2014

Employee and Organization Security Value Alignment Through Value Sensitive Security Policy Design

Dianne Blitstein Solomon
Nova Southeastern University, diannebsolomon@gmail.com

Employee and Organization Security Value Alignment Through Value Sensitive Security Policy Design

by

Dianne Blitstein Solomon

A dissertation submitted in partial fulfillment of the
requirements for the degree of Doctor of Philosophy
in
Information Systems

Graduate School of Computer and Information Sciences
Nova Southeastern University

2014

We hereby certify that this dissertation, submitted by Dianne Solomon, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

_____ _____

Maxine S. Cohen, Ph.D. Date
Chairperson of Dissertation Committee

_____ _____

Amon B. Seagull, Ph.D. Date
Dissertation Committee Member

_____ _____

Constance Mussa, Ph.D. Date
Dissertation Committee Member

Approved:

_____ _____

Eric S. Ackerman, Ph.D. Date
Dean, Graduate School of Computer and Information Sciences

Graduate School of Computer and Information Sciences
Nova Southeastern University

2014

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Employee and Organization Security Value Alignment Through Value Sensitive Security Policy Design

by
Dianne Blitstein Solomon
September 2014

Every member of the organization must be involved in proactively and consistently preventing data loss. Implementing a culture of security has proven to be a reliable method of enfranchising employees to embrace security behavior. However, it takes more than education and awareness of policies and directives to effect a culture of security. Research into organizational culture has shown that programs to promote organizational culture - and thus security behavior - are most successful when the organization's values are congruent with employee values. What has not been clear is how to integrate the security values of the organization and its employees in a manner that promotes security culture. This study extended current research related to values and security culture by applying Value Sensitive Design (VSD) methodology to the design of an end user security policy. Through VSD, employee and organizational security values were defined and integrated into the policy. In so doing, the study introduced the concept of value sensitive security policy (VSP) and identified a method for using VSPs to promote a culture of security. At a time when corporate values are playing such a public role in defining the organization, improving security by increasing employee-organization value congruence is both appealing and practical.

Acknowledgements

It is commonly said that each scholar stands on the shoulders of giants. I have been blessed with many giants whose efforts brought this work to a successful conclusion. My advisor, Dr. Maxine Cohen, has been both empowering and challenging, helping me find my place in the crossroads of security and usability, and guiding me toward an achievable and purposeful journey. Committee member Dr. Amon Seagull strategically intervened at pivotal moments making it possible for work to continue when it seemed to be breathing its last. Dr. Constance Mussa, a more recent addition to my academic life, brought a fresh perspective to the study that fleshed out unaddressed assumptions. The work is stronger because of all they brought to it.

My husband Daniel selflessly weathered all the highs and lows of this academic voyage, selflessly pitching in without complaint and going solo to family events while my head was buried in books and keyboard. Without his unfailing support, it would have been impossible to finish. My parents, Joan and Edward[z"l] Blitstein, themselves lifelong students, and my son, Joshua, born to swim scholarly waters, made post-midlife academic pursuits seem a matter of course. My brother Mark took on more than his share of family responsibilities so that I could carve out the time needed to complete such a long journey.

Not all my scholarly giants had formal roles in the process, making their contributions that much more valued. Professors Aaron Kershenbaum, Chino Rao, and Susan Solomon, for no other reason than their love of learning and respect for those in pursuit of it, generously gave their time and knowledge. These three passionate educators kept me moving forward when all rational cues said quit. Without their encouragement and wise counsel, I'd have a better-tended garden, but a mind less fertile.

Any academic pursuit, particularly when sandwiched in between home and work commitments, is not without its emotional challenges. My circle of close friends and colleagues - Ellen Sherba, Bonnie Hooker, Ramona Barnes, Dr. Wayne Pauley, and Dr. Jack Hyman – rescued me countless times from doldrums, never doubting that I would see this effort through to an auspicious end.

As important as my scholarly mentors, family, and friends have been in bringing this work to its conclusion, it never would have started without First Data Corporation and its forward thinking and talented security professionals, Phil Mellinger, Joanne Sebby, Susan Mauldin, Judy Weichbrodt, John Hellickson, and Rob Throckmorton. These inspiring colleagues brought me into the security community, ensured the funding of my education, and allowed me to test new knowledge in a real world setting. And lastly, a special thanks and note of respect to XYZ Corp, its privacy team and its security policy makers, whose accomplishments span 20 time zones and 35 countries. I am as proud of their efforts to build a more secure world as they are of my small contribution to it.

To all of these giants, I offer my thanks and profound appreciation.

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

"Culture, more than rulebooks, determines how an organization behaves." said Warren Buffet in his July 26, 2010 memo to Berkshire Hathaway managers (p. 27). Mr. Buffet intuitively knew what a recent industry study reported - current employees are the source of more than one third of security incidents (PwC, 2013). The security literature presents strong evidence that policies and management directives alone fail to ensure employee adoption of security practices designed to minimize unintentional data loss (Alavi, Islam, Jahankhani, & Al-Nemrat, 2013; Da Veiga & Eloff, 2007; Edwards, Poole, & Stoll, 2008; Thomson, von Solms, & Louw, 2006). Everyone within the organization must be actively involved in risk identification and data loss prevention.

Organizational security programs designed to promote and enhance the protection of information assets are not a new topic within the security literature. Research suggests security program content, how the program is presented, and the role of leadership are all significant success factors. Security awareness programs have been found to be effective instruments of organizational change when they are strategic and linked to organizational goals (Cline & Jensen, 2004; Tsohou, Kokolakis, Karyda, & Kiountouzis, 2008). Security program content is best communicated when targeted to the employee's role

within the organization (White & Ruh, 1973). Managers become effective drivers of organizational change toward enhanced security as their understanding of the risks associated with data loss increases, and when that understanding is communicated to employees through policy and action (Choi, Kim, Goo, & Whitmore, 2008).

Organizational security programs and management directives have not, in and of themselves, led to employee adoption of habitual and consistent security practices. Employees adopt habitual and consistent security practices when the organization establishes a culture of security (Corriss, 2010; Thomson, von Solms, & Louw, 2006; von Solms & von Solms, 2004). Security culture is achieved by aligning organizational and employee attitudes, beliefs, and values (Kolkowska, 2011; von Solms & von Solms, 2004). By developing programs congruent with attitudes, beliefs, and values, the organization engages employee motivation to embrace security controls (Lacey, 2010). In their seminal work on security culture, von Solms and von Solms (2004) concluded, "if management wants their employees to act in a specific way that is beneficial to the organization, they need to dictate the behaviour of the employees. This can be done by expressing collective values…" (p. 277).

When the goal of leadership is to align the organization's information security values with the values of its employees, the organization becomes well positioned to succeed in developing effective information security practices (Corriss, 2010; Furnell & Thomson, 2009; von Solms & von Solms, 2004). When those practices become habitual, a culture of security is established (Baggett, 2003; Chang & Lin, 2007; Thomson, von Solms, & Louw, 2006). Furthermore, when individuals within a group share values, those values influence security behavior within the organization (Alfawaz, Nelson, &

Mohannak, 2010; Dhillon & Torkzadeh, 2006; Killingsworth, 2012) and continue as an influence throughout an employee's tenure (Ostroff, 2005). These findings suggest that if employee and organizational values can be aligned, not only will the organization influence employees toward security culture, the employees will influence one another and strengthen the culture. The possibility of a self-perpetuating benefit provides compelling reason to explore values alignment as a means of promoting information security behaviors. There is scanty research in this area today.

The relationship between aligned organizational and employee security values and security behavior is illustrated in Figure 1. It shows the end goal as the state in which security culture and security behavior continuously influence one another. Security culture is established and sustained when employee and organizational security values are congruent. Whereas employees are able to give voice to values, organizational values are communicated through policies. Therefore the expression of security values begins within the security policy. Instead of traditional policy statements that read "Users must..." and "Users may not…" language reflecting shared values might read, "To safeguard the privacy of our customers, we…"

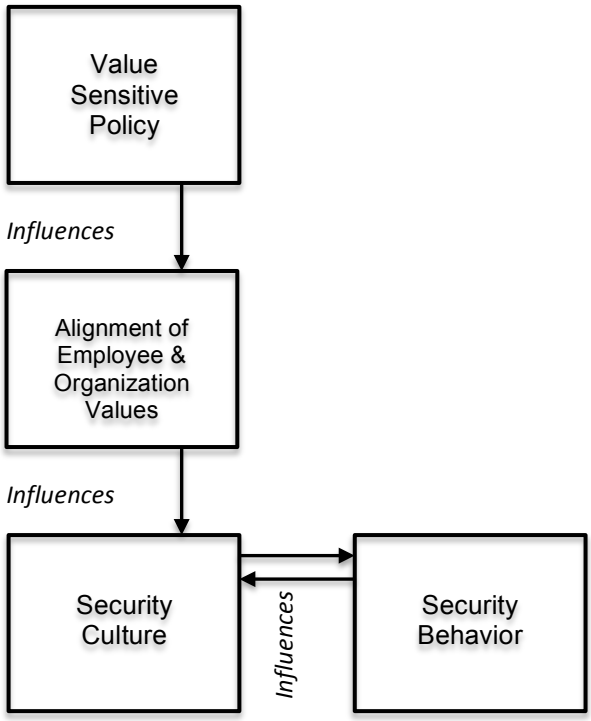


Figure 1. Value sensitive policy influences security behavior

The challenge in creating a values based security policy is two-fold. Organizations must identify the security values it shares with its employees and then find a way of incorporating those values into its policy. Value Sensitive Design (VSD) offers a method for doing both. VSD is a theoretically grounded and principled approach for integrating human values into technology-related design (Friedman, Kahn, & Borning, 2001). This study tested VSD as a method for creating security policy language that reflected both employee and organizational values.

The remainder of this chapter is organized as follows. The chapter opens with a description of the research problem. It then establishes the importance of the problem from both research and practical perspectives, explores the complexity of the topic, and establishes the limits of the study. The chapter concludes with definitions of key terms.

Problem Statement

How can an organization align the security values of the organization and its employees into the design of its policies to promote the habitual behaviors associated with security culture? Despite the considerable body of literature that suggests establishing a culture of security leads to habitual and consistent employee adoption of security practices, how organizations go about establishing a culture of security is not well understood. Values are a recurring topic of exploration in security culture research because it has been found that when employee and organizational values are aligned, employees are motivated to follow leaders and embrace organizational change (Krishnan, 2002; Lamm, Gordon, & Purser, 2010). The literature suggests that an organization communicates values through its policies (Da Veiga & Eloff, 2010; Kolkowska, 2011). Therefore, building values into the policy should present the opportunity for employees to identify shared values and thus promote the adoption of prescribed behaviors. However, the literature fails to address three fundamental questions: What values promote security behavior? How can the organization build security values into its policy? How can the policy incorporate both corporate and employee values?

