | Being someone who has these characteristics in an important part of who I am. |
| 3 | I would be ashamed to be a person who had these characteristics (Reverse coded) |
| 4 | Having these characteristics is not really important to me (Reverse coded) |
| 5 | I strongly desire to have these characteristics. |
| 6 | I often wear clothes that identify me as having these characteristics |
| 7 | The types of things I do in my spare time (e.g. hobbies) clearly identify me as having these characteristics |
| 8 | The kinds of books and magazines that I read identify me as having these characteristics. |
| 9 | The fact that I have these characteristics is communicated to others by my membership in certain organizations. |
| 10 | I am actively involved in activities that communicate to others that I have these characteristics. |

(Aquino & Freeman, 2009; Aquino & Reed, 2002)

# APPENDIX B: DELPHI TABLES

### *B.1 Delphi Rounds and Statistics*

| | |
|---|---|
| Round 1 | |
| Participants contacted via e-mail | 82 |
| Responses received | 17 |
| E-mail undeliverable (bounced back) | 4 |
| Out of office notification with now subsequent response | 1 |
| Lecture about links in e-mail | 1 |
| Responses to Delphi on Qualtrics | 11 |
| Abandoned without answering Delphi question | 1 |
| No e-mail address provided | 1 |
| Usable respondents | 9 |
| Questions received | 32 |
| Unique questions | 30 |
| Average questions per usable respondent | 3.3 |
| Maximum questions from respondent | 6 |
| Minimum questions from respondent | 1 |
| Round 2 | |
| Round 2 e-mails sent | 9 |
| Rankings received | 8 |
| Round 3 | |
| Round 3 e-mails sent | 8 |
| Round 3 re-rankings received | 0 |
| Round 3 confirmations | 8 |

### *B.2 Delphi Questions from Experts*

| | |
|---|---|
| 1. | Do you understand security scoring such as the Common Vulnerability Scoring System (CVSS)? |
| 2. | What Common Vulnerability & Exposure (CVE) alerts have you noticed recently that you would take action on right away? |
| 3. | Describe what you would consider to be a mature security posture? |
| 4. | Just how paranoid are you about the security threats facing my network? |
| 5. | How will you add value to our Information Security team? |
| 6. | What training and experience do you have in Information Security? |
| 7. | What certifications do you hold? |
| 8. | Why did you get into Information Security? |
| 9. | What do you see as the biggest issue for information Security Professionals today? |
| 10. | Describe your top accomplishments in Information Security |
| 11. | What is the most secure endpoint computer (server or workstation) that can be had? |
| 12. | Given a defined budget, what would be some things they would do to improve the company's Infosec posture? |
| 13. | Describe what is meant by an Advanced Persistent Threat (APT) |
| 14. | Which country do you believe presents the most risks or threats to our country |
| 15. | What is the biggest challenge you have faced in securing your past or current employer and how did you manage that challenge? |
| 16. | Describe the technologies in which your consider yourself an expert |
| 17. | In what technologies do you have a working understanding? |
| 18. | Rate your written skills on a scale of 1 to 10 with 10 being highest/best? |
| 19. | Rate your verbal skills on a scale of 1 to 10 with 10 being highest/best? |
| 20. | Describe your work experiences dealing with various technologies and your degree of involvement in those projects. |

## *B.3 Delphi Final Ranking of Expert's Questions*

| Average Ranking | Question |
|---|---|
| 3.67 | How will you add value to our Information Security team? |
| 4.000 | Describe what you would consider to be a mature security posture? |
| 5.000 | What training and experience do you have in Information Security? |
| 6.167 | What is the biggest challenge you have faced in securing your past or current employer and how did you manage that challenge? |
| 6.833 | Describe your top accomplishments in Information Security |
| 7.167 | What do you see as the biggest issue for information Security Professionals today? |
| 8.167 | Why did you get into Information Security? |
| 8.333 | What certifications do you hold? |
| 8.833 | Given a defined budget, what would be some things they would do to improve the company's Infosec posture? |
| 9.000 | Describe your work experiences dealing with various technologies and your degree of involvement in those projects. |
| 9.667 | Just how paranoid are you about the security threats facing my network? |
| 9.833 | Describe what is meant by an Advanced Persistent Threat (APT) |
| 9.833 | In what technologies do you have a working understanding? |
| 10.000 | Do you understand security scoring such as the Common Vulnerability Scoring System (CVSS)? |
| 10.167 | What Common Vulnerability & Exposure (CVE) alerts have you noticed recently that you would take action on right away? |
| 10.167 | What is the most secure endpoint computer (server or workstation) that can be had? |
| 10.167 | Which country do you believe presents the most risks or threats to our country |
| 10.167 | Rate your verbal skills on a scale of 1 to 10 with 10 being highest/best? |
| 10.667 | Describe the technologies in which your consider yourself an expert |
| 10.667 | Rate your written skills on a scale of 1 to 10 with 10 being highest/best? |

