School of Business
Virginia Commonwealth University

This is to certify that the dissertation prepared by Mark A. Harris entitled **The Shaping of Managers' Security Objectives Through Information Security Awareness Training** has been approved by his or her committee as satisfactory completion of the dissertation requirement for the degree of Doctor of Philosophy in Business.

Dr. Gurpreet Dhillon – Committee chair, Professor, School of Business

Dr. Amita G. Chin – Associate Professor, School of Business

Dr. George M. Kasper – Professor, School of Business

Dr. Carolyn S. Norman – Professor, School of Business

Dr. Richard Redmond – Associate Professor and Department Chair, Information Systems, School of Business

Dr. Richard Redmond - Department Chair, Information Systems

Dr. Allen Lee - Associate Dean for Research & Graduate Studies, School of Business

Dr. F. Douglas Boudinot, Dean of the Graduate School

THE SHAPING OF MANAGERS' SECURITY OBJECTIVES THROUGH INFORMATION SECURITY AWARENESS TRAINING

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at Virginia Commonwealth University

By:

Mark A. Harris

MS E-commerce, Old Dominion University, Norfolk, Virginia, 2003
BS, Information Systems, Old Dominion University, Norfolk, Virginia, 1999

Chair: Dr. Gurpreet Dhillon, Professor
Department of Information Systems

Virginia Commonwealth University
Richmond, Virginia
June 25, 2010

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

Acknowledgements

I would like to acknowledge all of my family and friends that believed in me over the years and encouraged me to keep working despite difficult times. Your support meant so much to me and the process would have been much harder without you.

More specifically, I would like to thank Dr. Gurpreet Dhillon for his continued support and hard work with my graduate program and dissertation research. Dr. Dhillon encouraged my initial application into the Ph.D. program and mentored me along the way. My relationship with Dr. Dhillon means a lot to me and I look forward to many more years of his friendship.

Most importantly, I would like to acknowledge my wife, Sarah, for her support of me during these challenging times in our lives. I met my wife, courted her, married her, and had a child with her all during my Ph.D. program. While some believe the stress of a Ph.D. program can hurt marriages- it strengthened ours. Sarah's support and understanding over the years was instrumental in me completing this program. I certainly could not have done it without her support.

Last, but not least, I would also like to thank my committee members for working with me on short notice at the conclusion of this dissertation and for agreeing to a summer defense.

Table of Contents

List of Tables

List of Figures

Abstract

THE SHAPING OF MANAGERS' SECURITY OBJECTIVES THROUGH INFORMATION SECURITY AWARENESS TRAINING

By: Mark A. Harris, Ph.D.

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at Virginia Commonwealth University

Virginia Commonwealth University, 2010

Chair: Dr. Gurpreet Dhillon, Professor
Department of Information Systems

Information security research states that corporate security policy and information security training should be socio-technical in nature and that corporations should consider training as a primary method of protecting their information systems. However, information security policies and training are predominately technical in nature. In addition, managers creating security policies rely heavily on security guidelines, which are also technically oriented. This study created a series of information security training videos that were viewed by four groups of managers. One video discussed the socio-technical aspects of security, another discussed only the social aspects of security, the third detailed only the technical aspects of security, and the fourth was a control video unrelated to information security. Each group was shown the video, and after this viewing, each group's values toward information security were ascertained and converted into security objectives following Keeney (1992)'s value-focused thinking approach. Each group's list of security objectives were used as the input to Schmidt (1997)'s ranking

Delphi methodology, which yielded a more concise and ranked list of security objectives. The results thus obtained, indicate that manager's objectives towards information security are affected by the nature and scope of the information security training they receive. Information security policy based on each group's value-based security objectives indicate that manager's receiving socio-technical training would produce the strongest information security policy when analyzing the value-focused thinking list of security objectives. However, the quality of security policy decreases when analyzing the ranked Delphi list of security objectives, thus providing mixed results. The theoretical contribution of this research states that technically oriented information security training found in corporations today affects manager's values and security objectives in a way that leads them to create and support technically oriented security policies, thus ignoring the social aspects of security. The practical contribution of this research states that managers should receive socio-technical information security training as a part of their regular job training, which would affect their values and lead to socio-technical information security policy based on the manager's socio-technical security objectives. The methodological contribution of this research demonstrates the successful use of the value-focused thinking approach as the input to the ranking of the Delphi methodology.

1. Introduction

1.1 Background:

This research investigated how different kinds of information security training affect the nature and scope of information security policies within a firm. Maximizing information security within an organization starts with the creation of information security policies. They are the security objectives for protecting the firm's information systems (Karyda et. al., 2005). For example, many firms have security policies regarding acceptable computer use, e-mail, and passwords (Rotvold, 2008). Information security training, also known as security awareness training, is a method of educating all employees on how best to protect the firm's information systems. For example, employees may learn about viruses and worms, or how to recognize phishing e-mails. The goal is for employees to utilize what they learned in training in real-time working, so that the organization optimizes the security of its information systems.

Why are information security policies and training so important? Security policies and training are important today because companies now rely heavily on information systems in almost every aspect of the business, making information security vital to corporate success. Information systems aid business strategy, organizational design, management control systems, the creation and maintaining of competitive advantages, and much more. The technological aspects of information systems give firms a presence on the Internet, make telecommuting possible, aid in unified communication of multiple media, create virtual meeting places, and much more. A

firm's information systems also include its data repositories, where sensitive corporate information, such as intellectual property and customer data may be kept. Because of the dependency on information systems and the potential high cost of disruptions or breaches, a top priority of any modern company is protecting its information systems. Information security policies are the backbone for protecting information systems and information security training is the mechanism used to educate employees about security policies.

The importance of security policies emerges without question when weighed against the billions of dollars that are lost each year from firms inadequately protecting their information systems. The Association of Certified Fraud Examiners 2006 survey reported that businesses lose 5% of their revenue to fraud each year, which equates to a $652 billion in total losses (ACFE, 2006). In the 2008 version of the survey, those numbers had increased to 7%, or $913 billion in total losses, indicating a sharp rise in the magnitude of the problem (ACFE, 2008). Organizations must do everything they can to protect their information systems. The risks of not doing so can be more costly and last longer than the immediate monetary loss caused by the crisis, in the form of collateral damage to the company's reputation and trust with stakeholders (ACFE, 2006).

Now that we accept the importance of information security policies and training for the protection of information systems and know that failing to do so properly can cost billions of dollars, what is this research attempting to demonstrate that can forward the cause of information security? This research attempted to demonstrate that the nature and scope of information security training a manager receives affects the nature and scope of the information security policies they will create. Previous research has demonstrated that socio-technical solutions are the best way to maximize information security (Backhouse & Dhillon, 1996; Dhillon and

Backhouse, 2000, 2001; Trompeter & Eloff, 2001; Siponen, 2001; Dhillon & Torkzadeh, 2006; Dhillon, 2007). Socio-technical solutions refers to a mix of technical aspects of security- such as access controls, virus detection, and encryption, as well as social aspects of security- such as having an ethics program and a strong security culture. If the nature and scope of information security training is socio-technical, will the manager's value-based objectives toward information security be socio-technical and what impact would socio-technical security objectives have on information security policy? These are fundamental questions this research attempted to answer.

Four different training videos were created and given to four different groups of managers, or future managers. The training consisted of a socio-technical video, social only video, technical only video, and control video. Using the value-focused method developed by Keeney (1992), each group developed a list of value-based security objectives that were then ranked using a ranking Delphi method developed by Schmidt (1997). Analysis of the data thus obtained demonstrates that socio-technical training given to managers will yield a stronger mix of socio-technical policies than social only training, technical only training, or no training at all.

The rest of this chapter is organized as follows: Section 1.2 describes the current problem that is to be addressed by this research. Section 1.3 and 1.4 describe the argument and research questions used to justify this research. Section 1.5 describes the definitions of common terms used throughout this research, such as information security and information security policies. Section 1.6 describes the remaining chapters of this research.

1.2 Current Problem:

Many researchers have stated that a socio-technical approach is best for maximizing information security and have stressed the importance of social aspects for information security (Backhouse & Dhillon, 1996; Straub & Welke, 1998; Dhillon and Backhouse, 2000, 2001; Trompeter & Eloff, 2001; Siponen, 2001; Dhillon & Torkzadeh, 2006; Dhillon, 2007). Recognizing the social aspects of information security can be known as the socio-technical or socio-organizational perspective (Siponen, 2001). For example, Dhillon (2001, p. 147) stated that the "socio-organizational perspective is the way forward if security of information systems is to be achieved." If recognizing social and technical aspects of information security is so important, one would expect organizations to have socio-technical information security policies and information security training. However, current research has reported that information security policies lack social aspects of security (Rotvold, 2008; CWS, 2010; Fulford & Doherty, 2003). For example, Rotvold (2007) reported 24 top security policies in use by organizations and only two were socially related policies, concerning ethics and social engineering. Ethics policies were used in 60.4% of the organizations and social engineering policies were used in 14.3% of the surveyed organizations. The top policies used by organizations were acceptable use policy (89%), e-mail policy (84.6%), and password policy (78%). In other research, the Cybersecurity Watch Survey 2010's top three security policies were password policy, acceptable use policy, and Internet monitoring policy (CWS, 2010). Of the more than 30 top security policies reported by the survey, over 90% used technical solutions. Fulford & Doherty (2003)'s research also demonstrated the lack of social aspects security in their list of security policies which are currently being used by organizations.

The content of information security training is predominately adopted from information security policies (Rotvold, 2007; CSI, 2006, 2007). Rotvold (2007) reported that security policies were the number one topic of security training. The CSI Survey (2006, 2007) also reported information security policies as a top topic of information security training. In discussing the content of information security training, Straub and Welke (1998, p. 451) stated that the content should include "employee policies…and other topics that have a bearing on preventing misuse of system assets." If information security policies are technically oriented, then so will be the information security training.

To further complicate the problem, researchers call for information security training to be a primary method for protecting information systems (Straub & Welke, 1998; Solms & Solms, 2004; May, 2008; Rezgui and Marks, 2008). Practitioners seem to be following the advice. The 2010 Cybersecurity Watch Survey reported that information security training was a top method for protecting information systems (CWS, 2010). What this means is that organizations are using information security awareness training as a primary means of protection, but their information security polices and policy-based training lacks social aspects of security. Those creating information security policies need to create socio-technical policies so that the information security training is socio-technical and information security is maximized.

Corporate information security policy is created at the strategic level of the organization by managers that have very little experience or knowledge of creating security policy (Hone & Eloff, 2002). The authors' state that those creating the policy often lack the knowledge to be able to do so. Their "lack of skills and understanding" in developing a security policy often compels the authors to "turn to other organization's policies, commercially available sources or

templates available from public sources, such as the Internet, for answers to their questions" (pp. 402-403). Among the commercially available options are checklists or standardized guidelines. According to Ernst & Young's 2008 Global Information Security Survey, 70% of those organizations surveyed used standardized guidelines to create security policies and that number is expected to increase (GISS, 2008). However, we know that checklists or guidelines have many shortcomings, including the lack of flexibility to changing business environments and lack of attention paid to social aspects of security (Baskerville & Siponen, 2002; Dhillon & Backhouse, 2001). Managers that lack the knowledge to create socio-technical information security policies and end up creating security policies based on standardized checklists will inevitably fail to maximize information security by not including social aspects of security.

1.3 Argument:

The fundamental argument of this research argues that the nature and scope of information security training that managers' receive impacts the nature and scope of the information security policies they create (figure 1.1).

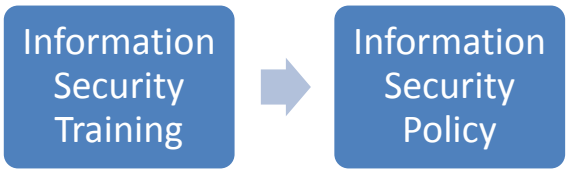

Figure 1.1: Fundamental Argument

The nature and scope of training can be socio-technical, social only, or technical only. It is also possible that managers will receive no training at all. Managers that create information security

policies will be influenced differently depending on which type of training they receive, or if they receive no training at all. That influence will affect the nature and scope of the security policies they create. For example, managers receiving socio-technical information security training will create socio-technical information security policies.

A more detailed argument involves the manager's values and objectives toward information security, where the nature and scope of the information security training a manager receives shapes the manager's values (see figure 1.2). The training shapes their beliefs (values) about how to best protect information systems. The manager's values then impact their individual objectives toward securing information systems. The manager's objectives then impact the nature and scope of the information security policies they create. Another way of thinking about it is that training affects a manager's beliefs and those beliefs influence the manager's goals and those goals influence the policies they create. For example, managers that receive socio-technical information security training will be influenced by the training to alter or reinforce their core beliefs about protecting information systems with socio-technical aspects of security. These socio-technical oriented core beliefs about how to protect information systems will impact their objectives for doing so. Their socio-technical oriented value-based objectives will then impact the nature and scope of the information security policies they create. In this example, the policies thus created would be socio-technically oriented.

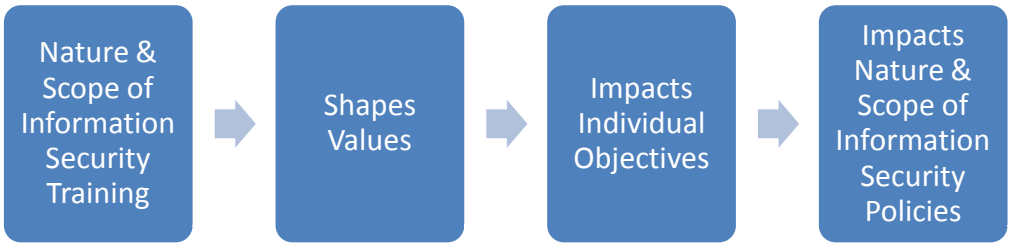

Figure 1.2: Detailed Argument

1.4 Research Questions:

The focus of this research leads to the following two research questions:

1. To what extent are manager's values towards securing information systems influenced by the nature and scope of information security training they receive?
2. To what extent do value-based objectives influence the nature and scope of information security policy?

The first research question will address the relationship between the first and second boxes of the detailed argument (figure 1.2). Will the training shape their core beliefs about how to protect information systems? For example, will socio-technical training, technical only training, or social only training lead to predominately socio-technical values, predominately technical values, or predominately social values? This first research question will also ascertain the values of managers that receive no information security training.

The second research question will address the relationship between the third and fourth boxes of the detailed argument (figure 1.2). Influenced by the manager's value-based objectives for securing information systems, what will be the nature and scope of the security policies they

create? Will they create socio-technical policy, technical policy, social policy, or something else?

1.5 Definitions:

This section gives a more detailed definition of the terms and phrases already introduced and used throughout this research. There are other terms or phrases that are not used throughout this research, but are particular to certain sections or chapters. Those terms and phrases are defined and described in those sections or chapters, where they are more relevant.

1.5.1 Information Systems:

An information system, as described by Dhillon (2007), is the system that handles information at three levels – technical, formal, and informal. Within an organization, the technical system is the organization's information technology infrastructure and consists primarily of hardware, software, data and network components. It is everything that supports the flow and processing of information. The formal system consists of rules and procedures, such as security strategy, policies, and processes (Dhillon, 2007). Acceptance of the formal system's rules and procedures by the people is a social process, which is part of the informal system. The informal system consists of social constructs, such as culture, norms, beliefs, attitudes and informal communication. An information system is the system that handles information in and across these three systems.

1.5.2 Information Security:

Information security, also known as information systems security, refers to the protection of an information system at three levels: technical, formal, and informal. There must be coordination between the three systems for the effective management of information security. At the technical level, information security is concerned with technological solutions to security, such as using firewalls, biometric scanners for authentication and anti-virus software. At the formal level, information security is concerned with creating organizational structures and processes to ensure security and integrity (Dhillon, 2007). This includes the creation of proper responsibility structures, maintaining integrity of roles, and creating and verifying proper business processes (Dhillon, 2007). At the informal level, information security is concerned with the social aspects of security, such as creating and maintaining a security culture, integrity of employees, trust relationships, and ethicality.

1.5.3 Information Security Policy:

Karyda et. al (2005, p. 247) state that "an IS security policy includes the intentions and priorities with regard to the protection of the IS, usually referred to as security objectives, together with a general description of the means and methods to achieve these objectives." At a high level, corporate security policy describes the overall security vision in the form of security objectives. These objectives are abstract in nature and written in generalized terms, such as the statement of the need to ensure that sensitive data is protected from unauthorized access. At a lower level, procedurally oriented policies are derived from the corporate level policies to reflect the means for achieving the higher level objectives. To continue the previous example of protecting sensitive data from unauthorized access, a procedurally oriented policy might be to create a

password policy that protects such data. Other procedurally oriented policies might be to require all employees to have passwords at least 8 characters long and to change their passwords every 30 days. There may be multiple procedurally oriented policies for each corporate level policy.

1.5.4 Information Security Training:

Information security training, also known as security awareness training, is a method of educating all employees on how best to protect an organization's information systems. Training most often reflects the procedure oriented security policies. The most effective information security training will address threats posed by technically oriented aspects of security as well as socially oriented aspects of security.

A goal of security awareness training is to create overall security awareness. According to Rezgui & Marks (2008), the meaning of security awareness falls into two categories. The first are those that consider security awareness to mean "attracting users' attention to IS security issues" and the second considers security awareness to mean "the user's understanding of IS security and optimally, committing to it" (p. 244). Whether computer security awareness training makes employees only aware of security issues or makes them fully understand and committed to upholding this security can depend on many factors, such as the quality of the training and the employees themselves. There is research that suggests using theories from psychology and sociology to create training in certain ways can lead to better absorption by employees and can increase the likelihood of employees following security policy (Siponen, 2000; Thomson & Von Solms, 1998). However, this research on the effect of information security training on information security policies is focused on the nature and scope of the training and not the delivery method or psychological acceptance of the training.

1.6 Thesis Structure:

This thesis is structured as follows: Chapter one of this research is the introduction, where the relationship between information security training and information security policy is introduced. This chapter includes the author's argument and definitions of key terms used throughout this research. Chapter two is a literature review that investigates information security training, information security policies, technical and social aspects of security, and how manager's objectives lead to practice. Chapter two concludes with a discussion of how the literature review is relevant to this research. Chapter three discusses the methodology of this research, starting with the creation of the training videos and a description of the experimental design and participants. The value focused research methodology is reviewed and discussed along with the ranking Delphi methodology. Chapter four describes the execution and analysis of the value focused method data collection and discusses the relevant results. Chapter five describes the execution and analysis of the ranking Delphi method and the relevant results. Chapter six discusses the key findings and the relevance to information security research. Chapter seven concludes this research by summarizing the study and the key findings, along with any research limitations.

2. Literature Review

2.1 Introduction:

This dissertation investigates how the nature and scope of information security training affects the nature and scope of information security policies within a firm. The central argument is that training affects policies, so it is important to review literature pertaining to information security training and information security policies. But before reviewing training and policies, it is important to review the nature and scope of training and policies, which involve the social and technical aspects of security. The argument believes that the particular type of training a manager receives will affect the policies he or she creates, so it is also important to establish a link between a manager's security objectives and the security policies he or she creates. These areas will be reviewed in the following sections, starting with a review of socio-technical security. Information security policy and information security training will then be reviewed. The discussion will link these topics and discuss the connection with creating information security policies. The final section is the conclusion that relates the overall literature review to this dissertation's argument and research questions.

2.2 Socio-technical Security:

Social aspects of security refer to human related aspects of organizations that need to be taken into consideration in order to maximize information security. This can include many concepts, such the responsibility, integrity, trust and ethicality (RITE) of individuals as described by Dhillon and Backhouse (2000). Social aspects of security can also include norms, security

culture, beliefs, and attitudes within organizations (Dhillon, 2007). The research below demonstrates the need for information security to go beyond merely focusing on technological solutions to security threats and highlights the need for the recognition of social aspects of security.

But before reviewing research related to the social aspects of security, it is important to briefly describe the technical aspects of security. Most organizations rely heavily on the technical solutions to security threats, as they are often the first line of defense. Examples of technical solutions to security threats include hardware and software firewalls, antivirus software, password usage, smart cards and much more. The goal of this section is to demonstrate the importance for information systems security research to go beyond the sole reliance on technical solutions to security threats and to incorporate the social aspects of security as well.

Over 30 years ago, Bostrom and Heinen (1977) called for systems development to include the social aspects of organizations. The socio-technical system (STS) was introduced in a paper discussing the redesign of management of information system's methodologies. The authors argued that system designers created flawed systems because they failed to recognize the importance of the social aspects of organizations. They describe a socio-technical system as "two jointly independent, but correlative interacting systems" (p. 17). The technical system is concerned with processes, tasks, and technology, while the social system is concerned with the attributes of people (attitudes, skills, and values), the relationships of people, reward systems, and authority structures (Bostrom and Heinen, 1977). The outputs of the system "are the result of joint interactions between these two systems" (p. 17). The authors go on to discuss areas where designers fail to recognize social aspects of organizations. The focus of this research may

have been on correcting failures in MIS development, but the recognition of the concept of there being a socio-technical system that must be considered in IS development is important for all subsequent information systems research.

Siponen's (2001) research analyzed three approaches to developing security for information systems. The approaches are called information/database modeling approaches, responsibility approaches and security-modified information systems development approaches and are classified into four generations. First and second generations focus on checklists and technical solutions. The third and fourth generations include modeling and socio-technical solutions respectively. Information/database modeling approaches includes "research on the organizational and conceptual level, along with methods covering database security" (p. 9). There are very few studies using this approach. Responsibility modeling refers to the use of responsibility as a basis for ensuring secure information systems development. Security-modified information system development approaches "refer to any approach that is modified from an information system or development approach" (p. 3). The third and fourth generations, which include responsibility modeling and security-modified information system development approaches, have an intellectual origin in data modeling, information systems and computer science (p. 17). The authors concluded that the most commonly held organizational role of information systems security was the technical view, which ignores the social aspects of security. "There is a lack of aforementioned approaches which recognize the social aspects of information systems, i.e. socio-technical and social organizational roles of information systems security" (p. 22). Social aspects of information systems security is part of the fourth and latest generation of secure information systems development.

In a (2001) paper by Dhillon and Backhouse, the authors map the current directions in information systems security research. The authors did so by using the Burrell and Morgan (1979) framework and four paradigms: functionalist, interpretative, radical humanist, and radical structuralist. Functionalists often derive their approaches from the natural sciences. Interpretivism "is concerned with the subjective understanding that individuals ascribe to their social situations" (p. 129). The radical paradigms oppose the regulation view of society and advocate radical change.

The authors concluded that there was a noticeable trend in information systems research which was moving away from the functionalist and technical view point, but not in information systems security research. They write that much of the information systems security research up to this date had been "classified under the functionalist paradigm and the theorists have treated security as something tangible and concrete" (p. 147). Information system security should not be considered in a mechanistic manner and doing so would relegate inter-organizational and intra-organizational social relationships as incidental (Dhillon & Backhouse, 2001). The authors suggest that if security of information systems is to be achieved, then the socio-organizational perspective is the way forward.

In other research, Trompeter and Eloff (2001) recommend that ethical aspects of security should be considered as important as the technical and functional aspects of security. Information security ethical principles should be incorporated with the inception, development, and maintenance of an organization's IT system and should govern security controls and measures (Trompeter & Eloff, 2001). The guiding principles should "include the right of both the individual and the organization to privacy, to property of their information and to the obligation

to uphold this socio-ethical commitment" (pp. 286-387). "The creation of a socio-ethical awareness of infosec *(information security)* that takes cognizance of the human dimension will help organizations and clients alike..." (p. 390).

Developing a strong security culture has also been linked to more secure information systems. A security culture "reflects the values and beliefs of information security shared by all members at all levels of the organization" (D'Arcy & Greene, 2009, p. 147). In a study of 105 computer using professionals, D'Arcy and Greene (2009) investigated the relationship between security culture and security policy compliance and security extra-role behavior. Compliant behavior refers to a user's compliance with security policies and regulations. Extra-role behavior refers to behaviors that go beyond the job description and are not part of the formal job duties. Examples of extra-role behavior include attending voluntary security training, promoting safe computing practices, and speaking out about inefficient security controls. The results of the survey provided strong evidence that security culture contributes to both compliant user behavior and extra-role behaviors. The authors state that "developing a security culture that consists of top management commitment to security and ongoing security communication is extremely beneficial in promoting both a compliant and proactive security-conscious user population" (p. 154).

In other security culture research, Vroom and von Solms (2004) stress the importance of a strong security culture and suggest ways of changing the culture. The authors propose to address security culture through three aspects of organizational behavior- the individual, the group and the formal organization. Individuals are unique and bring multiple characteristics into the organization. Individual attitudes, motivation, job satisfaction, etc. is influenced by organizational forces and the behavior of an individual is important for developing a culture

(Vroom & von Solms, 2004). Groups are made up of individuals and have their own values and norms. Groups develop characteristics beyond those of the individual. The formal organization can be compared according to characteristics common to them, such as the size of the organization (Vroom & von Solms, 2004). The behavior of the individual, group, and formal organization influences each other and are not mutually exclusive. In order to change culture, changes need to take place at all three levels. The authors suggest the best way to change the security culture is to change the shared values and knowledge of the group. Investigating the cultural influences on the group and changing them separately will slowly start to alter group behavior. The altered group behavior will then influence individual behavior, which will have an eventual effect on the formal organization. The authors suggest that changing one aspect "will filter through the organization at a formal and individual level and the culture will eventually change into a secure one" (p. 197).

Security culture is important for ensuring appropriate behavior, according to von Solms and von Solms (2004). The author's research investigates the integration of security polices, education and security culture. Management creates security polices and defines what they expect from group members within the organization. Groups are defined as collections of individuals that have shared basic assumptions. The group members must accept the policies created by management and agree that they benefit the organization. Managers can dictate the behavior of employees by "expressing collective values, norms, and knowledge, by defining specific policies and procedures" (p. 277). Security policies can be expressed in the group's beliefs, which form the security culture. Educating new group members then helps cultivate the security culture by teaching new members the group beliefs, which they will embrace as part of the group's basic shared assumptions. Aligning information security policies with the security culture and

educating employees on a continuous basis is one way of positively affecting employee behavior.

In a paper about organizational culture and security culture, Ruighaver et al. (2007) suggest that information security is generally a management problem and an organization's security culture reflects how management handles the problem. The authors argue that "technical security measures and security policies will often need to be (re)designed to support an organization's security culture" (p. 56). Suggesting that security culture is influenced by organizational culture, the authors investigate security culture using an eight dimensional framework developed by Detert et al. (2000) to study organizational culture. The framework was used to highlight aspects of security culture along the eight dimensions using empirical case study research from information systems. Based on the relation of security culture to organizational culture within the framework, the authors highlighted several aspects of good security culture. Below are some select findings (Ruighaver et al., 2007):

1. "Organizations with a high-quality security culture should place an emphasis on long-term commitment and strategic management" (p. 58);
2. a degree of trust and accountability needs to be established with employees;
3. employees with responsibility over particular aspects of security should be given a strong sense of ownership;
4. responsibility and accountability for security decision making should be clearly defined in policies;
5. educating employees about their roles and responsibilities is important; and

6. good security culture should find a balance between internal and external focus, where there is awareness of the external environment and its threats, as well as an awareness of the internal environment.

Other aspects of security culture, such as attitudes, norms and shared expectations did not fit into the framework, but were also considered important by the authors.

In research aiming to improve user security behavior, Leach (2003) discusses six factors that have strong influence over people's security behavior and three steps organizations can take to improve behavior. The threats include user errors and negligence, such as forgetting to apply security procedures, and deliberate acts, such as emailing sensitive data without protection. The factors that influence security behavior come from an organization's culture and practices and can be divided into two areas: (1) encompassing the users' understanding of what behaviors the company expects of them, and (2) the factors which influence the user's personal willingness to constrain their behavior to stay within accepted norms (Leach, 2003). The user's understanding of expectations are described by what they are told, what they see being practiced by others around them, and their experience built on decisions they made in the past. Personal willingness to comply with expectations are described by people's personal values and standards of conduct, sense of obligation towards their employer and the degree of difficulty they experience in complying with the company's procedures.

Not all of these factors which affect how people behave can be influenced by the organization, such as an employee's personal values. However, organizations can focus on the three key factors they can influence. The author suggests organizations should focus on the behavior demonstrated by management, the user's security common sense and decision-making skills, and

the user's psychological contract with their employer. Below is a summary of concepts related to these three factors (Leach, 2003):

1. ensure senior management and junior staff have good security behavior;
2. provide feedback on the correctness of security behavior;
3. reward staff for good security;
4. give additional training to staff that demonstrate bad security behavior;
5. teach the user's the principles they need to make good decisions;
6. provide continuous feedback and support;
7. create a strong security culture to motivate staff to behave consistently; and
8. discuss security regularly with management and staff.

The author suggests that leadership is the key to creating a more secure environment. Top management must support the security goals and lead by example.

In other research about socio-technical aspects of security, Dhillon and Backhouse (2000) move beyond the confidentiality, integrity and availability (CIA) of information with a paper that introduces a concept known as RITE. The authors suggest that information system security needs to change to not only addressing the data, but the changing organizational context as well. Organizations have focused much of their attention on CIA, where the authors define confidentiality as restricting data access to those who are authorized, integrity as preventing unauthorized modification of data, and availability as preventing unauthorized withholding of data or resources. If information systems are to be secure, there needs to be considerations beyond CIA. The authors suggest "inculcating a subculture where responsibility, integrity, trust

and ethicality (RITE) are considered important and are the first steps towards securing the information assets" (p. 127.)

Responsibility refers to individuals understanding their responsibilities and knowledge of roles within the organization, which also includes individual accountability. Responsibility is important in situations where formal guidance and rules are absent. Integrity refers to the integrity of the person employed by the organization. Before employees are given access to sensitive information, they should be properly screened. However, the integrity of an individual can change over time, such as when personal factors change. An economic recession, foreclosure, bankruptcy, divorce or many other such factors can lead a once honest employee down the wrong path. Organizations need to consider how they will continue to reassess the integrity of individuals as time passes.

Trust refers to a mutual system of trust between the individual and the organization. "Division of labor demands that your colleagues should be trusted to act in accordance with company norms and [the] accepted and agreed [upon] patterns of behavior" (p. 128). Today's organizations have less supervision, which gives employees more control. Mutual trust plays an important role in such environments. However, trust has a half life that needs to be reassured periodically. Ethicality goes beyond company rules and policies and into an area where rules do not exist. When a situation arises within an organization where a rule or policy stating how to handle the situation does not exist, individuals need to rely on some form of appropriate ethical norms. Responsibility, integrity, trust and ethicality (RITE) of individuals and confidentiality, integrity, and availability (CIA) of information are important for this dissertation because they

are core socio-technical aspects of information security that will be used to support this dissertation's argument.

In a book describing socio-technical security by Dhillon (2007), the author writes about maintaining the integrity of three vital systems of information systems security: the formal, informal and technical systems. The formal system within organizations represents the rules, regulations, governance, policies, procedures, or processes. The informal system represents social norms, security culture, beliefs, and attitudes of people. The technical system uses technology (computers) to automate parts of the formal system.

There must be coordination between the three systems to effectively manage information systems security. Dhillon describes the coordination among the three systems with an analogy of a fried egg. The yolk represents the technical system, which is held in place by the rules and regulations of the formal system. The formal system is the thin membrane holding the yolk. The white of the egg represents the informal system. The analogy "suggests the appropriate subservient role of the technical system within an organization" and "also cautions about the consequences of overbureaucratization of the formal systems and their relationship to the informal systems" (p. 5).

Managing security involves using controls with all three systems, meaning the controls themselves can be formal, informal, or technical. For example, a technical control might require a password or retinal scan to gain access to a computer. Expanding or shortening the organizational hierarchy is an example of formal control and giving security awareness training to employees is an example of an informal control (Dhillon, 2007). Controls must complement one another and Dhillon recommends "an overarching policy that determines the nature of

controls being implemented and therefore provides comprehensive security to the organization" (p. 6).

In other research by Dhillon and Torkzadeh (2006), the authors used the value-focused thinking method to interview 103 managers about their values in managing information systems security. This approach yielded 9 fundamental objectives for information systems security and 16 means objectives for achieving them within an organization. Of the 9 fundamental objectives, 7 are social objectives and 2 are technical objectives. The two technical objectives are to maximize access control and data integrity. The seven social objectives are to enhance management development practices and the integrity of business process, maximize privacy and organizational integrity, provide adequate human resource management practices, develop and sustain an ethical environment, and promote individual work ethic. The authors suggest that overall information security that primarily focuses on the technical aspects of confidentiality, integrity, and availability (CIA) of information is inadequate and that socio-organizational objectives must be taken into consideration. This paper was included in the socio-technical section of this literature review because of the result's socio-technical implications, but it is also important to this dissertation in that it used the value-focused thinking method in its methodology. The value-focused thinking method by Keeney (1994) is the same method used in this dissertation and will be described further in the next chapter.

In summary, the importance of social aspects in addition to technical aspects in information systems research is nothing new, as reported by Bostrom and Heinen in 1977. However, it took over 20 years before Dhillon and Backhouse (2001) reported a trend toward social aspects in mainstream information systems research. In the same paper, Dhillon and Backhouse state that

mainstream information systems security research had yet to make the transition and that socio-organizational aspects of security must be acknowledged in order to maximize security. Since that time, mainstream research has made that transition and social aspects of security are now considered an important part of overall security. For example, Trompeter and Eloff (2001) called for ethical principles in the development of information systems and security standards. Ruighaver et al. (2007) discussed the importance of a security culture in relation to the organizational culture and listed several aspects of good security culture, such as having an emphasis on employee responsibility and accountability, trust and security education. Also related to security culture was Leech's (2003) paper that suggested multiple ways of positively influencing employee behavior, by actions like managers leading by example by displaying good security practices of their own. D'Archy and Greene (2009) found that security culture contributes to compliant user behavior and extra-role behaviors. Dhillon (2007) reported the necessity of considering the social aspects of the informal system along with the formal and technical systems for achieving maximum security. Of particular importance to this research is the Dhillon and Backhouse (2000) paper describing the significance of responsibility, integrity, trust and ethicality (RITE) of individuals. Also of interest to this research is the use of the value-focused approach in demonstrating the importance of socio-organizational objectives in Dhillon and Torkzadeh's (2006) paper.