The field of Human Computer Interaction (HCI) has demonstrated long and continued interest in the idea of integrating human values into technology design (Flanagan, Howe, & Nissenbaum, 2005; Friedman, Kahn, & Borning, 2001; Le Dantec, Poole, & Wyche, 2009; Shneiderman, Plaisant, Cohen, & Jacobs, 2009). Within the field of HCI, VSD has evolved as a theoretically grounded approach to technology design that accounts for disparate stakeholder values in a principled and comprehensive manner (Flanagan et al., 2005; Friedman et al., 2001). Technology from a VSD perspective has

been broadly defined, and the methodology applied to the design efforts of a broad range of end products. Examples include decision support application software (Davis, 2006), browser redesign (Friedman, Howe, & Felten, 2002), weapons systems (Cummings, 2006), medical devices (Denning, Borning, Friedman, Gill, Kohno, & Maisel, 2010), and a privacy amendment to an open source software license agreement (Friedman, Smith, Kahn, Consolvo, & Selawski, 2006). In this study, VSD was applied to a corporate security end user policy, the vehicle by which an organization communicates its security values and sets expectations of employee security behavior. As Hedström, Kolkowska, Karlsson, and Allen (2011) stated, "security policies and regulations are expressions of values, as well as sets of instructions" (p. 373). Through VSD, the question of what values promote security and the challenge of identifying shared values and incorporating them into policy were addressed.

Dissertation Goal

The goal of this study was to determine if VSD is an effective method for defining organizational and employee security values and integrating them into the organization's end user security policy. The study explored VSD as the theory and method for such incorporation, drawing upon its systematic and principled approach for addressing the issue of values within the context of design. At a time when corporate values are playing a growing role in the organization's self-definition (Strugatch, 2011), improving security by increasing the organizational focus on values can be both appealing and practicable. From a research perspective, a better understanding of how the organization can align its

security values with those of its employees contributes to an overall understanding of building security culture.

Research Questions

The study is built on the premise that effectively incorporating security values into the organizational security policy will promote the habitual security behaviors associated with security culture. As explicated above, the relationships between values and organizational culture, between organizational culture and security culture, and between security culture and security behavior have been well established in literature. However, little attention had been paid to the three fundamental questions: What values promote security behavior? How can the organization build security values into its policy? How can the policy incorporate both corporate and employee values? These questions were addressed through two research questions. The first was:

> RQ 1: What values do employees and organizations associate with security behavior?

In their comprehensive analysis of literature related to business values, Agle and Caldwell (1999) identified close to 200 studies related to understanding individual, organizational, and institutional values. In the first study devoted to understanding security in terms of employee and organizational values, Dhillon and Torkzadeh (2006) identified 86 values-driven security objectives. Left unanswered was the question of what values must be expressed if, as Schlienger and Teufel (2003) claimed, security culture is an expression of an organization's collective values. The theory and principles of VSD suggest that there are ways to elicit values from the disparate stakeholders during

the technology design effort (Cummings, 2006; Friedman, Kahn, & Borning, 2006; Le Dantec, Poole, & Wyche, 2009). Through its application the first research question was be addressed.

As supported in the cited literature, organizations use policies to communicate values. Because the goal was for the policy to express the confluence of both employee and organizational values, a means by which this happens was needed. This led to the second research question that addressed the remaining two fundamental questions: How can an organization build security values into its policy? How can that policy incorporate both corporate and employee values?

RQ 2: Can VSD be used to create a security policy that reflects both organization and employee values?

The theory and principles of VSD provided a methodology for incorporating disparate stakeholder values into the technical design process (Borning, Friedman, Davis, & Lin, 2005; Denning, Borning, Friedman, Gill, Kohno, & Maisel, 2010; Friedman, Kahn, & Borning, 2006). However no example of VSD being used for policy design could be found in the VSD literature. The second research question explored VSD as a means of designing a values-based security policy.

Relevance and Significance

A growing body of research suggests that it takes a culture of security to foster in employees the habitual and consistent security practices necessary to protect organizational information assets (Corriss, 2010; Thomson, von Solms, & Louw, 2006; von Solms & von Solms, 2004). Security culture research suggests culture is both

established and self-perpetuating when the values of employees and the organization are aligned (Kolkowska, 2011; Lacey, 2010; von Solms & von Solms, 2004). With an average technical control confidence rating of 30% among respondents to the 2010/2011 Annual Computer Crime and Security Survey (Richardson, 2012), there was compelling reason to identify non-technical means of promoting security culture.

Research into security culture had been approached from two directions. One line of research explored the attributes of security culture. These included a framework against which culture could be measured (Baggett, 2003; Da Veiga & Eloff, 2010; Tejay & Dhillon, 2005), a well-defined governance program (Da Veiga & Eloff, 2007), repeated formal training (Rotvold, 2008), and clearly expressed expectations of employee behavior (Thomson, von Solms, & Louw, 2006). Management communications (Cline & Jensen, 2004) and programs to promote security knowledge and awareness (Van Niekerk & von Solms, 2010) were also proposed. These studies focused on the organizational constructs through which security-enhancing behaviors could be defined, observed, and evaluated.

The second line of research explored how an organization could promote the adoption of security culture. There were two assumptions underlying these studies. The first was that security culture could be learned, adopted, and nurtured. Examples included Furnell and Thomson (2009) and Thomson, von Solms, and Louw (2006) and their work on measuring changes in employee behavior as security culture is advanced. The second assumption was that employee adoption of security culture is achieved by aligning organizational and employee attitudes, beliefs, and values (Kolkowska, 2011; von Solms & von Solms, 2004). These studies suggested that in a culture of security,

policies and directives are an expression of already held and shared attitudes, beliefs, and values. By developing programs aligned with attitudes, beliefs, and values, the organization engages employee motivation to embrace security controls (Lacey, 2010). When there is no tie between security practices and employee attitudes, beliefs, and values, it is unlikely that employees will exercise security behavior with the consistency needed to safeguard the organization's information assets (Da Veiga & Eloff, 2010; Williams, 2009).

If the alignment of employee and organizational security values contributes to organizational security culture (Mishra & Dhillon, 2006) and organizational culture prescribes employee security behavior (Alfawaz, Nelson, & Mohannak, 2010; Baggett, 2003; Chang & Lin, 2007; Thomson, von Solms, & Louw, 2006), it follows that strengthening the security value alignment between the organization and its employees strengthens security culture, and in so doing, would strengthen employee security behavior. This is illustrated in Figure 2.

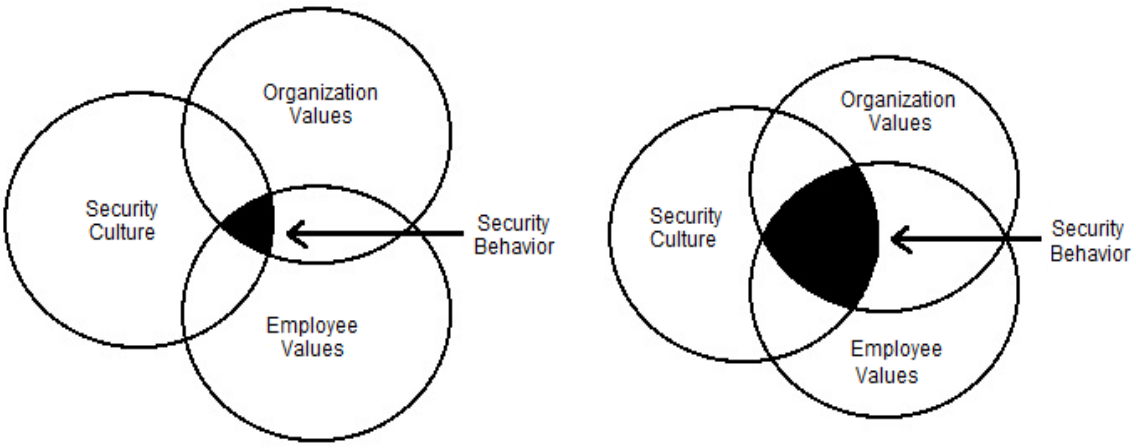


Figure 2. Value alignment strengthens employee security behavior

Although literature makes a compelling argument for establishing a culture of security through alignment of employee and organizational attitudes, beliefs, and values, there has been little research into what constitutes an effective, values-based, security culture change program. Lamm, Gordon, and Purser (2010) contributed by establishing a correlation between employee values and support of organizational change. Dhillon and Torkzadeh (2006) contributed by identifying values-based objectives associated with information security (i.e. emphasize importance of personal privacy and rules against disclosure). Research in the field of value congruence contributed by identifying structures within the organization (i.e. work groups, managers) where alignment with employee values was shown to influence organizational commitment (Meglino, Ravlin, & Adkins, 1989; Ostroff, Shin, & Kinicki, 2005; Posner, 2010). What was missing in the information security literature was an understanding of how organizations could align organizational and employee security values, and a systematic method by which it could be accomplished. This study proposed Value Sensitive Design as a means of accomplishing both.

Barriers and Issues

In their foundational work on understanding business values and creating a framework for future values research, Agle and Caldwell (1999) described the topic as inherently complex. Their review of values research found that personal values were difficult to measure because of imprecise and non-discrete definitions and subjective interpretations of what is theoretically significant. Organizational values research, they found, was also complex. There was little consistency in how organizational values had

been measured or in the theories upon which they were based. Agle and Caldwell suggested the need for research that builds upon existing measures, investigation into how existing measures correlate, and continued exploration of the relationship between shared values, organizational culture, and organizational performance.

Baggett (2003), in his exploration of values within the context of security culture, agreed that values research is challenging. He concluded, "…if identifying and measuring belief systems is difficult, identifying how the board of directors and management go about setting them is next to impossible" (p. 38). Manders-Huits (2011) drew a similar conclusion, describing difficulties in integrating moral values into technology design. She concluded that it was impossible to identify every stakeholder, definitions of values were not precise, stakeholders confused what was and what should be, and even when all these issues were addressed, stakeholders changed their minds.

Given the complexity of values research in general, and values research related to security culture in particular, it is unrealistic to expect one application of one methodology to yield a definitive set of security values, or to produce a policy that incorporates them all. However, one application did show that an organization and its employees could come to an agreement on what it considers its security values, and could create policy statements that incorporate them. In so doing, the study contributed to a better understanding of security values and made it possible for future researchers to test the resulting policy statements for efficacy in promoting the habitual behaviors associated with security culture.

From an operational perspective, the study presented three challenges. One challenge was finding an organization willing to lend its employees and staff and open its

policy to outside scrutiny as security policy is generally considered confidential (Lopes & de Sá-Soares, 2012). Because of the researcher's professional ties, this obstacle seemed surmountable. The second challenge was creating the interview questions and other materials to help participants articulate security values. This is considered one of the more difficult aspects of the VSD methodology to implement (Cummings, 2006; Flanagan, Howe, & Nissenbaum, 2005; Nathan, Friedman, Klasnja, Kane, & Miller, 2008). The literature offered a number of suggestions such as specific questioning practices (Friedman, Kahn, Hagman, Severson, & Gill, 2006), prototyping (Flanagan et al., 2005), a technique called value dams and flows (Denning, Borning, Friedman, Gill, Kohno, & Maisel, 2010; Miller, Friedman, Jancke, & Gill, 2007), and photo-elicitation (Le Dantec, Poole, & Wyche, 2009). Brey (2012), Wright (2011), and Yetim (2011a), ethicists looking for methods of incorporating ethical judgments into information technology designs, suggested using the Delphi method as a means of exchanging opinions, measuring consensus, and addressing the complexity of conflict resolution. Delphi is a process for bringing together disparate ideas and opinions and evolving group consensus (Delbecq, Van de Ven, & Gustafson, 1975; Hasson, Keeney, & McKenna, 2000).