# APPENDIX C: COMMUNICATION

## *C.1 Initial Delphi Participation E-Mail*

[Name Removed],

My name is David Pumphrey, and I am a PhD student at the University of Mississippi conducting Information Systems Security (ISS) research for my dissertation. As president of the [Chapter Name Removed] chapter of ISSA, you are clearly concerned with developments in Information Systems Security, and your expertise would be invaluable to research that will help us understand the human behavioral side of ISS. I would appreciate it if you could spend ten minutes providing your expertise. This study involves your responses in this first round and your assessment of your peers' responses in two additional rounds. I do not anticipate this, or either of the following two rounds, taking more than ten minutes of your time.

If interested in participating, please paste the following URL into the address line of your preferred browser.

http://uofmississippi.qualtrics.com/SE/?SID=SV_6zfUKV3Xfh37pQh&email=[e-mail address removed]

Please note that the link includes your e-mail address so I know you have responded and can contact you for the two brief, remaining rounds of the study. Upon accessing the questionnaire site, your e-mail address is presented for confirmation. After receiving all responses, I will use this address or an alternative you specify to contact you again to provide feedback on the aggregated, anonymous list of responses. Your e-mail is **never** provided to others and your responses remain completely anonymous to other participants.

As a 23-year I.T. veteran, I know the demands on your time, but if it would help you assess my credibility prior to agreeing to participate, please feel free to call my personal mobile number at 662-816-4927. I would be happy to answer any questions you have about my asking for your participation.

You will be providing the data upon which the research is built and I sincerely appreciate your assistant in this. As this study unfolds, I will gladly provide you with the findings. Simply let me know if you would like to be kept informed and I will do so.

Sincerely,
David Pumphrey
Doctoral Candidate – Information Systems
University of Mississippi

*This study has been reviewed by The University of Mississippi's Institutional Review Board (IRB). The IRB has determined that this study fulfills the human research subject protections obligations required by state and federal law and University policies. If you have any questions, concerns, or reports regarding your rights as a participant of research, please contact the IRB at (662) 915-7482.*

## *C.2 Delphi Ranking E-Mail*

[Name],

Thank you for your responses to our question regarding identifying effective information security professionals. We have organized the responses from your information security expert peers into a list of responses. The next step should take 10 minutes of your time to rank the questions we received.

The URL below will open a list of responses we received and allow you to rank the questions you and your peers ask to determine the effectiveness of an information security job candidate. Once the list opens, we ask that you rank the questions in order of importance in determining effective information security workers, with the questions at the top best identifying effectiveness and, at the bottom, questions you feel provide the least information to determine information security effectiveness.

[URL to Qualtrics "survey" allowing ranking]

Please provide your response by [date], and, again, this research is not possible without your input. So, please take a short time to assist in this research.

*This study has been reviewed by The University of Mississippi's Institutional Review Board (IRB). The IRB has determined that this study fulfills the human research subject protections obligations required by state and federal law and University policies. If you have any questions, concerns, or reports regarding your rights as a participant of research, please contact the IRB at (662) 915-7482.*

Thanks,
David Pumphrey
University of Mississippi
Doctoral Candidate - MIS

## *C.3 Delphi Second Request For Expert Participation*

[Name Removed],

I could really use your help with feedback from the [chapter name removed] area. Please consider not deleting this follow-up to my initial request to help with my dissertation research on the characteristics of information systems security professionals. I am a fellow I.T. colleague, and I was in your shoes prior to going back to school. I worked in I.T. for over 23 years, and frankly, I deleted e-mails like this, too. I had no idea the difficulty in collecting data from I.T. folks like us.