2.3 Information Security Policy:

Baskerville and Siponen (2002)'s paper describes a three level division of security policy: high-level policy, low-level policy, and meta-policy. At the highest level, "security policy is a high-level overall plan embracing the general security goals and acceptable procedures" (p. 338).

Policies at this level are generalized and more abstract than at the lower level. Lower level policies are derived from the high-level policies and are specific policies designed to support the objectives outlined at the highest level. Where a high level policy might describe a particular resource that needs to be protected and those responsible for protecting it, a lower level policy would describe the particular processes to be used to protect the resource. For instance, a high-level policy might state that department "A" needs to protect asset "X." A low-level policy that reflects the high-level policy might state that password or retinal scan technology needs to be in place to protect asset "X."

In the third level of the division of security policies, the authors introduce meta-policy. Meta-policy is "policy about policies." These policies "declare the organization's plan for creating and maintaining its information security policies" (p. 339). Meta-policy describes who is responsible for making policies, when policy creation is to take place, how policies are made, and how and when are polices reviewed, modified, or eliminated.

In support of the need for meta-policy, the authors point out that emergent organizations with changing business environments need meta-policy. Unlike checklist security standards, meta-policy can help organizations adapt their security policies to changes in the business environment. Checklists are security guidelines that can be used to help create security policies. However, the authors point out several shortcomings of such guidelines: (1) they fail to adequately address the fact that organizations are different and require different security policies (as cited by Baskerville, 1993), (2) they do not consider social aspects of security (as cited by Dhillon & Backhouse, 2001), (3) they "are broadly written, necessitation *ad hoc* decision making and judgment" (as cited by Ferris, 1994, p. 338), and (4) they overlook normal business

requirements, which may result in conflict between business and security requirements (Baskerville & Siponen, 2002).

In other security policy research, Karyda et al (2005) explore the processes of formulation, implementation and adoption of security policy in two different organizations. In both cases, the companies enlisted external consultants to conduct a risk analysis and create guidelines and recommendations. Management considered the recommendations and called upon their IT staff to implement the policies. The authors revisited each firm later to gauge the level of adoption by the users. In both cases, the consultants called for creating a security officer and establishing roles and responsibilities for that person.

The adoption of the security policy had mixed results. The first company had adopted the policy fairly well and the second company had not. However, the second company did not conduct security awareness training for their employees. Those employees had a negative attitude toward the security policies out of fear and lack of understanding. This emphasizes the importance of having an information security training program to educate employees on security policies. The first company already had an ethics policy in place and that policy worked well with the new security policies toward creating a security culture. The authors mentioned the importance of creating a security culture. In addition to the ethics policy in the first company, the authors did not report any other social aspects of security as being incorporated into the security policies. They mentioned roles and responsibilities, but only for the new security position and not for all the employees. There appears to be little or no consideration for socio-technical aspects of security in the creation of security policy in this study.

In other research, Doherty & Fulford (2006) argue that information security policy should be aligned with the strategic information systems plan (SISP). The "strategic information systems plan is a critical prerequisite for policy formulation, as it defines the business context in which information security will be managed and therefore the objectives of, and priorities for, security management" (p. 57). The strategic information systems plan is typically based on corporate objectives and the business plan. Aligning the information security plan to the SISP would link the security plan to the business plan. Mentioned below is how the authors summarized benefits of alignment- Doherty & Fulford (2006):

1. security can be more proactive instead of reactive to security threats;
2. security policy will have a stronger business orientation;
3. security policy can be adjusted in advance of strategic information systems initiatives;
4. strategic information systems plans can be viewed from a security perspective before implementation;
5. new systems created by the SISP can incorporate security controls identified by related security policy; and
6. this raises business manager's awareness of security threats and countermeasures.

Information security policy risk analysis is the topic of a paper from Spinellis et al. (1999), where the authors suggest that any information systems security policy should start with a risk analysis. "The objective of risk analysis is to identify and assess the risks to which the IS and its assets are exposed in order to select appropriate and justified security safeguards" (p. 122). The authors list five stages of risk analysis: (1) asset identification and valuation; (2) threats assessment; (3) vulnerabilities assessment; (4) existing/planned safeguards assessment; and (5)

risk assessment. A risk analysis methodology, CRAMM, was used to analyze a home-office and small enterprise scenario. The authors conclude that both environments have security weaknesses which are common to large enterprises, but the current security infrastructure and business practices of the smaller firms hinder effective risk management.

As mentioned earlier in research by Baskerville and Siponen (2002) and Dhillon and Backhouse (2001), checklists (standards) are often used by organizations to create information security policy. The Ernst & Young's 2008 Global Information Security Survey researched the use of security standards in developing security policy. The survey covered nearly 1400 organizations in more than 50 countries across all major industries. According to the survey, the use of information security standards has increased to 70% and the belief is that the use of international information security standards will continue to increase (GISS, 2008). The international standards used by respondents were ISO/IEC 27001:2005, ISO/IEC 27002:2005, and Information Security Forum's (ISF), the Standard of Good Practice for Information Security. ISO/IEC 27001:2005 is defined as a standard that "provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system" (p. 11). ISO/IEC 27002:2005 "outlines the potential control mechanisms which may be implemented based on the guidance provided within ISO/IEC 27001:2005" (p. 11). The Standard of Good Practice for Information Security "addresses information security from a business perspective, providing a practical basis for assessing an organization's information security arrangements" (p. 11).

Undertaking research to discover the content of information security policy, Fulford & Doherty (2003) questioned managers representing 158 organizations from multiple industries and varying

organizational size. The authors reported the top items and the percentage of inclusion in their security policy as: personal use of the information system (45%), disclosure of information (38%), physical security (37%), violations and breaches (36%), viruses, worms, and trojans (34%), system access (33%), mobile computing (32%), Internet access (30%), software (25%), encryption (25%), and contingency planning (17%). Of the 158 organizations surveyed, 76% of them had a formal written security policy. The authors statistically tested and verified that those without a security policy were not of the same organizational type.

In summary, in this information security policy literature review, we have learned that management at the strategic level of the organization is involved in creating the high-level security policies (Baskerville & Siponen, (2002). In order to create these policies, they gather information from various sources. These may include standardized checklists, external consultants, current organizational culture, current security measures, risk analysis, business objectives and the strategic information systems plan (Baskerville & Siponen, 2002; Karyda, et al, 2005; Spinellis, et al, 1999; Doherty & Fulford, 2006). High-level polices are used to create low level policies, known as corporate and procedure policies in this dissertation. Procedure policies are more specific policies that are usually created with the input of content specific professionals and not upper management. For example, technical policies at this level are often created by information technology professionals or legal considerations may involve lawyers (Karyda, et al, 2005). The procedural policies are based on the corporate policies, which should reflect the business plan (Spinellis, et al., 1999). Security policy is also primarily technical and lacks the social aspects of security. According to Fulford & Doherty (2003), some of the top items that organizations include in security policy are breaches, viruses, worms, trojans, system access, software and encryption. Checklists, which are often used as guidelines for security

policy are also technically oriented and lack social aspects of security (Baskerville & Siponen, 2002; Dhillon & Backhouse, 2001). In order to maximize security, social aspects of security must be considered along with technical aspects (Dhillon, 2007).

2.4 Information Security Training:

Information security training, also called security awareness training in some research, is a relatively small topic within information systems research. Only a few studies investigate information security training as the main focus of the research. Like in the case of many topics within the discipline, there are multiple definitions. Siponen (2000, p. 32) defines "information security awareness" as "a state where users in an organization are aware of – [and] ideally committed to – their security mission." Straub & Welke (1998, p. 450) define security awareness training as "the training of managers and other professionals in proper use of system assets." The authors state that training should review employee policies, such as system authorizations, conditionalities of use, password management, penalties for security breaches etc. (Straub & Welke, 1998). "The training should also make participants aware of the general effectiveness of deterrent, preventive, detective, and remedial countermeasures in lowering systems risk" (p. 451). This dissertation defines information security training as a method of educating all employees on how best to protect an organization's information systems.

Information security training research primarily falls into two research streams, one researches the necessity of having a training program and the other researches how to make training more effective. The necessity of training is important to this dissertation because this research forwards the suggestion that training of managers can help maximize information security. Making training more effective is also important to this dissertation because this research creates

training videos to support the central argument. Very little research has investigated the content of information security training, but a few studies and surveys were found. The content of current training is also important for this dissertation because this research argues that current training is technical in nature and is linked to the information security policies.

In researching the importance of information security training, Rezgui and Marks (2008) conducted a case study to investigate factors that affect the information security awareness of staff at an institution of higher education. Through questionnaires, interviews, observation and documents, the authors collected data and used various coding techniques for analysis. The research discovered that factors such as conscientiousness, cultural assumptions and beliefs and social conditions affect university staff behavior and attitude towards work and information security awareness (Rezgui & Marks, 2008). Of particular interest was the fact that the university did not have a computer security awareness training program and did not know how that affected employee security awareness. Rezgui and Marks recommend the establishment of an information security training program. The problems discovered with employee's security awareness are listed below (Rezgui & Marks, 2008, p. 250):

1. "many respondents were not acquainted with basic IS security practices, including how to change their passwords or how to back up their data;"
2. "users shared passwords;"
3. "operative, unlocked computers were left unattended;"
4. "laptops were not locked and left out;"
5. "users were confused about the existence of an IS policy and none had seen one;"
6. "users did not know how to locate an IS staff member;"

7. "users could not identify the university IS goals and objectives;" and
8. "users regarded university data as of no interest to them."

In other research that supports the need for security awareness training, May (2008) developed a decision model that provides informed alternatives to decision makers who desire to maximize IS security within an organization. The model is based on Dhillon & Torkzadeh's (2006) nine fundamental and sixteen means objectives that are essential in maximizing information systems security. This decision model consisted of 69 ranked value-driven tasks and associated security objectives they impact. Of particular interest is that security awareness training was ranked #1 of the 69 tasks. Therefore, security awareness training was found to be the most important task associated with maximizing information systems security. According to May's research, awareness training impacts 14 sub-objectives, such as ensuring sensitive data is adequately secured, emphasizing the importance of data privacy and maintaining personal accountability.

The need for security awareness training is nothing new. Straub and Welke (1998) stated that systems "risk can be managed or reduced when managers are aware of the full range of controls available and implement the most effective controls" (p. 441). Lacking knowledge can lead to less effective security. To cope with systems risk, the authors identify an approach that includes the use of a security risk planning model, security awareness training and countermeasure matrix analysis. The awareness program involves educating managers and users. The managers should be educated on the security action cycle, which involves deterrence, prevention, detection and remedies for computer abuse. Managers should also be educated on "obvious vulnerabilities and resources which are required to secure systems at some minimal 'acceptable' level" (p. 460). Everyone, including managers and users should receive security awareness training covering

high level objectives, such as the security action cycle, as well as specific lower level vulnerabilities and responses. This training should also cover security policies and be offered to new employees at orientation and veteran employees in refresher programs. While this paper suggests that managers receive specific training that is in addition to the information security training, the paper fails to recognize the importance of socio-technical aspects of security. Instead the authors suggest the use of checklists, which have been shown to be technically oriented.

In supporting the need for information security training, Von Solms and Von Solms (2004) create a list of the ten most deadly sins of information security management. In the list is "not realizing the core importance of information security awareness amongst users" (p. 372). The authors state that in some companies "no proper awareness programs exist, and users are unaware of the risks of using the company's IT infrastructure and the potential damage they can cause" (p. 375). The consequence of committing this sin, according to the authors, is that "many information security related intentions will fail to materialize" (p. 375).

In other research demonstrating the importance of security awareness training, Lamour (2008) used the Solomon four group experimental design to investigate the effects of training on security practitioners and users. The experimental design consisted of pre-tests and post-tests for groups that received training as well as control groups that did not receive training. Practitioners received training on how to secure Cisco routers. Users received training on how to recognize phishing attacks. The results showed that the practitioner group that received training nearly quadrupled their scores from pre-test to post-test, from about 25% to near 100%. The practitioner control group that did not receive training remained at the low 25% level. The user

treatment group also had a large increase in recognizing phishing attacks. They increased from 40% to over 90% from pre-test to post-test scores. The control group that did not receive training remained at the low 40% level. These results indicate that training can be useful for both practitioners and users.

In calling for more research in the area of security awareness training, Schultz (2004) states that he fears too many security awareness training programs are subpar. "Some simply present platitudes about security to their captive audiences instead of teaching things that could and should make a practical difference in each attendee's daily job" (Schultz, 2004, p. 2). Also, many programs are out of alignment with business goals and are taught by independent training organizations, resulting in a "one size fits all" approach (Schultz, 2004). Schultz suggests that posters, coffee cups, pens, and slogans are overused and have become meaningless and "gimmicky" (Schultz, 2004). Schultz suggests that research should work to address the following issues regarding security awareness training: (1) "How can we better measure and then maximize ROI for security training and awareness?" (p. 2); (2) "How can we better align security training and awareness efforts with business drivers?" (p. 2); (3) "How to impart users, system administrators, managers and others the security-related knowledge and skills they really need?" (p. 2); (4) "How can we enable them to better retain and put into practice what they learn?" (p. 2); and (5) that there is a need for evidence of success stories.

Another stream of information security training research attempts to make training more effective. For instance, in researching how people internalize training, Siponen (2000) believes current methods are descriptive and lack theoretical foundations in motivation and behavior. From the viewpoint of behavioral theories, a laissez-faire style of leadership and lax management

attitude concerning security and passing around of circulars are inept and inapplicable in security procedures (Siponen, 2000). "Successful organizational awareness or education requires more actions than merely the given of a set of rules" (Siponen, 2000, p. 36). Security guidelines need to be justified and relevant, in a way that people's cognitive states can be changed by justifying each guideline (Siponen, 2000). "End users may change their attitude and motivation towards the guidelines in the intended way" (p. 36). Siponen suggests a persuasion framework based on the theory of intrinsic motivation, the theory of planned behavior, and the technology acceptance model. The practical approaches or principles derived from these theories are morals and ethics, well-being, a feeling of security, rationality, logic and emotions. The goal is to create justifiable security guidelines based on these theoretically based principles. Doing so gives management the best chances that their employees will internalize the guidelines and minimize errors.

In other research about the psychological factors of security training, Thomson & von Solms (1998) suggest that techniques from social psychology can be applied to security awareness training to make training more effective. In order to bring a positive change in an employee's behavior, the authors suggest using social psychology principles such as changing behavior directly, using a change in behavior to influence a person's attitude, and changing a person's attitude through persuasion. A security awareness program should teach measures that become subconsciously entrenched into the end-user, so that they do not have to think in order to promote security (Thomson & von Solms, 1998). Examples include habitually signing off from the computer when leaving the office, making sure the screen is not visible to those not authorized to see it, and making regular backups of important data (Thomson & von Solms, 1998). Based on these principles, the authors make suggestions for conducting security awareness training. A summary of these suggestions follows (Thomson & von Solms, 1998):

1. an awareness program should be geared toward groups of similar work levels (upper management, line employees, etc.);
2. sessions should be divided into a number of short education sessions, to allow participants to be more relaxed and to retain their full attention;
3. commitment from employees is required at the conclusion of each session;
4. the material adherence should be evaluated, preferably without the participant's knowledge. The authors suggest this may be done through observation or each participant could report what they have done to implement what they have learned in previous sessions;
5. visible tokens of appreciation should be given to those that adhered to the training techniques. Tokens should be visible, but not of great monetary value;
6. each session should cover more topics than actually required. Getting commitment for all topics and then reducing down to what is necessary makes participants feel like the instructor has given them something and they may be more likely to adhere to the remaining topics; and
7. the presenter should be an expert and well presented.

How to make security training more effective was the topic of research from Cone et al. (2007), where the authors describe a video game, CyberCIEGE, that was developed to deliver security awareness training. The game was designed to make security awareness training more effective, while holding the trainee's attention long enough to get the message across. The game uses adaptable virtual scenarios to allow players to make choices about security in a particular enterprise environment and see the consequences of their choices, when the environment is under

attack from hackers, vandals, and potentially well-motivated professionals (Cone et al. 2007). The authors conclude that the game can be an effective addition to awareness training programs.

In investigating various formats of training, Shaw et al. (2009) reported on the impact of information richness on online information security awareness training effectiveness. The authors identify three levels of security awareness: perception, comprehension and projection. Perception is "to achieve an understanding of the presence or awareness of a threat" (p. 93). Comprehension refers to the user's ability to understand and assess the dangers posed by various security risks. Projection is the ability of users to project or predict the future course of security attacks.

The research investigates the impact of hypermedia, multimedia and hypertext to increase security awareness among the three awareness levels. Hypermedia is the richest medium and is defined as "an interactive medium that can consist of graphics, audio, video, plain text and hyperlinks, intertwined to create a generally non-linear medium of information" (p. 94). Multimedia has less richness than hypermedia and more than hypertext. "Multimedia combines text, image, sound, music, animation, video and virtual reality, but must be accessed in a linear sequence" (p. 95). Hypertext is the least rich medium and is described as "plain text with the hyperlink features that does not incorporate feedback capability, multiple cues, language variety and personal focus" (p. 95).

The authors find positive correlations between the degree of media richness and the improvement of security awareness among the awareness levels. Hypermedia was the most effective, followed by multimedia and hypertext. However, there was a negative effect of too much richness on learning performance at the perception level. The authors suggest media

richness is less important for learning at the perception level and most important for advancing to the comprehension and projection levels.

Only a few studies or surveys were found that investigated information security training in context with the actual content of training. One was Rotvold (2008), where the author attempted to discover the current state of security training within organizations by conducting a survey of 144 organizations representing small to large organizations in many sectors. Sixty percent of the organizations surveyed reported their organizations performed security awareness training, with 44.7% of the 60% reporting it was mandatory. In those 44.7%, attendance was tracked 72.8% of the time. Given these reported numbers, the actual percentage of employees receiving security awareness training can be quite low. Training was most frequently offered once a year (45%) and the training was conducted by IT staff 58% of the time, followed by management which conducted the training 28% of the time. The top delivery methods for security awareness training were face-to-face sessions (54%), e-mail messages (53%), online training (47%), presentations (32%), newsletters (29%), and posters/flyers (28%). The most common general topic in information security training was security policy. Some of Rovold's top policy training topics are 'acceptable use (89%), e-mail (85%), passwords (78%), backup and recovery (71%), antivirus (70%), software installation and licensing (67%) and disaster recovery (58.2%). Of the top 15 topics in information security training, where policies was number one, all were technically oriented.

In a government sponsored survey, the 2006 CSI\FBI Computer Crime and Security Survey found that information security policies were the most important topic of information security training (CSI, 2006). In the 2007 version of the survey, security policies were still a top topic for

security training (CSI, 2007). The 2008 and 2009 versions of the survey no longer investigated the primary topics of training.

In summary of current information security training research, this literature review demonstrates the need for information security training and shows how vulnerable security can be without a training program. The literature review also demonstrates the characteristics of effective training, and also describes ways to make it more effective. It does so in the form of theoretical models or frameworks, though none of these models are tested. These theoretical concepts focus on learning and obeying through persuasion and motivation to get trainees to remember and obey the content of the training. Very little research was found that investigated the actual content of information security training, with Rotvold's (2008) paper being the only in-depth study. Rotvold's study not only revealed to us that security policy was the content of training, but also listed the security policy topics. The CSI (2006, 2007) surveys also stated that security policy was a top topic of training, but did not list the actual policy topics.

2.5 Literature Review Discussion:

The nature and scope of information security training and information security policy is important to this dissertation because research demonstrates that the socio-technical approach is the best way to maximize the security of information systems (Dhillon and Backhouse, 2000, 2001; Trompeter & Eloff, 2001; Dhillon & Torkzadeh, 2006; Dhillon, 2007; Siponen, 2001). However, current information security training and information security policy is technically oriented, and lacking in the social aspects of security (Rotvold, 2008; CWS, 2010; Fulford & Doherty, 2003). The social aspects of information security are important because they engage the human element of information systems. While organizations rely heavily on computers and

other technology to compete, they still need people to use and maintain that technology. Focusing only on securing the technology and ignoring the people that use the technology is incomplete security.

To consider the people side of organizations, Dhillon and Backhouse (2000) describe a concept called RITE, which stands for responsibility, integrity, trust and ethicality of individuals. The authors state that organizations need to ensure that employees understand their roles and responsibilities within the organization. The integrity of employees is also very important, as well as having a trusting relationship between employees and the employer. Organizations should also consider the ethicality of employees. Ethical aspects of security are just as important as technical aspects and companies with ethics programs suffer less economic crime (Trompeter & Eloff, 2001, ECS, 2007). Another social aspect of information security that no organization should ignore is the creation of a strong security culture (Ruighaver et al., 2007; Dhillon, 2007; Karyda, et al., 2005; von Solms & von Solms, 2004; Leech, 2003; Vroom and von Solms, 2004). A strong security culture has been linked to such things as compliant user behavior and employees engaging in security enhancing conduct beyond their mandatory job descriptions (D'Arcy & Greene, 2009).

If socio-technical security is the best way to protect information systems, then how does an organization create socio-technical security? They do it through their information security policies. Information security policy is broken down into corporate security policy and procedural security policy, which Baskerville and Siponen (2002) call high and low level security policy. The creation of corporate security policy is the crucial beginning for overall information systems security because this level of policy affects lower level procedural policy

and information security training programs. Corporate security policy describes general goals for information security, but not the actual means for accomplishing those goals. Procedural security policy describes the means for carrying out the corporate security policy. Corporate security policy is used as the template for procedure oriented security policy (Baskerville & Siponen, 2002). A goal of any organization should be for managers to create socio-technical corporate security policy so that procedural security policies also become socio-technical.

Once corporate and procedural information security policies are socio-technical, how will information security training be affected? The connection between information security policy and information security training is that the topic of training is primarily the procedural security policies (Straub & Welke, 1998; Rotvold, 2006; CSI, 2006, 2007). Recall that the procedural security policies are the means for implementing the corporate policies. A part of the implementation process is to educate the employees about the policies. It is difficult to have policies and expect employees to follow them if they are not educated about them adequately. This inadequacy leads to employees/users that lack the proper security knowledge (Rezgui & Marks, 2008). This is why procedural policies are the primary subject of information security training. Organizations currently use information security training as a primary way of protecting their information systems (CWS, 2010).

We know that information systems should be protected with socio-technical solutions and that information security training is a primary method for protection. We also know that information security training is based on procedural security policy and that procedural security policy is a means for achieving corporate security policy. The last piece to the puzzle discusses the creation of the corporate security policy and possible reasons it is not created with socio-technical

solutions. Corporate security policy is created at the strategic level of the organization by managers that have very little experience or knowledge of creating security policy (Hone & Eloff, 2002; von Solms & von Solms, 2004). Their expertise is usually in some other area, such as business planning, forecasting, finance, etc. Hone and Eloff (2002) suggest that those creating the policy often lack the knowledge to do so. Their "lack of skills and understanding" in developing a security policy often leads the authors to "turn to other organization's policies, commercially available sources or templates available from public sources, such as the Internet, for answers to their questions" (pp. 402-403).

Among the commercially available options available to managers are checklists or standardized guidelines. According to Ernst & Young's 2008 Global Information Security Survey, 70% of those organizations surveyed used standardized guidelines to create security policies and that number is expected to increase (GISS, 2008). However, we know that checklists or guidelines have many shortcomings, including the lack of flexibility to changing business environments and the lack of attention to social aspects of security (Baskerville & Siponen, 2002; Dhillon & Backhouse, 2001). It is completely understandable why managers use checklists over 70% of the time to create security policies. Checklists have become widely used by organizations and are generally accepted.

In deciding what corporate security polices to create, a manager has many options to consider. They can use the above option, such as checklists, or they can also rely on their education, experience and knowledge. Their decision is likely to be based on a combination of all of these, but should be aligned with what they truly believe will be the most effective way of protecting their information systems. A manager's belief system about what they think are the most

effective ways of protecting their information systems is known as their value system, as described by Keeney (1992). Keeney's work with value-based objectives and decision making is discussed in chapter three's methodology. Keeney's research is getting introduced here to help make sense of the connection between the concepts reviewed in this chapter. A manager's internal values about how best to protect their information systems are expressed through their value-based objectives. Keeney defines value-based objectives as "statements of something that one wants to strive towards" (p. 34). It is these objectives that managers use to create corporate security policy. If their beliefs (values) are that socio-technical solutions are the best way for protecting their information systems, then they will create socio-technical information security objectives. As seen in figure 2.1, these socio-technical security objectives will influence the corporate security policy they create. Corporate security policy will then inform procedural security policy and the information security training will then be socio-technical as well.

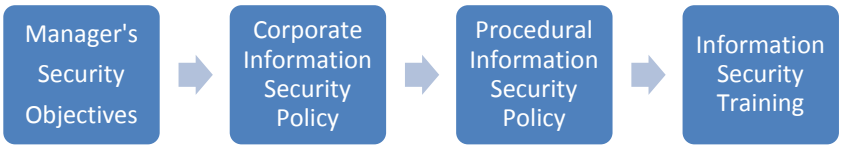

Figure 2.1: Policy to Training Relationship

2.6 Literature Review Conclusion:

There is a downward flowing relationship between a manager's individual objectives, corporate security policy, procedural security policy and information security training. This relationship stresses the importance of the manager's value-based security objectives on corporate security policy because of the effect on procedural policy and training. If managers have socio-technical

value-based security objectives, they will create socio-technical corporate security policies, thus leading to socio-technical procedural policies and training. A socio-technical approach to information security is necessary to maximize security. However, security policy and training is currently technical in most organizations, meaning manager's value-based security objectives are currently technically oriented. This research argues that manager's value-based security objectives can be influenced to be socio-technical, thus impacting security policy and training in a positive way.

3. Theory and Methodology

3.1 Introduction:

The literature review demonstrated the importance of social and technical aspects in maximizing overall security (Backhouse & Dhillon, 1996; Dhillon and Backhouse, 2000, 2001; Trompeter & Eloff, 2001; Siponen, 2001; Dhillon & Torkzadeh, 2006; Dhillon, 2007). The review also outlined the relationship between corporate information security policy, procedural information security policy and information security training, as well as the importance of all three to overall information security (Rezgui and Marks, 2008; May, 2008; Rotvold, 2007, 2008; CSI, 2006, 2007; Von Solms & Von Solms, 2004; Straub & Welke, 1998). The problem is that managers creating information security policy are creating technically oriented policy and minimizing or ignoring the social aspects of security (Rotvold, 2008; CWS, 2010; Fulford & Doherty, 2003). This may be because managers often lack the knowledge to create proper information security policy (Hone & Eloff, 2002). Therefore, this dissertation will attempt to train managers on the importance of socio-technical information security with the goal of encouraging them to implement it into their information security policy.

But how do we know that what managers learn in training will be used in the security policy they create? We know this from the theoretical foundation of value-focused thinking, described by Keeney (1992) and mentioned in the previous chapters. A manager's values and value-based objectives represent the manager's core beliefs about the decision situation, in this case, about

what security policies to create to maximize information security. By using the value-focused thinking approach, this dissertation will ascertain manager's values about maximizing information security after watching an information security training video. There will be four groups of managers and four types of training videos, with each video having a different nature and scope. Analyzing the group's values and value-based objectives toward maximizing information security will help us answer this dissertation's research questions.

Another important part of this dissertation is determining how the groups will rank their lists of value-based objectives. An output from the value-focused thinking method is an unranked list of value-based security objectives for maximizing information security. Because information security training often receives less than 1% of the security budget and is often the first to get cut in budget reductions, this dissertation is interested in ascertaining how managers would rank their value-based security objectives (CSI, 2006, 2007, 2008, 2009, Rotvold, 2007, 2008). If budget restrictions mean some value-based security objectives get implemented and some do not, which do managers feel are most and least important and what implications would their choices have on overall information security? To determine a ranked list of value-based objectives from each group of managers, a ranking Delphi methodology is used. The Delphi methodology has been around for over 50 years and the ranking Delphi methodology was formalized by Schmidt (1997) and is used to obtain group rankings of objectives that can then be used for decision making.

The next two sections describe the value-focused thinking method and how it has been used in research. The following two sections describe the ranking Delphi method and how it has been used in research, particularly information systems research. The following section describes this

dissertation's research method and the four groups of participants. The last section concludes this chapter.

3.2 Value-Focused Thinking:

Managers creating information security policy are faced with a decision problem. How do they decide what policies to create that will maximize information security? When faced with a problem, a typical decision maker considers the alternatives for solving the problem, and then considers the objectives for evaluating the alternatives (Keeney, 1992). This leads to the decision maker solving the decision problem by choosing among available alternatives. Keeney (1994) refers to this type of decision making as *alternative-focused thinking* and describes it as reactive and not proactive. "Solving decision problems is the sole aim of alternative focused thinking" (Keeney, 1992, p. 47).

Values also solve decision problems, but go beyond that narrowed focus by identifying decision opportunities, also known as problem finding (Keeney, 1994). Keeney introduced value-focused thinking in 1992 and described values as more fundamental than alternatives that define all a decision maker cares about in a given decision situation (Keeney, 1992). The idea of considering values first, before alternatives, is known as value-focused thinking and can be used to make better decisions. The reason a decision maker is concerned with a decision problem to begin with is because of consequences. If the decision maker did nothing, there would be undesirable consequences, thus this is the reason alternatives were generated. The alternatives presumably have more desirable consequences. The desirability of various consequences is based on one's values, so decision making should also be based on one's values and not alternatives. "Alternative-focused thinking is designed to solve decision problems," where

"value-focused thinking is designed to identify desirable decision opportunities and create alternatives" (Keeney, 1996, p. 538). Value focused thinking identifies the best possible outcome and assists in making it a reality versus other approaches which identify the best of what is available (Keeney, 1992). Value-focused thinking was chosen for this dissertation because the method identifies values first, which represent how managers truly feel about maximizing information security. Influencing manager's core beliefs about how to best maximize information security is central to this dissertation's argument. The best way to gauge the influence of training given to managers is to ascertain their values.

"Value-focused thinking is designed to focus the decision maker on the essential activities that must occur prior to solving a decision problem" (Keeney, 1994, p. 33). Figure 3.1 shows how thinking about values is at the core of many decision making constructs. According to Keeney (1994), value-focused thinking can help uncover hidden objectives, lead to more productive information collection, improve communication among concerned parties, facilitate involvement of multiple stakeholders, enhance the creation and evaluation of alternatives, guide strategic thinking, identify decision opportunities and enhance the coordination of interconnected decisions (Keeney, 1994). Thinking about values is at the core of all of these.

Value-focused thinking is a process that identifies objectives, where objectives are defined as "statements of something that one wants to strive toward" (p. 34). Objectives are characterized by three features: a decision context, an object and a direction of preference. For example, a security manager might have an objective to "minimize phishing email." The decision context is information security. The object is phishing email and the direction of preference is less

phishing email rather than more. Objectives are further distinguished as either fundamental objectives or means objectives.

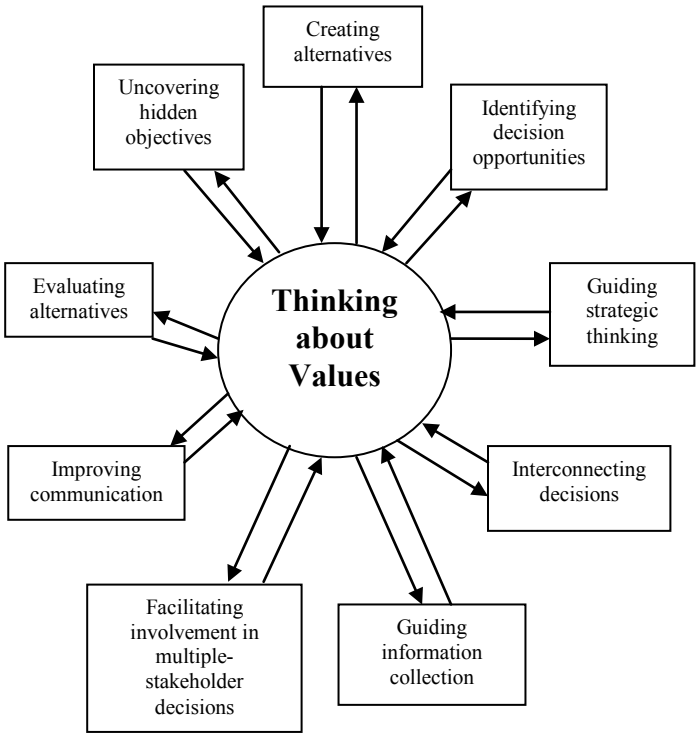

Figure 3.1: Thinking about Values:
The Basis for Quality Decision Making (Keeney, 1994)

Fundamental objectives are "the ends that decision makers value in a specific decision context" and means objectives are "methods to achieve ends" (p. 34). This dissertation's use of value-focused thinking yields a list of unranked security objectives for each of the four groups of participants.

Keeney (1992, p. 57) describes 10 different, but overlapping, methods for identifying objectives through values, such as using alternatives, consequences, goals, constraints, guidelines and

various perspectives. However, Keeney believes the best way to discover one's values is to ask for them (Keeny, 1994). If the goal is to obtain a list of objectives related to a decision problem from decision makers, start by asking them to develop a list of values, known as a wish list. This is an unranked list of one's values toward a given decision. For example, a person buying a car might list low maintenance costs, comfortable ride and safety as some of their core values. Some means for achieving these values might be good gas mileage, computerized suspension, leather seats, anti-lock brakes and air bags. Keeney (1999, p. 534) describes three steps for obtaining a list of fundamental and means objectives: (1) develop a list of values; (2) express values in common form; and (3) organize the values and indicate relationships.