A third challenge was developing a method for translating participant values into policy language as VSD had not yet been applied to the design of a security policy. The application of VSD to the design of a license agreement privacy amendment (Friedman, Smith, Kahn, Consolvo, & Selawski, 2006) provided insight into integrating values into a document. Mulligan and King (2012) offered insight into how policy can fail to address stakeholder values and provided examples of value-eliciting questions.

Assumptions

Because this research was conducted within a single organization with participants selected on the basis of role and geography, certain assumptions about the participants had to be made. The first was that participating employees would be sufficiently fluent in English to understand and articulate thoughts about security values. This was a reasonable assumption because at the site selected for the study, fluency in English was an employment requirement and all employees in the roles selected for participation had responsibilities that engaged them in English communications on a daily basis. The second assumption was that participants, once able to conceptualize and articulate security values through the VSD conceptual and empirical investigations, would be able to apply them to policy language as required in the technical investigation. This was a reasonable assumption because a requirement for participation in the study was job-related responsibility for communicating policy. The third assumption was that managers, selected because they were also security policy makers charged with representing corporate values, would be able to represent both their own concept of security values and those of the organization. A last assumption was that despite the disparate native languages and cultural backgrounds of participants, all would share a common understanding of the agreed upon value sensitive language. Testing that assumption was outside the scope of this research.

Limitations

There were limitations specific to this study and to VSD studies in general that potentially impacted internal validity. To meet the research goal, the resulting security

policy had to reflect the values of the organization's global employees. This meant that participants had to be recruited from offices that spanned 18 time zones. Despite the Manders-Huits (2011) suggestion that the empirical investigation requires explicit and critical discussion, time zone restrictions precluded face-to-face meetings or conference calls. An asynchronous data collection method had to be employed to ensure that participants across all regions had a voice in the design effort.

Inherent in the VSD methodology is value conflict among stakeholders that the design process may or may not be able to resolve (Flanagan, Howe, & Nissenbaum, 2005). Although one of the study goals was to address the conflict and align values, as Manders-Huits (2011) pointed out, participants are not always able to specifically articulate their interpretation of a value and therefore alignment is impeded. Furthermore, there may have been value conflicts within an individual participant. Managers, for example, are responsible for promoting corporate values that may or may not be consistent with their own. The designer also introduced limitations, or in this case the researcher, who decided which values were introduced to participants and how they were categorized (Steen & van de Poel, 2012). The end product the designer intended to create can differ from that which users envisioned (Albrechtslund, 2007). Similarly, the designer's concept of the end product may have been unduly influenced participants (Kujala & Väänänen-Vainio-Mattila, 2009). The designer may not have correctly interpreted or understood the values of participants from diverse cultures (Manders-Huits, 2011) or participants may not have adequately conveyed the values of all members of the constituent groups they represent (Alsheikh, Rode, & Lindley, 2011).

Another limitation of the study concerned the use of a policy document as a

representation of organizational values. Although security policies "are expressions of values as well as sets of instructions" (Hedström, Kolkowska, Karlsson, & Allen, 2011, p. 373), espoused and actual values are known to differ (Kolkowska, 2011). To minimize the difference, the study enlisted security managers over managers in general, as they were the security policy makers with experience representing and enforcing organizational values. However, security managers did not represent management in general, nor were they the policy makers who established the organization's core values from which some of the initial the security values were derived.

Delimitations

Study delimitations were imposed that constrained the scope of the study. The VSD methodology provides for the inclusion of both implicit and explicit stakeholders. With a target end product of a security policy, the explicit stakeholders were the managers that created the policy and the employees who were bound to it. The implicit stakeholders were customers and consumers whose data the policies were designed to protect. A decision was made to exclude implicit stakeholders because the organization deemed its security policies confidential. A second decision was made to limit the target end product to policy statements related to directives that were relevant to all employees. This excluded policies where technical controls enforced the directive or where required actions applied only to a specific employee group. Lastly, the study was constrained to testing a means of aligning employee and organizational values, an underexplored area of security culture research. The study did not test the efficacy of the resulting design.

Definitions of Terms

The information security literature is replete with references to security culture and values and the need to align employee and organizational values in order to bring about security culture. Because there are many different attributes associated with these terms, context-specific definitions are helpful in understanding this study.

Employee and Manager

The American Heritage Dictionary of the English Language (2011) defines employee as a person who works for another in return for financial or other compensation. It defines manager as one who handles, controls, or directs a business or other enterprise. For the purposes of this study, manager was further refined to include positions at director level or above in North America region, or manager and above in the international regions as these roles fit the definition of top management as defined by Ramachandran and Rao (2006). This distinction is important because it is the top management team that conveys how committed the organization is to information security, and commensurate with its commitment, influences adherence with security policy and security-related behavior (Knapp, Marshall, Rainer, & Ford, 2006; Mishra & Dhillon, 2006; Ramachandran & Rao, 2006). It was also important to make a distinction between employee and manager because the literature of organizational values, information security culture, and values congruence described alignment of values as an alignment between employees and management (for examples see Corriss, 2010; Furnell & Thomson, 2009; von Solms & von Solms, 2004) and it is the managers who communicate organizational values through the policies they create (Choi, Kim, Goo, &

Whitmore, 2008; von Solms & von Solms, 2004). It is reasonable to infer from the segregation that management and employees differently define and operationalize security values.

End User Policy / Security Policy

Organizational security values are typically expressed through governance, policies, and management directives that prescribe employee behavior (Da Veiga & Eloff, 2010; Kolkowska, 2011). The specific name of that policy varies widely among organizations (Lopes & de Sá-Soares, 2012). In this study, the terms *end user policy* and *security policy* were used interchangeably. The terms include what some organizations call the Acceptable Use Policy (Doherty, Anastasakis, & Fulford, 2011). They refer to the specific information security governance documents written to prescribe employee behavior with regards to the organization's information assets. This definition was consistent with Thomson, von Solms, and Louw (2006) who described the process of communicating culture as the transference of senior management vision into policy that is then communicated to employees through policy awareness and training.

Information Security and Information Security Program

The terms information security and information security program used in this study specifically related to a formal effort undertaken by an organization for its employees who are users of its information systems. The goal of an organization's information security program is to enhance information security. The U.S. Department of Commerce, National Institute of Standards and Technology (NIST) Glossary of Key Information

Security Terms (Kissel, 2013) defines information security as "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." (p. 94). It goes on to define integrity as a means of guarding against improper information modification or destruction, ensuring non-repudiation and information authenticity. Confidentiality was defined as the preserving of authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. Availability was defined as a means of ensuring timely and reliable access to and use of information. For the purposes of this study, the NIST definition was extended, adding that such protections may be through both technical and administrative controls, and included the management of employee behavior. Dhillon and Torkzadeh (2006) adopted this extension to more clearly connect values with organizational activities related to maintaining information security.

In building an information security program, an organization identifies information security risks and develops measures, performed by employees, to reduce risk. The success of the program is dependent upon employees executing the identified information security measures (Thomson, von Solms, & Louw, 2006; von Solms & von Solms, 2004). The attention to changing employee behavior was significant because information security depends on consistent execution.

Security Culture

In her exploration of security culture in small organizations, Williams (2009) described security culture as a group's shared values, goals, and behaviors, contributing

to its success through awareness of security risk, and day-to-day participation in preventive measures. Security culture drivers included knowledge of risk, formally defined responsibilities, and awareness of both personal and organizational motivators. The purpose of security culture, she claimed, is to create an environment where every member of the organization recognizes the important role each employee must play in protecting information assets.

The Williams (2009) definition of security culture addressed components of security culture with particular relevance to this study. First, it recognized that security culture is based upon shared organizational and employee values that contribute to the success of the organization. The second is that the achievement of security culture came from motivation to translate values into action. For organizations, actions included governance and programs to identify risk and educating employees in how to reduce it. For employees, it was the recognition that their habitual security-enhancing behavior is a critical success factor in safeguarding information. As such, information security culture is the result of aligned security values and security-enhancing behavior.

Security Values

There are numerous references to "values" and "shared values" in security culture research, yet a widely accepted definition of security values does not yet exist. For that reason, this study drew upon the literature of Value Sensitive Design to establish a definition of value, and then the literature of organizational culture to refine the definition within the context of information security. The literature of Value Sensitive Design drew an important distinction between value, marketing quantification based upon what

the end product of the design was worth to its users, and values with ethical or social importance within their context of use (Kujala & Väänänen-Vainio-Mattila, 2009). Friedman and Kahn (2003) and Friedman, Kahn, and Borning (2006) offered as examples human well-being, human dignity, justice, human rights, fairness, accountability, privacy, and support for the democratic process.

The literature of organizational culture put forth the definition of security values adopted in this research, an enduring belief in a behavior that brings about a desirable end state of information security. The idea that a value is an enduring belief that influences behavior was first established by Milton Rokeach (1973) and is widely referenced in the literature of organizational culture (for examples see Kalliath, Bluedorn, & Strube, 1999; Lamm, Gordon, & Purser, 2010; Meglino, Ravlin, & Adkins, 1989; Suar & Khuntia, 2010). Values as an expression of a desired end state is also well established (Agle & Caldwell, 1999; Enz, 1986; Smith, Wokutch, Harrington, & Dennis, 2001). To be a catalyst of change, security values must be expressed (Corriss, 2010). However, a precise set of values associated with security is yet to be determined. The closest work to date remains Dhillon and Torkzadeh (2006), which operationalized security values in terms of specific behaviors.

Value Sensitive Policy

Value sensitive policy is a term introduced in this study. It is defined as an integration of security values and security policy, resulting in a policy statement that includes both the human value associated with the policy and the specific action employees are directed to take in order to protect the organization's information assets. The study also introduces

two related terms – values based policy and values sensitivity policy. Both terms refer to policies into which security values are integrated. Values sensitivity policy is a more specific term, referencing a values based policy created through the VSD methodology.

Summary

This study started with a simple idea, well documented in security literature. Security values, when shared by both an organization and its employees, foster the automatic security-enhancing behavior associated with security culture. That raised the questions this study explored, specifically what are security values and what can an organization do to align its security values with those of its employees. VSD, a design methodology that has evolved from the field of Human Computer Interaction, is a means of addressing both questions. Through its processes, the values of disparate stakeholders were elicited and aligned, and integrated into the design of an end product. When that end product is the organization's end user security policy, the organization has a means of communicating those shared values, promoting security culture and the behaviors associated with it.