I wanted to make one more appeal; so, please forgive the intrusion on your workday. If you could help to provide real, expert data on which I can further my study, I would greatly appreciate it. I am asking for the following:

1. Open the URL below to help me gather critical information for the first step of my research. It includes this e-mail address so I can perform steps (4) & (5) below.
2. Answer six demographic questions such as age, years in IS Security, etc.
3. Provide a free-form response to a single question: What questions would you ask information systems security professionals (job candidates, colleagues, etc.) to determine whether they will be/are effective information security worker? (Not necessarily tool-/environment-specific questions)
4. A follow-up e-mail will be sent with a URL requesting you to rank the order of importance of the questions provided by everyone responding.
5. Finally, an e-mail with a URL to a request you to confirm or modify the ranking will be sent.

I anticipate you will only need to provide 5 minutes of your time for each of the three rounds.

Below is the URL to copy and paste into your browser. Unfortunately, on previous e-mails, my mail server has converted the URL to a link. That was not my intention, because I don't click on links, either.

http://uofmississippi.qualtrics.com/SE/?SID=SV_6zfUKV3Xfh37pQh&email=[e-mail address removed]
Respectfully,

David Pumphrey
Doctoral Candidate
University of Mississippi

## *C.4 Delphi Second Request for Expert Participation*

Thank you for providing an excellent list of questions and tasks to help assess information security knowledge and abilities.

The next step is to **rank the questions below, identifying, at least, the top 10 questions/tasks** from the list provided by you and by your peers. I would very much appreciate it if you could reply by close of business on Thursday, October 17, 2013, if at all possible.

You may notice that I may have reworded some of your shorter suggested questions. I did this for consistency or clarity. If I changed your intent too drastically, please e-mail me with my error, please.

Please hit Reply on this note and then follow the directions below.

To rank them, please do so in **one of the following two ways,** after hitting Reply (no link to Qualtrics for this round):

1. Provide the letters in ranked order in the table below:

First:
Second:
Third:
Fourth:
Fifth:
Sixth:
Seventh:
Eighth:
Ninth:
Tenth:
Add more, if desired.

- OR -

2. Type the ranking (1 through at least 10) in the blank to the left of the question/task.

_____ A. Do you understand security scoring such as the Common Vulnerability Scoring System (CVSS)?
_____ B. What Common Vulnerability & Exposure (CVE) alerts have you noticed recently that you would take action on right away?
_____ C. Describe what you would consider to be a mature security posture?
_____ D. Just how paranoid are you about the security threats facing my network?
_____ E. How will you add value to our Information Security team?
_____ F. What training and experience do you have in Information Security?
_____ G. What certifications do you hold?
_____ H. Why did you get into Information Security?
_____ I. What do you see as the biggest issue for information Security Professionals today?
_____ J. Describe your top accomplishments in Information Security
_____ K. What is the most secure endpoint computer (server or workstation) that can be had?
_____ L. Given a defined budget, what would be some things they would do to improve the company's Infosec posture?
_____ M. Describe what is meant by an Advanced Persistent Threat (APT)
_____ N. Which country do you believe presents the most risks or threats to our country
_____ O. What is the biggest challenge you have faced in securing your past or current employer and how did you manage that challenge?

_____ P. Describe the technologies in which your consider yourself an expert
_____ Q. In what technologies do you have a working understanding?
_____ R. Rate your written skills on a scale of 1 to 10 with 10 being highest/best?
_____ S. Rate your verbal skills on a scale of 1 to 10 with 10 being highest/best?
_____ T. Describe your work experiences dealing with various technologies and your degree of involvement in those projects.

# VITA

## DAVID L PUMPHREY

Doctoral Candidate - Management Information Systems
School of Business Administration
University of Mississippi, 226 Holman Hall, University, MS 38677
970.261.7699
Email: dpumphrey@bus.olemiss.edu

### EDUCATION

2014 (Expected) PhD, Management Information Systems. University of Mississippi, Oxford, MS

1992 M.S., Computer Information Systems. Georgia State University, Atlanta, GA

1987 B.S.B.A Data Processing & Quantitative Analysis. University of Arkansas, Fayetteville, AR

### PUBLICATIONS

Pumphrey, D., Aiken, M., & Vanjani, M. (2011). A Research Model for Multilingual Electronic Meeting Systems. *Business Research Yearbook.* 110.