The first step involves asking people to develop a wish list of values about a certain topic. The second step involves the researcher converting the values to objectives by restating the values into a common form. For example, the person purchasing the car might have written down that they wished for a car that did not cost a lot to maintain. The researcher might restate this value into the objective "ensure low maintenance costs." The third step involves separating fundamental objectives from means objectives. Using the same car example, there may be the means objectives "ensure car safety," "ensure the use of anti-lock brakes," "ensure the use of front air bags," and "ensure the use of side air bags." These can be the means objectives for the fundamental objective "ensure car safety."

Value-focused thinking has been used in a wide variety of research, ranging from military to environmental applications. Sample topics where value-focused thinking have been used include fighting terrorists (Bullock, et al, 2008), selecting automatic rifles for the Croatian Army (Peharda & Hunjak, 2008), locating community correction centers (Johnson, 2006),

understanding organizational safety (Merrick, et al, 2005), climate change (Keeney & McDaniels, 2001), Internet commerce (Keeney, 1999), mobile communications (Yoo, et al, 2001), and business process modeling (Neiger & Churilov, 2004). Because value-focused thinking is a decision making methodology, it can be used in almost any situation where decisions need to be made, whether a personal decision or an organizational decision. This is why value-focused thinking has been used in such a wide variety of research topics.

Value-focused thinking has not been widely used in information systems or information security research. Dhillon and Torkzadeh (2006) used value-focused thinking when they interviewed 103 managers to assess their values on information security. As discussed in chapter two, the authors described 9 fundamental objectives and 16 means objectives related to information security. In the only other information systems research found that used value-focused thinking, Barclay and Osei-Bryson (2010) used value-focused thinking to evaluate the values of stakeholders of information systems projects. The authors proposed a formal method to develop a comprehensive set of objectives grounded in the views of the project stakeholders (Barclay & Osei-Bryson, 2010).

3.3 Ranking Delphi Method:

The output of the value-focused thinking method in this dissertation is a robust list of security objectives for each of the four groups. This list helps answer the research questions about the affect of training on the values of the participants and the affect of their value-based objectives on information security policy. Next, we determine which objectives the groups feel are most important. In a time of budget constraints or when it is just not possible to implement every security objective listed, which security objectives are important enough to implement and which

are expendable? To determine the answer to this question, a ranking Delphi method was used to create a ranked list of security objectives.

The Delphi method originated with the Rand Corporation in the 1950's and was used to generate a consensus of opinion from an anonymous group of experts. It was first used by the military to investigate nuclear arsenal levels. However, the Delphi method can be used to achieve consensus on just about any non-complex topic, such as developing a list of criteria, forecasting trends, ranking and answering specific questions about a topic. For complex topics that cannot be described in a short and precise research question, other methodologies, like scenarios, are better suited. There are a series of rounds (iterations) with the group members about the topic that leads to a higher level of mutual agreement. In each round, the participants are told the results of the previous round and given a chance to change their opinion. Changing one's opinion to reflect the group opinion leads to higher group consensus. The anonymity of the group members eliminates group think and personality conflicts that may otherwise bias results. Anonymity also makes it easier for group members to change their mind about a topic without the knowledge of other group members.

The ranking-type Delphi method is a group exercise and group size can vary dramatically depending on the nature of the topic and the availability of experts. Some topics may only have a few people in the world considered to be knowledgeable enough to warrant a Delphi study. Okoli & Pawlowski (2004) suggest adequate group size for a Delphi study is 10-18 participants, but can be lower depending on group dynamics. Loo (2002) suggests group sizes of 5-10 can be adequate.

Because the Delphi method can be applied to multiple forms of research questions, there are multiple variations of the methodology. This dissertation is interested in ranking the list of security objectives produced by the groups, so a ranking methodology was chosen. The ranking Delphi methodology is what is typically used in information systems research. This variation uses group members to obtain a ranking of key objectives, which can then be used for decision making. Prior to Schmidt (1997), a problem with the ranking-type Delphi method was the lack of a formal set of published rules. Researchers followed inconsistent methodologies, lacked statistical support for many conclusions, and did not follow for a consistent means of reporting results (Schmidt, 1997). Schmidt (1997) presented "a method based on nonparametric statistical techniques, to conduct ranking-type Delphi surveys, perform analysis and report results" (Schmidt, 1997, p. 763). Schmidt's technique allowed for statistical support of conclusions, outlined a clear method, and defined a definitive stopping point for the iterations. Since then, many Delphi studies wishing to employ ranking utilized the ranking-type Delphi method described by Schmidt. This dissertation chose Schmidt's technique because of the methodological improvements over previous techniques and for the rich supply of literature support for the Schmidt's method.

Schmidt's techniques for conducting ranking-type Delphi research follow a three phase approach. The first phase discovers the issues, the second determines the most important issues and the third phase ranks the issues. Below are step by step guidelines for conducting ranking-type Delphi Research, as presented by Schmidt (1997). In this dissertation, phase one was conducted using the value-focused thinking approach, which yielded an unranked list of security objectives.

Phase 1: Discovery of Issues

1. Encourage respondents to submit as many issues as possible.
2. Ask for a description of each issue.
3. The researcher consolidates the list, including different terms that appear to mean the same thing. Put similar terms together and give a consolidated description.
4. Respondents now verify proper mapping and that their ideas are fairly represented.

Phase 2: Determining the Most Important Issues

1. Send each participant a randomly ordered consolidated list from phase 1 (this list was created with the value-focused thinking method).
2. Participants select at least 10% (more if less than 100 items) of the issues they feel are most important. Do not ask participants to limit their list to a particular number of issues. Ask them to list the minimum number and go beyond if necessary.
3. The researcher eliminates all issues not selected by a simple majority of respondents, which creates a new consolidated list. Groups will have varying lengths of lists.
4. If the list is still too long, conduct phase 2 again with the shortened list.

Phase 3: Ranking the Issues

1. Arrange the paired list in random order and ask respondents to rank all the issues. Statistics can be used to rank ties, but it's easier to ask respondents to avoid ties.
2. Apply Kendall's Method to create a consensual ranking of the individual lists. Kendall's coefficient of concordance (W) (Kendall & Gibbons, 1990; Siegel & Castellan, 1988).

3. After each round in this phase, the researcher must ask the participants if another round should be conducted to obtain a better consensus.
4. Monitor Kendall's W (see table 3.1). A leveling off of Kendall's W indicates lack of progress from the previous round, so polling should stop. This coupled with verbal group consensus strongly supports stopping. Consider the actual value of W as the indication of consensus strength and not the statistical significance of W. A high value indicates consensus in groups of 10 or less. In groups of 10 or more, a smaller value of W can be significant. Kendall's W ranges from 0 (no agreement) to 1 (complete agreement). A strong consensus is W = .7 and is a good indicator to stop polling.
5. Information to monitor beyond mean ranks: (1) interpretation of Kendall's W from the previous round; (2) percentage of respondents placing each item in the top half of their list; and (3) comments from the participants. The first two convey the degree of consensus. Do not consider standard deviation as a form of consensus because it cannot be applied to ordinal level data.

Table 3.1: Interpretation of Kendall's W. (Schmidt, 1997)

W	Interpretation	Confidence in Ranks
.1	Very weak agreement	None
.3	Weak agreement	Low
.5	Moderate agreement	Fair
.7	Strong agreement	High
.9	Unusually strong agreement	Very high

The Delphi method has been utilized in research for over 50 years, so hundreds of studies were found utilizing the method. Many of the studies focused on forecasting or developing a framework and most identified some set of issues or factors pertaining to the topic under study. Since the Delphi method is used to get a consensus of opinion from an anonymous group, it can

be utilized in a large variety of disciplines and fields. Recent examples were found in molecular genetics (Marsden, 2009), medical ethics (Vorm, 2009), psychotherapy (Opie, 2008), ecology (Prato, 2008), tourism (Lee, 2008), biological conservation (Patrick, 2008), engineering (Miura, 2008) and accident analysis (Kim, 2008).

There were dozens of studies found in information systems/information technology research that utilized the Delphi method. Table 3.2 lists five of the studies found that utilized the Delphi method, but did not utilize the techniques for ranking described by Schmidt (1997). Those studies will now be described in more detail to demonstrate their inconsistencies with Schmidt's formal methodology.

Table 3.2: Delphi Method in IS Research

Author	Purpose	Group Size
Doke & Swanson (1995)	Identify decision variables for selecting prototyping in information systems development.	31, 29, 27
Brancheau, et al. (1996)	Identify critical issues facing information systems executives in the forthcoming 3-5 years.	78, 87, 83
Hayne & Pollard (2000)	Identify the critical issues in information systems for the forthcoming 5 years.	176, 157
Mulligan (2002)	Classify information technology within the financial services industry	25, 24, 23
Nakatsu & Iacovou (2009)	Identify risk factors for domestic and offshore outsourced projects (two groups)	15, 15, 15 14, 11, 12

Doke and Swanson (1995) used a ranking Delphi method to identify decision variables for selecting prototyping in information systems development. Thirty one MIS managers completed round one of the group iterations, which yielded nine decision variables for selecting prototyping. Twenty nine participated in the second round, where a tenth decision variable was added. Twenty seven participated in the third and final round. This ranking method was one of

the older methodologies that did not utilize Schmidt's (1997) techniques. Schmidt's techniques would not have allowed for the addition of new decision variables in the second round.

In a paper published in MIS Quarterly, Brancheau et al. (1996) forecasted critical issues facing information systems executives in the forthcoming 3-5 years. Participants were members of the Society for Information Management (SIM), where 78 participated in the first round, 87 in the second round, and 83 in the third round. Not all of these participants were the same throughout the rounds and 108 overall participants were used. Interchanging participants during the iterations is one of the inconsistencies of previous methodologies. The results of this study yielded 21 critical issues, where business relationship issues declined and technology infrastructure issues increased in importance.

In another paper forecasting the critical issues in information systems in the forthcoming five years, Hayne and Pollard (2000) used a modified Delphi technique. The authors invited 920 members from the Canadian Information Processing Society (CIPS) to join the study and 176 participated in round one. To boost participation, the authors sent out 536 additional requests to the non-respondents for a total of 712 invitations. Of those 712, 157 participated in round two. However, the authors do not disclose how many of those that participated in round two did not participate in round one and how results may be affected by those participants not having had input in the previous round. The authors reported results on the top 10 upcoming critical issues facing information systems.

In other research, Mullican (2002) used a Delphi Study to help classify information technology within the financial services industry. The group was made up of senior information technology managers from 11 organizations. Round one had 25 participants, round two had 24, and round

three had 23 participants. A positive point in the author's methodology was that while participation decreased, each remaining participant did participate in the previous round. Since each round builds on the previous, it is much better to lose participants than it is to add new ones in later rounds. The results of the Delphi portion of this research produced the initial specification of a capability-based typology for information technology. The authors used this specification for a follow-up case study.

In the last study reviewed that did not use Schmidt's Delphi techniques, Nakatsu and Iacovau (2009) used a Delphi study to identify risk factors for domestic and offshore outsourced projects. Two Delphi panels were assembled, one for domestic risk factors and one for offshore risk factors. The domestic panel started with 17 participants and the offshore panel started with 15 participants. The participants consisted of experienced information technology managers that engage in outsourcing. In round one of the Delphi study, 15 domestic panelists and 14 offshore panelists participated. In round two, the same 15 domestic panelists participated, but only 11 offshore panelists participated. In round three, the domestic panel again had 15 participants, and the offshore panel increased to 12, meaning the additional panelist did not participate in the previous round. While the authors did calculate a Kendall's coefficient of concordance (W), they chose to quit the iterations because of their panelist's busy schedules and not according to a consensus of the panelists, which is described in Schmidt's techniques. Neither panel reported strong consensus, as Kendall's W was .51 for the domestic group and .53 for the offshore group after round 3. Both are moderate consensus indicators. In the final results, the authors reported 20 domestic risk factors and 25 offshore risk factors.

All of the studies just discussed used the Delphi method in information systems research. However, there was no consistency in the methodology, particularly on when the study should end. They all went for several rounds, whether it was necessary or not. Only one reported a Kendall's coefficient of concordance (W) for measuring consensus, but did not use the measurement to determine if further iterations should be conducted. The primary reason Schmidt's Delphi techniques were chosen for this dissertation is because of the well defined methodology, versus the inconsistent methodologies just reviewed.

Table 3.3 describes five studies that used Schmidt's ranking techniques and reported the relevant information. The Schmidt ranking Delphi method is what is used in this dissertation. The studies will now be described in more detail.

Table 3.3: Ranking Delphi Method in IS Research (Schmidt, 1997)

Author	Purpose	Group Size	Kendall's W
Schmidt et al. (2001)	Develops a list of common risk factors of information technology project failure.	Group 1: 9 Group 2: 13 Group 3: 19	.19, .53, .51 .17, .39, .46, .50 .35, .60, .73
Keil, et al. (2002)	Compares the perceptions of information technology project risk factors between users and project managers.	15, 10	.5, .24
Mursu et al. (2003)	Identify key software project risks in Nigeria.	11, 5	.142, .256
Lee & Anderson (2006)	Identify factors impacting the information technology project management capability.	33, 33, 32	.28
Kasi, et al. (2008)	Identify the most important barriers to conducting post mortem evaluations on failed information technology projects.	23, 23, 23	.26, .33, .52

Schmidt et al. (2001) used his own methodology to develop a list of common risk factors of information technology project failure. The authors ran three separate ranking Delphi panels at the same time, one from the United States (19 panelists), one from Hong Kong (9 panelists), and

one from Finland (13 panelists). This was done to include cultural differences and to compare the group's results. Participants were experienced project managers from each culture. The initial list of 53 risk factors was created in combination with all 3 groups. The master list was sent to all three groups to be reduced in size. The United States group reduced the list to 17 items, Hong Kong reduced their list to 15 items, and the Finnish group reduced their list to 23 items. Kendall's W for the United States group for 3 rounds of ranking was .35, .60, and .73, ending with strong consensus. Kendall's W for the Hong Kong group through three rounds of ranking was .19, .53, and .51. Ranking ended with moderate consensus because round three failed to significantly increase Kendall's W, but instead decreased it. The Finnish group needed four iterations to reach consensus. Kendall's W for the Finnish group's four rounds was .17, .39, .46, and .50, ending with moderate consensus. The iterations were stopped because the fourth iteration failed to significantly increase Kendall's W. The authors reported results of the final rankings from the three groups and compared the group's rankings to one another. They also compared rankings to other Delphi studies. This study from Schmidt et al. (2001) is the closest study in relation to this dissertation. This dissertation also has multiple groups requiring varying number of iterations to reach consensus.

In research that compares the perceptions of information technology project risk factors between users and project managers, Keil, et al. (2002) used Schmidt's Delphi techniques. Fifteen participants started with an initial list of 53 project risk factors and the list was narrowed to 13 by majority. The initial list was provided to the participants and they were asked to shorten it starting with phase two of Schmidt's technique. This dissertation also starts with Schmidt's phase two, as phase one was accomplished by value-focused thinking. The participants first round of ranking yielded a Kendall's W of .5. The second round of ranking lost 5 participants

and Kendall's W dropped to .24. After contacting participants, the authors concluded that participants no longer believed a better consensus could be achieved beyond the initial .5, which indicates moderate agreement. The study was stopped and consensus results were reported at .5, after the first iteration.

In another study about project risks, Mursu et al. (2003) identified key software project risks in Nigeria. The 11 participants were project managers representing 11 different companies. The panel initially created a list of 72 key software lists. That list was then narrowed to 19 risk factors. The first round of ranking yielded a Kendall's W of .142, which is not unusual for the first round. Like the Keil, et al. (2002) study, the second round dropped several participants, leaving only 5. Kendall's W increased to .256, which still indicates weak agreement. Because there was little movement in Kendall's W and both rounds resulted in weak agreement, the authors decided to stop the study with questionable results.

Changing research topics to project management capabilities, Lee and Anderson (2006) used a Delphi method to identify factors that impact capability. The participants consisted of 33 information technology project managers. The authors started with a predetermined list of 35 factors that influence project effectiveness and the group narrowed the list to 13. There were three iterations of ranking with a final Kendall's W of .28. This can be considered weak agreement, but smaller values of Kendall's W can be considered significant for larger group sizes. The values of Kendall's W were not reported after the first two rounds. The authors reported results as the final list of 13 factors impacting project management capabilities.

The last Delphi study to be reviewed is research from Kasi et al. (2008), where the authors identify the most important barriers to conducting post mortem evaluations on failed information

technology projects. The panelists consisted of 23 experienced practitioners. Like the Keil et al. (2002) research, the authors started with a predetermined list of 31 barriers. The group was asked to use that list to brainstorm additional barriers, from which they generated 7 more, forming a total of 38. The panelists then reduced the list from 38 to 19. There were then three rounds of ranking with Kendall's W improving from .26 to .33 in the second iteration, and then to .52 in the third iteration. The authors stated that they believed an additional round would not produce better results and that they were satisfied with .52, which indicates moderate consensus. This decision to stop should be a consensus of the group according to Schmidt, but the authors did not report if the group was consulted in the decision. The authors also did not report if the number of participants changed in iterations two and three, and the assumption is that they did not. The final results of 19 ranked barriers to conducting post mortem evaluations of failed information technology projects was reported.

All of these Delphi studies followed Schmidt's techniques and reported the step by step process, making the results easy to comprehend. The studies also reported the relevant information, such as the size of the initial list, the size of the shortened list and Kendall's W of the final ranking. There were other studies that stated they followed Schmidt's techniques, but failed to report important data, such as Kendall's W (Addison, 2003; Okoli & Pawlowski, 2004; Weimer & Seuring, 2008).

3.4 Research Design:

Value-focused thinking and Delphi studies can consist of any number of groups, with each group coming to its own conclusion about a topic of interest. Typically, only one group is used to create objectives or make a decision about a particular topic and that group is usually a group of

experts, as evident in most studies in the review of research. This dissertation instead assembled four groups of panelists, each of which developed their own list of security objectives using the value-focused thinking approach. Each group then ranked those security objectives using Schmidt's ranking Delphi method.

The four groups were assembled and asked to watch a 35 minute video, followed by a value-focused thinking exercise to ascertain the participant's values about the topic of information security. There was a socio-technical group, social group, technical group, and control group. The socio-technical group watched a video describing social and technical aspects of information security (see table 3.4). The social group's video covered only the social aspects of information security for half of the video and the second half was padded with sexual harassment training. The technical group's video covered only technical aspects of information security for the first half of the video and the second half was padded with sexual harassment training. The sexual harassment part of the videos was added to lengthen the video to 35 minutes to make all groups equal in video length. Group four was the control group that watched a video about anger management and sexual harassment, which are topics believed to be unrelated to information security and would not affect the results. More specific content for each video is discussed in chapter four.

After watching the video, the participants were asked to write down what they valued as the most important topics to corporate information security and information security training. Participants were told to act as if they were managers in charge of maximizing information security and the effectiveness of information security training program (see appendix A for a full description of the survey instrument).

Table 3.4: Experimental Design

	Gets Technical Training	No Technical Training
Gets Social Training	Group #1 (Socio-Technical)	Group #2 (Social)
No Social Training	Group #3 (Technical)	Group #4 (Control)

Following Keeney's (1992) value-focused thinking methodology, the participant's values were ascertained and converted to security objectives. The objectives for each individual participant were then combined into a group master list to be ranked by the participant's working as a group. Similar objectives listed by different names were clustered into common form for the master list. Participants were given an opportunity to review the master list to verify their original values were converted to objectives properly and described in the master list accordingly. This process is explained in much more detail in the next chapter.

Ranking the objectives was performed using Schmidt's (1997) ranking-type Delphi methodology. Several rounds of anonymous ranking were conducted with each group. Analysis of the group consensus was measured with Kendall's W, as determined by using PASW statistical software (formally SPSS). The outcome of each group was a list of ranked objectives identifying what the group determined as the most important security objectives in creating an effective information security awareness program and maximizing overall information security. This process is explained in detail in chapter five.

3.5 Conclusion:

Four groups of managers were used to determine the influence of training on security objectives and the ranking of those objectives. To help panelists think about social and technical aspects of security before writing down their values about information security, a series of videos were produced. One group watched a video explaining the importance of both social and technical aspects of information security. Another group watched a video explaining the importance of only the social aspects of information security. A third group watched a video of only the importance of the technical aspects of information security. The fourth group was a control group to see how managers would perform with no education imparted from a training video.

Keeney's (1992) value-focused thinking methodology was used to determine the manager's values about information security and to create security objectives. Schmidt's (1997) ranking-type Delphi methodology was used to rank the security objectives to determine their importance. Both methodologies have a proven research record. The procedure and analysis of these methodologies and the discussion of the results are in the next chapters. Chapter four discusses the value-focused thinking analysis and chapter five discusses the ranking-type Delphi analysis. Chapter six discusses the results and overall implications to information systems research.

4. Defining Objectives That Inform Security Policy

The objective of this chapter is to illustrate the impact of different kinds of information security training on information security policy formulation. This was a long process that involved creating four training videos, collecting data, and following Keeney's method of converting values to objectives. Each of these areas will be discussed in detail below.

4.1 Training Video Creation:

Four different training videos were produced that lasted a total of 35 minutes each. One video covered social and technical topics, another covered only social topics, a third covered only technical topics and the fourth video was used as a control video and covered none of those topics. More specific content of each video will be discussed in the following sections and a more detailed outline of each video can be found in appendix B. The format of the videos involved a combination of a series of one-on-one interviews with an expert in social and technical aspects of information security and how-to video lectures. In the expert interviews, the interviewer asked questions pertaining to socio-technical topics and the expert responded in a way that explained the topic, thus creating a learning environment for the viewer. The how-to videos were an assortment of educational lectures on particular topics, such as how to backup computer data or how to create a secure password. All of the how-to videos are free public interest videos available to anyone from companies such as Microsoft and Cisco. A more detailed look at the content of each video is given next.

4.1.1 Socio-Technical Group Training Video:

The socio-technical training video covered social and technical aspects of information security, as discussed in the literature review. The overall theme of the video covered Dhillon and Backhouse's (2000) confidentiality, integrity and availability (CIA) of data as the starting point for the technical discussion and the responsibility, integrity, trust, and ethicality (RITE) of people as the starting point of the social discussion. One question asked by the interviewer that opened the dialog with the subject matter expert was how to manage the insider threat. The expert responded by discussing Dhillon's (2007) formal, informal, and technical systems of information security, as well as policies, procedures, processes, guiding principles, security culture, legal systems and standards. Further questioning led to examples of the formal, informal, and technical systems. Norms and culture were discussed in detail as examples of the informal system. Rules, regulations and processes were discussed as examples of the formal system. Access rights, encryption, and passwords were used as examples of the technical system, as mentioned by Dhillon and Backhouse (2000) and Rotvold (2008). More examples of topics discussed in this video include responsibility and authority structures, leadership styles, management commitment, deterrents, resource allocation, user involvement and regulations.

4.1.2 Social Group Training Video:

The social group training video contains the social elements of information security and not the technical elements. Therefore, to have the video last for 35 minutes to be equal to the length of the other videos, part of the social video contained filler. This filler video was in the form of training on sexual harassment and was chosen because the topic is unrelated to securing information resources and poses the minimum risk of affecting the values of the participants.

Adding this filler was necessary to make up the time of the missing technical aspects of information security.

The social aspects of security in this video primarily focused on the responsibility, integrity, trust and ethicality (RITE) of people from Dhillon and Backhouse (2000). One question asked by the interviewer was how to manage people and culture. The expert responded by explaining motivation through good leadership, power of groups, people relationships and positive and negative intentions. Another interview question asked about tools or techniques that could be used to teach proper social systems. The expert then explained how to understand silent messages from groups or organizations, group associations and interactions with others. Other topics covered in this video include motivating and influencing people through leadership, power relationships, belief systems influencing attitudes, work situations, personal factors, opportunities for crime, privacy, social and emotional intelligence and empathy.

4.1.3 Technical Group Training Video:

The technical group training video contained technical aspects of information security and not the social aspects. Like the social video, filler was needed to make up for the missing content so that the total video length would be 35 minutes. Sexual harassment was the topic chosen for the filler video because it is a topic believed to have a minimal influence on the values of the participants.

The technical part of this video consisted of a series of presentations on multiple technical security topics. The primary topics covered are those reported by Rotvold (2007) as those organizations currently include in security awareness training and what Fulford & Doherty

(2003) reported as those which organizations currently include in their information security policy. A sample of topics include computer updates, viruses, malware, secure e-mail, data backup, physical security, encryption, passwords, firewalls and phishing. This video represents what research suggests is the typical security awareness training video given by most corporations today.

4.1.4 Control Group Training Video:

The control group video was intended to last 35 minutes like the other videos, but with material that was believed to have a minimal affect on the participant's values. Since this video does not contain any social or technical aspects of security, it had to be filled with unrelated information. Like the filler used in the social and technical videos, sexual harassment was used as part of the filler. However, more filler was needed to meet the time requirements. Therefore, a video segment on anger management was added to extend the total time to 35 minutes. Both topics are unrelated to social and technical aspects of information security.

4.2 Data Collection:

The four groups in this research were made up of current and future business managers that were enrolled in a Master's of Business Administration degree program. Forty-one participants were randomly assigned to one of the four groups, resulting in three groups of ten and one group of eleven (see table 4.1 for group dynamics). The forty-one participants represented 31 different corporations.

Table 4.1: Group Dynamics

Group	Group Size	Male	Female	Average Age	Average Management Experience (years)	Companies Represented
Socio-Technical	10	7	3	32	1.7	7
Social	10	8	2	27	1.3	8
Technical	10	8	2	28	.8	9
Control	11	9	2	30	1.2	7

Before watching the training video, each group was told that their input was to help maximize information security and information security training and that they would get to help in choosing what security topics to include. They were told that information security training is the method of educating all employees on how best to protect an organization's information systems. Each group was presented with one of the four training videos and participants were allowed to take notes if needed. At the conclusion of the video, participants were asked to write down and briefly describe what topics they believed are most important if they were a manager in charge of maximizing information security and the effectiveness of the information security training program. They were asked to format their answers as if they were creating a wish list with no constraints.

4.3 Values to Objectives:

According to Keeney (1994), the best way to learn someone's values about a particular subject is to ask them to tell you in the form of a wish list. Participants listed what they wished to be included in an information security program that maximized information security. These wishes are the participant's values toward information security. However, the raw data from the

participants came in many forms. Many included one value in a statement, such as "I think training should include password use," but some included several values per statement, such as "I think training should include password use and virus protection." Others wrote in paragraph form that contained even more values. This raw data had to be converted to a common form that represented single values, which is described in section 4.3.1. An example of a value would be "I wish training included a topic on passwords." The values then needed to be converted to objectives and clustered. An example of an objective could be converting the previous value to the objective "ensure password protection is fully utilized." Clustering refers to grouping similar objectives into a single objective. Many objectives may end up referring to utilizing password protection, but were stated using different words. In this case, they can be clustered into a single objective. This involved converting the values into objective statements and clustering similar objectives. This process is described in section 4.3.2 and results in a final list of security objectives representative of each group of participants. The socio-technical group was chosen to demonstrate this process. The next few sections follow the process through to the completion of five objectives, out of the 72 the group finished with. For a complete conversion process, see appendices D and E.

4.3.1 Raw Data to Common Form

Participant's raw data input had to be broken down into a single common form, where only one value was represented at a time. To simply the statements in the process of converting the raw data, participant statements were reworded and expressed as wishes. Raw data that contained multiple wishes were broken down into individual statements. For example, in table 4.2, ST1's raw data stated "all computers must be password protected, something as easy as screen saver

passwords might deter an intruder." The common form of this statement yields two wishes, "I wish computers were password protected," and "I wish screen saver passwords were utilized." If there was any confusion, any additional descriptions or elaboration given by the participants was used to better understand the participant's intended value. The letters ST is a code that represents the socio-technical group. The codes S, T, and C were used to represent the social group, technical group, and control group respectively. The number following the code represents the number assigned to each participant, 1-10 or 1-11 for the control group. Adding codes to the original input for each participant makes it easier to trace the final objectives back to the participant or participants from which they originated. See appendix D for the complete conversion of all raw data to common form.

Table 4.2: Socio-technical Group Raw Data Conversion to Common Form Sample

Raw data from participant	Formatted in common form as wishes
Issue passwords to all employees.	ST1: I wish all employees were issued passwords
In order to get access, an employee must enter his or her password.	ST1: I wish passwords were required for access
All computers must be password protected, something as easy as screen saver passwords might deter an intruder.	ST1: I wish all computers were password protected
	ST1: I wish screen saver passwords were utilized
Integrity of the people in the organization, trust between the organization and the employees are more important than everything.	ST2: I wish employees had integrity
	ST2: I wish for trust between the organization and employees
Emphasize individual integrity in the video as much as possible.	ST8: I wish employees were taught about individual integrity
Make sure people are familiar with the basic procedures, passwords, logging in, logging off, not sharing confidential data, and so forth.	ST3: I wish employees were familiar with basic procedures
	ST3: I wish employees were familiar with password policy
	ST3: I wish employees were familiar with procedures of logging in and logging off
	ST3: I wish employees were familiar with the policy of not sharing confidential data
Can you share information, for example, in many companies in "development and research department for new products?" Are they allowed to email or share facts?	ST7: I wish there were confidentiality policies
Ethics – people need to be ethical and trusting.	ST5: I wish employees were ethical
	ST5: I wish employees were trustworthy
The training that would be given to the employee should involve mutual trust.	ST2: I wish employees received training in mutual trust

Because success is going to come with employees. Employees need to trust the company.	ST2: I wish employees knew that trusting the company leads to success
Reinforce ethics. There is no need for any of this if people are not compelled to do unethical things.	ST6: I wish ethics were stressed

4.3.2 Clustering and Converting Values to Objectives

The output of the previous section of converting the raw data to values is a list of single values expressed as wishes from each of the participants for each group. However, many of these values expressed as wishes are similar to one another. For example, two values from two different participants in the control group stated "I wish training included an Internet policy" and "I wish training included acceptable Internet usage." These values are both about establishing rules that govern the use of the Internet. Clustering them together and converting them into an actionable objective can be done in the same step. Converting a value in the form of a wish to an objective that is actionable is a fairly straightforward process. Just add a verb to the value and restate it as an objective. In our example, the two Internet usage related values can be clustered and converted into the objective "ensure training includes an Internet usage policy." This converts two values into one actionable objective. Table 4.3 follows the values from the previous table for the socio-technical group through the clustering and conversion process into final objectives. Again, for a complete list of this conversion process, see appendix E.

Table 4.3: Socio-technical Group Objective conversion and Cluster Sample

Values	Objectives
ST1: I wish all employees were issued passwords	Ensure password protection is fully utilized
ST1: I wish passwords were required for access	
ST1: I wish all computers were password protected	
ST1: I wish screen saver passwords were utilized	
ST2: I wish employees had integrity	Ensure training covers employee integrity
ST8: I wish employees were taught about individual integrity	
ST3: I wish employees were familiar with the policy of not sharing confidential data	Ensure data confidentiality policies are in place

ST7: I wish there were confidentiality policies	
ST5: I wish employees were trustworthy	Ensure a trust relationship between employees and the company
ST2: I wish for trust between the organization and employees	
ST2: I wish employees received training in mutual trust	
ST2: I wish employees knew that trusting the company leads to success	
ST5: I wish employees were ethical	Ensure appropriate ethics training
ST6: I wish ethics were stressed	

4.3.3 Final Group Objectives

The previous section clustered and converted values to objectives, yielding a final list of group objectives (see appendix F). The socio-technical group finished with the most objectives at 72. The social group finished with 37, the technical group finished with 43, and the control group finished with 49 security objectives. These lists of security objectives do not represent a ranked order, but instead are represented randomly. In chapter five, the ranking Delphi method is used to shorten and rank the security objectives of each group.

The significance of the final list of objectives is that it represents the security objectives that the group members feel are important for maximizing the effectiveness of information security and information security training. Each objective was analyzed and placed into one of three categories for group analysis. The technical category (T) represents all objectives there were technical in nature and require a technical implementation in order to satisfy the objective, such as "ensuring password protection is fully utilized." The social category (S) represents all objectives that are social in nature, such as "ensuring appropriate ethics training." The general category (G) represents objectives that are neither technical nor social. General objectives are often related to how security training should be presented, such as "ensure examples are fully utilized in security training," and "ensure training is simple and short." The pie charts in

appendix E represent the technical, social, or general orientation of each group's objectives as percentages. The next section discusses the group's final objectives in much more detail and the significance of their relation to information security policy.

4.4 Discussion:

Taking a closer look at the final security objectives of the four groups, the first result that emerges is that the socio-technical group created a lot more objectives than did the other groups, almost 60% more than the average of the other groups. More important than the total number of objectives created by each group, is the quality of those objectives and the mix of social, technical and general objectives. Too few social objectives and many technical objectives mean that security policy will lack adequate social aspects and be technically dominant. Too many general objectives means the participants were focused too much on aesthetics, such as having hands-on training and colorful presentations, and not focused enough on social and technical aspects of security.

The socio-technical group not only had more objectives, but had an adequate representation of social and technical objectives. Of the 72 total security objectives, 25% were social, 34.72% were technical, and 40.28% were general objectives. This is a good percentage of social and technical objectives. It is to be expected that there will be a higher percentage of technical objectives than social objectives, mainly because there are more technical solutions to information security than there are social solutions. While there were too many general objectives from all groups, the socio-technical group was among the best at minimizing them. Most of the general objectives were appropriate for conducting awareness training, such as using examples in training, using stimulating videos and involving management in training.

The socio-technical group's final list of social security objectives included many objectives that the literature review stated were most important. In representing the responsibility, integrity, trust and ethicality of employees (RITE), the group listed multiple objectives. For instance, they had a security objective to create an ethics training program. Ethical aspects of security are just as important as technical aspects and companies with ethics programs suffer less economic crime (Trompeter & Eloff, 2001, ECS, 2007). The group also had security objectives to ensure a trusting relationship between the employee and the employer and to clearly define the employee's roles and responsibilities. In current organizations where employees are empowered with more responsibility, building a trusting relationship between the employee and the employer is more important than ever (Dhillon, 2007). In addition, employees need to understand their roles within the organization, which also includes individual accountability (Dhillon & Backhouse, 2000). The group also had security objectives relating to the screening of employees, hiring responsible employees, and promoting the integrity of the individual. Dhillon and Backhouse (2000) warn about ensuring the integrity of the individual before giving them access to sensitive resources, so these objectives are also very important.