Following Chapter 1 is the literature review. It situates the study within the Information Security literature, tracing influences on employee behavior from values to Value Sensitive Design. It also situates the study within the field of organizational culture that provides the foundational theory of this work. Chapter 3 describes the VSD method, its suitability for accomplishing the study's research goals, and how it was applied to create a value sensitive security policy. Chapter 4 presents detailed study results and an analysis of findings. Chapter 5 presents an explanation of the study's

findings, conclusions, and commentary on the extent to which the study's objectives were accomplished. Chapter 5 also discusses the impact of the work on the field of security culture, its contribution to knowledge and professional practice, and implications for future research. The chapter concludes with a summary of the study.

The lists of values used in the conceptual investigation to establish the initial set of security values described in Chapter 3 are included as Appendices A through G. Study instruments and related materials are included as Appendices H through Z. They include the pre-study communication to prospective participants (Appendices H through L), the empirical investigation instructional letters and survey instruments (Appendices M through R), and the technical investigation instructional letters and survey instruments (Appendices S through X). The follow up letter and survey sent to participants to evaluate the methodology are included as Appendices Y and Z.

Chapter 2

Review of the Literature

Introduction

The premise of the study was that security culture requires the alignment of employee and organizational security values. This section provides an overview of seminal works and key research themes related to security culture. It traces the history of security culture research from its roots in organizational culture to themes in values-based security programs and recent work in Value Sensitive Design as a method of building values into the design of technology-related work products. The chapter concludes with a table that summarizes values research from organizational culture to Value Sensitive Design.

Organizational Culture, Organizational Values, and Employee Values

In their study of the challenges of information technology management, Werlinger, Hawkey, and Beznosov (2009) concluded that organizational culture influences security practices and that an understanding of an organization's culture is an important factor in influencing the adoption of those practices. They argued that more research is needed to understand the rationale behind decisions related to information security. The literature of value congruence provided an explanation of why employees adopt security culture and how behavior can be associated with values (Lamm, Gordon, & Purser, 2010).

The concept of congruence as applied in this study came from the Kalliath, Bluedorn, and Strube (1999) definition, "the degree to which an individual and an organization's culture share the same values" (p. 1176). The greater the alignment between employee and organizational values, the greater value congruence. The greater value congruence, the higher the level of organizational commitment and the more likely employees will behave in manner that is consistent with the organization's values, goals, and culture (Kalliath et al., 1999; Ostroff, Shin, & Kinicki, 2005). Much of the exploration of value congruence examined its usefulness in predicting employee attitude (Lamm, Gordon, & Purser, 2010; Meglino, Ravlin, & Adkins, 1989, Posner, 2010) and employee commitment (Amos & Weathington, 2008; Kalliath et al., 1999). It was also used in developing pre-employment screening practices to help minimize new hire turnover and its associated exposure of proprietary information (Maurer, 2006). Posner (2010) found that value congruence's usefulness in predicting employee attitude held across employees of disparate age, gender, educational level, functional discipline, and level of management experience. The finding suggested that value congruence related to security attitude could hold across organizations with diverse employee populations.

Although alignment of employee and organizational values is a fundamental component of security culture (Thomson, von Solms, & Louw, 2006; Van Niekerk & von Solms, 2010), research offered limited guidance in applying that understanding to the development of a security culture program. Obstacles to building a program based on aligned values were explored. They included the complicating factor of conflicting employee values (Kolkowska, 2011) and inconsistencies between actual and espoused security behavior when policy and employee values conflict (Hedström, Kolkowska,

Karlsson, & Allen, 2011; Suar & Khuntia, 2010). However, research based on a value congruence framework proved useful in predicting employee behavior (Lamm, Gordon, & Purser, 2010; Meglino, Ravlin, & Adkins, 1989). For that reason, it may be useful in predicting behavior associated with security culture.

From Organizational to Security Culture

The concept of security culture grew out of Schein's (1990) work on organizational culture and the framework he established for examining it. Schein defined attributes of culture as patterns of assumptions developed by a group, considered valid, and taught to new group members. Organizational culture research extended the definition to include assumptions, perceptions, learning, and automatic patterns of behavior shared by group members. Schein's work had three significant influences on the study of information security. The first was the basic framework for describing and improving security culture. Examples included Vroom and von Solms (2004) who applied the framework as a means of improving the effectiveness of security audits, and Furnell and Thomson (2009) who applied it in their work to improve compliance. The second influence was the structure Schein established for the analysis of organizational culture: observable artifacts, values, and basic assumptions. This has led to definitions and explorations of these concepts within the context of information security. Examples included the explorations of security governance artifacts such policies and awareness programs (Corriss, 2010; Da Veiga & Eloff, 2007) and research into defining security values (Faily & Fléchais, 2010; Schlienger & Teufel, 2003). It is the third Schein influence that has

the most relevance to the goal of this study - the association of organizational culture with automatic patterns of behavior.

Dimensions of Security Culture

Conceptual models of security culture have been proposed to identify the dimensions of security culture and understand the relationship between them. Ramachandran and Rao (2006) proposed a model based on the idea that an organization is comprised of many cultures, each with its own security subculture. Each security subculture has its own set of beliefs and values, and therefore each group will exhibit different security behaviors. A group's true values and beliefs may differ from that which is espoused. Because behavior is influenced by true values and beliefs, a group's behavior may be inconsistent with what the espoused values would suggest. The Ramachandran and Rao model included senior management as one of the many subcultures, with values and beliefs that influence member behavior in ways that differ from non-management employees.

Kolkowska (2011) built upon Schein (1999) and Ramachandran and Rao (2006), offering a model for understanding value conflicts between security subcultures. As suggested by Ramachandran and Rao, Kolkowska found conflicts between espoused values and observed behaviors, and value differences among subcultures. For example, differences were observed between employees in similar roles within different departments. Understanding these value differences and the conflict it generates can be a useful starting point when designing a values-based program of organizational change.

Van Niekerk and von Solms (2010) looked at differences in values that came from differences in organizational priorities such as the classic conflict between business and security objectives. Their model added a fourth level of security culture, knowledge, to Schein's (1999) artifacts, values, and shared assumptions. The addition suggested that organizations incorrectly ignore knowledge because it is assumed that employees have the basic knowledge to do their jobs. Information security, they argued, cannot make that assumption because it cannot be assumed the typical employee knows how to do their job securely.

Da Veiga and Eloff (2010) created a model to describe the interaction between information security, behavior, and culture within an organization, proposing and validating a framework for cultivating security culture. Their model illustrated how security components such as policies, programs, and technical controls influence organizational, group, and individual security behavior, and how these security components interact in a manner that cultivates security culture. By way of illustration, a decision to improve the efficiency of procedures was described. Activities related to the decision such as risk assessment at the organizational level, training at the group level, and policy awareness at the individual level could be identified. Impact on artifacts, values, and beliefs could be assessed. The authors claimed that integrating the framework into strategic security decision-making cultivates security culture by instituting habitual and consistent security behavior.

Brady (2011) explored factors that predict compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA): management support, security awareness, security culture, and computer self-efficacy. Models of influencing factors

were constructed and validated. Security culture was shown to predict security effectiveness, and security culture combined with management support predicted both security behavior and security effectiveness.

In one of the few quantitative studies in security culture research, Tejay and Dhillon (2005) developed a method of measuring the dimensions of security culture in terms of influence on information security. Their method measured the strength of construct components related to cohesiveness, professional codes, awareness, work practice, planning, empowerment, and organizational structure. The researchers suggested that the method could be used to establish an organization's security culture baseline and measure changes to it.

Building Security Culture

The concept of culture as a means of promoting consistent and automatic patterns of behavior has triggered a body of research into what organizations can do to promote employee adoption of habitual security practices. Three themes emerge. The first is that management changes behavior and behavior creates culture. The second is that education and enforcement foster security culture. The third is that organizations can use culture to build security.

Baggett (2003) set responsibility for framing employee attitude with senior management, claiming they are responsible for establishing the organization's belief systems. The example of the Organisation for Economic Co-operation and Development (OECD) Guidelines was offered. The OECD Guidelines established and defined principles of security culture that reflect organizational beliefs: awareness, responsibility,

response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment. The Guidelines could be used as an audit framework defining evidence of security culture. Such evidence could include Board of Directors' and executives' stated policy and responsibilities for securing a company's information systems, plans for incident response, identified risk and implemented safeguards, and the periodic review of programs and corrective actions taken on the basis of them. Baggett claimed that it was the responsibility of auditors to uncover gaps in the controls that evolve from these policies, plans, and reviews. It was the responsibility of employees to be compliant. It was the responsibility of management to enforce the Guidelines and take corrective actions.

Vroom and von Solms (2004) contributed insights into the evolution from organizational to security culture. They established a model of security culture based on the premise that when employees are knowledgeable about security policies and believe in their importance, that knowledge and belief will influence their behavior and the behavior of the organization as a whole. Culture change, they claimed, occurs at the individual, group, and organizational levels, and each level influences the others. Organizational behavior influences shared values and knowledge. Shared values and knowledge changes group behavior and influences individual behavior. Vroom and von Solms claimed that although the employees' role in protecting assets was known to be critical, obstacles to auditing employee behavior remained. Traditional information technology audits evaluated technical, strategic, and operational aspects of security, not human. The audit baseline was company policies. There was no comparable baseline for auditing employee behavior. However, understanding the organization's employee

culture – individual and collective behavior – aided in structuring the business in a manner conducive to information security.

Da Veiga and Eloff (2007) considered security culture to be derived from information security governance. Its purpose was to control employee behavior. From that perspective they combined the components of four governance frameworks: ISO 17799; Policies, Risks, Objectives, Technology, Execute, Compliance and Team (PROTECT); the Capability Maturity Model; and Information Security Architecture. Collectively these four identified the requirements of a security program. Implementing controls identified in the combined framework, they suggested, was the first step management must take toward establishing security culture.

Thomson, von Solms, and Louw (2006) explored how employees should build the correct information security skills into day-to-day behavior and offered a model for achieving information security obedience. Because organizational culture influences employee behavior, they argued, it could be used to model security behavior. They described how culture operates at conscious and unconscious levels, communicating explicitly and tacitly. At the first level, senior management must establish a vision for security culture through policy and transfer it to employees through awareness and training. Employees must then practice the skills until they are understood and absorbed, and become part of their unconscious set of behaviors. Through socialization these behaviors are transferred to others in the group and across groups, and are enforced by both culture and policy.

Furnell and Thomson (2009) looked at security culture as means of compliance and suggested there is a broad range of attitudes and knowledge from which it is comprised.

Security training and awareness were means of influencing attitude, which when increased, fostered security culture. However, there are limitations in training and education programs suggesting that security culture must be reinforced by management and measured as changes in the behavior of its employees. Boss, Kirsch, Angermeier, Shingler, and Boss (2009) also looked at employee compliance and management enforcement outside the context of security culture. Their study found that employees were more likely to comply with policies when they specified expected behavior, when compliance behavior was monitored, and when compliance was perceived to be mandatory. Rewards for compliance were not found to improve employee perception that policy compliance was mandatory. Although the study was about security compliance, not culture, the researchers suggested that employees in an organization with a strong security culture could differently perceive specification, evaluation, and rewards.