### PRESENTATIONS

Eason, C., Pumphrey, D. (2012) Stuckiness: Exploring Online Social Media Usage. Presented at the Southeast Marketing Symposium. Knoxville, TN, February 2012.

Reithel, B. & Pumphrey, D. (2013). Android Forensics. 2013 Mississippi Digital Forensics Conference hosted by the Federal Bureau of Investigation

### HONORS

Outstanding PhD Student for the University of Mississippi School of Business Administration, 2012-2013

## DISSERTATION

Mr. Hyde or Dr. Jekyll? Characteristics of the Information Systems Security Mindset

Abstract: Information security professionals have a unique challenge in today's connected world. They are charged with protecting digital assets from individuals, groups, and even foreign governments with little or no restrictions limiting their behavior. To be successful, security experts must have the mindset and skills of those who seek to harm their organization, but most are not allowed to retaliate, in kind. Instead, they must use these skills only to predict and to prevent future attacks; thus using their technical prowess for good and not for evil. In a survey of 330 information security professionals, the data reveals six mindsets of security experts through a latent class analysis. One class emerged containing approximately 52% of the respondents, which indicates that the information security field is consistent with social identity theory and contains significant homogeneity in mindset toward securing an organization's digital assets. Additionally, personality characteristics such as Creativity, Trait Competitiveness, and Morality influence membership in one of six information security mindsets.

## CURRENT RESEARCH INTERESTS AND FOCUS

My primary interest is the behavioral characteristics of information security professionals and the drivers of the deviant behavior of the people they are charged to stop. Following my initial study of the behavioral characteristics of information security professional, I intend to extend this research into the study of hacker behavioral characteristics and their similarity to those of the information security professional. I, also, leverage my practical experience into the study of software development team formation and the use of agile software development approaches. Therefore, I have an interest in contributing to and extending theory of agile software project management, selection and formation.

## RESEARCH IN PROGRESS

Pumphrey, D. & Eason, C. "Hotel California effect on social networking: The inadequate explanation of the network effect on individuals' social media migration"

Reithel, B., Pumphrey, D, Guo, X., & Mukhopadyay, S. "Counterproductive spoliation behavior of I.S. professional in eDiscovery"

Pumphrey, D, Ammeter A., & Reithel B. "Determinants of Senior IT Management Decisions to Hire Virtual IT Contractors"

Novicevic, M. & Pumphrey D. "Latent class analysis: A review of the management literature"

## CLASSROOM/TEACHING

Joint teaching appointment in both Information Systems and Computer Science

| | |
|---|---|
| 2013 Fall | CSCI 103 – Survey of Computing (45 students) |
| 2013 Summer | CSCI 111 – Computer Science I (Java Programming) (17 students) |
| 2013 Spring | CSCI 103 – Survey of Computing (49 students)<br>BUS 400 – Agile Software Development. (11 students). Created course material and providing instruction to MIS & Computer Science students.<br>MIS 309 – Managing Information Systems (Teaching Assistant, 130 students) |
| 2012 Fall | CSCI 103 – Survey of Computing (44 students)<br>MIS 309 – Managing Information Systems (Teaching Assistant, 130 students) |
| 2012 Spring | MIS 309 – Managing Information Systems (42 students)<br>MIS 309 – Managing Information Systems (Teaching Assistant, 130 students) |
| 2011 Summer | MIS 309 – Managing Information Systems (24 students) |
| 2011 Spring | MIS 619 – Information Systems Strategy (Teaching Assistant, 75 students) |

## PROFESSIONAL EXPERIENCE

| | |
|---|---|
| 2005 - 2010 | *Information Technology Management.* Tulsa, OK. Provided strategic direction for mid-tier oil & gas exploration & production information technology department. |
| 2003 – 2005 | *Software Development Management*. Tulsa, OK. Provided direction to software development teams. Product & project management. |
| 2000 – 2003 | *Enterprise Architect*. Tulsa, OK. Guided technical direction for over 500 software development professionals in Java & Microsoft.NET software development at national energy generation & distribution company |
| 1993 – 1999 | *Enterprise Consultant*. Atlanta, GA. Consultant to numerous information technology departments for mid-sized and Fortune 500 companies. |
| 1987 – 1993 | *Programmer, Systems Analyst, Project Manager.* Ft. Smith, AR; Atlanta, GA. Various programming, analyst, & project management roles for companies in insurance, transportation, & credit scoring industries. |