The socio-technical group was the only group to completely represent all aspects of RITE. Other important social objectives created by this group include the creation of a mix of formal, informal, and technical control systems, creating reward systems, acknowledging employee commitment and employee motivation. The only important social aspect that this group omitted was creating a security culture, which is a major oversight. A strong security culture is very important for information security and has been linked to such things as compliant user behavior and employees engaging in security measures beyond their mandatory job descriptions (Ruighaver et al., 2007; Dhillon, 2007; Karyda, et al., 2005; von Solms & von Solms, 2004;

Leech, 2003; Vroom and von Solms, 2004; D'Arcy & Greene, 2009). While creating a security culture is very important and not creating a security objective to do so is a significant omission, the socio-technical group otherwise created a robust list of social security objectives.

On the technical side, the socio-technical group created an adequate list of technical objectives and represented the confidentiality, integrity, and availability (CIA) of information. For instance they included technical objectives to ensure data confidentiality, appropriate access, intrusion detection, password management, biometric authentication, data monitoring, firewalls, proper infrastructure planning, and system reliability. Restricting data access to those that are authorized is crucial to protecting the confidentiality of data (Dhillon, 2007). This group's objective for ensuring data confidentiality specifically addresses this task. The integrity of data is important because it is concerned with the trustworthiness and correctness of the data (Dhillon, 2007). Data that cannot be trusted as correct is worthless data. The socio-technical group's objectives for intrusion detection and data monitoring help protect the integrity of data. Beyond the confidentiality and integrity of data, making it available to those in need is equally important. This can mean contingency planning, disaster recovery planning, or ensuring the reliability of data access (Dhillon, 2007). The socio-technical group's objectives for the use of firewalls, ensuring system reliability, and proper infrastructure planning relate to ensuring the reliability of data access. The socio-technical group also listed technical objectives for protection from portable devices, physical access to systems, and securing Web servers. Overall, the socio-technical group created a robust list of social and technical security objectives. These socio-technical security objectives implemented as the organization's information security policies and distributed through the information security training program would come close to

maximizing overall information security. The only exception would be the lack of a security culture.

The social group's final list of security objectives consisted of 27.03% social, 24.32% technical, and 48.65% general objectives. This is a large percentage of general objectives. The true test is to evaluate the quality of social and technical objectives against RITE, CIA, and other important social and technical aspects. It is good to recall here that the social group only received social training, so any technical security objectives listed were not influenced by the training. Therefore, it was anticipated that this group would have a robust list of social objectives and a moderate list of technical objectives. However, the social security objectives listed by this group in regard to RITE were not as comprehensive as anticipated. They listed objectives for considering employee integrity and employee ethics, but failed to create security objectives for defining roles and responsibilities and creating trusting relationships. They also failed to list the creation of a positive security culture, as did the socio-technical group. The above mentioned are three important social security objectives omitted by this group and all three were covered in their training video. It is unclear why the group failed to list these objectives and is perhaps a topic to be addressed in future research. The group did list other important social objectives, such as recognizing employee cultural differences, manager emotional intelligence, employee decision making, corporate values, morale, employee gender differences and the effects of employee dissatisfaction.

On the technical side of security, the social group also left a few security holes. In support of CIA, the social group created security objectives for confidentiality and integrity of information, but failed to create objectives to preserve the availability of data. However, they did list other

important technical objectives, such as password protection, physical security, personal data protection, and identity theft.

Overall, the social group's list of social objectives was incomplete, which is a surprise considering they received social training. They also created an incomplete list of technical security objectives, which is understandable considering they did not receive technical training. There was an overabundance of general objectives, with many relating to conducting awareness training and some completely unrelated. For instance, how to handle the media is unrelated to information security and security awareness training, while hands-on training is relevant to conducting information security training. These socio-technical security objectives when implemented as the organization's information security policies and distributed through the information security training program would not maximize overall information security and would leave some security holes in both the social and technical areas.

The technical group received technical training and no social training. Therefore, they were expected to be strong in technical aspects of security, but relatively weak in social aspects. This group listed 11.63% social objectives, 48.84% technical objectives, and 39.53% general objectives. This is the largest percentage of technical objectives from all the groups. In representing RITE, they created a security objective to address employee roles and responsibilities, but failed to list objectives in regard to employee integrity, trust, and ethicality. This was no surprise, but what was a surprise was that the technical group listed security culture, employee culture and corporate values. This is the only group to create an objective for security culture and they did not receive training on the topic. This shows that without social training, the

group still came up with several important social objectives. However, the overall list of social objectives is poor and not nearly as comprehensive as the social or socio-technical group.

Technical objectives were very strong for the technical group, as they had an abundance of objectives related to CIA. For instance, they listed data protection, data recovery, data backups and data confidentiality as security objectives. They also listed many other technical aspects of information security, such as password protection, physical security, the use of encryption, auditing, SPAM filtering, phishing, virus detection, worm detection, spyware detection and the use of virtual private networks.

Overall, the technical group created an incomplete list of social objectives and a robust list of technical objectives. They also had less general objectives than the other three groups, at 34.9%. Many of those objectives were about the aesthetics of training, such as using bright imagery, interactive training, hands-on exercises, and using humor in training. These socio-technical security objectives when implemented as the organization's information security policies and distributed through the information security training program would not maximize overall information security and would leave many security holes in the social side of security. This type of security depicts the scenario in today's organizations, as we learned from the literature review; organizations today have technically oriented information security policy and training (Rotvold, 2008; CWS, 2010; Fulford & Doherty, 2003).

The control group represents managers that get no formal training on how to maximize information security, which is the status quo for most organizations (Hone & Eloff, 2002). The training this group received had nothing to do with information security, so it is expected that the group will produce a weak list of social objectives and a moderate list of technical objectives. In

regard to percentages, the control group's final list of security objectives included only 6.12% social objectives, but had 44.9% technical and 48.98% general objectives. This is a very low percentage of social objectives and large percentage of general objectives. Out of 49 total objectives, only 3 were socially related. Two of those social objectives related to RITE's trust and ethics components and the third related to social engineering. Only the control group included social engineering as a security objective, which was somewhat of a surprise. Beyond those three objectives, which were very good, the control group was missing many other social aspects of information security and was by far the worst representation of social objectives of all the groups.

The control group's list of technical objectives was much more comprehensive. All aspects of CIA were represented. For instance, the group listed data confidentiality, data backup, and encryption as technical security objectives. They also included physical security, wireless networking, intrusion detection, firewall configuration, virus detection, SPAM detection and domain naming service security.

Overall, the control group had an incomplete representation of social objectives and a nice representation of technical objectives. It was a surprise that their technical security objectives were well represented. The social group also did not receive technical training, but was only able to produce a moderate list of technical objectives. The control group listed far too many general objectives and had the largest percentage out of all the groups at 48.98%. Like the other groups, many were related to information security training, like having interactive training, using examples and using qualified trainers. These socio-technical security objectives when implemented as the organization's information security policies and distributed through the

information security training program would not maximize overall information security and would leave many security holes in the social area of security.

In regard to social objectives, the socio-technical group created 20 total social objectives, compared to 10 for the social group, 5 for the technical group, and 3 for the control group. The socio-technical group was the only group to create a robust list of social objectives and to list satisfactory objectives for RITE, which is somewhat of a surprise that they were the only group to do it. The social group received the same training on RITE as the socio-technical group, but failed to enlist trust, and roles and responsibilities. However, the social group did have a moderate list of social objectives and performed better than the technical and control groups. Both the technical and control groups had insufficient lists of social security objectives.

For the technical objectives, the socio-technical group created 25 total technical objectives, compared to 9 for the social group, 21 for the technical group, and 22 for the control group. Only the social group failed to have a comprehensive list of technical objectives, failing to satisfy the availability of data part of CIA. All other groups satisfied CIA and listed plenty of additional technical objectives.

The lists of security objectives from all four groups produced a few other interesting results. For instance, the results of the control group are similar to the technical group, in that the social aspects of information security policy and training would be poor and the technical aspects of information security policy and training would be excellent. It was not expected that the control group would have excellent technical representation. This implies that training managers on the technical aspects of security only is no better than not training them at all. With no training, managers are still aware of the technical aspects of security. However, the results are mixed in

that the social group did not receive technical training either and produced only a moderate list of technical objectives. The social group's second surprise was that they only produced a moderate list of social objectives as well. Since they received in depth social training, it was expected their social list of security objectives would be excellent. Another unexpected result was that the technical group was the only group to list the creation of a security culture as a security objective. They did not receive social training and the social and socio-technical groups did, but neither of the latter groups listed that objective. That was the only surprise for the socio-technical group. They otherwise produced an excellent list of social and technical security objectives.

4.5 Conclusion:

The objective of this chapter was to demonstrate the impact of different kinds of information security training on information security policy formulation. The chapter started with the creation of four training videos, including a socio-technical video, a social only video, a technical only video, and a control video. Groups of managers were formed and each group watched one of the videos. Following the video, each group participant wrote down their values for maximizing the effectiveness of information security and information security training. Following Keeney's value-focused thinking methodology, the values were converted and clustered into lists of value-based security objectives. Each group's security objectives were analyzed in regard to the nature and scope of the information security policy they would inform.

Overall, the socio-technical group had the most comprehensive list of security objectives, satisfying both RITE and CIA. They were the only group to have satisfied both and have many

other important social and technical objectives. The social group failed to completely satisfy both RITE and CIA, but had moderate lists of social and technical objectives. The technical and control groups both had excellent lists of technical security objectives, but weak lists of social security objectives. The output of this chapter is an unranked list of security objectives representative of each group's values. Chapter five uses the ranking Delphi method to narrow and rank the lists of security objectives to discover which objectives the groups feel are most and least important.

5. Ranking Delphi Analysis

5.1 Background:

The last chapter used Keeney's value-focused thinking methodology to create lists of value-based security objectives from four groups of panelists. The nature and scope of each list of security objectives was analyzed for their social and technical aspects as deemed important from the literature review. For instance, the lists were analyzed for representation of the responsibility, integrity, trust and ethicality of individuals (RITE) and the confidentiality, integrity and availability of information (CIA) in addition to other important social and technical security objectives. Also discussed in chapter four was the nature and scope of the information security policy informed by each list of security objectives. What we do not know from chapter four is the degree of importance attached to each security objective. Which security objectives would get eliminated if the security budget was reduced? Recall that the lists of value-based objectives are wish lists developed by the participants without other constraints such as budgets. In the real world, there may be money to do some things and not others. The purpose of chapter five is to use a ranking Delphi method to shorten the lists and rank the remaining security objectives. The shortened ranked lists will tell us which security objectives the participants feel are most and least important.

According to Schmidt's (1997) guidelines for conducting ranking-type Delphi research, three phases must be conducted. The first phase involves discovering the issues pertaining to a particular topic. This was accomplished with the value-focused method discussed in chapter

four, where each group produced an unranked list of objectives they thought were important for maximizing the effectiveness of information security and training. The socio-technical group listed 72 objectives, the social group had 37 objectives, the technical group had 43 objectives, and the control group had 49 objectives. This chapter starts with Schmidt's phase two, which was to shorten the lists before they could be arranged in a ranked order.

Phase two of Schmidt's guidelines states that the panelists are to be asked to shorten the list to no less than 10% of the original number of objectives and no more than 100 objectives. An ideal list would be somewhere around 20 objectives, according to Schmidt, but could certainly be more or less depending on the topic. Since none of the groups had more than 100 objectives to begin with, the upper limit was not a constraint. According to Schmidt's guidelines, participants were told there was no correct number of final objectives, but to include what they believed were the most important objectives from the list. Once each group member submitted a shortened list of what they believed were the most important objectives from the original list, a final list was created. This was accomplished by retaining objectives that appeared on a majority of the participant's shortened lists. For example, if 60% of the participants thought a particular objective was important and they included that objective on their shortened list, then that objective would be included in the final list. If a particular objective was only represented by 40% of the participant's shortened lists, then it did not get included in the final list. Phase two could be repeated if necessary to shorten the list further.

Phase three of Schmidt's guidelines created a group ranking of the final list of objectives from most important to least important. This phase involved asking the group members to rank the final list of objectives from what they believed were the most important objectives to the least

important objectives and each participant was given a randomly ordered list of objectives to start. Kendall's coefficient of concordance (Kendall's W) was then determined by analyzing the ranked lists from the group members, which was used to determine group consensus. The higher the coefficient, the better group consensus was. There were multiple iterations of this process, with each iteration producing a newly ranked list of objectives based on the group mean rank of each objective. The new group ranking was then sent back to each group member to be ranked again. This process was repeated until one of two things happened. The first is when Kendall's coefficient of concordance is .7 or greater and the group agrees further iterations would not significantly improve consensus. A coefficient of .7 or greater indicates strong agreement on the ranked list of objectives. The second stopping point could be if the group's coefficient levels off at some point below .7 and does not significantly increase with further iterations. This would mean the group failed to reach strong agreement on the final ranked list of objectives and they would never be in strong agreement.

The next few sections of this chapter discuss phases two and three of Schmidt's guidelines as they pertain to this research. Section 5.2 narrows the long lists of objectives from the value-focused thinking chapter down to manageable lists of final objectives. Section 5.3 discusses the ranking process through multiple iterations and produces a final ranked list of objectives from each group. Section 5.4 discusses the ranked lists and the affect on information security policy and section 5.5 concludes the chapter.

5.2 Determining the Most Important Objectives:

Each group was given a randomly ordered list of objectives that their group produced in the value-focused thinking piece of this research. They were asked to keep the objectives they believed were most important and discard the rest. They were given no particular goal for a final number of objectives they should have. This process was accomplished via e-mail with each of the participants. Once the shortened list was received from each of the participants, a final list of objectives was produced. This was accomplished by keeping objectives that appeared on the shortened lists of the majority of group members, according to Schmidt's guidelines. Since three of the groups had ten members and one of the groups had eleven members, it was decided that an objective would be kept for the final list if it was found on six of the participants shortened lists. Six participants agreeing to the objective as important would be in the majority for all groups, whereas five would not be the majority for any of the groups. The shortened unranked lists of objectives for each group can be found in appendix G. The socio-technical group shortened their list to 12 objectives they believed were most important. The social group shortened their list to 23, the technical group to 22, and the control group to 25 objectives. The number of final objectives for each group falls within Schmidt's goal of greater than 10% of the original list and less than 100 objectives. Also included in the tables in appendix G is the percentage of participants from each group that included that objective in their shortened list. The higher that percentage, the more group members that believed the objective was important enough to include on their final list of objectives. The lists are sorted by percentage of inclusion from participants and should not to be confused with the ranking process discussed in the next section.

5.3 Ranking the Objectives:

The previous step narrowed each group's list of objectives down to what they believed were the most important objectives, which yielded a much shorter list of objectives for each group. The next step was to rank the objectives from most important to least important. A randomly ordered list was sent to each participant for ranking. The participants were told the list is randomly ordered and to not imply any ranking. PASW-17, formally known as SPSS-17, was used to perform statistical analysis on the ranked lists. In order to use PASW to determine the mean rank and group consensus, each objective was translated into an alphabetic letter. The random list of objectives that was sent to each group participant was represented in PAWS as the letters of the alphabet as seen on tables 5.1 and 5.2 for the social group. The participants only received a list of objectives without the letters, but the researcher uses the letters for the columns in PASW's data view. The social group had 23 objectives, so the columns in PASW were labeled A-W to represent the 23 objectives. The rows in PASW were numbered 1-10 to represent the 10 participants in the social group. To explain this process as efficiently as possible, the social group was chosen for this example because that group had group consensus and stopped after two iterations and the others stopped after three.

Table 5.1: Social Group Objective Conversion to Letters Iteration One

A.	Ensure hand's on training
B.	Ensure managers are involved in providing training
C.	Ensure the importance of security is addressed with all employees
D.	Ensure training addresses corporate information theft
E.	Ensure training addresses data protection
F.	Ensure training addresses employee ethics
G.	Ensure training addresses employee integrity
H.	Ensure training addresses factors affecting employee decision making
I.	Ensure training addresses how employee dissatisfaction affects security
J.	Ensure training addresses strong passwords while minimizing the need to write them down
K.	Ensure training addresses the relationship between emotional intelligence and security
L.	Ensure training addresses the social interaction between companies and individuals

M.	Ensure training considers employee cultural differences
N.	Ensure training covers legal aspects of security
O.	Ensure training covers personal data security
P.	Ensure training covers privacy rights
Q.	Ensure training covers the most common threats and how to prevent them
R.	Ensure training describes corporate values
S.	Ensure training includes confidentiality policy
T.	Ensure training includes continuing education as threats change
U.	Ensure training includes technical aspects
V.	Ensure training is up to date with current security issues
W.	Ensure training utilizes real world examples, including the corporate consequences of bad security

Table 5.2 is the data view from PASW for the social group's first iteration. The letters A-W from table 5.1 that represent the objectives are the columns in PASW. The ten participants are the rows. The data that fills the cells are the actual rankings provided by each of the participants for iteration one. For example, participant number one thought that "ensure training covers the most common threats and how to prevent them" was the most important objective. This can be seen by looking at row "Part 1" for participant one and column "Q," where that participant placed the number one. Because the number one is in that column, this means that participant listed that objective as number one in their ranking. All 23 of their rankings are listed in this manner. Recall that the participants did not receive a list with the letters, but only the objectives. This means that the researcher had to apply the letters back to each participant's ranked list based on table 5.1. Think of it as a conversion process from objectives to letters for easy entry into PASW. Once PASW gives the results, they can be easily converted from letters back to objectives. This process of using letters to represent the objectives in PASW was performed for all participants for each group and for each iteration.

Table 5.2: Social Group PASW Input for Iteration One

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**
Part. 1	6	18	7	19	8	10	9	11	22	12	21	20	23	13	5	14	1	15	16	2	4	3	17
Part. 2	22	2	3	16	7	17	18	10	21	11	9	8	23	12	5	19	4	13	20	15	6	1	14

Part. 3	9	13	3	17	14	7	20	18	21	23	12	22	5	6	16	11	1	15	19	4	10	8	2
Part. 4	23	8	2	10	11	3	4	15	16	17	18	19	21	9	12	13	6	1	14	20	22	5	7
Part. 5	1	23	5	21	22	2	3	18	4	20	9	10	11	13	14	19	8	12	16	15	17	6	7
Part. 6	19	8	17	2	6	15	7	21	9	12	3	10	11	18	1	13	4	16	14	5	23	22	20
Part. 7	1	7	2	10	3	16	17	20	21	18	22	23	19	8	4	5	11	12	13	14	15	9	6
Part. 8	8	7	6	17	18	9	5	19	2	22	3	4	20	10	16	15	11	12	21	13	23	14	1
Part. 9	19	17	18	11	10	9	12	13	8	23	5	14	15	2	3	4	20	1	16	6	22	7	21
Part. 10	22	5	10	17	4	6	11	19	21	20	18	12	7	13	1	14	15	23	8	16	3	2	9

Analysis of the participant's rankings using PASW yielded the following results for the first iteration of the social group (table 5.3). Each objective has a mean rank and standard deviation. This table is sorted by the mean and then standard deviation to break ties. The first column represents the alphabetic letter originally assigned to each objective, so it is easy to see how the original random list was moved around to form this ranked list. Objective "C" comes in first, which is "ensure the importance of security is addressed with all employees." It has the lowest mean of 7.3. Several objectives have the same mean, such as "O" and "V," which came in number 2 and 3 in the ranked list. In such cases, the objective with the lower standard deviation earns the higher ranking, according to Schmidt's guidelines. This is why objective "O" comes in second with a standard deviation of 6.111 and objective "V" comes in third with a standard deviation of 6.29.

Table 5.3: Social Group First Iteration Sorted by Mean

Letter	Mean	Std. Deviation	Objective
C	7.3	5.926	Ensure the importance of security is addressed with all employees
O	7.7	6.111	Ensure training covers personal data security
V	7.7	6.29	Ensure training is up to date with current security issues
Q	8.1	6.19	Ensure training covers the most common threats and how to prevent them
F	9.4	5.232	Ensure training addresses employee ethics
E	10.3	6.129	Ensure training addresses data protection
N	10.4	4.452	Ensure training covers legal aspects of security
W	10.4	7.183	Ensure training utilizes real world examples, including the corporate consequences of bad
G	10.6	6.096	Ensure training addresses employee integrity
B	10.8	6.663	Ensure managers are involved in providing training

T	11	6.164	Ensure training includes continuing education as threats change
R	12	6.65	Ensure training describes corporate values
K	12	7.318	Ensure training addresses the relationship between emotional intelligence and security
P	12.7	5.012	Ensure training covers privacy rights
A	13	8.894	Ensure hand's on training
D	14	5.676	Ensure training addresses corporate information theft
L	14.2	6.477	Ensure training addresses the social interaction between companies and individuals
I	14.5	7.934	Ensure training addresses how employee dissatisfaction affects security
U	14.5	8.155	Ensure training includes technical aspects
M	15.5	6.654	Ensure training considers employee cultural differences
S	15.7	3.802	Ensure training includes confidentiality policy
H	16.4	3.893	Ensure training addresses factors affecting employee decision making
J	17.8	4.662	Ensure training addresses strong passwords while minimizing the need to write them down
Kendall's W = .193			

In addition to the mean rank and standard deviation, PASW also yields Kendall's Coefficient of Concordance, also known as Kendall's W, which is reported at the bottom of the table. Kendall's Coefficient of Concordance (W) is used to calculate consensus among three or more people. Kendall's W ranges from 0-1, with zero indicating no agreement and one indicating full agreement. For the first iteration, the social group's consensus was .193, which is very weak agreement according to Schmidt's scale (see chapter 3). Another round must be done to see if the group is capable of achieving better agreement.

The second round of ranking for the social group started with each participant receiving the group ranking results from the first round. The new list was created using the mean rank from round one, as seen in table 5.4. This is the first time each participant saw the ranked objectives as a group. Again, letters are added to the ranked list for easy input into PASW, but the participants only receive the ranked objectives and not the letters. Each participant was asked to make any changes they believed were necessary, such as moving objectives up and down the list to satisfy their individual values. If they believed the list was satisfactory, they did not have to change anything. Group consensus is expected to increase at this point because individuals usually only

move the objectives they feel strongly about and leave the others alone. The more that get left alone, the greater the group consensus.

Table 5.4 represents the social group's first list of ranked objectives with letters assigned for representation in PASW. This group of assigned letters A-W is different than the original list sent to participants, as the letters now represent the first ranking and not the randomly ordered list. Just like in the first round, the researcher converts the participant's newly ranked list for round two to the letters represented in table 5.4 and enters them into PASW. The results from PASW are then converted from letters back to objectives.

Table 5.4: Social Group Objective Conversion to Letters Iteration Two

A. Ensure the importance of security is addressed with all employees
B. Ensure training covers personal data security
C. Ensure training is up to date with current security issues
D. Ensure training covers the most common threats and how to prevent them
E. Ensure training addresses employee ethics
F. Ensure training addresses data protection
G. Ensure training covers legal aspects of security
H. Ensure training utilizes real world examples, including the corporate consequences of bad
I. Ensure training addresses employee integrity
J. Ensure managers are involved in providing training
K. Ensure training includes continuing education as threats change
L. Ensure training describes corporate values
M. Ensure training addresses the relationship between emotional intelligence and security
N. Ensure training covers privacy rights
O. Ensure hand's on training
P. Ensure training addresses corporate information theft
Q. Ensure training addresses the social interaction between companies and individuals
R. Ensure training addresses how employee dissatisfaction affects security
S. Ensure training includes technical aspects
T. Ensure training considers employee cultural differences
U. Ensure training includes confidentiality policy
V. Ensure training addresses factors affecting employee decision making
W. Ensure training addresses strong passwords while minimizing the need to write them down

Table 5.5 displays the results from PASW for the group's second ranking iteration. The letters in the left column represent the previous ranking, so you can see which items moved up and down the list. As you can see, letter "A" remained in the top spot, which means the participants did not change the number one ranking for that objective. Its standard deviation is also very low, indicating strong agreement on the number one ranking. Kendall's W increased dramatically to .744, which means the group now has strong consensus. According to Schmidt, the researcher should ask the participants if they feel a third iteration will produce any better results. If a majority of the group feels that a third iteration will strengthen consensus, then a third iteration should be performed. In this case, the majority of the social group's participants responded that an additional iteration would not improve consensus, so this was the final ranking for the social group.

Table 5.5: Social Group Second Iteration (Sorted by Mean)

Letter	Mean	Std. Deviation	Objective
A	1.10	0.32	Ensure the importance of security is addressed with all employees
C	4.40	3.44	Ensure training is up to date with current security issues
E	4.90	1.52	Ensure training addresses employee ethics
D	5.10	2.23	Ensure training covers the most common threats and how to prevent them
B	7.10	6.67	Ensure training covers personal data security
H	7.50	2.84	Ensure training utilizes real world examples, including the corporate consequences of bad security
F	7.70	4.14	Ensure training addresses data protection
I	8.20	2.70	Ensure training addresses employee integrity
G	8.50	1.35	Ensure training covers legal aspects of security
J	10.00	1.89	Ensure managers are involved in providing training
K	11.30	4.03	Ensure training includes continuing education as threats change
L	11.80	4.10	Ensure training describes corporate values
M	13.10	3.54	Ensure training addresses the relationship between emotional intelligence and
O	13.50	6.13	Ensure hand's on training
P	14.20	3.65	Ensure training addresses corporate information theft
N	14.50	0.85	Ensure training covers privacy rights
R	16.20	5.05	Ensure training addresses how employee dissatisfaction affects security
Q	17.00	3.74	Ensure training addresses the social interaction between companies and

S	18.70	2.54	Ensure training includes technical aspects
T	18.90	4.20	Ensure training considers employee cultural differences
U	19.70	2.54	Ensure training includes confidentiality policy
V	20.20	3.91	Ensure training addresses factors affecting employee decision making
W	22.40	1.90	Ensure training addresses strong passwords while minimizing the need to
Kendall's W = .744			

The process described above was for the social group, but the same process was used with the socio-technical, technical, and control groups. The final ranked list of objectives for each group with Kendall's W results can be found in appendix G. The social group had consensus after the second round and so did the socio-technical group when they had a Kendall's W of .734 after the second iteration, but the socio-technical group decided to go another round and improved their consensus to .825, while the social group agreed to stop after the second round. For the socio-technical group, one hundred percent of the group felt they could do better with the additional round.

The technical group was the only group to not reach a strong consensus. A Kendall's W of .627 falls between moderate and strong agreement- according to Schmidt's guidelines, which is perfectly fine. A Kendall's W of .7 is desirable, but not mandatory. When a group appears to stall or makes little progress with successive iterations according to Kendall's W, as this group did with a score of .582 advancing to .627, the researcher may stop if the group agrees they can no longer make progress. In this case, the majority of the technical group agreed that no further progress could be made with an additional iteration. One interesting point should be made about this group. One of the ten participants believed very strongly about their rankings and those rankings were dramatically different than the rest of the group. While nine of the ten participants were coming to a consensus, this one individual was standing out in disagreement. If that one individual were excluded from the group, the group consensus would have been .890. The

difference between .890 that could have been and the .627 that the group stopped with can be explained by one individual participant who strongly disagreed with the others.

The control group finished with a very strong consensus of .992. However, it should be noted that only four of the eleven participants made any changes to the final ranking. This means they were satisfied with the results of second round. The four that did make changes only made minor changes, thus resulting in an almost perfect group consensus.

5.4 Discussion:

Chapter four concluded with a long list of security objectives for each group. The percentages of social, technical, and general objectives were noted for each group. More importantly, the objectives chosen by each group were compared against the social objectives for RITE, the technical objectives of CIA, and other important socio-technical objectives. Chapter five's goal was to have the groups rank what they thought were the most important objectives to information security. The ranking process makes the group narrow the list by eliminating some objectives and keeping others. The objectives that remain are then ranked from most important to least important. To analyze the results of the final rankings, it is important to ask some of the same questions we did with the full objective lists from chapter four. What are the social, technical, and general objective percentages from the final rankings? How do the final rankings compare to RITE, CIA, and other important socio-technical objectives? In addition, what important objectives were in the original list of objectives, but did not make it to the final rankings list? Eliminating important objectives would mean the group did not feel they were important enough to keep on the final ranked list. Another question to answer is what objectives did the groups feel were worthy of a top ten ranking? The most important question to answer is how

information security policies are affected by the now shortened list of security objectives. All of these questions will be answered for each group next.

The final percentages of social, technical, and general objectives are displayed in figure 5.1. All of the groups maintained percentages similar to what they had with the complete list in chapter four. The socio-technical and social groups both reduced the percentage of general objectives and increased technical objectives, which is a positive note. The social group also increased their percentage of social objectives. The technical group reduced their general objectives by 3%, adding that percentage to their social objectives. The control group is the only group that deteriorated by increasing the general objective percentage by 18% at the expense of lowering technical and social objective percentages.

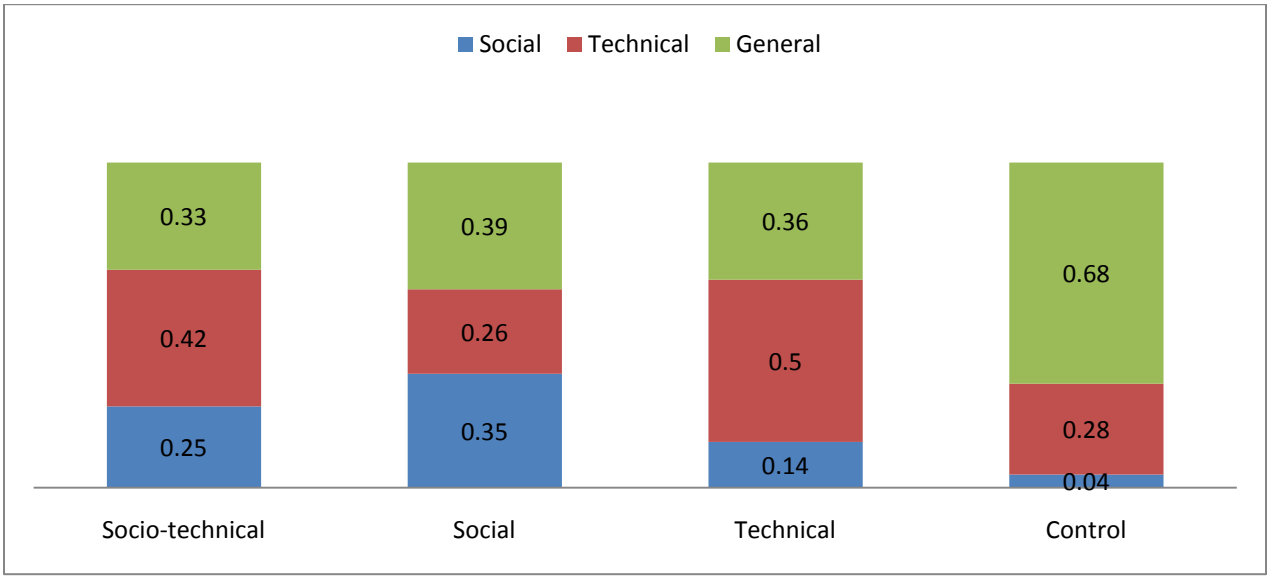

Figure 5.1: Group Percentages

As was discussed in chapter four, the percentages of social, technical, and general objectives are not as important as the quality of the chosen objectives. The socio-technical group started with the most robust list of 72 objectives and narrowed it down to 12, by far the shortest ranked list of all the groups. In doing so, the group failed to include many important objectives they had in the initial list. Significant objectives they included relating to RITE are "ensure clearly defined roles and responsibilities," and "ensure potential employees are screened before being hired," which can relate to the integrity of the employee. However, the group eliminated the two other important RITE objectives relating to trust and ethics. Other social objectives dropped by this group include the creation of a mix of formal, informal, and technical control systems, creating reward systems, acknowledging employee commitment and employee motivation.

From CIA, the group included "ensure data confidentiality policies are in place," which of course relates to the confidentiality of data. They also included "ensure computers are updated regularly," which can relate to availability of data. Maintaining computers and networks is essential for ensuring data is accessible by those that need it when they need it. However, the group eliminated their objectives relating to the integrity of data, which leaves some security holes related to CIA. The group also eliminated the technical objectives for implementing firewalls, protection from portable devices, physical access to systems and securing Web servers.

The socio-technical group eliminated many important objectives when they narrowed their 72 objectives to 12. For instance, ethics training did not make the final list because it was only chosen by 30% of the respondents for inclusion in the final list. Others that did not make the final list include employee integrity (20%), protecting databases from intrusion (30%), and

building a trust relationship between employee and employer (50%). It was a surprise that ethics, employee integrity, and building trust relationships scored so low and the first two were not even close to making the final list. Those topics were stressed as very important in the video training the group received. Overall, the socio-technical group left some holes in security by eliminating important objectives. They also included too many general objectives, though the percentage decreased when compared to the larger list. Overall, the socio-technical group ended with an incomplete list of social and technical security objectives, which is definitely a setback from the excellent socio-technical objectives they did have. These socio-technical security objectives implemented as the organization's information security policies and distributed through the information security training program would not maximize overall information security and would leave some security holes in both the social and technical areas.

The social group was able to keep most of the important objectives that they had originally listed. Though this group did not fully represent RITE and CIA to begin with, they did keep what objectives they did have relating to those concepts. They ranked employee ethics and employee integrity both in the top ten, which is great for social aspects that often get ignored. Other important social objectives that made the list relate to employees, such as understanding social interactions between individuals (employees) and their employers, factors affecting employee decision making and employee cultural differences. Social objectives that were dropped from the ranked list include employee morale, which only 30% of the participants thought was important, and employee gender (10%).