Corriss (2010), too, claimed that security culture comes from the top down and is achieved through education and policy enforcement. Senior management holds the strongest influence, they suggested, because management defines the strategy, strategy defines the structure, and structure influences culture. It is also senior management that establishes the mission statement and statement of core values. Corriss concluded, “The problem [of integrating security into organizational culture] is that managers are not enforcing security policy because top-level management either is not complying with the organization’s security policy or is lax in enforcing it.” (p. 40).

Chang and Lin (2007) described security culture as an organizational culture trait that facilitates security by building upon shared values, beliefs, and norms. Their work explored the relationship between organizational culture and effective information

security management. The influence of an organization's culture on information security practices could be negative or positive. Cultural traits such as flexibility do not positively influence security, but control-oriented traits such as effectiveness and consistency do. They concluded that it was management's responsibility to integrate a program of security controls with an understanding of cultural influences to achieve information security objectives.

Alfawaz, Nelson, and Mohannak (2010) also investigated national and organizational cultural values on employee security behavior and found cultural obstacles to compliance. In a culture where employees relied on managers for guidance and problem solving, employees expected a specific group such as Information Technology to be responsible for information security. Employees expected management to tell them what to do if a problem arises. Like Chang and Lin (2007), this study concluded that it was management's responsibility to understand cultural influences on information security and integrate that understanding into its security program. The findings went one step further and illustrated the need for consistent policy enforcement and consequences for noncompliance.

Ghernouti-Helie, Tashi, and Simms (2010) agreed with Da Veiga and Eloff (2007) that a governance framework is the starting point of security culture. However, they also agreed with Chang and Lin (2007) and Alfawaz, Nelson, and Mohannak (2010) that a single governance framework for organizations and collaborations spanning disparate security cultures is insufficient. Defining security culture as "the norms and behaviors that user's [sic] follow voluntarily" (p. 353), they suggested governance must provide for differing cultural norms. It must also include processes and activities that address

culture-specific concerns and the varying levels of assurance. This facilitates consistency across differing regulatory environments and corporate cultures.

Lacey (2010) reviewed critical success factors related to transformative organizational security change. Organizational culture continuously changes through mergers, acquisitions, recruitment drives, globalizations, and new communication media, he claimed. Therefore vehicles for change must start with a basic understanding of culture: attitudes, values, beliefs, and norms. Change requires a process of self-discovery that employees could absorb on their own terms, as well as an understanding of and empathy with circumstances.

Security Values

Of the described studies, values played a prominent role in Alfawaz, Nelson, and Mohannak (2010), Corriss (2010), Kolkowska (2011), Ramachandran and Rao (2006), and Tejay and Dhillon (2005). The common thread in these studies was the focus on how employee values could be aligned with those of the organization. Little attention was given to how both parties could actively work toward value alignment.

Dhillon and Torkzadeh (2006) represented the first attempt to describe security practices in terms of values. Using values-focused thinking, managers identified values associated with security controls and evolved 86 objectives related to organizational security. Among the values-based objectives were items such as: create an environment that promotes organizational loyalty; emphasize the importance of personal privacy; and create an environment that promotes respect. The Dhillon and Torkzadeh study did not specify the human values associated with the objectives.

Schlienger and Teufel (2003) looked at methods for analyzing organization culture that are useful in analyzing security culture. They found values to be important in security culture research because behavior is driven by values and because lasting changes in behavior are driven by changes in values. Leach (2003) examined influences on employee behavior: what employees are told, what they see in practice, and past experiences. Communication of security values was a factor in each: policies and directives (what is told), managerial conduct and corporate practices (what is evident), and programs to monitor and respond to instances of good and bad behavior (what is rewarded or punished). According to Leach, organizations building a security culture must focus on clear and consistent communication to employees of organizational values. Communication of employee values to the organization was not considered useful.

In their exploration of security values related to e-Science, Faily and Fléchais (2010) echoed many of the aforementioned themes. For example, they cited the frequently referenced statement that it is management's responsibility to communicate security culture, and this is most frequently done through policies. However, they went on to say it is not policy that brings security to their attention, but the various controls that constrain activities. Formal responsibilities also highlighted employee security issues, yet employees did not adopt a sense of moral responsibility until the organization made them aware of the responsibility. Faily and Fléchais also found users to be indifferent to security issues when they were perceived to be beyond their control. Here again, it is the responsibility of the organization to get the employee to change perceptions of security. It is not perceived to be a partnership.

Communicating Organizational Values

Communicating values as a means of influencing behavior is not a new topic within the information security literature. There is broad consensus that formal communications are essential components in safeguarding information assets (Lopes & de Sá-Soares, 2012). Organizations have numerous mechanisms for communications. Among them are information systems policies (von Solms & von Solms, 2004), codes of ethics (Burmeister, 2013; Stevens, 2008; Timmermans, Zhao, & van den Hoven, 2011), acceptable use policies (Doherty, Anastasakis, & Fulford, 2011), formal security training (Thomson, von Solms, & Louw, 2006), and security awareness programs (Gundu & Flowerday, 2013). Beyond formal communications mechanisms, organizations can provide additional awareness through oral or written communiqués (Corriss, 2010; Doherty et al., 2011; Stevens, 1999). Written channels include handbooks, email reminders, and posters. Oral channels include voicemail messages, meetings, group discussions, and conversations with managers

Regardless of communication mechanism, to create a values-driven organization, the behavior associated with those values must be clearly articulated (Stevens, 2008). The communiqué must create a shared vision and reflect a message consistent throughout the management team (Young & Post, 1993). Doherty, Anastasakis, and Fulford (2011) found little consistency among organizations in the particular type of communications provided (i.e. handbook, acceptable use policy, code of ethics, etc.) or the type of information included in each (i.e. policy, procedure, standards, legal compliance requirements). The plethora of communication vehicles within a single organization could be a source of confusion, particularly when there is no overriding framework, when

communication lacks specific references to other communications, and when finding the source of a specific mandate is difficult (Doherty et al., 2011; Tsohou, Kokolakis, Lambrinoudakis, & Gritzalis, 2010).

The aforementioned studies reflect an understanding of the importance of integrating values into behavior-influencing communications. However, much of the values literature focuses on top-down communications – what managers must do to change employees. Vroom and von Solms (2004), for example, suggested that changing organizational artifacts changed behavior, and changing behavior changed shared values. Killingsworth (2012) suggested communicating values by first understanding how employees perceive the organization's values. Publishing a values statement and telling hypothetical and real stories about values-related decisions could systematically change perceptions that are inconsistent with the organization's values. Publicly recognizing employees would "reinforce the employee's commitment to the organization and her acceptance of its authority" (Killingsworth, 2012, p. 985). Corriss (2010) stated, "Inclusion of the words 'privacy' or 'information security' in an organization's list of core values does not guarantee that everyone in the organization will value them unless management demonstrates their commitment." (p. 37). Management commitment was described as a combination of "carrot and stick" activities such as educating employees on the positive impact on customers associated with compliance and the legal ramifications of non-compliance.

The concept of shared values is foundational to security culture (Chang & Lin, 2007; Killingsworth, 2012; Vroom & von Solms, 2004; Williams, 2009). Young and Post (1993) suggested that to effectively influence behavior, the values discussion must

be two-way, including both management and employees. However, the information security literature offers little instruction in how to communicate values other than from management to employees. Value Sensitive Design, discussed in the next session, was introduced as means of facilitating a discussion of values that includes all stakeholders as equal participants in the discussion.

Value Sensitive Design

Friedman and Kahn (2003) situated the study of values within other approaches to the intersection of technology, values, and ethics, and made two unique contributions. The first contribution was its basis in principle, with moral values epistemologically independent of any person or group. The second was that it prescribes a methodology for identifying and building into the design of a technical asset the human value requirements of its stakeholders. The methodology provided a means of addressing competing values and testing value decisions throughout the design process. The VSD literature can be organized into two areas of research. One area includes theory, methodology, and related discussion on attributes and limitations. The second consists of case studies where VSD is applied as a means of integrating stakeholder values into the design of a technical artifact. As a body of work, VSD has been shown to be flexible in its implementation and still evolutionary as a design methodology.

VSD was introduced by Batya Friedman (1996). In that foundation article, Friedman described the problems that occur when human values are not addressed in technical design, and what the design effort looks like when they are. Integrating values into the design goes beyond the usability considerations of HCI, addressing a range of

ethical considerations. Freedom from bias, for example, is a value that when recognized, can prevent educational software from favoring learners from one cultural background over another. Friedman, Kahn, and Borning (2001) evolved Value Sensitive Design into a theoretical and methodological framework through which the value dimensions of design work are incorporated. Its goal was to operationalize computer ethics, building into design efforts the human values that intersect with technology. Friedman and Kahn (2003) situated the methodology within the field of Human Computer Interaction, fleshing out the activities undertaken in three iterative, but distinct types of investigations to identify relevant values, address value conflicts among stakeholders, and modify a design to incorporate value-related attributes.

At the core of VSD is an iterative, tripartite, methodology that identifies the human value requirements of stakeholders, addresses competing values, and tests value decisions throughout the design process (Friedman & Kahn, 2003). The methodology is comprised of three investigations: conceptual, empirical, and technical. The first VSD activity is the conceptual investigation, beginning with a literature search to identify values associated with the design. During this investigation the philosophical ontological literature is used to help define and understand the relevant values. To aid in the investigation, Friedman, Kahn, and Borning (2006) established a list of human values with ethical import (see Appendix A) for researchers to use as a starting point. The concept of human values with ethical import was introduced in Friedman and Kahn (2003) as a means of distinguishing usability factors, which in and of themselves can be a human value, from moral values – issues of fairness, justice, virtue, and human welfare. The Friedman, Kahn, and Borning (2006) list included values frequently implicated in

system design, along with definitions, and references to relevant philosophical literature. Once a set of relevant values has been conceptualized, the empirical investigation can begin.

In the empirical investigation, participants are guided toward a collective expression of values. VSD methodology does not prescribe specific techniques, but Friedman, Kahn, and Borning (2006) suggested drawing upon quantitative and qualitative social science research methods for helping participants articulate values. This includes using semi-structured interviews with probing questions such as "Why?", "What is..?" or "What problem have you encountered with…?" As values are identified, their philosophical roots are explored (a return to the conceptual phase) and then reintroduced to participants for further explication. Iterative returns to the conceptual and empirical investigations continue until participants agree on the key values and their definitions. At that point, and in keeping with Friedman, Kahn, and Borning (2001), the study moves to the technology investigation.

The technology investigation focuses on the object of the design effort – how to integrate the values identified in the previous investigations into the design object. Decisions must be explored to ensure an understanding of how different groups of stakeholders are affected and what trade-offs have to be made to address value conflicts. New values may arise that must go through conceptual investigation, and new value understandings may emerge through continued empirical investigation. The tripartite, iterative VSD process is diagrammed in Figure 3.