The technical objectives listed by the social group were sparse to begin with. Beyond confidentiality and data protection, their ranked list included the use of strong passwords and

personal data protection. Technical objectives dropped from the longer list related to physical security and identity theft. Also making the final list was an overabundance of general objectives. Overall, the social group kept most of the important socio-technical objectives they originally had, but they started with an incomplete list of social and technical objectives. These socio-technical security objectives when implemented as the organization's information security policies and distributed through the information security training program would not maximize overall information security and would leave some security holes in both the social and technical areas.

The technical group started with a list strong in technical objectives and weak in social objectives, but they had listed a few surprise social objectives. The good news is that almost every social objective originally listed was included on the final ranked list of objectives. They maintained their surprise social objectives relating to roles and responsibilities and developing a security culture. The only important social objective that was eliminated related to employee cultural differences. This group also did well maintaining their technical objectives in the final list. All objectives relating to CIA were maintained and the only important objective eliminated related to physical security, which only 20% of the participants thought was important. Overall, the technical group maintained the important socio-technical objectives and maintained their weak showing for social objectives and excellent showing of technical objectives. These socio-technical security objectives when implemented as the organization's information security policies and distributed through the information security training program would not maximize overall information security and would leave some security holes in the social side of information security.

The control group started with a strong technical list of objectives and a very weak social list of objectives. They only had three social objectives out of forty-nine to start. Unfortunately, only one of those was included in the final list, which was the need for ethics training. Only 20% of the group believed employee trust was important and 10% thought social engineering was important. The group maintained many of the original technical objectives, but eliminated some important ones, including some related to CIA. The most notable technical objectives eliminated were encryption, which only 20% of the participants found important, firewalls (50%), SPAM (40%), virus scanning (30%), and intrusion detection (20%). While the group started with an adequate list of technical objectives, they finished with an incomplete list by eliminating too many important objectives. These socio-technical security objectives when implemented as the organization's information security policies and distributed through the information security training program would not maximize overall information security and would leave some security holes in both the social and technical areas.

Analyzing the top 10 objectives from each of the groups is a little more revealing as to what the groups believed were important objectives. In times of budget constraints, the top 10 have the best chance of getting implemented. As in the original list of objectives, the socio-technical group outperformed the others. This group had the least number of general objectives in the top ten, with 30%, and only one general objective in the top five. They had 40% technical objectives, which was better than all the other groups, and 30% social objectives, which was equal to the best from the other groups. The top three objectives were social objectives and included two from RITE, relating to responsibilities and integrity. Several of the technical objectives related to confidentiality and availability of information from CIA. This is the best top 10 of all the groups, but still leaves many security holes.

The social group had the second best outcome, but overall was not very good. The group had a lot of general objectives in the top ten, at 60%, including the top two ranked objectives. The other four included two social and two technical objectives. The two social objectives included two pieces from RITE, ethics and employee integrity. One of the technical objectives related to the integrity of information from CIA.

The technical group had poor socio-technical representation from the top 10 objectives, with 60% general objectives, 10% technical, and 30% social. The top four objectives were general objectives. It is surprising that the group that received technical training would only have one technical objective in the top ten, which was ranked number ten, and three times as many social objectives. That one technical objective related to the confidentiality of information from CIA. Building a security culture was ranked number seven.

The control group was by far the worst performer with the top ten objectives. Ninety percent of the top ten were general objectives. There were no social objectives and one technical objective, which related to data confidentiality of information from CIA. Overall, the top 10 security objectives for the control group would provide little or no security.

5.5 Conclusion:

This chapter asked the groups to narrow down their long lists of security objectives by keeping the objectives the group believed were most important. They were then asked to rank the objectives from most important to least important. Overall, the socio-technical group dropped some important socio-technical objectives, such as objectives relating to employee ethics and employee integrity. While they started off well with a robust list, they narrowed it too much,

leaving out important objectives and compromising security. The social group started with a moderate list of socio-technical objectives and maintained most of them in the final ranked list. The technical group started with strong technical objectives and weak social objectives and decided to keep many of those for the final ranked list. On the other hand, the control group also started with a strong list of technical objectives and a weak list of social objectives, but made it weaker by eliminating all but one social objective from the final ranked list. On the technical side, the control group eliminated several important objectives, such as encryption, which is important for ensuring the integrity of data in CIA.

Analyzing the final ranked list of objectives and the top ten objectives from each group makes it clear that the socio-technical group produced the best list of objectives, even though they narrowed their list too much and eliminated some important objectives. The socio-technical group still had the strongest showing, especially if we only analyze the top ten objectives. The social group had the second best performance, ranking ethics and integrity in the top ten. Analysis also makes it clear that the technical and control groups had the worst lists of objectives. The technical group did a good job of keeping important objectives in the final ranked list, but failed to include them in the top ten. The control group performed poorly from the beginning and got worse as they eliminated important objectives from the final ranking and filled 90% of the top ten with general objectives.

6. Discussion

6.1 General Discussion:

The purpose of this research was to investigate how different kinds of information security training affect the nature and scope of information security policies within a firm. Previous research had not investigated this connection and it was not known if such a relationship existed. Four groups of current or potential managers were shown different types of information security training; (1) socio-technical training, (2) social training, (3) technical training, and (4) control group training. Each group then listed their values toward information security and those values were clustered and converted into security objectives using Keeney's (1992) value-focused thinking methodology. A manager's value-based security objectives are what managers use to make security decisions. Their value-based security objectives toward maximizing information security indicate the nature and scope of the information security policies they will create. This research found that the nature and scope of information security training given to managers does influence the nature and scope of information security policies. Making this connection changes our understanding of the relationship between managers, information security policy and information security training.

Prior to this research, the connection between these constructs was fuzzy at best. According to information systems security research, managers create the information security policies and information security training is based on those policies (Hone & Eloff, 2002; Rotvold, 2007;

Figure 6.1: Prior Policy to Training Relationship Understanding

CSI, 2006, 2007; Straub & Welke, 1998). The training teaches employees about the policies with the intent of them using and following what they learned to better protect information systems. The connection between managers, policies, and training is the extent to which information systems security literature previously understood the relationship (figure 6.1).

What this dissertation's findings suggest is that the relationship is not flat and does not flow in one direction from the manager to the training, but in fact comes full circle back to the manager. Security awareness training is intended for all employees, including management. This means that the managers that create information security policy influence the nature and scope of information security training that they themselves will get as part of their regular security training. A significant finding of this research is that training affects policy, which creates the loopback seen in figure 6.2.

Managers are affected by the nature and scope of the information security training they receive. The training influences or reinforces their way of thinking about security and thus the information security policy they create or modify, which leads to the creation or modification of future information security training.

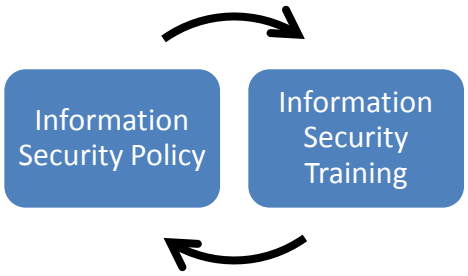

Figure 6.2: Policy to Training Relationship

A more detailed understanding of this relationship suggests that the nature and scope of information security training that a manager receives shapes the manager's values toward information security (figure 6.3). A manager's values impact the manager's objectives toward information security, which influences the nature and scope of corporate security policies they create. The corporate security policies are high level security policies that are the basis for lower level procedural security policies, which in turn is the basis for information security training. The loop back to the managers is through the training. The information security training is intended for all employees, including the managers that created the security policy in the first place. More importantly, middle managers that will someday create corporate information security policy are also influenced by the training, thus helping to maintain the cyclic nature and scope of security policy and training.

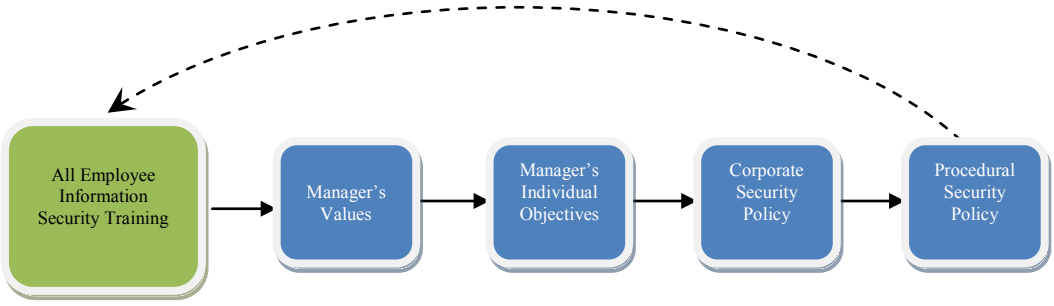

Figure 6.3: Low Level Policy\Training Relationship

The problem with this cycle is that current information security policy and information security training is technical in nature (Rotvold, 2008; CWS, 2010; Fulford & Doherty, 2003). Therefore, manager's values and objectives toward information security must be technically oriented, so security policy and training become technically oriented. This technically oriented information security training then reinforces current manager's technical thinking and influences new manager's values and objectives into technical thinking. This represents the state of information security policy and information security training in organizations today, which is a major problem.

There has to be a break in the cycle to introduce socio-technical aspects of security. The literature review strongly indicates that socio-technical aspects of security are necessary for maximizing information security (Dhillon and Backhouse, 2000, 2001; Trompeter & Eloff, 2001; Dhillon & Torkzadeh, 2006; Dhillon, 2007; Siponen, 2001). This dissertation suggests that giving managers' socio-technical information security training will impact their values and objectives toward information security, thus impacting the information security policy they create. The security policy then created will be influenced by the manager's value-based objectives for securing information systems. According to the cycle, creating socio-technical security policy will lead to socio-technical information security training, which in turn will start a new cycle of socio-technical security policy and training, thus maximizing information security. This process is defined in more detail later in this chapter under the emergent issues section 6.3.1.

Another reason there needs to be a break in the cycle is because of the heavy dependence on checklists. We know that 70% of companies use checklists, which are technically oriented

(GISS, 2008; Baskerville & Siponen, 2002; Dhillon & Backhouse, 2001). Checklists seem like a great idea for managers that are unaware of what should be included in security policies and have only been exposed to technically oriented training. Both their basis for security thinking and their value-based objectives for securing information systems are technically oriented. Since industry standard security guidelines are technically oriented, using them as the basis for security policies seems like the proper course of action. However, doing so leads to technically oriented corporate and procedural security polices, which leads to technically oriented information security training. The result is less than optimal information security. Also, the technically oriented information security training leads to the next generation of managers that have technically oriented value-based security objectives.

To demonstrate the relationship between information security training and information security policy created by managers, four groups of current or potential managers were given various kinds of training. The control and technical groups will be discussed first. The control group received no relevant training and was used to compare the other three groups. This means that participants were asked to list their objectives for securing information systems based on their current values without any influence from the training video. They had to rely on their own feelings, experiences, and education about how they wished to maximize information security. The technical group received relevant technical training and represents companies that offer technically oriented information security training currently. Neither group received training on the social aspects of security.

Results indicate that both groups did an excellent job representing technical objectives and both represented social objectives poorly. The technical group did slightly better in both areas, but

not significantly. The control group's results indicate that no training at all satisfies a great deal of the technical aspects of security, as they fared very well with listing technical objectives. The control group did satisfy all aspects of CIA and included several other important objectives. CIA strands for the confidentiality, integrity and availability of information.

The major problem with both of these groups is the lack of social aspects of security, which research has stated as important for maximizing information security (Dhillon and Backhouse, 2000, 2001; Trompeter & Eloff, 2001; Dhillon & Torkzadeh, 2006; Dhillon, 2007; Siponen, 2001). Both groups had major deficiencies and did not come close to satisfying the requirements of RITE and were missing many other important social objectives. RITE stands for the responsibility, integrity, trust and ethicality of individuals. However, the technical group did list a couple of important social objectives, including the creation of a security culture. They were the only group of the four to list this objective, which is very important for information security.

The significant difference between the control group and the technical group was the ranking of the security objectives. This tells us what objectives each group feels are the most important. The original list of objectives was reduced in size by keeping the objectives that the majority of the group believed were more important and the rest were eliminated. The shortened list was then ranked. The technical group's final list of objectives kept many of the important technical objectives and the most important social objectives. Creating a security culture was introduced by only one of the ten participants, yet 90% of the group agreed creating a security culture was important enough to keep in the final list and the objective finished ranked 7th out of all objectives.

In contrast to the technical group that maintained most of the best objectives in their final ranking, the control group eliminated many of their important objectives, including many that related to CIA. The control group only had 3 social objects out of 49 total objectives to begin with and then eliminated two of them from the final rankings. The only positive point is that the one they kept was creating an ethics program, but the objective barely made the list. Two participants suggested ethics in the initial list and 55% of the group agreed to keep it on the final list and it finished outside the top 10 in the final ranking. It is clear from the results of the technical and control groups that companies with technically oriented training and companies with no training leave large gaps in information security. Both groups supported technical aspects of security but mostly ignored the social aspects.

The socio-technical and the social groups had different outcomes than did the technical and control groups. The social group did not have as strong a result for social objectives as was anticipated, though the result was better than the technical and control groups. Overall, the social group had an inadequate list of social objectives. They failed to fully represent RITE, but did include several other important social objectives. On the technical side, the social group's final list of objectives was not as robust as the technical and control groups. But the group did produce a moderate list of technical objectives. A positive point for the social group is their realization of the important social and technical objectives. In their shortened list of ranked objectives, they kept most of their important social and technical objectives and kept all of their objectives relating to CIA and RITE. Employee ethics and employee integrity were both ranked in the top ten objectives.

The socio-technical group received social and technical information security training and produced the best mix of socio-technical objectives out of all the groups. The socio-technical group produced a robust list of social objectives and was the only group to include all of the objectives relating to RITE. The major social aspect omission from the socio-technical group, and the social group, was the creation of a security culture. Only the technical group included that objective. The surprise is not so much that the technical group listed it when they did not receive training about security culture, but that the social and socio-technical groups did receive security culture training and failed to include it in their objective lists. The socio-technical group also produced a robust list of technical objectives, representing all aspects of CIA and beyond.

While the socio-technical group started with an excellent list of social and technical objectives, the ranking Delphi study indicates they did not realize the importance of some of those objectives. The complete representation of RITE was stripped down in the final ranking to only two of those constructs. They also dropped some important technical objectives, including the integrity of data component of CIA. Examples of important objectives dropped by the socio-technical group include employee ethics and integrity, motivation, commitment, and intrusion detection.

Overall, the socio-technical group produced the best list of security objectives and was the only group to fully represent RITE and CIA and include many other important security objectives. This demonstrates that training did affect their values toward securing information systems. The disappointing result from this group is that they eliminated many of those important security objectives in their ranked list. The social group's results were also a little disappointing because they failed to fully represent RITE. However, they did include several other important social

security objectives. The technical and control groups did not have many surprises. Both created a robust list of technical objectives and a poor list of social objectives, but the technical group was a little better in both areas.

6.2 Research Questions:

This research had two primary research questions related to the effect of training given to managers on their values toward security of information systems and the security policy they create. Value-focused thinking research was used to ascertain individual values toward securing information systems from four groups of managers that completed four different training programs. The security values of each group were converted into security objectives and clustered into similar objectives. Each group's list of security objectives were then reduced and ranked according to importance. The first research question discusses the group's values toward securing information systems in relation to the nature and scope of the training they received. Did the training affect the way managers think and feel about securing information systems? The second research question discusses the security policy implications in relation to each group's value-based objectives. Managers will create security policy based on their value-based objectives, so will that security policy maximize information security?

6.2.1 Influence of Training on Values:

The first research question asked to what extent manager's values toward securing information systems are influenced by the nature and scope of information security training they receive. Each group listed their values toward securing information systems after watching one of four different training videos. One's values define all a decision maker cares about in a given

decision situation (Keeney, 1994). The values listed by the participants from each group describe how they feel and care about securing information systems at a personal level. Based on the responses of the technical, social, and socio-technical groups compared to the responses of the control group, one can see that the nature and scope of information security training has influence on manager's values toward securing information systems, though the results are mixed.

The control group represents a company that does not train managers on the importance of socio-technical security. Their values would be molded by their education, personal experiences, and beliefs. The resultant values of the control group were technically dominant and very weak socially. This means that with no training, manager's basic beliefs toward securing information systems would be to primarily use technical solutions and little or no social solutions. In the control group's original list of security objectives, only 3 socially oriented value-based security objectives were represented. However, the group listed 22 technically oriented value-based security objectives, such as data confidentiality, data backup, and passwords. The complete list of technically oriented value-based security objectives was very good for securing information systems and represented all components of CIA. Overall, the control group, with no training, had an adequate representation of technically oriented value-based security objectives and a poor representation of socially oriented value-based security objectives. The difference between the results from the control group and the results of the other three groups is attributed to the training those other groups received.

The technical group's training represents training that occurs in most companies today. It is technical in nature and does not include social aspects of security. The values of the group's

participants following the training were also technical in nature and were weak in representing the social aspects of security. However the technical group's value-base objectives were a little more robust than were the control group's technically oriented value-based security objectives. Among the technical group's 25 technical values were additional concepts, like encryption, malware, and phishing. The technical group's superior technical values are attributed to the technical training they received. As with the control group, the poor social representation is attributed to the lack of social training imparted in both groups.

The social group received only social training and no technical training. Therefore, if their values were affected by the training, then it would be expected that their technically oriented value-based security objectives would be similar to the control group's values. However, the results indicate that the social group's value-based objectives toward technical solutions for information security would provide only moderate information security, which is not as strong as the control group's technical objectives. The social group produced only 9 technically oriented security objectives, compared to 22 for the control group. It appears that social-only training affected the manager's values in a negative way, leading them to produce far few technical objectives than the control group.

The social group's socially oriented value-based objectives were expected to be better than the control group and the technical group's objectives. The control group and the technical group did not receive social training, so the social group's socially oriented value-based objectives can be compared to both. The social group's socially oriented value-based objectives were better than the control group and the technical group. The social group had 10 total socially oriented value-based objectives, compared to 3 from the control group and 5 for the technical group. The

social group also listed many socially oriented value-based objectives that the control and technical groups did not, like, employee integrity, employee dissatisfaction, emotional intelligence, social interactions between companies and employees, and cultural differences. These additional values were topics discussed in their training video and the inclusion of these topics in the group's value-based security objectives is attributed to the training.

The socio-technical group is the only group that received both social and technical training, so the expectation would be that this group's values toward social and technical aspects of security would be stronger than the control group. Since the control group and the social group did not receive technical training, the technical values of the socio-technical group can be compared to both. The results show that the socio-technical group created 25 technically oriented value-based security objectives, compared to 22 for the control group and 9 for the social group. This is comparable to the control group and far better than the social group. The social values of the socio-technical group were also well represented, with 20 in all, and better than the other groups, even the social group that also received social training.

Overall, the nature and scope of information security training does affect the manager's values toward securing information systems, but more so for social values than technical values. Groups that received technical training had similar representation of technical values than did groups that did not receive technical training. This is attributed to people already having technically oriented values going in. Groups that received social training had a much better social value representation than did groups that did not receive social training. An unexpected result is the negative impact on technical values from receiving only social training and no

technical training, where the social group's technically oriented value-based objectives were far less than the other groups. These results indicate that training has an effect on values.

6.2.2 Implications for Information Security Policy:

The second research question asked to what extent value-based objectives influence the nature and scope of information security policy. To answer this question, categories were created to represent the quality of the information security policy that would be created from the manager's value-based objectives. For the social aspects of information security, five components were identified from the literature review as most important. Those are the responsibility, integrity, trust, and ethicality (RITE) of individuals and the creation of a security culture. Five categories used to rate the inclusion of the five social components are very good, good, moderate, poor, and very poor (see table 6.1). All five of these components must be represented in the information security policy in order to maximize information security and receive a very good rating. For the technical components, the three components found to be most important from the literature review were confidentiality, integrity and availability (CIA) of information. The three categories used to rate the inclusion of these components were very good, moderate and very poor (see table 6.1).

Table 6.1: Security Policy Categorization Criteria

Categories	Social	Technical
Very Good	Full support of RITE and a security culture (5 components)	Full support of CIA (3 components)
Good	4 of 5 components	
Moderate	3 of 5 components	2 of 3 components
Poor	2 of 5 components	
Very Poor	1 or less component	1 or less component

This dissertation used the value-focused thinking methodology to produce a list of value-based security objectives for each of the four groups. That list was then reduced and ranked using a ranking Delphi methodology, producing a shorter list of security objectives. Both lists are analyzed in this section in regard to the information security policy they would inform. The quality of that policy is based on the categories described in table 6.1. The security policy based on the longer unranked lists of security objectives will be discussed first, followed by a discussion of the shorter, ranked lists (see table 6.2).

Information security policy informed by the value-based security objectives created by the socio-technical group came the closest to maximizing information security. The social policy was categorized as good and not very good only because the group failed to include the creation of a security culture. Information security policy that does not provide for the creation of a strong security culture is not maximizing information security. On the technical side, the information security policy was very good and supports all aspects of CIA. By far, the socio-technical group's information security policy produced the strongest overall information security of all the groups.

The social group's information security policy informed by their value-based security objectives was a disappointment. It was anticipated that their social security policy would be good or very good, but instead it was poor. They failed to create policy for instituting a security culture as well as two of the four components of RITE. On the technical side, security policy from the social group was also less than adequate. They were the only group to have moderate technical security policy and not fully represent CIA, while all the other groups produced very good technical policy.

The technical group and the control group both produced poor social security policy. This fit into expectations because both groups did not receive training on the social aspects of security and they both produced a poor list of socially oriented value-based objectives, thus leading to poor social security policy. On the technical side, both the technical group and the control group produced very good technical security policy. Of course this is no surprise for the technical group since they received technical training and produced an excellent list of technically oriented value-based objectives. The control group also produced an excellent list of technically oriented value-based objectives and their very good technical security policy was a minor surprise. Employees are predominately exposed to technically oriented policies and these get reinforced through technically oriented information security training. It was therefore expected that all participants from all groups would have a technically oriented view for protecting information systems, not from the training given in this dissertation, but from their own education and personal experiences. The training in this dissertation would only enhance that technical view if they received technical training. It was expected that the control group would have moderate technical information security policy, but not very good policy. Very good technical security policy required the representation of all aspects of the confidentiality, integrity, and availability (CIA) of information. The expectation was that the control group would represent most, but not all aspects of CIA.

Table 6.2: Socio-technical Security Policy (all objectives)

Group	Social Policy	Technical Policy
Socio-Technical	Good	Very Good
Social	Poor	Moderate
Technical	Poor	Very Good
Control	Poor	Very Good

Table 6.3 represents the information security policy created with the value-based security objectives from the shortened and ranked list of security objectives from chapter five. The ranking Delphi method called for the original list to be shortened before it was ranked. Doing so eliminated many objectives from each group's list, some of which were important for maximizing information security. If constraints, such as budgets, meant that managers could not implement all value-based security objectives in security policy- which would they choose to implement and which would they chose to eliminate. The ranking Delphi method gave us this answer by keeping only what the managers considered the most important value-based security objectives and discarding the rest. The security policy implemented based on these value-based security objectives is the biggest surprise of this dissertation.

The socio-technical, social, and technical groups all produced poor social security policy and the control group produced very poor social security policy. The surprise here is that the socio-technical group did not consider the trust and ethicality pieces of RITE important enough to keep in their final list of ranked objectives. This prevented the group from producing good social security policy and made them present poor social security policy. In a time of budget constraints the socio-technical group would consider eliminating ethics training as a means of security. The social, technical, and control groups all had poor social policy in the original list, so it was no surprise that the social and technical groups remained poor and the control group sank a little lower to very poor.

The technical aspects of information security policy also produced some unexpected results with the socio-technical group. The group eliminated value based security objectives relating to the integrity of data, so the quality of their technical security policy decreased from very good in the

initial list to moderate in the ranked list. The social group started with moderate technical security policy and continued with moderate technical security policy in the ranked list. The technical group started with very good technical security policy and continued with very good technical security policy in the ranked list. The control group decreased from very good technical security policy to moderate technical security policy in the ranked list because they eliminated one of their important CIA objectives.

Table 6.3: Socio-technical Security Policy (ranked objectives)

Group	Social Policy	Technical Policy
Socio-Technical	Poor	Moderate
Social	Poor	Moderate
Technical	Poor	Very Good
Control	Very Poor	Moderate

Overall, the social and technical groups maintained their important value-based security objectives from the original list to the ranked list, so the quality of their information security policy remained the same. The socio-technical and control groups both eliminated important value-based security objectives relating to RITE and CIA, so the quality of their information security policy diminished.

If constraints did not exist and the organization could create security policy based on the original list of value-based security objectives, the socio-technical group by far would produce the highest quality information security policy. The social group would produce the worst. Both the technical and control groups would produce poor social policy and very good technical policy. The technical group represents how organizations are handling things today. The literature review showed that organizations predominately had technically oriented security policy.

If constraints are a problem, such as budget cuts, the information security policy produced from the ranked list of value-based security objectives leaves a lot of security holes. The technical group produced the highest quality information security policy, which comprised poor social policy and very good technical policy. The socio-technical and social groups tied for second with poor social policy and moderate technical policy. The control group came in last with very poor social policy and moderate technical policy.

6.3 Emergent Issues:

This dissertation has shown that specialized information security training given to managers can influence their values for protecting information systems and the information security policy they create. The emerging issues stemming from such findings are in the area of information security training, policy planning and policy creation. The next section discusses the information security training giving to all employees and the specialized information security training that should be given to management. The following section discusses the implications of such training on policy planning and creation.

6.3.1 Information Security Training:

Information security training is a method of educating all employees on how best to protect an organization's information systems. Rotvold (2008) reported that it is imparted to employees most often once a year by IT staff. The literature review also told us that the nature and scope of information security training is based on information security policies and that both were technically oriented in today's organizations (Rotvold, 2008; CWS, 2010; Fulford & Doherty, 2003; Straub & Welke, 1998). In order to change the nature and scope of information security

training to socio-technical, information security policy must change its nature and scope to socio-technical. This can be accomplished by creating another type of information security training that is to be given to managers, and not just the managers that create and modify information security policies, but to all managers. This training needs to be in addition to the training given to all employees and specifically given to management (figure 6.4). Like the training given to the socio-technical group in this dissertation, the training needs to teach both social and technical aspects of information security. There are several reasons it should be given to all managers and not just those that create or modify information security policy. One is that some of those middle managers will eventually work their way up to be the ones creating and modifying policy and the earlier they understand the socio-technical perspective, the better. Another reason to include all managers is because all managers will need to be involved to implement some socio-technical aspects of security, such as creating a strong security culture.

Figure 6.4 represents managers receiving two types of training, one being the regular training giving to all employees that is based on the procedural security policy. The second training is a socio-technical training that teaches managers about the importance of socio-technical security and how to create and modify information security policy. Like the socio-technical group in this dissertation, the goal of this training is to produce socio-technical security policy by influencing manager's values and individual objectives toward securing information systems. Once the managers implement socio-technical security policy, the regular information security training given to all employees will then become socio-technical. This will not happen overnight, but instead will take some time for the new socio-technical security policies to be implemented and for the previously technically oriented information security training to be modified to become socio-technical to reflect the new policies. The loopback depicted in the diagram reflects the

new socio-technical procedural security policy's influence on information security training given to all employees. Once the cycle is complete and policies and training become socio-technical, managers will then receive socio-technical security training as a part of the regular training program that all employees receive as well as socio-technical training on how to create and modify socio-technical information security policies.

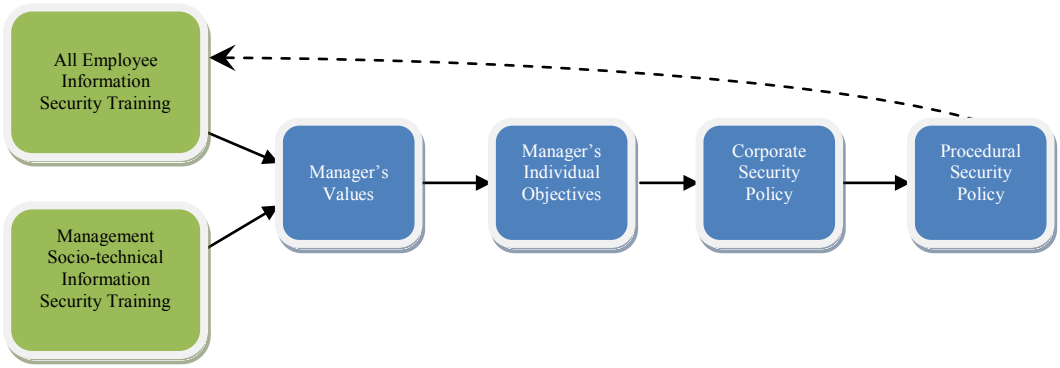

Figure 6.4: New Policy to Training Relationship

At the least, the special training given to managers should cover the concepts of RITE, CIA, and the creation of a security culture (Dhillon & Backhouse, 2000; Dhillon, 2007). The concepts of RITE are the responsibility, integrity, trust, and ethicality of individuals. Examples include creating proper responsibility and authority structures, background checks, building a trusting culture and ensuring good ethical principles. The concepts of CIA are the confidentiality, integrity and availability of information. Examples include ensuring appropriate access to data, backing up data, encrypting data, data integrity checks, and maintaining a functioning network and equipment. The creation of a security culture is also very important for maximizing information security (Ruighaver et al., 2007; Dhillon, 2007; Karyda, et al., 2005; von Solms & von Solms, 2004; Leech, 2003; Vroom and von Solms, 2004). A strong security culture has been linked to such things as compliant user behavior and employees engaging in security practices

beyond their mandatory job descriptions (D'Arcy & Greene, 2009). Beyond those already mentioned, other socio-technical aspects of security that should be discussed include describing the formal, informal and technical systems (Dhillon, 2007), leadership styles, management commitment, user involvement, reward systems, motivation, group association and interpreting and dealing with negative silent messages.

The goal of this training is to influence the values of the managers that receive it in regard to what they believe are the best ways of maximizing information security. If the nature and scope of their values are influenced to be socio-technical, then their value-based security objectives for protecting information systems will also be socio-technical. Like this dissertation's socio-technical group's original list of security objectives, the managers receiving this training will also have strong value-based security objectives. Those value-based objectives will in turn inform the information security policy they create or modify and that information security policy will then become socio-technical. This would mean security policies would support the creation of a security culture and would include policies supporting RITE and CIA. As these policies trickle down and inform the creation of new information security training, employees will start learning about their roles and responsibilities, accountability and about good ethical principles. Reward systems will be created, users will be more involved, management will be more committed, and trusting relationships between employees and the employer will be established. These among others mentioned earlier will strengthen the organization's security culture, all of which leads to maximized information security.

6.3.2 Policy Planning and Creation:

The development of information security policies does not just start with a to-do list that can be checked off as completed. Managers have to know what assets need to be protected and determine what policies are best for protecting those assets. This usually involves some form of risk analysis and SWOT (strengths, weaknesses, opportunities, and threats) analysis. Before creating policies, it just makes sense to understand what it is you have that needs protection, the level of importance the assets have for the organization, what the cost would be if protection fails, what the threats to the assets are, where the threats come from, what policies are currently in place to protect the assets, and anything else that will help determine the best policies to create, modify or eliminate.

Baskerville and Siponen (2002) state that organizations should first have a meta-policy about how to create, modify, and implement information security policy. A meta-policy is a policy about how to handle the creation, modification, and elimination of security policies. Meta-policy details who is responsible for making policies, when policy creation is to take place, how policies are made, and how and when policies are reviewed, modified or eliminated. This dissertation research believes that meta-policy should include training for all managers, and especially those involved in policy creation and modification. Meta-policy dictates everything from who makes the policies to how and when they are created, modified and eliminated. It should also include the training for those involved in this process.

Once managers have received training, completed the analysis of the assets, and determined the strengths and weaknesses of the current security policy, they are ready to create, modify, or eliminate information security policies. We know from the literature review that checklists are

used by 70% of organizations (CWS, 2010). However, we also know that checklists are technical by nature and lack flexibility to changing business environments (Baskerville & Siponen, 2002; Dhillon & Backhouse, 2001). Managers should understand that they can use checklists, but only as references for the technical aspects of security and only if they fit the organizations business requirements and processes. The technical aspects of security have never been the problem; the problem has been the lack of social aspects. In addition to the technical solutions to information security as informed by checklists, managers must still ensure the creation of the social aspects of security they learned about in their training.

One social aspect that should never be overlooked is the creation of a strong security culture. To create a strong security culture, it needs to be tied to the information security policies. Managers can dictate the behavior of employees by "expressing collective values, norms, and knowledge, through defining specific policies" (Solms & von Solms, 2004, p. 277). In research from Ruighaver et al. (2007), the authors highlight several factors of good security culture. One of them is developing a degree of trust and accountability between employees and employers, which is a part of Dhillon and Backhouse (2000)'s RITE and should be included in the security policies. Another factor of good security culture identified by Ruighaver et al. (2007) was that employees should be educated on their roles and responsibilities. This was another part of RITE and should also be included in the information security policies. The two other parts of RITE that should also be part of the information security policy and support the security culture are the integrity and ethicality of individuals. Integrity can start with a background check. Ethicality can be positively influenced through a formal ethics training program. Companies with ethics programs suffer less economic crime (Trompeter & Eloff, 2001, ECS, 2007). Beyond creating policies that support a strong security culture and represent the social aspects of RITE and the

technical aspects of CIA, policies should also incorporate some of the social concepts described in the training section, such as involving users, creating reward systems and motivating employees.

6.4 Conclusion:

This chapter reported the findings of this research, answered the primary research questions and discussed emergent issues. A significant finding of this research was that the nature and scope of information security training giving to managers affects the nature and scope of their values. Another significant finding was that the quality of information security policy was affected by manager's value-based security objectives. The group of managers receiving socio-technical training would produce the highest quality information security policies based on their original list of value-based security objectives. The group that received no training would produce the worst information security policies. The implications of these findings lead us to believe that specialized socio-technical training should be given to managers and that this training should be part of a meta-policy within the organization. If managers were to receive socio-technical training, the security policies they create or modify would be socio-technical. Socio-technical policies would lead to socio-technical information security policy given to all employees, thus maximizing information security.

7. Conclusion

7.1 Overview of the Research:

This dissertation argues that the nature and scope of information security training that managers' receive impacts the nature and scope of the information security policies they create. It is argued that the training affects manager's values toward maximizing information security and that their value-based objectives influence the nature and scope of the information security policy they create. The motivation for this research stems from a recent trend in information systems security research; that the best way to maximize information security is a socio-technical approach (Backhouse & Dhillon, 1996; Dhillon and Backhouse, 2000, 2001; Trompeter & Eloff, 2001; Siponen, 2001; Dhillon & Torkzadeh, 2006; Dhillon, 2007). While the research trend has come to this conclusion, the means for achieving socio-technical security is mostly unanswered.

This research attempts to achieve socio-technical security through the heart of the information security program, the information security policies and the information security training program. Information security policies are the guiding principles for securing information systems and information security training is the education given to employees to teach them how to best protect information systems using the methods described in the policies. Information security training is primarily based on the information security policies (Rotvold, 2007; CSI, 2006, 2007).

A major problem discussed in the literature review is that current information security policies and information security training is predominately technical in nature, ignoring the social aspects of security (Rotvold, 2008; CWS, 2010; Fulford & Doherty, 2003). This may be because 70% of organizations use standardized guidelines (checklists) to create security policies and the reliance on checklists is expected to rise (GISS, 2008). However, checklists have many shortcomings, including the lack of flexibility to changing business environments and the lack of attention to social aspects of security (Baskerville & Siponen, 2002; Dhillon & Backhouse, 2001). Organizations that rely on checklists to create their security policies will no doubt have technically oriented security policies and training. Another reason that policies and training may be technical in nature and the use of checklists is high is that managers that create information security policies lack the skills and knowledge to do so (Hone & Eloff, 2002). This lack of knowledge leads managers to turn to other sources for help, such as standardized checklists (Hone & Eloff, 2002).

To potentially solve these problems, this dissertation created four types of information security training and used four groups of managers to see if there was an effect on the information security policy they would create. The four types of training were socio-technical training, social only training, technical only training, and control group non-related training. The experimental design called for the groups to watch their respective videos and then write down what topics they believed were most important if they were a manager in charge of maximizing information security and the effectiveness of the information security training program. This exercise is part of Keeney's (1992) value-focused thinking methodology where each group produces a list of values. The values represent how managers truly feel about maximizing information security. Following the methodology, the values were converted and clustered into lists of value-based

security objectives for each group. The value-based security objectives represent what the managers wish to strive toward in order to maximize information security. When faced with the decisions involved with creating the organizations information security policy that maximizes information security, the managers will use their value-based security objectives. The lists of values and value-based objectives created by each group were used to answer two research questions.

This dissertations first research question asked as to what extent manager's values toward securing information systems are influenced by the nature and scope of information security training they receive. The findings indicate that values are affected by training, but the results are mixed. The control group with no relevant training produced an excellent list of technical values and a poor list of social values. The technical group that received only technical training also produced an excellent list of technical values and a poor list of social values, which was expected. The socio-technical group that received both technical and social training produced an excellent list of technical values and an adequate list of social values. This confirmed that the social training affected the values of the socio-technical group. The social group was the group that produced the mixed results. They received only social training, yet produced a poor list of social values. However, they did have many more social values than the control or technical groups. This indicates that their values were affected by the training, but not as significantly as with the socio-technical group. The social group's technical values were also not as good as the other groups. While the other three groups had excellent lists of technical values, the social group had a moderate list. This indicates that social only training may have had a negative impact on producing technical values.

This dissertations second research question asked to what extent value-based objectives influence the nature and scope of information security policy. This question was answered in two parts. The first part used the full lists of value-based security objectives to determine the quality of information security policy they would inform. The second part answered the same question, but with a shortened and ranked list of security objectives. The second list was produced using a ranking Delphi methodology developed by Schmidt (1997). Following the ranking Delphi method, the groups were asked to reduce their original lists of value-based objectives by keeping only those objectives they believed were most important and discarding the rest. This process produced a shortened list of security objectives that the groups then ranked from most important to least important. The ranking process took several iterations.

Information security policy informed by the value-based objectives from the original lists represented the highest quality for the socio-technical group. Their value-based security objectives would have created good social policy and very good technical policy. They were the only group that would have produced good social policy, as the other groups all would have created poor social policy. For technical security policy, the technical and control group's would have produced very good policy and the social group would have produced moderate policy. The socio-technical group would have produced the best overall security policy of the four groups.

The shortened lists that resulted from using the ranking Delphi methodology produced different results. Because the original lists of security objectives were shortened, some groups eliminated important security objectives. In particular, the socio-technical group eliminated many important value-based security objectives and the effect on information security policy was dramatic.

Information security policy based on the shortened ranked list would have produced poor social policy and moderate technical policy. This indicates that managers from this group did not believe many of the important security objectives were actually important, so they were eliminated from the list. If security policy were created based on the shortened list of objectives, overall security would be dramatically weaker. The social and technical groups both maintained their quality of information security policy with the shortened lists. However, the control group's potential security policy got weaker as they also discarded some important security objectives. Their potential social security policy dropped from being poor to very poor and their potential technical security policy dropped from being very good to moderate.

Overall results of this dissertation indicate that information security training given to managers does affect their values toward securing information systems. The quality of information security policy informed by the manager's value based security objectives is also affected by training. In order to maximize information security with socio-technical aspects of security, managers should receive socio-technical information security training. The results indicate that managers receiving socio-technical training would produce socio-technical security policies.

7.2 Contributions:

The most important part of a dissertation is the contribution the research makes to knowledge. There are several contributions this research makes that cross the practical, methodological, and theoretical realms. The first two subsections describe the practical and theoretical contributions this research makes to information systems security. The last subsection describes the methodological contribution that can be applied not only to the information systems discipline, but beyond.

7.2.1 Practical:

The practical contribution this research makes explains how organizations should go about creating, and modifying information security policies to maximize overall information security. Done properly, organizations will no longer have such a strong dependence on security checklists and will have socio-technical information security policies. To accomplish this, this dissertation calls for all organizations to have a specialized information security training program for managers that teaches them the importance of socio-technical security. The socio-technical training should cover the important technical aspects of security as well as the important social aspects of security, such as the concepts of RITE, CIA, and the creation of a security culture. If done properly, manager's values toward securing information systems will be affected by the training and result in socio-technical security policies. The security policies will inform socio-technical versions of information security training that is given to all employees. The result is maximized information security through socio-technical information security policies and a socio-technical information security training program.

7.2.2 Theoretical:

The theoretical contribution of this dissertation is through a model that describes information security policy and information security training as affecting one another (figure 7.1). The prior understanding of this relationship was that it was a one way relationship where information security policy affected information security training, where the training is based on the policies.

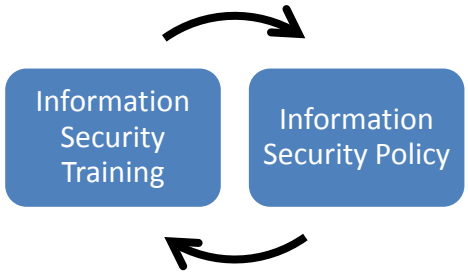

Figure 7.1: Policy to Training Relationship

However, this model suggests that the makeup of information security training also affects information security policies. The primary reason managers create technically oriented information security policies is that they do not know any better. This could be because the only training they have seen is the information security training given to them each year. The control group in this dissertation demonstrates what the literature review told us in that organizations currently have technically oriented information security policies and training. Managers receiving technically oriented training over the years become technically oriented toward securing information systems, as we saw in the control group's excellent technical security policy. Adding a specialized training for managers to the existing information security training program can break this cycle of technically oriented policies and training and lead to a new socio-technical cycle.

7.2.3 Methodological:

The methodological contribution of this dissertation was the use of the value-focused thinking approach as the input to the ranking Delphi study. No other study has been found that combined these methodologies. The ranking Delphi methodology consists of three phases, the first of which is the discovery of issues. This is where panelists brainstorm for an initial list of issues

pertaining to the topic under study. The second and third phases are to shorten the list and rank the issues. Some researchers choose to alter the first phase by introducing the panelists to a predetermined list of issues (Keil, et al., 2002; Lee & Anderson, 2006; Kasi et al., 2008). The panelists do not have any input as to the makeup of this predetermined list of issues. They only get to shorten the list and rank the remaining issues. This dissertation instead chose to use the value-focused thinking approach to determine the initial list of issues, called objectives in this research. The value-focused thinking approach is superior to phase one's brainstorming activity in that the panelist's values are determined. The output of phase one is still a list of issues (objectives), but obtained through the participants' values. In addition, there is no predetermined list and the same panelists are used for all three phases of the ranking Delphi methodology.

7.3 Limitations:

There are two major limitations to this research, including generalizability and thoroughness of training. The non-random selection of MBA students to represent managers is a limitation on several fronts. The first is that while over 90% of them were managers, not all of them were managers. Those that were not managers were studying to become managers, but were not currently employed as managers. The second limitation with using students was that they were junior managers and not managers that created or modified information security policies. Their average number of years as managers was relatively low. The last limitation with using MBA students is generalizing results to all managers. While the non-random selection represented 31 different companies, the results are only generalizable to other non-random selections of MBA students.

The second major limitation of this research is the training given to the participants. Each training video was 35 minutes in length, which is a short period of time to adequately teach the complicated concepts of socio-technical security. In order to cover all the topics necessary, each topic was discussed quickly and efficiently. This may have led to an under emphasis on certain topics.

7.4 Future Research Directions:

Given the limitation, this research still produced significant results. However, future research directions should attempt to minimize the limitations. The next logical step should be to conduct this study with a random selection of managers and not MBA students. Another research direction could be an action research study involving managers that create or modify information security policy. Those manager's values could be ascertained before and after training as a pre and post test. The training should be socio-technical training and the video should be lengthened to at least an hour to give more time to adequately address all the topics. The video could also be replaced with a one hour lecture. The information security policies should be analyzed before the training and at some point after the training to see if the training affected the creation or modification of security policies. Information security training given to all employees should also be analyzed before and after the training given to managers to see if it too was affected by the management training.

If follow-up studies demonstrate that training managers affects information security policy and information security training by making them both more socio-technical in nature, then another study should try to determine if socio-technical security affects security incidents. The number

of security incidents by insiders and outsiders could be monitored for a time period before and after the implementation of socio-technical security.

References:

AFCE (2006). (Association of Certified Fraud Examiners: Report to the Nation on Occupational Fraud and Abuse). Retrieved 3-1-2008 from http://www.acfe.com/resources/publications.asp?copy=rttn.

AFCE (2008). (Association of Certified Fraud Examiners: Report to the Nation on Occupational Fraud and Abuse). Retrieved 9-21-2009 from http://www.acfe.com/resources/publications.asp?copy=rttn.

Backhouse, J., & Dhillon, G. (1996). Structures of responsibility and security of information systems. *European Journal of Information Systems*, 5, 2–9.

Barclay, C., & Osei-Bryson, K. (2010). Project Performance development framework: An approach for developing performance criteria & measures for information systems (IS) projects. *International Journal of Production Economics,* 124(1), 272.

Baskerville, J. (1993). Information systems security design methods: implications for information systems development. ACM Computing Surveys, 25 (4), 375.

Baskerville, J., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*. 15, 337.

Berger, L., & Berger, D. (2004). The talent management handbook, creating organizational excellence by identifying, developing, & promoting your best people. McGraw Hill, Madison, WI, USA.

Bostrom, R., & Heinen, J. (1977). MIS problems and failures: a socio-technical perspective (Part I: the causes). *MIS Quarterly*, September, 17.

Brancheau, J., Janz, B., & Wetherbe, J. (1996). Key issues in information systems management: 1994-1995 SIM Delphi Results. *MIS Quarterly*, 20(2), 225.

Bullock, R., Deckro, R., & Weir, J. (2008). Methodology for competitive strategy development. *Computers & Operations Research*, 35, 1865-1873.

Burrell, G., & Morgan, G. (1979). Sociological paradigms and organizational analysis. Heinemann, London.

Cone, B., Irvine, C., Thompson, Michael, & Nguyen, D. (2007). A video game for cyber security training and awareness. *Computers & Security*. 26, 63-72.

CSI (2006). (CSI/FBI Computer crime and security survey). Retrieved 4-30-2010 from http://www.gocsi.com/.

CSI (2007). (Computer crime and security survey). Retrieved 3-2-2008 from http://www.gocsi.com/.

CSI (2008). (Computer crime and security survey). Retrieved 11-4-2009 from http://www.gocsi.com/.

CSI (2009). (Computer crime and security survey). Retrieved 5-17-2010 from http://www.gocsi.com/.

CWS (2010). (Cybersecurity watch survey: cybercrime increasing faster than some company defenses). Retrieved 3-7-2010 from http://www.csoonline.com.

D'Arcy, J., & Greene, G. (2009). The multifaceted nature of security culture and its influence on end user behavior. IFIP TC 8 International Workshop on Information Systems Security Research, 145-157.

Detert J, Schroeder R, & Mauriel J. (2000). A framework for linking culture and improvement initiatives in organisations. *The Academy of Management Review,* 25(4), 850–63.

Dhillon, G., & Backhouse, J. (2000). Information systems security management in the new millennium. *Communicaitons of the ACM*, 43(7), 125-128.

Dhilllon, G., & Backhouse, J. (2001). Current directions in IS research: towards socio-organizational perspectives. *Information Systems Journal*, 11, 127-153.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information systems security in organizations. *Information Systems Journal*, 16, 293-314.

Dhillon, G. (2007). Principles of information systems security, New York, NY: John Wiley & Sons.

Doherty, N., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security*, 25, 55-63.

Doke, E., & Swanson, N. (1995). Decision variables for selecting prototyping in information systems development: a Delphi study of MIS managers. *Information & Management*, 29, 173-182.

Fulford, H., & Doherty, N. (2003). The application of information security policies in large UK-based organizations: an exploratory investigation. *Information Management & Computer Security*, 11(3), 106-114.

GISS (Ernst & Young's 2008 global information security survey) (2008). Retrieved 4-12-2009 from http://www.ey.com.

Goold, M., & Luchs, K. (1996). Managing the multi-business company, strategic issues for diversified groups. New York, NY: Routledge.

Hayne, S., & Pollard, C. (2000). A comparative analysis of critical issues facing Canadian information systems personnel: a national and global perspective. *Information & Management*, 38, 73-86.

Hone, K., & Eloff, J. (2002). Information security policy - what do international information security standards say? *Computers & Security*, 21(5), 402-409.

Johnson, M., (2006). Decision models for the location of community corrections centers. *Environment and Planning B-Planning & Design*, 33(3), 393-412.

Kasi, V., Keil, M., Mathiassen, L., & Pederson, K. (2008). The post mortem paradox: a Delphi study of IT specialists perceptions. *European Journal of Information Systems*, 17, 62-78.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information Systems Security Policies: A Contextual Perspective. *Computers & Security*, 24, 246-260.

Keeney, R. (1992). Value-focused Thinking: A path to creative decisionmaking. Cambridge, MA: Harvard University Press.

Keeney, R. (1994). Creativity in decision making with value-focused thinking. *Sloan Management Review*, 35(4), 33.

Keeney, R. (1996). Value focused thinking: identifying decision opportunities and creating alternatives. *European Journal of Operational Research*, 92, 537-549.

Keeney, R. (1999). The value of Internet commerce to the customer. *Management Science*, 45(4), 533.

Keeney, R., & McDaniels, T., (2001). A framework to guide thinking and analysis regarding climate change policies. *Risk Analysis*, 21, 989-1000.

Keil, M., Tiwana, A., & Bush, A. (2002). Reconciling user and project manager perceptions of IT project risk: a Delphi study. *Information Systems Journal*, 12, 103-119.

Kim, T., Donnell, E., & Lee, D. (2008). Use of cultural consensus analysis to evaluate expert feedback of medium safety. *Accident Analysis and Prevention*, 40, 1458.

Lamour, J. (2008). Impact of user awareness and training of infosec practitioners on data security. PhD. Dissertation, Walden University.

Lee, L., & Anderson, R. (2006). An exploratory investigation of the antecedents of the IT project management capability. *e-Service Journal*, Retrieved 3-19-2009 from http://proquest.umi.com.

Lee, C., Song, H., & Mjelde, J. (2008). The forecasting of international expo tourism using quantitative and qualitative techniques. *Tourism Management*, 29, 1084.

Leech, J. (2003). Improving security behavior. *Computers & Security*, 22, 8.

Loo, R. (2002). The Delphi method: a powerful tool for strategic management. *Policing, An International Journal of Police Strategies & Management*, 25(4), 762.

Marsden, D. (2009). Commentary on a Delphi clinical practice protocol for the diagnosis and management of very long chain acyl-Coa dehydrogenase deficiency by Arnold et al. *Molecular Genetics and Metabolism*, 96, 81-82.

May, J. (2008). Developing a multi-objective decision model for maximizing IS security within an organization. Ph.D. Dissertation, Virginia Commonwealth University, Richmond, VA.

Merrick, J., Grabowski, M., Ayyalasomayajula, P., & Harrald, J. (2005). Understanding organizational safety using value-focused thinking. *Risk Analysis*, 25(4), 1029-1041.

Miura, H., Midorikawa, S., Fujimoto, K., Pacheco, B, & Yamanaka, H. (2008). Earthquake damage estimation in metro Manila, Philippines based on seismic performance of buildings evaluated by local experts judgments. *Soil Dynamics and Earthquake Engineering*, 28, 764.

Mulligan, P. (2002). Specification of a capability-based IT classification framework. *Information & Management*, 39, 647.

Mursu, A., Lyytinen, K., Soriyan, H., & Korpela, M. (2003). Identifying software project risks in Nigeria: an international comparative study. *European Journal of Information Systems*, 12, 182-194.

Nakatsu, R., & Iacovou, C. (2009). A comparative study of important risk factors involved in offshore and domestic outsourcing of software development projects: a two panel Delphi study. *Information & Management*, 46, 57-68.

Neiger, D., & Churilov, L. (2004). Goal-oriented business process modeling with EPCs and value-focused thinking. *Business Process Management*, 3080, 98-115.

Okoli, C., & Pawlowski, S. (2004). The Delphi method as a research tool: and example, design considerations and applications. *Information & Management*, 42, 15-29.

Opie, J., & Taylor, T. (2008). An exploratory Delphi study on the integration of disabled students into physiotherapy education. *Physiotherapy*, 94, 292.

Patrick, W., & Damon-Randall, K. (2008). Using a five-factored structured decision analysis to evaluate the extinction risk of Atlantic sturgeon (Acipenser oxyrinchus oxyrinchus). Biological Conservation, 141, 2906.

Peharda, I., & Hunjak, T. (2008). Selecting an automatic rifle using the value-focused thinking approach. Military Operations Research, 13, 19-26.

Prato, M. (2008). Conceptual framework for assessment and management of ecosystem impacts of climate change. *Ecological Complexity*, 5, 329.

Rezgui, Y. & Marks, A. (2008). Information security awareness in higher education: an exploratory study. *Computers & Security*, 27, 241-253.

Rotvold, G. (2007). Status of security awareness in business organizations and colleges of business: an analysis of training and education, policies, and social engineering testing. Ph.D. Dissertation, University of North Dakota, Grand Folks, NC.

Rotvold, G. (2008). How to create a security culture in your organization. *Information Management Journal*, 42(6), 32.

Ruighaver, A., Maynard, S., & Chang, S. (2007). Organizational security culture: extending the end-user perspective. *Computers & Security*, 26, 56-62.

Schmidt, R. (1997). Managing Delphi surveys using nonparametric statistical techniques. *Decision Sciences*, 28(3), 763-774.

Schmidt, R., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying software project risks: an international Delphi study. *Journal of Management Information Systems*, 17(4), 5.

Schultz, E. (2004). Security training and awareness – fitting a square peg into a round hole. *Computers & Security*. 23, 1-2.

Shaw, R., Chen, C., Harris, A., & Huang, H. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*. 52, 92-100.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*. 8(1), 31-41.

Siponen, M. (2001). An analysis of the recent IS security development approaches: descriptive and prescriptive implications. In: *Information Security Management: Global Challenges in the New Millennium*, Dhillon, G. (ed.) (pp. 101–124), Hershey, PA: Idea Group Publishing.

Spinellis, D., Kokolakis, S., & Gritzalis, S. (1999). Security requirements, risk and recommendations for small enterprise and home-office environments. *Information Management & Computer Security*, 7(3), 121.

Straub, D., & Welke, R. (1998). Coping with systems risks: security planning models for management decision making. *MIS Quarterly*, 22, 441–469.

Thomson, M., & Von Solms, R. (1998). Information security awareness: educating your users effectively. *Information Management & Computer Security,* 6(4), 167.

Trompeter, C., & Eloff, J. (2001). A framework for implementation of socio-ethical controls in information security. *Computers and Security*, 20, 384–391.

Von Solms, R., & Von Solms, B. (2004). From policies to culture. *Computers & Security*. 23, 275-279.

Vorm, A., Vernooij-Dassen, M., Kehoe, P, et al. (2009). Ethical aspects of research into Alzheimer disease. A European Delphi study focused on genetic and non-genetic research. *Journal of Medical Research*, 35, 140-144.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, 23, 191-198.

Yoo, S., Kim, J., & Kim, T. (2001). Value-focused thinking about strategic management of radio spectrum for mobile communications in Korea. *Telecommunications Policy*, 25, 703-718.

Appendix A: Data Collection Form

Name: _____ Place of Employment (optional): _____

Email: _____ Years Employed at Above Employer: _____

Alt. Email: _____ Years Employed in Similar Work: _____

Phone: _____ Years of Management Experience: _____

Sex: (circle one): Male; Female Age (circle one): 18-24; 25-29; 30-34; 35-39
40-44; 45-49; 50-54; >54

Study Description: The purpose of this study is to maximize information security and the effectiveness of the information security training program.

Information Security Training: the method of educating all employees on how best to protect an organization's information systems.

Please write down and briefly describe what topics you believe are most important if you were a manager in charge of maximizing information security and the effectiveness of the information security training program. Think about what topics should be considered to most effectively secure information systems. Draw more lines and write on the back if necessary.

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____

Appendix B: Video Content

Socio-Technical Video Outline:

What are the major issues and challenges of managing corporate information security?

- Subverting the controls
- Insider threat

How do we manage the insider threat?

- Formal, informal, technical systems
- Policies
- Procedures
- Processes
- Guiding principles
- Security culture
- Legal systems, international systems, standards, regulatory aspects

Can you give examples of the technical, formal, and informal systems?

- Communication example
    - Email (technical communication)
    - Rules and procedures for email (formal communication)
    - System of obligations (informal communication)

How do these systems relate to corporate information security?

- Security is when one of the systems fails
- Controls need to be in place for all three systems
- Informal controls
    - Norms
    - Security Culture
    - Supports the technical and formal systems
- Formal controls
    - Checks and balances are in place
    - Processes are clear
    - Rules and procedures communicated properly
- Technical controls
    - Access rights
- Need a mix of control systems

- Managerial training educates managers on how to balance these systems.

Can you elaborate on these systems more?

- Access control and password control
    - Organizational fit of the employee
    - Access is a function of the role within the organization
    - Integrity of the person
    - Responsibility and authority structures must be defined first
    - Passwords assess depends on them
    - Formal structures must be addressed first

How can you assure proper resources are allocated to create authority and responsibility structures?

- High resources and high authority = good situation
    - Sufficient resources allocated properly
- Limited resources and limited authority = problem situation
    - No resources allocated to security or allocated incorrectly
- Limited resources and high authority = innovation
    - Look for creative ways to ensure good security
- High resources and limited authority = wastage
    - Hard to get security executed

Do you think authority and resource allocation come into play because of the unique characteristics of the organization?

- Yes, it's a function of organizational culture, management style, and leadership styles
- Leadership styles
    - Authoritative
    - Consultative
    - Delegate

There have been a lot of advances in encryption and secure communication. How do you ensure that these advances get inculturated into the corporation?

- Encryption algorithms
- Deterrents
    - Consequences of non-compliance
- Leadership commitment is needed
- Good governance
- High management commitment and high deterrence
    - High compliance
- Low management commitment and low deterrence
    - High vulnerability
- High management commitment and low deterrence

    - Sloppy management
- Low management commitment and high deterrence
    - Fear
    - Unhappy working
- Some reasons for subverting controls
    - Unhappy working conditions
    - Personal factors
    - Opportunity is there (broken process)

What are the three most important things for ensuring confidentiality, integrity, and availability of data?

- User involvement
    - Creating controls
    - Nuances of technical and formal controls
- Process integrity
- Resources and good resource allocation
- Low user involvement and bad process integrity
    - Bad security governance
- High user involvement and high process integrity
    - Good security governance
- High user involvement and low process integrity
    - Average security governance
    - Need to improve process integrity
- Low user involvement and high process integrity
    - Average security governance
    - Need to improve user involvement

How do you ensure you are complying with regulations?

- High user involvement and high process integrity = compliance
- Regulations are afterthoughts
    - Something went wrong in the past

How do you ensure total security? What are the takeaways from this conversation?

- Technical measures
    - Passwords
    - User access to data resources
    - Confidentiality
    - Integrity of data
    - Availability of data
- Proper responsibility and authority structures
- Integrity of people
    - Background checks
- Trust of people

    - Verify the trust
    - Ensure a trusting culture
- Ethics
    - Ensure good ethics
    - Follow ethical principles
- CIA and RITE

Social Video Outline:

What do you think is the most important element for managing security?

- People
    - take care of the needs of the people
- Good security culture
- RITE: responsibility, integrity, trust, ethicality of people

How do you mange the people and culture?

- Motivating and influencing people through good leadership
- Power of groups and management of security
- People relationships
- Positive and negative intentions

How does all of that relate to how security gets managed?

- Belief systems influence attitudes
- Security culture aspects
- Hospital example
    - Tracking nursing care time with patients
    - Resulted in disgruntled employees, which is bad for security
- Security problems can occur for several reasons
    - Work situation (disgruntled people)
    - Personal factors (divorce, addiction, etc.)
    - Opportunity (broken processes)

Are there any tools or techniques that can used to teach these kinds of social systems?

- Understand incoming silent messages from groups or organizations
    - Interpret and deal with negative messages
    - Group associations
    - How do you learn, defend yourself, interact with others, hobbies, etc?
    - There is a message emendating from the work situation
        - Understanding negative messages is critical to security

Dhillon Privacy Interview:

- Privacy
- Identity theft

Social and Emotional Intelligence Video Segment:

- Awareness of feelings
- Management of emotions
- Empathy
- Leader's emotional and social intelligence
- Enhancing leadership and culture

Technical Video Outline:

- Computer updates
- Viruses
- Secure email
- Malware
- Data backup
- Physical Security
- Encryption
- Passwords
- Firewalls
- Phishing
- Acceptable Internet Usage
- Acceptable Email Usage

Control Video Outline:

- Sexual harassment
- Anger Management

Appendix C: Information Security Training Videos

The training videos are large files and are available upon request from the author.

Appendix D: Raw Values to Common Form

Table D1: Socio-technical Group Common Form

Raw Data from Participant	Formatted in common form as wishes
Issue passwords to all employees.	ST1: I wish all employees were issued passwords
In order to get access, an employee must enter his or her password.	ST1: I wish passwords were required for access
Create your own network and upload all company computers with only needed for work software programs.	ST1: I wish the company would create its own network
	ST1: I wish company computers only had necessary software installed
Limit Internet access, remove unneeded software and hardware, such as USB ports.	ST1: I wish Internet access was limited
	ST1: I wish unnecessary software was removed
	ST1: I wish unnecessary hardware was removed
	ST1: I wish unnecessary USB ports were removed
All computers must be password protected, something as easy as screen saver passwords might deter an intruder.	ST1: I wish all computers were password protected
	ST1: I wish screen saver passwords were utilized
More data and overall executive powers should be available as employees get promoted.	ST1: I wish more data was available to promoted employees
	ST1: I wish more executive power was given to promoted employees
At the same time, the simple data available let's say to clerks should not be available to executives. Each person should deal and have access to the data needed for his or her job performance.	ST1: I wish data only be available to those that need it
I wish the company should have the right employee in the right place in the company.	ST2: I wish companies would correctly place employees
Integrity of the people in the organization, trust between the organization and the employees are more important than everything.	ST2: I wish employees had integrity
	ST2: I wish for trust between the organization and employees
The company should know that the employee is doing the right thing for the company.	ST2: I wish companies knew if employees were right for the company
Lack of commitment of the employee and lack of responsibility would make lower the success of the organization and also security of the system.	ST2: I wish companies would hire employees with high commitment and responsibility
Every organization should have technical, formal, and informal control systems.	ST2: I wish organizations had technical, formal, and informal control systems
Processes, procedures, rules should be clearly understood by the employees.	ST2: I wish processes, procedures, and rules were clearly understood by employees
One of the control systems cannot work alone so you need the mix of systems.	ST2: I wish organizations had a mix of control systems
The training that would be given to the employee should involve mutual trust.	ST2: I wish employees received training in mutual trust
Because success is going to come with employees. Employees need to trust the company.	ST2: I wish employees knew that trusting the company leads to success
Higher motivation with good incentives may help the company to gain good user involvement.	ST2: I wish companies used incentives and motivation to gain good user involvement

The company structure and good risk assessment would help the company to keep the balance of security.	ST2: I wish companies had good company structure and risk assessment
Educate employees about the importance of security. Make sure that they know that it will have a direct affect on their salaries and careers.	ST3: I wish employees were trained in the importance of security
	ST3: I wish employees were told security was related to their salaries and careers
Make sure people are familiar with the basic procedures, passwords, logging in, logging off, not sharing confidential data, and so forth.	ST3: I wish employees were familiar with basic procedures
	ST3: I wish employees were familiar with password policy
	ST3: I wish employees were familiar with procedures of logging in and logging off
	ST3: I wish employees were familiar with the policy of not sharing confidential data
Reward employees for notifying about any kind of lack of integrity in data and security systems.	ST3: I wish employees were rewarded for notifying management about data integrity breaches
	ST3: I wish employees were rewarded for notifying management about security breaches
Make sure that employees know that security is a serious issue and any kind of bad behavior will be punished.	ST3: I wish employees were notified about the seriousness of security
	ST3: I wish employees were punished for bad behavior
Make sure that employees well understand their level of access.	ST3: I wish employees understood their level of access
Good infrastructure, IDS, firewall.	ST4: I wish companies had a good infrastructure
	ST4: I wish companies had IDS
	ST4: I wish companies had firewalls
Good policy allowing people to do what they need to do and still be secure and have integrity.	ST4: I wish companies had policies that allowed people to effectively work while maintaining security and integrity
Integrity of database/protection against intrusion through database (like SQL injection).	ST4: I wish companies protected the integrity of databases from intrusion
Secure web server.	ST4: I wish companies secured their web servers
Get good people through screening.	ST4: I wish companies hired good people by screening them
Set up controls = corporate policies and standards	ST4: I wish companies used policies and standards to set up controls
People awareness about security and how it affects its surroundings.	ST4: I wish employees were aware of security
Ethics – people need to be ethical and trusting.	ST5: I wish employees were ethical
	ST5: I wish employees were trustworthy
Consequences of non-compliance (fear).	ST5: I wish there were consequences for non-compliance
Situations outside of the obvious, for example blackberry security.	ST5: I wish companies were aware of less obvious threats, such as blackberries
Roles and responsibilities (formal). For example, supervisor approves refunds in excess of $2500.	ST5: I wish companies set up proper roles and responsibilities
Resources – structure of compliance team. Let people know that corporate security is more than one person in a cubicle.	ST5: I wish employees were notified that security was more than just one person
Why? – Reasons for security. Explain to end users who do not always see the benefit or consequence.	ST5: I wish employees were taught the benefits and consequences of security
Make computer settings so that no information is remembered or can be.	ST6: I wish computers were set to not remember information
Use fingerprints or iris scanning for actual access to localities with sensitive data.	ST6: I wish fingerprints or retinal scans were used to access sensitive data

Employee audits, activity tracking, monitor suspicious activities without instilling distrust.	ST6: I wish employees were audited, activity tracked, and monitored without instilling distrust
Background checks for crimes or dishonesty	ST6: I wish background checks were utilized
Make sure users are informed.	ST6: I wish employees were informed
Single design so that employees are aware of when something is awry.	ST6: I wish single design was utilized so employees would recognize when something is wrong
Make clear provisions as to who is allowed in what.	ST6: I wish employees were clear as to who had access to what
Constantly checking for system glitches, have friendly hacking identify potential weaknesses and hesitations to system entry.	ST6: I wish there was constant checking for system glitches
	ST6: I wish "friendly hacking" was used to identify weaknesses
Make security tight but not to the point of compromising work quality.	ST6: I wish security could be strong without compromising work quality
Reinforce ethics. There is no need for any of this if people are not compelled to do unethical things.	ST6: I wish ethics were stressed
Assign proper knowledge outlets who should know what and why.	ST6: I wish there were knowledge outlets identifying who should know what and why
Keep automated systems limited. People get very use to the way things ought to be.	ST6: I wish automated systems were limited
Who is allowed to view certain types of information – is it getting to the right place?	ST7: I wish data was only viewable to the appropriate people
Who can modify this information – like personal records in case of, for example, hospital and patient information?	ST7: I wish there were rules in place to identify those allowed to modify data
Who can read or go into personal computers.	ST7: I wish there were rules identifying who had access to computers
Can you share information, for example, in many companies in "development and research department for new products?" Are they allowed to email or share facts?	ST7: I wish there were confidentiality policies
What information is expected of me to know and I am responsible for.	ST7: I wish there were clearly defined roles of responsibilities
I wish there were a clear set of rules or guidelines to follow in the case of security information. What does the organization expect?	ST7: I wish employee expectations were clearly defined.
	ST7: I wish there were clearly defined rules
	ST7: I wish there were defined expectations regarding the security of information
The video should stay away from abstractions. Clear, concise, colorful examples demonstrating IT security issues.	ST8: I wish employees were trained with clear, concise, colorful examples of IS security
Make the video as visually stimulation as possible.	ST8: I wish employees were trained with visually stimulating videos
Force the viewer to answer questions at the conclusion of each example case or scenario.	ST8: I wish trainees were asked questions regarding topics demonstrated in the training video
Emphasize individual integrity in the video as much as possible.	ST8: I wish employees were taught about individual integrity
Incorporate existing management in the video, which may resonate more with the viewer.	ST8: I wish management was used in training videos
Make a series of videos demonstrating basic advanced cases on security for the various roles in the organization.	ST8: I wish there were training for the various roles in the organization
Don't speak overly technical, keep it simple and short.	ST8: I wish training were not too technical
	ST8: I wish training were kept simple and short
Put the viewer in the shoes of the actor in the video.	ST8: I wish training put the viewer in the shoes of the actor in the video