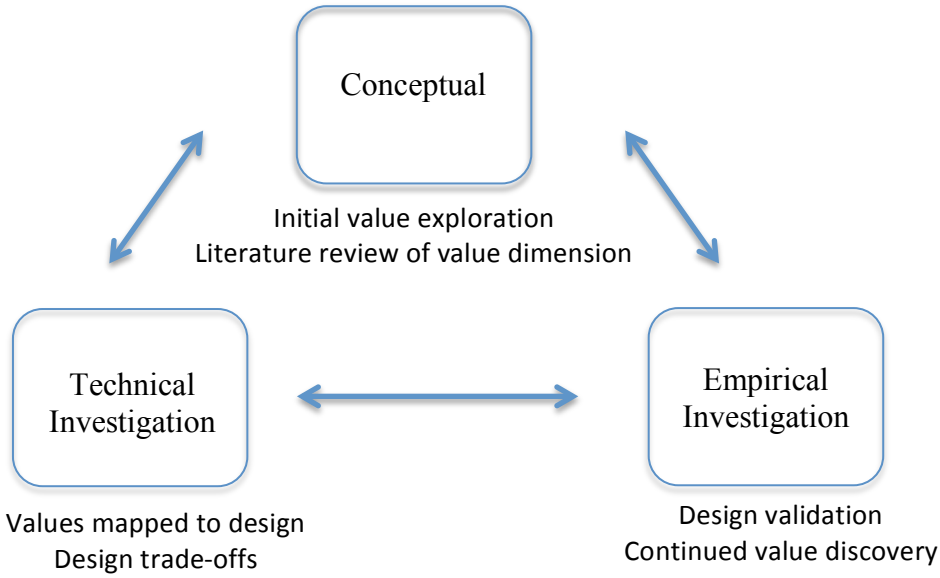


Figure 3. The tripartite, iterative VSD process. VSD is comprised of three types of investigations. When a new value relevant to the design is suggested in the course of one investigation, it is necessary to subject it to the other two investigations. This process continues until there is an agreed upon value set that has undergone all three investigations.

Since the publication of the VSD foundational studies (Friedman, 1996; Friedman & Kahn, 2003; Friedman, Kahn, & Borning, 2001), scores of case studies have been published in which VSD is applied. This research has extended both the breadth of what is considered a technical design, as well as the activities undertaken in each of the three investigations. This has also led to a better understanding of the limitations of VSD, and suggested modifications. In its earlier applications, technical design efforts were traditional technologies such as the web browser (Friedman, Howe, & Felten, 2002), application software (Borning, Friedman, Davis, & Lin, 2005), and educational gaming software (Flanagan, Howe, & Nissenbaum, 2005). Later studies reflected a broader definition of technical design, including end products such as weapon systems (Cummings, 2006), public transport systems (Ferris, Watkins, & Borning, 2009), and

medical devices (Denning, Borning, Friedman, Gill, Kohno, & Maisel, 2010).

The extensive application of VSD has also led to an understanding of its limitations. Calling VSD "the most reviewed approach pertaining to values in technology design" (p. 273), Manders-Huits (2011) focused on VSD's shortcomings. She claimed the process for understanding underlying issues is insufficiently rigorous. VSD cannot identify every indirect stakeholder, and because technology is so complex, those stakeholders who are interviewed would have insufficient information to address technical issues or evaluate design alternatives. VSD value descriptors are also too broad, putting into question the usefulness of user interviews. Even when stakeholders arrive at consensus, individuals change their minds. Lastly, the methods used to address values in technology confuse the stakeholders "should" with the normative "is," making the assumption that the recommendations of interviewed users are equivalent to fact of the human condition.

VSD practitioners have overcome limitations in the methodology, extending empirical investigation methods and adding to an ever-growing toolset of techniques for identifying and integrating values into design. These extensions have proved useful because they provide explicit methods for fleshing out stakeholder values, particularly when the value extends beyond Friedman and Kahn's (2003) original list of 12 human values (Le Dantec, Poole, & Wyche, 2009)[1]. Much of the evolutionary literature addresses ways of helping users articulate values.

Friedman, Kahn, Hagman, Severson, and Gill (2006) gave study participants a simple vocabulary for expressing ethical decisions by asking if a particular scenario was "All right" or "Not all right," and also asking how that response might differ from the

[1] A list of the original 12 human values of ethical import, and the Friedman and Kahn (2006) addition of a 13th is included in Appendix A.

perspective of different stakeholders. Flanagan, Nissenbaum, Belman, and Diamond (2007) developed a deck of cards called value cards. Each card represented a value identified in the conceptual investigation. Each participant in turn drew a card from the deck and discussed the value within the context of the design project. Denning, Borning, Friedman, Gill, Kohno, and Maisel (2010) suggested using a dams and flows categorization to quickly rule in or rule out language or concepts strongly in agreement (flows) or contested (dams). Dams and flows is a particularly useful approach when there is a large study population who produce an extensive initial set of values for consideration.

Friedman, Smith, Kahn, Consolvo, and Selawski (2006) used a modified scenario-based value elicitation method, creating what they called a threat model. A threat model evolved from the stakeholder's description of what was to be prevented and what an adversary could do to perpetrate an exploit. The method asked such questions as what can be harmed (asset), who or what can do the harm (threat), how easy would it be to cause harm (vulnerability), and what mitigations may be taken to prevent harm. Cummings (2006) focused on the problem of competing values and their influence on the design. She suggested starting the empirical investigation by identifying the ethical context of the object under design and then assessing the values within that context. A matrix was constructed that tracks responses to two questions: Does the feature reflect the conceptual attribute associated with the required value? Why is it (not) a good feature to include? By fleshing out competing values, the full range of ethical issues could be addressed in the design.

Finding the full VSD methodology beyond the time and budget of their

development effort, Nathan, Friedman, Klasnja, Kane, and Miller (2008) used scenario-based design to facilitate conversations around value sensitive solutions, effectively combining conceptual and empirical investigations. They employed a method called envisioning that presented participants with systematic and strategic activities designed to help weigh the value of a feature against its social cost. Potential value concerns were incorporated into scenarios, and then structured interviews were employed to elicit stakeholder judgments. Deploying this method throughout the design cycle could be an effective means of integrating long-term systemic envisioning into design practice. Yoo, Huldtgren, Woelfer, Hendry, and Friedman (2013) built upon the Nathan, Friedman, Klasnja, Kane, and Miller envisioning technique by creating what they called envisioning cards. Envisioning cards, along with values scenarios, helped stakeholders imagine the effect of the technology, particularly negative effects, over a time.

Le Dantec, Poole, and Wyche (2009) also sought to streamline the methodology, but at the same time, found that local values were of greater relevance to the overall design than universal values. As such, they suggested starting with the empirical investigation. To facilitate in situ discovery, they used photo-elicitation to identify moral values relevant to or possibly in conflict with stakeholders. This method involved showing participants images of objects and situations and asking if they related to the design. For example, in a study of the public's perception of radio frequency identification (RFID) technology, participants were shown photos of every day objects and, through semi-structured interviews, were asked to imagine how RFID might be used in the scenario. Through this exercise researchers were able to explore participants' thinking about values associated with RFID applications. Pommeranz, Detweiler,

Wiggers, and Jonker (2012) built upon Le Dantec et al. with an even greater effort toward in situ discovery, arguing that the discussion of values must be within the context of real life. They employed photo elicitation using photos taken by the participants within the context of their daily activities. This, they found, helped elicit values specific to the personal use of the design object.

In a review of design efforts that incorporate VSD, Borning and Muller (2012) described areas in which VSD practitioners have made overreaching claims. They suggested ways of incorporating other HCI research methods into design activities to improve the methodology. One current problem related to the universality of the values – or rather that the values identified might not be universal. Another set of problems was around the question of whose values were included in the final design. The list of values a researcher brings to the conceptual investigation, the stakeholders participating in value identification, and the designers and researchers themselves bring cultural biases to the discussion. Citing some of the aforementioned references, the researchers reminded their readers that values do not have to be universal and that the list of values offered in Friedman, Kahn, and Borning (2006) should be treated as a heuristic, not a definitive list. Stakeholder bias could be countered by including a broadened scope of stakeholders in the design, and designer and researcher bias could be overcome by better informing participants of relevant personal values.

As already noted, VSD has not yet been used to develop a value sensitive information security policy. However, there is one VSD application that has enough similarity with the study to warrant a more detailed review. Burmeister (2013) described a 25-year effort to establish an information and communications technology (ICT) Code

of Ethics (CoE) for the International Federation of Information Processing (IFIP). IFIP is a global society made up of IT professional associations from 50 member nations. In analyzing prior attempts to formulate an ICT CoE, he found that it was considered too difficult to establish because of continuous changes in technology and because of cultural diversity. Changes in technology were challenging because a CoE that was specific enough to prescribe technology-related behavior could require more frequent updates than was practical for the organization. Cultural diversity was challenging because research suggested that culture strongly influences what is considered ethical behavior.

Burmeister (2013) distinguished between values and behaviors associated with values. Whereas values stay relatively static, behaviors associated with values change over time and vary across cultures. He suggested that identifying shared values associated with professional information processing practices rather than individual member ethics could transcend challenges with both cultural diversity and changes in technology. As supporting argument, he cited successful VSD research in the engineering field and the application of VSD-identified shared values within engineering design. For the ICT project, Burmeister suggested a hybrid CoE with global values associated with local practices. Burmeister's suggestion was an important consideration for this study because a corporate end user policy, by definition, dictates behavior across the global, multi-cultural organization.

Trends in Current Research

Within the literature of human aspects of information security, employee behavior and how to best communicate policy compliance expectations continue to be a topic of

interest. Pieters, Padget, Dechesne, Dignum, and Aldewereld (2013) suggested aligning policies to threats can help employees understand the risks associated with noncompliance. Kirlappos, Parkin, and Sasse (2014) explored the complex and cumbersome nature of policies that lead well-intentioned employees to develop workarounds to them. Ashenden and Lawrence (2013) adapted social marketing techniques as a means of preventing workarounds. The approach involved employees in creating awareness, designing the processes that support controls, and addressing noncompliance. Parsons, McCormac, Butavicius, Pattinson, and Jerram (2014) developed an instrument to measure employee knowledge, attitude, and behavior against which control strategies can be measured. Their research found that knowledge influences attitude but it is attitude that influences behavior. This is consistent with work undertaken by Kim, Yang, and Park (2014). In their study of behavior and policy compliance, they found a number of factors that affected compliance. These included employee belief in the effectiveness of the policy, the attitude of other members of the organization toward the policy, and the employees' understanding the benefits of policy compliance. To some extent, all five of these studies looked at what employees value and explored means of aligning those values with security policy.