Understand what data will be monitored by IT and how it will be used.	ST9: I wish there were rules for what data are monitored
	ST9: I wish there were rules for how data is used
Understand corrective actions that will be taken for violation of policies (suspension, termination, etc.).	ST9: I wish punishment were clearly defined for violations
Understand what constitutes inappropriate use of computers and how it can be used personally.	ST9: I wish there were computer usage policies
Understand that there is a "need to know" for data and by being an employee you do not necessarily have full access to everything.	ST9: I wish there were data access policies limiting access to those that need the data
Understand that business is not to be conducted on non-company (i.e. personal) computers or cell phones.	ST9: I wish there were a policy prohibiting company business on personal computers or cell phones
Understand that updated software will be pushed to your company machine and software will not be installed without permission.	ST9: I wish computers were updated regularly
	ST9: I wish there were a policy limiting the installation of software without permission
Understand where policies and procedures are posted, who owns them, and how to make or suggest changes.	ST9: I wish employees were notified as to where policies and procedures were posted
	ST9: I wish employees were notified as to how to suggest changes to policies and procedures
Employees should be well trained in high security areas.	ST10: I wish employees in high security areas are well trained
There should be limited access to secure areas.	ST10: I wish there were limited access to secure areas
The organizational structure should be formed in a way that designates proper access to appropriate people.	ST10: I wish organizational structure designated proper access to the appropriate people
The company should demonstrate ways to eliminate opportunities for broken processes.	ST10: I wish companies worked to eliminate broken processes
The change process should be so that employees know exactly what to expect and embrace it accordingly.	ST10: I wish employees knew what to expect with a change process and embraced it
A demonstration of regulatory compliance should be covered.	ST10: I wish regulation compliance was covered with employees
Total security process should include a very thorough pre-employment process to eliminate any potential risks.	ST10: I wish employees were screened before hiring
Communication should be formal and streamlined so that there is no confusion coming if the communication from that person is not clear. That person would be the one to correct any misunderstandings.	ST10: I wish corporate communication were clear and concise, eliminating confusion

Table D2: Social Group Common Form

Raw Data from Participant	**Formatted in common form as wishes**
Importance of customer privacy.	S1: I wish security training included the importance of customer privacy
How to handle correspondence (e-mail) appropriately.	S1: I wish security training included how to handle email appropriately
What information to release and what information to withhold from 3rd parties.	S1: I wish security training included confidentiality of information from outside parties
How to secure your own data, lock your systems.	S1: I wish security training included personal data security
While you are away from your computer, do not leave private information out and unattended.	S1: I wish security training included physical security of data around employee computers
How to handle the media when applicable.	S1: I wish security training included how to handle the media
I would like to see less online tutorial based training.	S2: I wish security training were not online training
I would like to see more hands on or actual interaction	S2: I wish security training were hands on

with real security issues.	S2: I wish security training included interaction with real security issues
I would like to see more education given to protecting home personal computer users or the "average" computer user.	S2: I wish security training included how to protect home computers
I would like to see password security strengthened. Current organizations require too many, so people write them down.	S2: I wish security training included password strengthening that minimized writing down passwords
I would like to see more average and novice computer training given to employees. I think general computer knowledge would have a positive impact on overall security.	S2: I wish security training included novice and beginner training
Continuing education as trends change.	S2: I wish security training included continuing education as threats change
Needs to be current, like bleeding edge current, or else something will get the upper hand.	S3: I wish security training should be current and cutting edge
Needs to make good points that seem relevant to employees.	S3: I wish security training included points relevant to employees
Go over the most common security threats and train how to prevent them.	S3: I wish security training included the most common threats and how to prevent them
Clearly explain rights, especially corporate e-mail, privacy, etc. Leave no loophole.	S3: I wish security training included corporate email privacy rights
I wish they would actually demonstrate the consequences of a security breach.	S4: I wish security training included the consequences to the company of security breaches
I wish the training was not so technically specific. Not everyone is computer minded.	S4: I wish security training was not too technical
I wish they would actually explain why it was necessary to have a security policy.	S4: I wish it were explained why a security policy were necessary
I wish they would convey that a person's "mood" actually affects their decision making ability.	S4: I wish it were explained that a person's mood affects decision making
Contrary to previous statements, I wish they would put the "fear of God," or express the importance of proper information security decisions on a personal level.	S4: I wish the importance of security were stressed to employees
Above all, convey that people do make mistakes and let them know it is not the end of the world.	S4: I wish employees were told that people do make mistakes and it is not the end of the world
I believe security awareness training should include a description of the corporation's values and what it expects of its employees regarding ethical and moral issues.	S5: I wish security training included a description of corporate values
	S5: I wish security training included expectations of employee moral values
	S5: I wish security training included expectations of employee ethical values
In addition to the technical and legal aspects of security training, it should include some of the factors that contribute or facilitate security incidents, such as employee dissatisfaction, and other relevant factors that could affect an employee's decision.	S5: I wish security training included technical aspects
	S5: I wish security training included legal aspects
	S5: I wish employee dissatisfaction related to security were addressed
	S5: I wish factors affecting employee decision making were addressed
The thought process of the individual from different cultural backgrounds.	S6: I wish cultural backgrounds were taken into consideration
How peer pressure can affect one's perceptions.	S6: I wish peer pressure were considered
How managers can help in providing the awareness.	S6: I wish managers were involved in providing awareness
Values include greater privacy and privacy protection training. Greater understanding of how user actions affect overall security within an organization needs to be	S7: I wish security training included privacy training
	S7: I wish security training included consequences to corporations for and individuals inappropriate actions

better knowledge to know the consequence or reaction of your actions.	
Also, security awareness training in a format that the less technical user can comprehend and is interested in.	S7: I wish security training interested the less technical user
I believe the emotional intelligence dimension should be used. In the book, there are four competencies, two deal with personal, 2 deal with social. A person needs to understand how people view them and also understand their personal background.	S8: I wish security training included emotional intelligence
I believe in order to prevent security issues, one must be taught values of high integrity and they must know the importance of them.	S8: I wish security training included values of high integrity
Give examples of how firms that suffered security issues or incidents and show how it damaged the firm and people. This may scar or create a sensitive feeling for the trainee.	S8: I wish security training included real examples of incidents and the damage caused
Highlight the importance of security within the firm and show how it is top importance. This may veer potential threats away.	S8: I wish security training stressed the importance of security
I would like to see more information based concepts included in security awareness programs. Identity theft and more importantly secure company information theft is a large problem faced by many corporations. This topic should be the main focus of the training and also should include: Social interactions between companies and individuals (how that can negatively affect security), cultural differences in security technology data protection, levels of sophistication differences, employee interactions and use of system applications.	S9: I wish security training included identity theft
	S9: I wish security training included corporate information theft
	S9: I wish security training included social interaction between companies and individuals
	S9: I wish security training included cultural differences
	S9: I wish security training acknowledged the various levels of sophistication
	S9: I wish security training included data protection
	S9: I wish security training included appropriate employee usage of applications
The security awareness is different in my life and the workplace. My value in my life is basically the political and economic environments. As a Taiwanese, the political issue of China and Taiwan is the big issue. The economic environment also puts the stress into the daily life. In the workplace, in traditional Taiwan culture, the female position always has been un-balanced with males. The security training I wish that it would focus on the value of the culture transition and the female value in employee value.	S10: I wish security training considered culture (not corporate culture)
	S10: I wish security training considered sex (male\female)

Table D3: Technical Group Common Form

Raw Data from Participant	Formatted in common form as wishes
The suggestions for passwords were very helpful. We are required to change our password every 60 days, but there are very few requirements.	T1: I wish there were stricter requirements for passwords
The phishing piece was good. Well known (the scams) but good to see it frequently.	T1: I wish there was phishing training available to employees
Storing data backups: it never occurred to me to keep backups in a separate location.	T1: I wish there was backup training available to employees
Virus scan part was good too. I didn't know that weekly patches were available.	T1: I wish there was virus training available to employees

	T1: I wish virus updates were known to employees
Security awareness should be interactive rather than just plain video presentation to help answer any questions or concerns the viewers may have regarding the topic.	T2: I wish security awareness training were interactive with someone to answer questions
Little more awareness could be given on viruses, worms, spam, etc. which will help the tech support maintenance efforts.	T2: I wish virus training were more in depth
	T2: I with worm training were more in depth
	T2: I wish spam training were more in depth
Email security should also include topics like avoiding "reply all" whenever possible, threats from "pharming," just like "phishing."	T2: I wish email security was included in training
	T2: I wish pharming training were available (like phishing)
Employees should be made aware of protecting passwords in a safe place and not sharing company information with outside people.	T2: I wish password protection were included in training
	T2: I wish there were policies about confidentiality of information
Email and web surfing monitoring policies should be explained in detail.	T2: I wish email policies were adequately explained to employees
	T2: I wish Internet policies were adequately explained to employees
As for email communication, I think the security awareness training should also mention those attachment files which are highly possible to have viruses, such as .exe, website links, and compressed files.	T3: I wish security training included the risk of e-mail attachments
	T3: I wish security training included the risk of web links
	T3: I wish security training included the risk of e-mail compressed files
Users should be taught to delete any other email addresses displayed in the specific email when users are forwarding it.	T3: I wish security training included deleting previous recipients email addresses on forwarded emails
I wish security awareness training was simplistic.	T4: I wish security training were simplistic
I wish it entailed actual examples of past events and the consequences as a result of negligent actions.	T4: I wish training included past examples and consequences to the company
I wish employees could see the real harm and financial recovery and protection cost for security awareness.	T4: I wish training informed employees of the cost of security awareness
Perhaps it would help them to adopt a mindset of "this is a critical issue."	T4: I wish training could change the mindset of employees to make them aware of "critical issues"
I wish the training would provide the basic abc's of data protection and the greatest threats against such data.	T4: I wish training taught the basics of data protection
	T4: I wish training taught the greatest threats to data
I wish that security awareness training was more concise and gave clear reference points for employees to access help after training.	T4: I wish training were concise
	T4: I wish training provided employees with ways to get help after the training (reference points)
Stress management.	T5: I wish security training included stress management
Corporate values.	T5: I wish security training included corporate values
Security policies and procedures.	T5: I wish security training included security policies
	T5: I wish security training included security procedures
Filters/audits.	T5: I wish security training included filters
	T5: I wish security training included audits
Email security.	T5: I wish security training included email security
Antiviral software.	T5: I wish security training included antivirus software
Encryption.	T5: I wish security training included encryption
Internet navigation – spyware.	T5: I wish security training included Internet navigation
	T5: I wish security training included spyware
Password training.	T5: I wish security training included password training
Device hardware security.	T5: I wish security training included device hardware security
Backup databases.	T5: I wish security training included database backup
Appropriate storage facilities.	T5: I wish security training included appropriate storage

	facilities
Adverse affects financial etc.	T5: I wish security training included the adverse affects of bad security
I believe there could be more hands-on workshops, such as how to use the TrueCrypt software to encrypt confidential files. It would be much more effective to show employees the importance of IT security through a hands-on approach.	T6: I wish security training included hands on workshops
I wish training should have more in depth training so I can understand all issues and I also wish it showed how to avoid it means how I practically do it at work, or home to be a victim of security breach.	T7: I wish security training were more in-depth
	T7: I wish security training demonstrated all issues and ways to avoid them
I also wish that before starting IT security training, they should consider audience level of knowledge about security.	T7: I wish trainee knowledge level were taken into consideration before training
First thing that should be included in such a video is the physical security that is provided at the workplace.	T8: I wish security training included physical security
There should be a detailed explanation of what needs to be done in case of different types of emergencies.	T8: I wish security training included appropriate responses to various emergencies
The different aspects of the online security. Things that need to be included are what are the different online threats and how to effectively deal with those.	T8: I wish security training included online threats and how to deal with them.
Full hard disk encryption.	T9: I wish security training included full hard disk encryption
Exercise every year to make sure that data from backup devices can be retrieved.	T9: I wish security training stressed the importance of annual backup recovery practice to make sure it works
Keep 2 backups in physically separated places, far away, east coast vs. west coast.	T9: I wish security training included the need to keep more than one backup separated physically
Email encryption always.	T9: I wish security training included email encryption
Use of VPN while out from secured network.	T9: I wish security training included the usage of VPN's when out of the office
Create security culture.	T9: I wish security training included creating a security culture
Define roles and responsibilities.	T9: I wish security training defined roles and responsibilities
Handle cultural issues which may impact security standards.	T9: I wish security training included how to handle cultural issues that may affect security
Security awareness training needs to be based on details specific to the company and utilize company specific examples. If this is not possible industry specific training should be used. People tend to tune out when shown generic videos.	T10: I wish security training included company or industry specific examples
Also, strictly showing a video is a poor way to get across any type of training. Training should be as interactive as possible.	T10: I wish security training included were interactive
Another important factor is humor. Humor if properly used can leave a lasting impression on an audience without losing the point your making.	T10: I wish security training included humor for a lasting impression
Using bright imagery also helps.	T10: I wish security training included bright imagery

Table D4: Control Group Common Form

Raw Data from Participant	Formatted in common form as wishes
It is important to have some sort of interaction with the audience ala the first session, not just to be lectured to as in the second session or with an interview don by a perhaps celebrity DJ.	C1: I wish security training included interaction with trainees
It is also important for the person giving the training to have some legit credentials and to look the part.	C1: I wish trainers had appropriate credentials and looked the part
It is not as important to emphasize the negatives or punishments of breaking or lax security. It is much more important to stress the benefits achieved.	C1: I wish training emphasized the benefits of following security policy, instead of emphasizing the punishment or negatives of not following security policy
I wish they would be informative on past security breaches.	C2: I wish security training included examples of past security breaches
I wish they would say what to do when security is breached (guidelines on reporting).	C2: I wish security training included guidelines for reporting security breaches
I wish they would train on how to handle incidents.	C2: I wish security training included how to handle incidents
What happens/consequences?	C2: I wish security training included consequences of security breaches
If it is confidential.	C2: I wish security training included confidentiality
I think that there needs to first be a demonstration on what computer security awareness is.	C3: I wish security training included demonstrations
I feel that computer security awareness training should show breaches of security.	C3: I wish security training included examples of breaches
I feel it should show how security is performed properly.	C3: I wish security training demonstrated how to properly perform security
To end the training, there should be a shorts segment to summarize what was learned.	C3: I wish security training included a summary of what was taught
Role of security and security awareness. Aspects of security awareness.	C4: I wish security training included the role of security
Benefits and challenges of security awareness.	C4: I wish security training included the benefits and challenges of security
Consequences of poor security awareness.	C4: I wish security training included corporate consequences of bad security
Personalize the issues to me role in the workplace.	C4: I wish security training included personalization to a particular role in the company
Speeches of security at my workplace.	C4: I wish security training included lectures at the workplace
Training must be strong and interactive.	C4: I wish security training were strong
	C4: I wish security training were interactive
Past examples of security issues at my workplace.	C4: I wish security training included examples from the trainee's workplace
Punishments of noncompliance.	C4: I wish security training included punishments for non-compliance
Common security holes, downloading of files from company computers, taking home company files via email, flash drive, CD, etc.	C5: I wish security training included common security vulnerabilities
	C5: I wish security training included Internet policy
	C5: I wish security training included policy taking home corporate information via email attachment
	C5: I wish security training included policy taking home corporate information via portable media
Physical access to the building.	C5: I wish security training included physical security
Do not hand out your ID.	C5: I wish security training included policy on corporate

	ID's
Security is everyone's job, not just IT. Be realistic in your assumptions.	C5: I wish security training stressed the importance of everyone being involved
Do not dumb it down to the point of being insulting, but don't talk over their heads either.	C5: I wish security training taught at the level of the trainee
Don't make policies so strict that employees feel distrusted.	C5: I wish security was not so strict that employees felt distrusted
Recognize that they will use the Internet for personal business and plan for that.	C5: I wish it was recognized that employees were going to use the Internet for personal use
Keep it interesting and keep the employees involved, short and to the point.	C5: I wish security training were interesting
Maintaining secure email account enables a sexually harassed employee to know there is verification and evidence of the harassment they suffered.	C6: I wish security training included email policy
People need to be aware of their actions and consequences thereof.	C7: I wish security training included employee consequences
I wish people respected privacy of others at the office as this seems to lead to problems.	C7: I wish security training included personal privacy of others at the office
I wish people would do less inappropriate things on the Internet during business hours; it is distracting and could get us in trouble.	C7: I wish security training included and Internet policy
People do not do a good job of protecting company information when they leave the office (i.e. leave their computer logged on). Others could damage the company and us wind up in a lawsuit.	C7: I wish security training included physical security of their workstations
Anti-virus software.	C8: I wish training covered anti-virus software
Password identification.	C8: I wish training included password protection
Firewall software.	C8: I wish training included firewall configuration
Information and data backup.	C8: I wish training included data backup
Consistent security policy.	C8: I wish training included consistent security policy
Published formal standard.	C8: I wish there was a published formal standard
Host network intrusion detection.	C8: I wish training included host network intrusion detection
Ethics Training.	C8: I wish training included ethics training
Control of workstation.	C8: I wish training included workstation control
Encourage violations reporting.	C8: I wish training included violation reporting
Knowledge basics of computers and networking. Discuss Internet Protocol, routing, Domain Name Service, access points, firewalls, and other network devices.	C9: I wish training included firewalls
	C9: I wish training included Internet Protocols
	C9: I wish training included Domain Name Service
	C9: I wish training included Access Points
Cover the basics of cryptography, security management, and wireless networking.	C9: I wish training included encryption
	C9: I wish training included security management
	C9: I wish training included wireless networking
Give managers and other employees "how to develop security policies," like ethical code of conduct, employee's disciplines, basic activities to keep computer network safe (passwords secrecy).	C9: I wish training included ethical conduct
	C9: I wish training included passwords
Give knowledge about threats and problems that a network may face, such as hacking, social engineering, virus attack, network failure, etc.	C9: I wish training included hacking threats
	C9: I wish training included social engineering
	C9: I wish training included virus attacks
	C9: I wish training included network failures
Now the tools to tackle them such as antivirus, good configuration, contingency planning, etc. Good idea would be to give students some topics of security of	C9: I wish training included contingency planning
	C9: I wish training included special training, such as CCNA, CCNP, MCSC, and Linux

courses like, CCNA, CCNP, MCSC (window's server) and Linux. This will help students how to configure secured network and tools to tackle when failure occurs.	
Virus – use of genuine antivirus (no pirated versions). Keep the anti-virus updated.	C10: I wish training included virus training
Do not ask and store information from the customers that you do not require. For example, if your industry type does not need the social security number of the customers, don't ask for it.	C10: I wish training included customer data confidentiality
	C10: I wish training included a policy to only keep necessary customer information
Do not download random files from the Internet, especially movies or videos.	C10: I wish training included acceptable Internet usage
Password training – use a strong password (no date of birth, name, etc.) instead a mix of numbers and alphabets. Keep changing the password frequently. Do not share your passwords with others.	C10: I wish training included strong password training
All company information should be discussed via company emails and equipment only.	C10: I wish training included a policy about not using personal emails or devices for company data
When someone sends a reply it would be better if they sent it without the attachment which has been previously snet so that mail boxes don't get clogged.	C11: I wish training discusses email attachments
	C11: I wish training taught employees to not send attachments back to the original sender when replying to emails
Setting up and updating of proper antivirus systems.	C11: I wish training included antivirus training and scanning
Set screen saver passwords when leaving the desk. Set up automatic configuration of screen saver passwords.	C11: I wish training taught employees to use screen saver passwords
Password change periodically, including bios passwords.	C11: I wish training included a policy about changing BIOS passwords frequently
Protection from SPAM.	C11: I wish training included protection from SPAM

Appendix E: Group Clustering

Table E1: Socio-Technical Group Clustering

ST3: I wish employees were rewarded for notifying management about data integrity breaches	Ensure a reward system for disclosing security breaches
ST3: I wish employees were rewarded for notifying management about security breaches	
ST5: I wish employees were ethical	Ensure appropriate ethics training
ST6: I wish ethics were stressed	
ST5: I wish employees were trustworthy	Ensure a trust relationship between employees and the company
ST2: I wish for trust between the organization and employees	
ST2: I wish employees received training in mutual trust	
ST2: I wish employees knew that trusting the company leads to success	
ST2: I wish employees had integrity	Ensure training covers employee integrity
ST8: I wish employees were taught about individual integrity	
ST2: I wish companies would correctly place employees	Ensure employees are a good fit for the position before they are hired
ST2: I wish companies knew if employees were right for the company	
ST2: I wish companies would hire employees with high commitment	Ensure the hiring of committed employees
I wish companies would hire responsible employees	Ensure the hiring of responsible employees
ST4: I wish companies hired good people by screening them	Ensure potential employees are screened before hiring
ST6: I wish background checks were utilized	
ST10: I wish employees were screened before hiring	
ST3: I wish employees were punished for bad behavior	Ensure employees are aware of consequences of non-compliance
ST5: I wish there were consequences for non-compliance	
ST9: I wish punishment were clearly defined for violations	
ST7: I wish data was only viewable to the appropriate people	Ensure data access is limited to appropriate individuals
ST9: I wish there were data access policies limiting access to those that need the data	
ST1: I wish data only be available to those that need it	
ST3: I wish employees understood their level of access	
ST6: I wish employees were clear as to who had access to what	
ST7: I wish there were rules in place to identify those allowed to modify data	
ST7: I wish there were rules identifying who had access to computers	Ensure rules to identify who has appropriate access to computers
ST10: I wish organizational structure designated proper access to the appropriate people	Ensure organizational structure designates proper access to the appropriate people
ST1: I wish more data was available to promoted employees	Ensure promoted employees have more access to data
ST8: I wish employees were trained with clear, concise, colorful examples of IS security	Ensure examples are fully utilized in security training

ST8: I wish employees were trained with visually stimulating videos	Ensure training with visually stimulating videos
ST8: I wish trainees were asked questions regarding topics demonstrated in the training video	Ensure trainees are asked questions to verify understanding of training concepts
ST8: I wish management was used in training videos	Ensure management appears in training videos
ST8: I wish there were training for the various roles in the organization	Ensure training is appropriate for the various roles within the organization
ST8: I wish training were not too technical	Ensure training is not too technical
ST8: I wish training were kept simple and short	Ensure training is simple and short
ST8: I wish training put the viewer in the shoes of the actor in the video	Ensure video training attempts to put the trainee in the shoes of the actor
ST1: I wish company computers only had necessary software installed	Ensure only appropriate software is installed on corporate computers
ST1: I wish unnecessary software was removed	
ST9: I wish there were a policy limiting the installation of software without permission	Ensure there are software installation polices in place
ST2: I wish organizations had technical, formal, and informal control systems	Ensure a mix of the technical, formal, and informal control systems
ST2: I wish organizations had a mix of control systems	
ST6: I wish security could be strong without compromising work quality	Ensure the highest security while minimizing effects on employee's ability to work effectively
ST4: I wish companies had policies that allowed people to effectively work while maintaining security and integrity	
ST6: I wish employees were audited, activity tracked, and monitored without instilling distrust	
ST3: I wish employees were familiar with basic procedures	Ensure clearly defined roles and responsibilities
ST7: I wish there were clearly defined roles of responsibility	
ST5: I wish companies set up proper roles and responsibilities	
ST7: I wish employee expectations were clearly defined.	
ST7: I wish there were defined expectations regarding the security of information	
ST7: I wish there were clearly defined rules	
ST3: I wish employees were familiar with the policy of not sharing confidential data	Ensure data confidentiality policies are in place
ST7: I wish there were confidentiality policies	
ST9: I wish there were a policy prohibiting company business on personal computers or cell phones	Ensure there is a policy concerning company business on personal computers
ST9: I wish there were a policy prohibiting company business on personal cell phones	Ensure there is a policy concerning company business on personal cell phones
ST1: I wish the company would create its own network	Ensure companies create their own networks
ST1: I wish Internet access was limited	Ensure there is an Internet usage policy
ST1: I wish unnecessary hardware was removed	Ensure unnecessary hardware, including USB ports, are removed from computers
ST1: I wish unnecessary USB ports were removed	
ST1: I wish more executive power was given to promoted employees	Ensure promoted employees are given more executive powers
ST2: I wish processes, procedures, and rules were clearly understood by employees	Ensure employees clearly understand processes, procedures, and rules
ST2: I wish employees received training in motivation	Ensure employees receive motivation training
ST2: I wish employees received training in commitment	Ensure employees receive commitment training
ST2: I wish employees knew that and end user commitment leads to success	
ST2: I wish companies used incentives and motivation to gain good user involvement	Ensure user involvement through incentives and motivation

ST2: I wish companies had good company structure	Ensure companies have proper structure
ST2: I wish companies had good risk assessment	Ensure companies have proper risk assessment
ST3: I wish employees were trained in the importance of security	Ensure employees understand the importance of security
ST3: I wish employees were notified about the seriousness of security	
ST4: I wish employees were aware of security	
ST5: I wish employees were taught the benefits of security	
ST3: I wish employees were told security was related to their salaries and careers	Ensure employees are told security is related to their salaries and careers
ST3: I wish employees were familiar with procedures of logging in and logging off	Ensure employees are trained on logging on and off computers
ST4: I wish companies had a good infrastructure	Ensure companies have a good infrastructure
ST4: I wish companies had IDS	Ensure companies properly use intrusion detection systems (IDS)
ST4: I wish companies had firewalls	Ensure companies properly use firewalls
ST4: I wish companies secured their web servers	Ensure companies have secure web servers
ST4: I wish companies used policies and standards to set up controls	Ensure companies use policies and standards to set up controls
ST4: I wish companies protected the integrity of databases from intrusion	Ensure companies protect databases from intrusion
ST5: I wish companies were aware of less obvious threats, such as blackberries	Ensure companies are aware of less obvious threats, such as personal portable devices
ST5: I wish employees were notified that security was more than just one person	Ensure employees are aware that security is everyone's responsibility and not just an individual
ST5: I wish employees were taught the corporate consequences of bad security	Ensure employees are given examples of corporate consequences of bad security
ST6: I wish computers were set to not remember information	Ensure computers are set to not remember information
ST6: I wish fingerprints or retinal scans were used to access sensitive data	Ensure the use of fingerprints or retinal scans to protect sensitive data
ST10: I wish there were limited access to secure areas	Ensure limited physical access to secure areas
ST6: I wish employees were informed	Ensure employees are informed
ST6: I wish single design was utilized so employees would recognize when something is wrong	Ensure the utilization of single design
ST6: I wish there was constant checking for system glitches	Ensure constant checking for system glitches
ST6: I wish "friendly hacking" was used to identify weaknesses	Use "friendly hacking" to identify security weaknesses
ST6: I wish there were knowledge outlets identifying who should know what and why	Create knowledge outlets identifying who should know what and why
ST6: I wish automated systems were limited	Limit the use of automated systems
ST9: I wish there were rules for what data are monitored	Define what data is to be monitored
ST9: I wish there were rules for how data is used	Define rules as to how data is used
ST9: I wish there were computer usage policies	Create acceptable computer usage policies
ST9: I wish computers were updated regularly	Ensure computers are updated regularly
ST9: I wish employees were notified as to where policies and procedures were posted	Ensure employees are aware of where they can access policies and procedures
ST9: I wish employees were notified as to how to suggest changes to policies and procedures	Ensure employees know how to suggest changes to policies and procedures
ST10: I wish employees in high security areas are well trained	Ensure employees in high security areas are well trained
ST10: I wish companies worked to eliminate broken processes	Ensure companies work to eliminate broken processes
ST10: I wish employees knew what to expect with a change	Ensure employees understand what to expect with a

process and embraced it	change process
ST10: I wish regulation compliance was covered with employees	Ensure employees understand regulation compliance
ST10: I wish corporate communication were clear and concise, eliminating confusion	Ensure corporate communication is clear and concise

Table E2: Social Group Clustering

S1: I wish security training included how to handle email appropriately	Ensure in-depth training on acceptable email use
S3: I wish security training included corporate email privacy rights	
S2: I wish security training were not online training	Minimize the use of online training
S2: I wish security training included novice and beginner training	Ensure training is appropriate for the trainee's level of expertise
S7: I wish security training interested the less technical user	
S9: I wish security training acknowledged the various levels of sophistication	
S4: I wish security training was not too technical	
S3: I wish security training should be current and cutting edge	Ensure training is up to date with current security issues
S6: I wish managers were involved in providing awareness	Ensure managers are involved in providing training
S2: I wish security training were hands on	Ensure hand's on training
S3: I wish security training included points relevant to employees	Ensure training is relevant to all employees
S2: I wish security training included interaction with real security issues	Ensure training utilizes real world examples, including the corporate consequences of bad security
S4: I wish security training included the consequences to the company of security breaches	
S7: I wish security training included consequences to corporations for and individuals inappropriate actions	
S8: I wish security training included real examples of incidents and the damage caused	
S3: I wish security training included corporate email privacy rights	Ensure training covers privacy rights
S7: I wish security training included privacy training	
S1: I wish security training included the importance of customer privacy	
S9: I wish security training included cultural differences	Ensure training considers employee cultural differences
S10: I wish security training considered culture (not corporate culture)	
S6: I wish cultural backgrounds were taken into consideration	
S5: I wish employee dissatisfaction related to security were addressed	Ensure training addresses how employee dissatisfaction affects security
S5: I wish factors affecting employee decision making were addressed	Ensure training addresses factors affecting employee decision making
S4: I wish it were explained that a person's mood affects decision making	
S6: I wish peer pressure were considered	
S1: I wish security training included confidentiality of information from outside parties	Ensure training includes confidentiality policy
S1: I wish security training included personal data security	Ensure training covers personal data security

S1: I wish security training included how to handle the media	Ensure security training includes how to handle the media
S1: I wish security training included physical security of data around employee computers	Ensure training addresses physical security, including employee work spaces
S2: I wish security training included how to protect home computers	Ensure training addresses protecting employee's home computers
S2: I wish security training included continuing education as threats change	Ensure training includes continuing education as threats change
S2: I wish security training included password strengthening that minimized writing down passwords	Ensure training addresses strong passwords while minimizing the need to write them down
S3: I wish security training included the most common threats and how to prevent them	Ensure training covers the most common threats and how to prevent them
S4: I wish it were explained why a security policy were necessary	Explain why security policies are necessary
S4: I wish the importance of security were stressed to employees	Ensure the importance of security is addressed with all employees
S4: I wish employees were told that people do make mistakes and it is not the end of the world	Ensure employees are told that making mistakes is alright
S5: I wish security training included a description of corporate values	Ensure training describes corporate values
S5: I wish security training included expectations of employee moral values	Ensure training addresses employee moral
S5: I wish security training included expectations of employee ethical values	Ensure training addresses employee ethics
S5: I wish security training included technical aspects	Ensure training includes technical aspects
S5: I wish security training included legal aspects	Ensure training covers legal aspects of security
S8: I wish security training included emotional intelligence	Ensure training addresses the relationship between emotional intelligence and security
S8: I wish security training included values of high integrity	Ensure training addresses employee integrity
S8: I wish security training stressed the importance of security	Ensure employees are aware of the importance of good security
S9: I wish security training included identity theft	Include identity theft in security training
S9: I wish security training included corporate information theft	Ensure training addresses corporate information theft
S9: I wish security training included social interaction between companies and individuals	Ensure training addresses the social interaction between companies and individuals
S9: I wish security training included data protection	Ensure training addresses data protection
S9: I wish security training included appropriate employee usage of applications	Ensure training address acceptable software usage policy
S10: I wish security training considered sex (male/female)	Ensure training takes into consideration an employee's gender

Table E3: Technical Group Clustering

T1: I wish there were stricter requirements for passwords	Ensure training includes strict password policy
T2: I wish password protection were included in training	
T5: I wish security training included password training	
T2: I wish security awareness training were interactive with someone to answer questions	Ensure interactive training
T10: I wish security training included were interactive	
T4: I wish security training were simplistic	Ensure simplistic training

T4: I wish training were concise	Ensure concise training
T7: I wish security training were more in-depth	Ensure in-depth training
T7: I wish trainee knowledge level were taken into consideration before training	Ensure training to the knowledge level of the trainee
T10: I wish security training included humor for a lasting impression	Ensure humor is included in training
T10: I wish security training included bright imagery	Ensure training includes bright imagery
T6: I wish security training included hands on workshops	Ensure hands on training
T4: I wish training included past examples and consequences to the company	Ensure training includes company or industry past examples of security breaches
T5: I wish security training included the adverse affects of bad security	
T10: I wish security training included company or industry specific examples	
T2: I wish email security was included in training	Ensure training includes email acceptable use policy
T2: I wish email policies were adequately explained to employees	
T5: I wish security training included email security	
T3: I wish security training included the risk of e-mail compressed files	Ensure email training includes the risk of attachments
T1: I wish virus updates were known to employees	Ensure in-depth virus and worm training
T1: I wish there was virus training available to employees	
T2: I wish virus training were more in depth	
T5: I wish security training included antivirus software	
T2: I wish worm training were more in depth	
T3: I wish security training included the risk of e-mail attachments	Ensure email training includes the risk of attachments
T3: I wish security training included the risk of web links	Ensure training includes the risk of web links
T9: I wish security training included full hard disk encryption	Ensure training includes hard disk encryption
T9: I wish security training included email encryption	Ensure training includes email encryption
T5: I wish security training included encryption	Ensure training includes encryption
T4: I wish training taught the basics of data protection	Ensure training includes data protection
T4: I wish training taught the greatest threats to data	
T9: I wish security training stressed the importance of annual backup recovery practice to make sure it works	Ensure training stresses annual data recovery practice
T9: I wish security training included the need to keep more than one backup separated physically	Ensure training stresses the need for physical separation of multiple backups
T5: I wish security training included appropriate storage facilities	
T1: I wish there was backup training available to employees	Ensure training includes data backup
T5: I wish security training included database backup	
T4: I wish training could change the mindset of employees to make them aware of "critical issues"	Ensure the creation of a security culture
T9: I wish security training included creating a security culture	
T1: I wish there was phishing training available to employees	Ensure training includes phishing
T2: I wish pharming training were available (like phishing)	
T2: I wish spam training were more in depth	Ensure training include in-depth spam
T2: I wish there were policies about confidentiality of information	Ensure data confidentiality training
T2: I wish Internet policies were adequately explained to employees	Ensure Internet usage policy is explained

T3: I wish security training included deleting previous recipients email addresses on forwarded emails	Ensure training includes deleting previous recipients email addresses in forwarded emails
T4: I wish training informed employees of the cost of security awareness	Ensure employees are told the cost of security awareness
T4: I wish training provided employees with ways to get help after the training (reference points)	Ensure employees have access to references and help after training
T5: I wish security training included stress management	Ensure stress management is included
T5: I wish security training included corporate values	Ensure training on corporate values
T5: I wish security training included security policies	Ensure training on security policies
T5: I wish security training included security procedures	Ensure training on security procedures
T5: I wish security training included filters	Ensure training on the use of filters
T5: I wish security training included audits	Ensure training covers audits
T5: I wish security training included Internet navigation	Ensure training on navigating the Internet
T5: I wish security training included device hardware security	Ensure training on the security of device hardware
T5: I wish security training included spyware	Ensure spyware training
T7: I wish security training demonstrated all issues and ways to avoid them	Ensure all security issues are demonstrated with ways to avoid them
T8: I wish security training included physical security	Ensure physical security is included
T8: I wish security training included appropriate responses to various emergencies	Ensure appropriate responses to various security incidents
T8: I wish security training included online threats and how to deal with them.	Ensure training on avoiding online threats
T9: I wish security training included the usage of VPN's when out of the office	Cover VPN usage for telecommuting
T9: I wish security training defined roles and responsibilities	Ensure roles and responsibilities are defined
T9: I wish security training included how to handle cultural issues (people culture) that may affect security	Ensure training covers people's cultural differences

Table E4: Control Group Clustering

C2: I wish security training included examples of past security breaches	Ensure past examples of security breaches in training
C3: I wish security training included examples of breaches	
C4: I wish security training included examples from the trainee's workplace	Ensure security examples from the trainee's workplace
C2: I wish security training included consequences of security breaches	Ensure examples of the corporate consequences of security breaches
C4: I wish security training included corporate consequences of bad security	
C1: I wish security training included interaction with trainees	Ensure interactive training
C4: I wish security training were interactive	
C4: I wish security training included lectures at the workplace	Ensure training in the form of lectures
C5: I wish security training were interesting	Ensure interesting training
C3: I wish security training included a summary of what was taught	Ensure a summary of topics at the end of training
C1: I wish trainers had appropriate credentials and looked the part	Ensure qualified trainers
C4: I wish security training included personalization to a particular role in the company	Ensure training is directed to specific job roles
C5: I wish security training was taught at the level of the	Ensure training matches expertise level

trainee	
C3: I wish security training demonstrated how to properly perform security	Ensure appropriate security demonstrations
C4: I wish security training included punishments for non-compliance	Ensure training includes consequences for non-compliance
C7: I wish security training included employee consequences	
C7: I wish security training included physical security of their workstations	Ensure training includes physical security
C5: I wish security training included physical security	
C7: I wish security training included Internet policy	Ensure training includes Internet usage policy
C5: I wish security training included Internet policy	
C10: I wish training included acceptable Internet usage	
C5: I wish it was recognized that employees were going to use the Internet for personal use	
C2: I wish security training included guidelines for reporting security breaches	Ensure training provides guidelines for incident reporting
C2: I wish security training included how to handle incidents	
C5: I wish security training included policy taking about home corporate information via email attachment	Ensure training provides guidelines for transporting corporate data home
C5: I wish security training included policy about taking home corporate information via portable media	
C1: I wish training emphasized the benefits of following security policy, instead of emphasizing the punishment or negatives of not following security policy	Ensure training emphasizes the benefits of following policy and not the negatives of not following policy
C2: I wish security training included confidentiality	Ensure training includes data confidentiality
C10: I wish training included customer data confidentiality	
C4: I wish security training included the role of security	Ensure training demonstrates the benefits of security
C4: I wish security training included the benefits of security	
C4: I wish security training included the challenges of security	Ensure training acknowledges the challenges of good security
C5: I wish security training included common security vulnerabilities	Ensure training covers the most common vulnerabilities
C5: I wish security training included policy on corporate ID's	Ensure training covers corporate identification card policy
C5: I wish security training stressed the importance of everyone being involved	Ensure training stresses the involvement of everyone
C5: I wish security was not so strict that employees felt distrusted	Ensure proper security without employees feeling distrusted
C6: I wish security training included email policy	Ensure training includes email policy
C11: I wish training discusses email attachments	
C7: I wish security training included personal privacy of others at the office	Ensure training includes personal privacy of coworkers
C8: I wish training covered anti-virus software	Ensure training includes virus scanning, detecting, and updating
C9: I wish training included virus attacks	
C10: I wish training included virus training	
C11: I wish training included antivirus training and scanning	
C8: I wish training included password protection	Ensure training includes strong password policy
C9: I wish training included passwords	
C10: I wish training included strong password training	
C11: I wish training taught employees to use screen saver	

passwords C11: I wish training included a policy about changing BIOS passwords frequently	
C8: I wish training included firewall configuration C9: I wish training included firewalls	Ensure training includes firewall configuration
C8: I wish training included data backup	Ensure training includes data backup
C8: I wish training included consistent security policy	Ensure security policy is consistent
C8: I wish there was a published formal standard	Ensure a published formal standard
C8: I wish training included host network intrusion detection	Ensure training on host network intrusion detection
C8: I wish training included ethics training C9: I wish training included ethical conduct	Ensure employees receive ethics training
C8: I wish training included workstation control	Ensure training on workstation control
C8: I wish training included violation reporting	Encourage reporting violations
C9: I wish training included Internet Protocols	Ensure training covers Internet Protocol (IP addresses)
C9: I wish training included Domain Name Service	Ensure training covers Domain Name Services (DNS)
C9: I wish training included Access Points	Ensure training covers access points
C9: I wish training included encryption	Ensure training covers encryption
C9: I wish training included security management	Ensure training includes security management
C9: I wish training included wireless networking	Ensure training includes wireless networking
C9: I wish training included hacking threats	Ensure training includes hacking threats
C9: I wish training included social engineering	Ensure training includes social engineering
C9: I wish training included network failures	Ensure training covers how to handle network failures
C9: I wish training included contingency planning	Ensure training includes contingency planning
C9: I wish training included special training, such as CCNA, CCNP, MCSC, and Linux	Ensure employees get specialized certification training, such as CCNA, CCNP, MCSC, and Linux
C10: I wish training included a policy to only keep necessary customer information	Ensure there is a policy to only keep necessary customer information
C10: I wish training included a policy about not using personal emails or devices for company data	Ensure there is a policy about not using personal emails or devices for company data
C11: I wish training included protection from SPAM	Ensure training includes protection from SPAM emails
C11: I wish training taught employees to not send attachments back to the original sender when replying to emails	Ensure employees are taught to not send attachments back to the original sender when replying to emails

Appendix F: Final Group Objectives

Table F1: Socio-Technical Group Final Objectives

Objective	Orientation
1. Ensure password protection is fully utilized	T
2. Ensure a reward system for disclosing security breaches	S
3. Ensure appropriate ethics training	S
4. Ensure a trust relationship between employees and the company	S
5. Ensure training covers employee integrity	S
6. Ensure rules to identify who has appropriate access to computers	T
7. Ensure organizational structure designates proper access to the appropriate people	S
8. Ensure promoted employees have more access to data	T
9. Ensure examples are fully utilized in security training	G
10. Ensure training with visually stimulating videos	G
11. Ensure trainees are asked questions to verify understanding of training concepts	G
12. Ensure management appears in training videos	G
13. Ensure training is appropriate for the various roles within the organization	G
14. Ensure training is not too technical	G
15. Ensure training is simple and short	G
16. Ensure video training attempts to put the trainee in the shoes of the actor	G
17. Ensure only appropriate software is installed on corporate computers	T
18. Ensure a mix of the technical, formal, and informal control systems	S
19. Ensure the highest security while minimizing effects on employee's ability to work effectively	G
20. Ensure clearly defined roles and responsibilities	S
21. Ensure data confidentiality policies are in place	T
22. Ensure there is a policy concerning company business on personal computers	G
23. Ensure there is a policy concerning company business on personal cell phones	G
24. Ensure companies create their own networks	T
25. Ensure there is an Internet usage policy	G
26. Ensure unnecessary hardware, including USB ports, are removed from computers	T
27. Ensure promoted employees are given more executive powers	S
28. Ensure employees clearly understand processes, procedures, and rules	S
29. Ensure there are software installation polices in place	T
30. Ensure employees receive motivation training	S
31. Ensure employees receive commitment training	S
32. Ensure user involvement through incentives and motivation	S
33. Ensure companies have proper structure	S
34. Ensure companies have proper risk assessment	G
35. Ensure employees understand the importance of security	G
36. Ensure employees are told security is related to their salaries and careers	G
37. Ensure employees are trained on logging on and off computers	T
38. Ensure companies have a good infrastructure	T
39. Ensure companies properly use intrusion detection systems (IDS)	T
40. Ensure companies properly use firewalls	T
41. Ensure companies have secure web servers	T
42. Ensure companies use policies and standards to set up controls	S

43. Ensure companies protect databases from intrusion	T
44. Ensure companies are aware of less obvious threats, such as personal portable devices	T
45. Ensure employees are aware that security is everyone's responsibility and not just an individual	G
46. Ensure employees are given examples of corporate consequences of bad security	G
47. Ensure employees are a good fit for the position before they are hired	G
48. Ensure the hiring of committed employees	S
49. Ensure the hiring of responsible employees	S
50. Ensure potential employees are screened before hiring	S
51. Ensure employees are aware of consequences of non-compliance	G
52. Ensure data access is limited to appropriate individuals	T
53. Ensure computers are set to not remember information	T
54. Ensure the use of fingerprints or retinal scans to protect sensitive data	T
55. Ensure limited physical access to secure areas	T
56. Ensure employees are informed	G
57. Ensure the utilization of single design	T
58. Ensure constant checking for system glitches	T
59. Use "friendly hacking" to identify security weaknesses	T
60. Create knowledge outlets identifying who should know what and why	S
61. Limit the use of automated systems	G
62. Define what data is to be monitored	T
63. Define rules as to how data is used	T
64. Create acceptable computer usage policies	G
65. Ensure computers are updated regularly	T
66. Ensure employees are aware of where they can access policies and procedures	G
67. Ensure employees know how to suggest changes to policies and procedures	G
68. Ensure employees in high security areas are well trained	G
69. Ensure companies work to eliminate broken processes	G
70. Ensure employees understand what to expect with a change process	G
71. Ensure employees understand regulation compliance	G
72. Ensure corporate communication is clear and concise	G

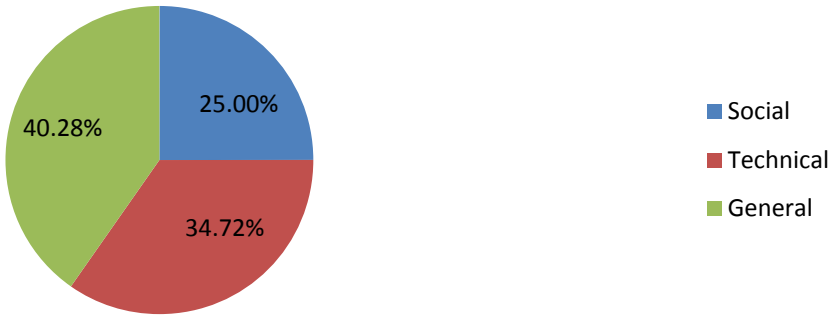

Figure F1: Socio-technical Orientation Percentage

Table F2: Social Group Final Objectives

Objective	Orientation
1. Ensure in-depth training on acceptable email use	G
2. Minimize the use of online training	G
3. Ensure training is appropriate for the trainee's level of expertise	G
4. Ensure training is up to date with current security issues	G
5. Ensure managers are involved in providing training	G
6. Ensure hand's on training	G
7. Ensure training is relevant to all employees	G
8. Ensure training utilizes real world examples, including the corporate consequences of bad security	G
9. Ensure training covers privacy rights	T
10. Ensure training addresses data protection	T
11. Ensure training considers employee cultural differences	S
12. Ensure training addresses how employee dissatisfaction affects security	S
13. Ensure training addresses employee integrity	S
14. Ensure training addresses factors affecting employee decision making	S
15. Ensure training includes confidentiality policy	T
16. Ensure training covers personal data security	T
17. Ensure security training includes how to handle the media	G
18. Ensure training addresses physical security, including employee work spaces	T
19. Ensure training addresses protecting employee's home computers	T
20. Ensure training includes continuing education as threats change	G
21. Ensure training addresses strong passwords while minimizing the need to write them down	T
22. Ensure training addresses employee ethics	S
23. Ensure training covers the most common threats and how to prevent them	G
24. Explain why security policies are necessary	G
25. Ensure the importance of security is addressed with all employees	G
26. Ensure employees are told that making mistakes is alright	G
27. Ensure training describes corporate values	S
28. Ensure training addresses employee morale	S
29. Ensure training includes technical aspects	T
30. Ensure training covers legal aspects of security	G
31. Ensure training addresses the relationship between emotional intelligence and security	S
32. Ensure employees are aware of the importance of good security	G
33. Include identity theft in security training	T
34. Ensure training addresses corporate information theft	G
35. Ensure training addresses the social interaction between companies and individuals	S
36. Ensure training addresses acceptable software usage policy	G
37. Ensure training takes into consideration an employee's gender	S

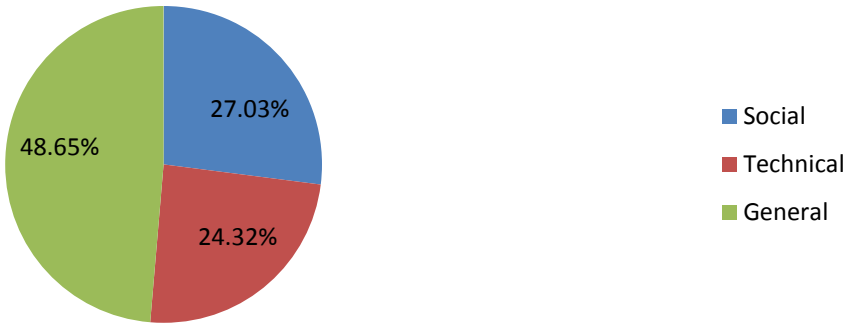

Figure F2: Social Group Orientation Percentage

Table F3: Technical Group Final Objectives

Objectives	Orientation
1. Ensure in-depth training	G
2. Ensure training to the knowledge level of the trainee	G
3. Ensure humor is included in training	G
4. Ensure hands on training	G
5. Ensure training includes company or industry past examples of security breaches	G
6. Ensure training includes strict password policy	T
7. Ensure training includes email acceptable use policy	G
8. Ensure email training includes the risk of attachments	T
9. Ensure training includes the risk of web links	T
10. Ensure training fully utilizes encryption	T
11. Ensure simplistic training	G
12. Ensure training includes data protection	T
13. Ensure training stresses annual data recovery practice	T
14. Ensure training stresses the need for physical separation of multiple backups	T
15. Ensure training includes bright imagery	G
16. Ensure training includes data backup	T
17. Ensure the creation of a security culture	S
18. Ensure training includes phishing	T
19. Ensure training includes in-depth SPAM training	T
20. Ensure training covers people's cultural differences	S
21. Ensure data confidentiality training	T
22. Ensure concise training	G
23. Ensure Internet usage policy is explained	G
24. Ensure training includes deleting previous recipients email addresses in forwarded emails	T
25. Ensure employees are told the cost of security awareness	G
26. Ensure employees have access to references and help after training	G
27. Ensure in-depth virus and worm training	T
28. Ensure stress management is included	S
29. Ensure training on corporate values	S
30. Ensure roles and responsibilities are defined	S
31. Ensure training on security policies	G
32. Cover VPN usage for telecommuting	T

33. Ensure training on security procedures	G
34. Ensure interactive training	G
35. Ensure training on the use of filters	T
36. Ensure training covers audits	T
37. Ensure training on navigating the Internet	T
38. Ensure training on the security of device hardware	T
39. Ensure spyware training	T
40. Ensure all security issues are demonstrated with ways to avoid them	G
41. Ensure physical security is included	T
42. Ensure appropriate responses to various security incidents	G
43. Ensure training on avoiding online threats	T

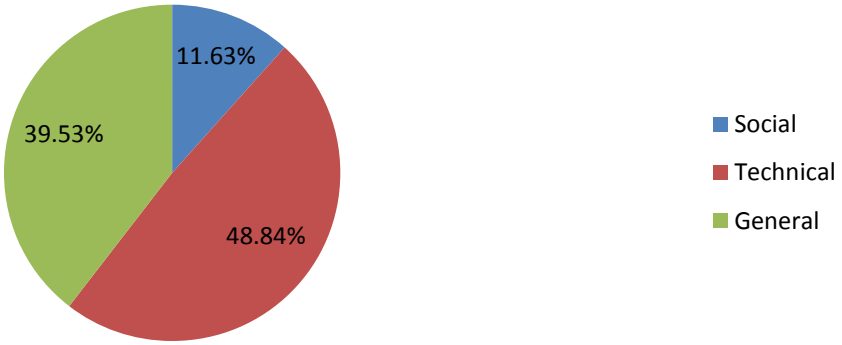

Figure F3: Technical Group Orientation Percentage

Table F4: Control Group Final Objectives

Objective	Orientation
1. Ensure interactive training	G
2. Ensure a summary of topics at the end of training	G
3. Ensure training matches expertise level	G
4. Ensure training includes consequences for non-compliance	G
5. Ensure training includes physical security	T
6. Ensure training includes wireless networking	T
7. Ensure training includes hacking threats	T
8. Ensure a published formal standard	G
9. Ensure training on host network intrusion detection	T
10. Ensure employees receive ethics training	S
11. Ensure training on workstation control	T
12. Ensure training includes data backup	T
13. Ensure training includes firewall configuration	T
14. Encourage reporting violations	G
15. Ensure training covers Internet Protocol (IP addresses)	T
16. Ensure training covers encryption	T
17. Ensure training includes security management	G
18. Ensure training includes social engineering	S
19. Ensure training covers how to handle network failures	T
20. Ensure training includes strong password policy	T
21. Ensure training includes contingency planning	T

22. Ensure employees get specialized certification training, such as CCNA, CCNP, MCSC, and Linux	T
23. Ensure training includes Internet usage policy	G
24. Ensure training provides guidelines for incident reporting	G
25. Ensure training is directed to specific job roles	G
26. Ensure training provides guidelines for transporting corporate data home	G
27. Ensure training emphasizes the benefits of following policy and not the negatives of non-compliance	G
28. Maximize examples in training	G
29. Ensure training includes data confidentiality	T
30. Ensure training demonstrates the benefits of security	G
31. Ensure trainers are qualified	G
32. Ensure training includes virus scanning, detecting, and updating	T
33. Ensure training covers Domain Name Services (DNS)	T
34. Ensure training covers access points	T
35. Ensure interesting training	G
36. Ensure training acknowledges the challenges of good security	G
37. Ensure security policy is consistent	G
38. Ensure training covers the most common vulnerabilities	G
39. Ensure training in the form of lectures	G
40. Ensure training covers corporate identification card policy	G
41. Ensure training stresses the involvement of everyone	G
42. Ensure appropriate security demonstrations	G
43. Ensure proper security without employees feeling distrusted	S
44. Ensure training includes email policy	G
45. Ensure training includes personal privacy of coworkers	T
46. Ensure there is a policy to only keep necessary customer information	T
47. Ensure there is a policy about not using personal devices for company data	T
48. Ensure training includes protection from SPAM emails	T
49. Ensure employees are taught to not send attachments back to the original sender when replying to emails	T

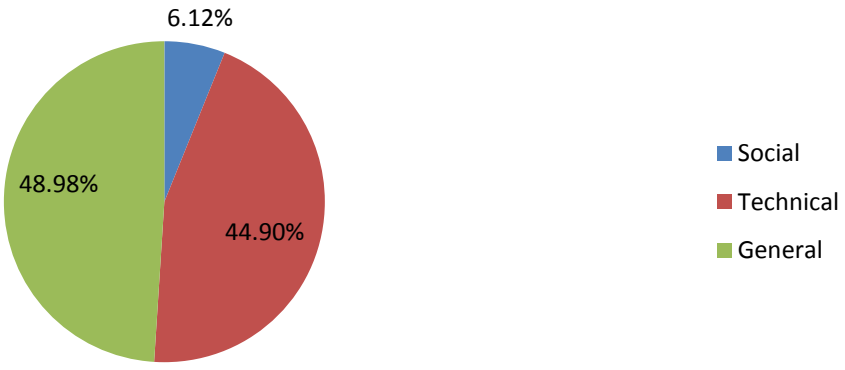

Figure F4: Control Group Orientation Percentage

Appendix G: Delphi Results

Table G1: Socio-Technical Group Shortened List

Objective	Percentage Selected by Group Participants
1. Ensure data confidentiality policies are in place	70%
2. Ensure there is an Internet usage policy	70%
3. Ensure clearly defined roles and responsibilities	70%
4. Ensure employees clearly understand processes, procedures, and rules	70%
5. Ensure data access is limited to appropriate individuals	60%
6. Ensure employees are aware of consequences of non-compliance	60%
7. Ensure companies are aware of less obvious threats, such as personal portable devices	60%
8. Ensure computers are updated regularly	60%
9. Ensure employees are given examples of corporate consequences of bad security	60%
10. Ensure employees understand the importance of security	60%
11. Ensure password protection is fully utilized	60%
12. Ensure potential employees are screened before hiring	60%

Table G2: Social Group Shortened List

Objective	Percentage Selected by Group Participants
1. Ensure training is up to date with current security issues	90%
2. Ensure training describes corporate values	90%
3. Ensure training utilizes real world examples, including the corporate consequences of bad security	80%
4. Ensure training includes confidentiality policy	80%
5. Ensure training addresses strong passwords while minimizing the need to write them down	80%
6. Ensure training covers legal aspects of security	80%
7. Ensure training covers personal data security	80%
8. Ensure training covers privacy rights	80%
9. Ensure training covers the most common threats and how to prevent them	80%
10. Ensure the importance of security is addressed with all employees	80%
11. Ensure training addresses data protection	80%
12. Ensure training addresses employee ethics	90%
13. Ensure training addresses employee integrity	80%
14. Ensure training addresses corporate information theft	70%
15. Ensure hand's on training	70%
16. Ensure managers are involved in providing training	70%
17. Ensure training addresses the social interaction between companies and	70%

individuals	
18. Ensure training includes continuing education as threats change	70%
19. Ensure training considers employee cultural differences	70%
20. Ensure training includes technical aspects	60%
21. Ensure training addresses the relationship between emotional intelligence and security	60%
22. Ensure training addresses factors affecting employee decision making	60%
23. Ensure training addresses how employee dissatisfaction affects security	60%

Table G3: Technical Group Shortened List

Objective	Percentage Selected by Group Participants
1. Ensure training includes email acceptable use policy	90%
2. Ensure in-depth training	90%
3. Ensure email training includes the risk of attachments	90%
4. Ensure the creation of a security culture	90%
5. Ensure training on security policies	80%
6. Ensure training includes data protection	80%
7. Ensure data confidentiality training	70%
8. Ensure training includes phishing	70%
9. Ensure training includes strict password policy	70%
10. Ensure training includes the risk of web links	70%
11. Ensure training includes data backup	70%
12. Ensure training on corporate values	70%
13. Ensure in-depth virus and worm training	60%
14. Ensure Internet usage policy is explained	60%
15. Ensure roles and responsibilities are define	60%
16. Ensure spyware training	60%
17. Ensure training fully utilizes encryption	60%
18. Ensure training includes company or industry past examples of security breaches	60%
19. Ensure employees have access to references and help after training	60%
20. Ensure training on avoiding online threats	60%
21. Ensure all security issues are demonstrated with ways to avoid them	60%
22. Ensure training to the knowledge level of the trainee	60%

Table G4: Control Group Shortened List

Objective	Percentage Selected by Group Participants
1. Ensure training includes email policy	91%
2. Ensure training includes strong password policy	82%
3. Ensure training includes Internet usage policy	82%
4. Ensure training includes security management	73%
5. Ensure training demonstrates the benefits of security	73%
6. Ensure interactive training	73%
7. Encourage reporting violations	64%
8. Ensure a published formal standard	64%
9. Ensure a summary of topics at the end of training	64%

10. Ensure appropriate security demonstrations	64%
11. Ensure training includes hacking threats	64%
12. Ensure training includes physical security	64%
13. Ensure training provides guidelines for incident reporting	64%
14. Maximize examples in training	64%
15. Ensure security policy is consistent	64%
16. Ensure training includes consequences for non-compliance	64%
17. Ensure training includes data backup	64%
18. Ensure training includes data confidentiality	64%
19. Ensure there is a policy about not using personal devices for company data	55%
20. Ensure trainers are qualified	55%
21. Ensure training covers the most common vulnerabilities	55%
22. Ensure employees receive ethics training	55%
23. Ensure training emphasizes the benefits of following policy and not the negatives of non-compliance	55%
24. Ensure training matches expertise level	55%
25. Ensure training on workstation control	55%

Table G5: Socio-Technical Group Final Ranking

Mean Rank	Objective	Orientation
1.20	1. Ensure employees clearly understand processes, procedures, and rules	Social
2.60	2. Ensure clearly defined roles and responsibilities	Social
3.10	3. Ensure potential employees are screened before hiring	Social
4.50	4. Ensure data access is limited to appropriate individuals	Technical
5.20	5. Ensure employees are aware of consequences of non-compliance	General
6.60	6. Ensure data confidentiality policies are in place	Technical
6.70	7. Ensure employees understand the importance of security	General
9.00	8. Ensure employees are given examples of corporate consequences of bad security	General
9.10	9. Ensure password protection is fully utilized	Technical
9.10	10. Ensure companies are aware of less obvious threats, such as personal portable devices	Technical
10.50	11. Ensure there is an Internet usage policy	General
11.30	12. Ensure computers are updated regularly	Technical

Kendall's W		
Round 1	Round 2	Round 3
.318	.734	.825

Table G6: Social Group Final Ranking

Mean Rank	Objective	Orientation
1.10	1. Ensure the importance of security is addressed with all employees	General
4.40	2. Ensure training is up to date with current security issues	General
4.90	3. Ensure training addresses employee ethics	Social

5.10	4. Ensure training covers the most common threats and how to prevent them	General
7.10	5. Ensure training covers personal data security	Technical
7.50	6. Ensure training utilizes real world examples, including the corporate consequences of bad security	General
7.70	7. Ensure training addresses data protection	Technical
8.20	8. Ensure training addresses employee integrity	Social
8.50	9. Ensure training covers legal aspects of security	General
10.00	10. Ensure managers are involved in providing training	General
11.30	11. Ensure training includes continuing education as threats change	General
11.80	12. Ensure training describes corporate values	Social
13.10	13. Ensure training addresses the relationship between emotional intelligence and security	Social
13.50	14. Ensure hand's on training	General
14.20	15. Ensure training addresses corporate information theft	General
14.50	16. Ensure training covers privacy rights	Technical
16.20	17. Ensure training addresses how employee dissatisfaction affects security	Social
17.00	18. Ensure training addresses the social interaction between companies and individuals	Social
18.70	19. Ensure training includes technical aspects	Technical
18.90	20. Ensure training considers employee cultural differences	Social
19.70	21. Ensure training includes confidentiality policy	Technical
20.20	22. Ensure training addresses factors affecting employee decision making	Social
22.40	23. Ensure training addresses strong passwords while minimizing the need to write them down	Technical

Kendall's W	
Round 1	**Round 2**
.193	.744

Table G7: Technical Group Final Ranking

Mean Rank	Objective	Orientation
4.10	1. Ensure all security issues are demonstrated with ways to avoid them	General
4.20	2. Ensure training to the knowledge level of the trainee	General
4.90	3. Ensure in-depth training	General
5.80	4. Ensure training on security policies	General
7.00	5. Ensure training on corporate values	Social
7.20	6. Ensure training includes company or industry past examples of security breaches	General
7.50	7. Ensure the creation of a security culture	Social
8.70	8. Ensure employees have access to references and help after training	General
8.80	9. Ensure roles and responsibilities are defined	Social
9.90	10. Ensure data confidentiality training	Technical
10.90	11. Ensure Internet usage policy is explained	General
11.20	12. Ensure training on avoiding online threats	Technical
13.10	13. Ensure training includes strict password policy	Technical
14.20	14. Ensure training includes data protection	Technical
14.40	15. Ensure training includes the risk of web links	Technical
15.80	16. Ensure training includes email acceptable use policy	General
16.00	17. Ensure email training includes the risk of attachments	Technical

16.80	18. Ensure in-depth virus and worm training	Technical
17.50	19. Ensure training includes data backup	Technical
17.70	20. Ensure spyware training	Technical
19.10	21. Ensure training includes phishing	Technical
20.10	22. Ensure training fully utilizes encryption	Technical

Kendall's W		
Round 1	**Round 2**	**Round 3**
.270	.582	.627

Table G8: Control Group Final Ranking

Mean Rank	Objective	Orientation
1.00	1. Ensure training demonstrates the benefits of security	General
2.00	2. Ensure interactive training	General
3.09	3. Ensure security policy is consistent	General
4.27	4. Ensure training includes security management	General
5.45	5. Ensure training includes email policy	General
5.82	6. Ensure a published formal standard	General
6.91	7. Ensure training includes data confidentiality	Technical
8.09	8. Ensure trainers are qualified	General
8.91	9. Ensure training matches expertise level	General
9.55	10. Ensure training covers the most common vulnerabilities	General
10.91	11. Ensure employees receive ethics training	Social
12.27	12. Ensure training includes Internet usage policy	General
12.91	13. Ensure appropriate security demonstrations	General
13.91	14. Ensure training includes strong password policy	Technical
14.91	15. Ensure there is a policy about not using personal devices for company data	Technical
16.00	16. Ensure training emphasizes the benefits of following policy and not the negatives of non-compliance	General
17.00	17. Maximize examples in training	General
18.00	18. Ensure training includes hacking threats	Technical
19.09	19. Ensure training provides guidelines for incident reporting	General
20.00	20. Ensure training includes data backup	Technical
21.18	21. Ensure training on workstation control	Technical
22.00	22. Encourage reporting violations	General
23.18	23. Ensure training includes consequences for non-compliance	General
24.00	24. Ensure training includes physical security	Technical
24.55	25. Ensure a summary of topics at the end of training	General

Kendall's W		
Round 1	**Round 2**	**Round 3**
.130	.675	.992

Vita

Mark Alan Harris was born June 25, 1970 in Norfolk, Virginia and is a United States citizen. He graduated in 1988 from Great Bridge High School in Chesapeake, Virginia. He received an Associate's degree in Business Administration from Tidewater Community College in 1997. In 1999, he received a Bachelor of Science degree in Business Administration with a major of Information Technology from Old Dominion University in Norfolk, Virginia. His BS degree came with the *magna cum laude* distinction. Mark's 2003 Master's degree was in E-commerce and was also from Old Dominion University. Mark started the Ph.D. program at Virginia Commonwealth University in 2004.

Mark's professional experience includes over ten years as the Senior Network Engineer for Old Dominion University's School of Business, where he oversaw a vast network of computers and thousands of users. During that same time, Mark taught undergraduate and graduate courses in the university's department of information technology. Some of the courses he taught include systems analysis and design, programming languages, and advanced networking.

In 2009, Mark started as a full time faculty member at the University of South Carolina. He teaches information technology courses within the Integrated Information Technology program. He is currently teaching introduction to networking, advanced networking, and management of information systems.

Mark's primary research interest is in the area of information systems security (ISS). More specifically, he is interested in the theoretical foundations of ISS, human factors and ISS, and socio-organizational influences on ISS. His secondary research interests include systems analysis and design and strategic management of information systems.

His past publications include:

"Human Behavior Aspects in Information Systems Security," with Sushma Mishra, in the *5th Annual Security Conference*, Las Vegas, Nevada, April 19-20, 2006.

"Information Systems-Strategy Alignment: Planning for the Next Decade of Research," with Peter Aiken, in the *2nd Enterprise Systems pre-ICIS 2007 Workshop*. Montreal, Quebec, Canada. December 8-9, 2007.

"Does User Participation Lead to System Success?" with Roland Weistroffer, in the *SAIS Conference*, Richmond, Virginia, March 13-15, 2008.

"Issues and Challenges of Managing Corporate Computer Crime" in the *11th Annual Working Conference on Information Security Management*, Richmond, Virginia, October 16-17, 2008.

"The Relationship between User Involvement and System Success: A Review of Empirical Research," with Roland Weistroffer to *Communications of the AIS*, June, 2009.

"Shaping of Employee Objectives for Protecting Corporate Information Systems," in the *9th Annual Security Conference*, Las Vegas, Nevada, April 7-9, 2010.