Methods for integrating values into design continues to flourish in literature and in practice with two or three new studies each month documenting values in the design of everything from cloud storage (Stark & Tierney, 2013) to wind turbines (Oosterlaken, 2014). Three studies in particular contributed to meeting the challenges of eliciting and understanding stakeholder values. Koepfler, Shilton, and Fleischmann (2013) developed a method for the online solicitation of shared and conflicting values when face-to-face

communication is not practical. They introduced the concept of stakeholder associations, a means of acknowledging in the design effort the multiple and sometimes overlapping roles an individual may hold. Their work provided a more nuanced understanding of competing values and is useful for recruiting participants with diverse values. Epstein, Borning, and Fogarty (2013) explored the elicitation of values when stakeholders hold multiple and conflicting values. The scenarios they developed are similar in nature to the ones developed for this study, but were paired with semi-structured interviews. Whereas earlier work on values conflict focused on differences among participants, this work provided insight into addressing value conflicts within the individual participant. Voida, Dombrowski, Hayes, and Mazmanian (2014) explored a third dimension of value conflicts, stakeholders who articulated shared values during the values elicitation segment of a design effort, but found conflicting interpretations of those values in practice. Their study suggested that values elicitation must extend beyond asking what values are of interest to include how the values will be operationalized.

Although not specifically VSD research, Winschiers-Theophilus and Bidwell (2013) presented an insightful study of cross-cultural design and how data collection techniques contributed to inaccurate conclusions. Their work explored HCI as a paradigm "…deeply rooted in a Western epistemology and intrinsically privilege certain assumptions, values, definitions, techniques, representations, and models." (p 253). In so doing, they provided insight into the limitations of language translations and offered techniques that can be applied in VSD empirical and technical investigations to obtain more comprehensive cultural perspectives.

Table 1 summarizes the key research themes and related literature described in this section.

Table 1

Values Research from Organizational Culture to Value Sensitive Design

Topic	Key Research Themes	Literature
Organizational culture	Organizational culture includes assumptions, perceptions, learning, and automatic patterns of behavior shared by group members.	Schein, 1990
Value congruence	Value congruence explains why employees adopt security culture and how behavior can be associated with values.	Lamm, Gordon, & Purser, 2010.
	Value congruence explores the degree to which an individual and the organization share the same values.	Amos & Weathington, 2008; Kalliath, Bluedorn, & Strube, 1999; Ostroff, Shin, & Kinicki, 2005
	Value congruence can predict attitude and commitment across employees of disparate age, gender, educational level, functional discipline, and level of management experience.	Maurer, 2006; Meglino, Ravlin, & Adkins, 1989; Posner, 2010
Communicating expectations of security behavior	Expectations of behavior are communicated through policy, codes of ethics, training, awareness programs, and conversation between managers and employees.	Ashenden & Lawrence, 2013; Burmeister, 2013; Corriss, 2010; Doherty, Anastasakis, & Fulford, 2011; Gundu & Flowerday, 2013; Kim, Yang, & Park, 2014; Kirlappos, Parkin, & Sasse, 2014; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; Pieters, Padget, Dechesne, Dignum, & Aldewereld, 2013; Stevens, 1999; Stevens, 2008; Thomson,

		von Solms, & Louw, 2006; Tsohou, Kokolakis, Lambrinoudakis, & Gritzalis, 2010; von Solms & von Solms, 2004
Organizational culture as a framework for security culture	Organizational culture influences security practices. It is analyzed through observable artifacts, values, and basic assumptions, and provides a framework for describing and improving security culture.	Furnell & Thomson, 2009; Vroom & von Solms, 2004; Werlinger, Hawkey, & Beznosov, 2009
	When employees are knowledgeable about security policies and believe in their importance, that knowledge and belief will influence their behavior and the behavior of the organization as a whole.	Corriss, 2010; Da Veiga & Eloff, 2007; Lacey, 2010; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; Vroom & von Solms, 2004
Building security culture	Organizations can use culture to build security and predict security behavior. Management changes behavior and behavior creates culture. Culture, in turn, influences behavior. Components of the program may include governance, education, socialization, and enforcement with and for employees and managers.	Alfawaz, Nelson, & Mohannak, 2010; Baggett, 2003; Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Brady, 2011; Corriss, 2010; Da Veiga & Eloff, 2007; Faily & Fléchais, 2010; Furnell & Thomson, 2009; Ghernouti-Helie, Tashi, & Simms, 2010; von Solms, & Louw, 2006
	Organizations are comprised of many cultures and subcultures, each with their own behavior-influencing values and beliefs. Differences in values may come from differences in organizational priorities, or may reflect conflicts between espoused values and observed behaviors.	Kolkowska, 2011; Ramachandran & Rao, 2006; Van Niekerk & von Solms, 2010

Security values	Alignment of employee and organizational values is fundamental to security culture.	Chang & Lin, 2007; Dhillon & Torkzadeh, 2006; Thomson, von Solms, & Louw, 2006; Van Niekerk & von Solms, 2010
	Cultural values influence how employees interpret security expectations.	Alfawaz, Nelson, & Mohannak, 2010
	Values are important in security culture research because behavior is driven by values, and because lasting change in behavior is driven by change in values.	Schlienger & Teufel, 2003
	Organizations building a security culture must focus on clear and consistent communication to employees of organizational values.	Chang & Lin, 2007; Corriss, 2010; Killingsworth, 2012; Leach, 2003; Vroom & von Solms, 2004; Williams, 2009; Young & Post, 1993
Obstacles to values alignment	Conflicting values, inconsistencies between actual and espoused values based security programs.	Epstein, Borning, & Fogarty, 2013; Hedström, Kolkowska, Karlsson, & Allen, 2011; Koepfler, Shilton, & Fleischmann, 2013; Kolkowska, 2011; Suar & Khuntia, 2010; Voida, Dombrowski, Hayes, & Mazmanian, 2014
Value Sensitive Design	VSD theory, methodology, attributes, and limitations	Borning & Muller, 2012; Friedman, 1996; Friedman & Kahn, 2003; Friedman, Kahn, & Borning, 2001; Friedman, Kahn, & Borning, 2006; Le Dantec, Poole, & Wyche, 2009; Manders-Huits**,** 2011
	Application of the VSD methodology	Burmeister, 2013; Borning, Friedman, Davis, & Lin, 2005; Cummings, 2006; Denning, Borning, Friedman, Gill, Kohno, &

	Maisel, 2010; Epstein, Borning, & Fogarty, 2013; Ferris, Watkins, & Borning, 2009; Flanagan, Howe, & Nissenbaum, 2005; Friedman, Howe, & Felten, 2002; Friedman, Kahn, Hagman, Severson, & Gill, 2006; Friedman, Smith, Kahn, Consolvo, & Selawski, 2006; Koepfler, Shilton, & Fleischmann, 2013; Nathan, Friedman, Klasnja, Kane, & Miller, 2008

Summary

Chapter 2 provided an overview of research on security values and their influence on security behavior. The section started with the concept of value congruence, an alignment of employee and organizational values shown to be useful in predicting employee behavior. It established parallels between fostering employee behavior in a manner that is consistent with the organization's general values and fostering security behavior in a manner consistent with its security values. The chapter then described the literature of organizational and security culture. It is this line of research from which two conclusions, central to the study, were drawn. One was that security culture is, in part, disseminated within the organization through artifacts such as policy documents. The second was that once adopted, security culture is self-perpetuating. New employees adopt culture, and through that adoption, habitually follow the associated security behaviors.

Having established the relationship between security values and consistent security behavior, the literature review focused attention on how the organization goes about aligning employee security values with those of the organization. The first question asks, "What are security values?" Here the literature is sparse. Aspects of security values have been explored such as defining values in terms of organizational objectives and practices. However, an empirically validated list of security values has not yet been established. Despite the lack of empirically defined security values, the literature has investigated numerous verbal and written mechanisms for communicating them. Although there is an understanding that value alignment must include two-way communication, there are few examples in the literature on how to communicate values other than from senior management down.

The chapter concluded with an overview of the VSD literature. The three investigations that make up the methodology were described, and examples were presented illustrating how VSD has been used to build stakeholder values into a wide variety of design projects. Particular attention was paid to research related to building consensus on non-IT security values and building values into other types of policy documents. This research formed the basis for the study, suggesting that VSD could be used to define security values, build organizational and employee consensus on that definition, and potentially incorporate the shared understanding into a policy document.

Chapter 3

Methodology

Introduction

The goal of the study was to determine if VSD is an effective method for integrating organizational and employee values into the organization's end user security policy. There were two components of the exploration. The first was to test if VSD is useful in identifying values that both employees and organizations associate with security behavior (RQ 1: What values do employees and organizations associate with security behavior?). The second was to test if VSD is useful for creating a security policy that reflects those values (RQ 2: Can VSD be used to create a security policy that reflects both organization and employee values?). As referenced in earlier chapters, the literature offered VSD as a well-established method for identifying and aligning stakeholder values and integrating the resulting value set into the design of a technology related end product (Manders-Huits**,** 2011; Wright, 2011; Yetim, 2011a). The study tested VSD as a methodology when the technology end product is an end user policy. An end user policy was selected as the end product because it had been established that organizations articulate their values through policy (Hedström, Kolkowska, Karlsson, & Allen, 2011; Thomson, von Solms, & Louw, 2006) and because of its ubiquity across all types of organizations. The study contributed to the literature and practice of building security

culture by showing how security values can be defined and how employee and organizational values can be aligned. It also contributed to the VSD literature, as Friedman, Smith, Kahn, Consolvo, and Selawski (2006) noted, when the methodology is applied to new types of technology designs, the field of VSD moves forward.

Conceptual Investigation

As prescribed by Friedman and Kahn (2003), the study followed VSD's iterative, tripartite, methodology to identify the human value requirements of stakeholders, address competing values, and test value decisions throughout the design process. The first part of the methodology was the conceptual investigation, made up of two components. In one component stakeholders were identified and a means of ensuring their inclusion in the study was established. In the second component, an initial set of security values, the starting point for participants in the empirical investigation, was determined. The VSD literature offered a variety of methodologies for each of these two components. The methods chosen to support the goals of this study are described in the next section.

Site and Participant Selection

The VSD literature did not prescribe a specific method for deciding who should determine values or through what process (Yetim, 2011b), but rather focused on including direct and indirect stakeholders in the process (Friedman, Kahn, & Borning, 2006). There was no expectation that every value consideration for the life span of the end product would be identified (Manders-Huits, 2011) or that the identified values were universal (Borning & Muller, 2012). The VSD literature illustrated the wide variation in

both the size of the study group and methods of data collection. For example, a study that involved the use of HDTV cameras in a busy public area was conducted with a paper-based survey, capturing responses from 750 passersby (Friedman, Kahn, Hagman, Severson, & Gill, 2006). A study of a specialized implantable medical device had 17 participants who interacted with mockups of the technical end product during a single semi-structured interview (Denning, Borning, Friedman, Gill, Kohno, & Maisel, 2010). A study of an artificial office window had seven participants who completed seven structured interviews, 30 surveys, and ongoing journal entries over a 16-week period (Friedman, Freier, Kahn, Lin, & Sodeman, 2008). In each study, participation and data collection decisions were based on the characteristics of the stakeholder group and type of product under design.

It was important to select a study population diverse enough to allow generalization of the study findings. Purposeful sampling was chosen as the means to do that as, by definition, it identifies a study group based on its ability to provide information better than other choices (Maxwell, 2005). Purposeful sampling was also appropriate for the data collection method as it is designed to generate a broad range of knowledgeable opinions rather than a representative set (Hasson, Keeney, & McKenna, 2000). It also addressed the requirement set forth in Linstone and Turoff (2002) suggesting that participation must include representatives of many perspectives, as well as the goal described by Okoli and Pawlowski (2004), to bring together a panel of experts in a forum akin to a virtual meeting to arrive at an answer to a difficult question.

The study was conducted within XYZ Corp, a business-to-business financial services firm with a staff of 24,000 worldwide and a global security program. A financial

services firm was selected because stringent regulatory and industry mandates made end user behavior critical to its authority to operate. A global firm was chosen so that participants would represent a variety of cultures, a particular challenge in creating an effective information security policy (Filho, Hashimoto, Rosa, Souza, & Chaves, 2011).

XYZ Corp had other attributes that made it a good sample to study. It had a mature security program with an annual, mandatory end user policy awareness program, but was rules-, not values-based. It had published corporate values, but there had been no formal attempt to tie the corporate values to the policy or use policy to establish culture. The organization had two pools of potential participants. One pool was the Privacy Champions, approximately 100 employees worldwide who were fluent in English and regularly assisted with privacy and security related initiatives. This group of men and women had widely disparate work responsibilities and operated at a range of levels within the organization, representing a cross-section of the organization's general employee. What they had in common, however, was a desire to help the security team by attending periodic information sessions and participating in local security awareness activities. This gave them insight into the goals of security and attributes of security behavior, providing a level of subject matter required by the study methodology.

The second pool consisted of more than 30 security managers and compliance officers, also worldwide and also fluent in English, who had responsibility for writing information technology security policy. XYZ Corp management was a strong supporter of the study, willing to facilitate communication with potential international participants through its global Privacy Office, to provide corporate intranet resources for communications and data collection, and to give employees time during the workday to

participate in study activities.

Pulling participants from the global security management and Privacy Champion rosters helped ensure that stakeholders who created policy, and thereby represented the organization's security values, as well as employees who were responsible for communicating and following security policy, contributed to the design effort. Facility in a common language was important for the exchange of ideas that occurred in the empirical and technical VSD investigations. It was important for the study group to include participants from the four global regions, Asia Pacific (APAC), Europe/Middle East/Asia (EMEA), Latin America (LAC), and North America (NA), as this offered the broadest cultural diversity. In addition, a small group of American and European employees within the security organization pilot-tested the empirical investigation questionnaires. They checked the usability of the form, anonymity of response, clarity of the questions, and completion time within the promised 15-minute timeframe.

Although VSD provided a means of including both direct and indirect stakeholders in the design effort, indirect stakeholders, XYZ Corp customers who supplied data and their customers who owned the data, were not included in this study. That decision was made for two practical reasons. The first was that the organization participating in the study did not share its policies with customers or consumers. The second was that there were legal obligations associated with security policies that could more effectively be managed by limiting participation to XYZ Corp employees.

Because the VSD study involved human subjects, Institutional Review Board (IRB) approval was sought prior to the request for volunteers. In addition, the study followed IRB recommended practices. Volunteers were treated with respect. It was explained that

the VSD methodology was being evaluated, not the participants. Volunteers were able to stop participating at any time, and study instruments did not include personally identifying information.

Identification of the Initial Set of Security Values

As suggested in Flanagan, Howe, and Nissenbaum (2005) and Borning and Muller (2012), having identified the stakeholders and having established a means of soliciting representatives from their respective groups, the next task was to explore an initial set of values associated with information security. A variety of sources were explored including Friedman, Kahn, and Borning's (2006) Human Values with Ethical Import (Appendix A), the Kujala and Väänänen-Vainio-Mattila (2009) Category Framework of User Values (Appendix B), Dhillon and Torkzadeh's (2006) Fundamental and Means Objectives Related to IS Security (Appendices C and D), the VSD research reviewed in the Literature Review, Chapter 2 of this study (Appendix E), and previously stated stakeholder values supplied by XYZ Corp (Appendix F).

To establish a meaningful set of security values, useful as a starting point for participants, the study employed a variation of the four-step analytic process developed by Burmeister (2012). Like this study, Burmeister used VSD to explore descriptions of values not well established in other studies. In the first step, the initial list of values culled from the aforementioned sources was fleshed out into discrete value categories. In the second step, value categories were clustered into themes. In the third step, duplicates were removed and values that were specific instances of a larger theme were consolidated. This left a list of unique security value themes. In the fourth step, key

values within each theme were identified, and duplicates removed. The resulting set of key values became the starting point for participants in the empirical investigation. The process is illustrated in Figure 4.

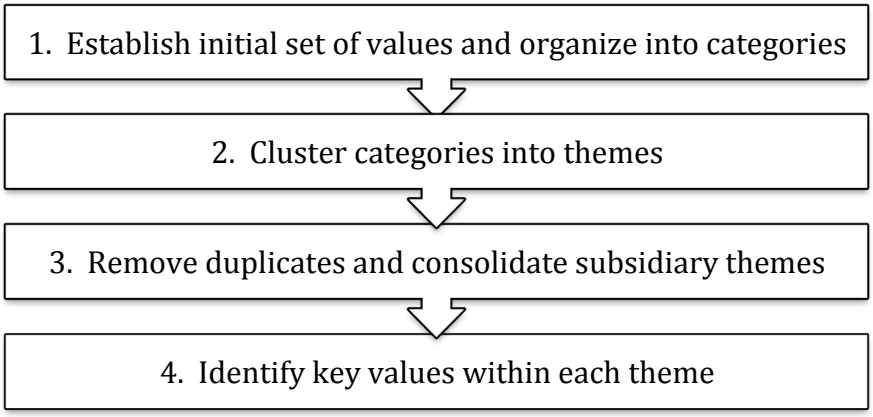


Figure 4. Burmeister (2012) offered a four-step analytic process for the VSD conceptual investigation. Through this process, an initial list of security values was formulated, and then systematically reduced until the key values remained. Key values were then presented to participants in the empirical investigation. Adapted from "What Seniors Value about Online Community," by O. K. Burmeister, 2012, *The Journal of Community Informatics, 8*, p. 3. Protected by and subject to the Creative Commons Public License "Attribution-NonCommercial-ShareAlike 2.5."

Empirical Investigation

In the empirical investigation, participants were guided toward a collective expression of security values associated with three policy statements by way of iterative rounds of Delphi questionnaires. As described in the Site and Participant Selection section, the organization that participated in the study was global, with participants from Australia, Europe, and the Americas. The span of 18 time zones made real-time conversation impractical.

Delphi was chosen for the empirical investigation because it met the unique data collection requirements for the study's population. Delphi brings together the ideas of an asynchronous group via a series of questionnaires rather than through face-to-face

collaboration (Delbecq, Van de Ven, & Gustafson, 1975). The process evolves opinions into group consensus (Goldman et al., 2008; Hasson, Keeney, & McKenna, 2000) and facilitates collaboration among geographically dispersed populations when participants have facility in a common language and can both understand and express themselves through written communications (Delbecq et al., 1975). Delphi provides a method of data collection when statistical methods are not practical or possible (Rowe & Wright, 1999). It is also useful for solving problems related to collective attitudes and feelings, where participants have varying experiences and expertise, face-to-face communication is not practical, and anonymity of opinion improves the exchange of ideas (Linstone & Turoff, 2002).

The Delphi process employed for the empirical investigation followed the recommended implementation of three to five rounds of pilot-tested questionnaires (Delbecq, Van de Ven, & Gustafson, 1975) with each round building upon the responses of the previous one. Questionnaires were posted online and continuously available for three business days (Monday morning in Sydney, Australia to Wednesday evening in Denver, Colorado). Responses were analyzed in the latter part of the week, after which a new round of questions was created and tested. The following Monday, and every Monday thereafter, a follow up round was posted. The process stopped when consensus on security values was reached. Specific questions drew upon both VSD and Delphi methods to elicit participants' values. This blend of methods was compatible with VSD, as Friedman, Kahn, and Borning (2006) stated, "Value Sensitive Design supports and encourages multiple empirical methods to be used in concert to address the question at hand." (p. 355).

The goal of the Round 1 was to gain a fundamental understanding of how stakeholders defined the security values associated with each of the three policy statements (Linstone & Turoff, 2002). Participants were presented with three policy statements from the XYZ Corp's End User Policy. Following each statement was a scenario that illustrated conflicting values that might influence whether the policy was followed (Table 2).

Table 2

Policy and Scenario Statements

	Policy	Scenario
Value 1	XYZ business can be conducted using XYZ equipment and from non-XYZ equipment in compliance with the Remote Access Standard. The use of computer systems or email accounts not provided by XYZ is prohibited.	Maria is working on a report for an important customer that must be presented on Monday. It is late on Friday and she hasn't made nearly the progress she had planned. She emails sensitive account information to her home email address so that she can prepare the report at home. What Maria doesn't realize is that XYZ has contractual agreement with the customer to keep the customer's data within a secure environment – and Maria's home mail file is not secure.
Value 2	Users must not leave XYZ information resources unsecured or visible and unattended outside XYZ's facilities.	Tomorrow was going to be a busy day. More than 500 customers were being sent a special mailing to introduce a new service that detailed monthly account activity and suggested personalized marketing strategies. Concerned that they wouldn't finish on time for tomorrow's 3 pm mail pick up, Lee decided to get started today. He printed out all the reports and laid them out in a nearby conference room so they would be ready for stuffing and sorting in the morning.

Value 3	Lending XYZ information resources, including company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited.	All was in a panic when Petrov came last night. Both boys had papers due for school and were fighting over the use of the family computer. Luckily, Petrov brought his laptop home that night and could lend it to his older son.

Using an approach similar to the Nathan, Friedman, Klasnja, Kane, and Miller (2008) envisioning technique, participants were asked to envision themselves in the scenario and identify up to three values associated with upholding the policy. Participants were asked to choose from the initial list of security values identified in the conceptual investigation, and/or create their own, up to a total of three. They were also asked to briefly explain the thinking behind their choices. Two data sets emerged for each of the three values. The first was a simple tally, identifying the values most frequently identified by participants as associated with upholding the policy. The second was qualitative, analyzing each participant explanation for its underlying security theme (Hasson, Keeney, & McKenna, 2000).

The goal of Round 2 was to further refine Round 1 responses (Hasson, Keeney, & McKenna, 2000) through understanding competing and common values, and then moving toward consensus on security values that addressed the desired security behavior. Following the method described by Delbecq, Van de Ven, and Gustafson (1975), participants were given the policy statements and scenarios again, along with the values most often identified with it in the previous round and the underlying theme most often referenced in the comments. They were asked to give each of the three values a unique ranking so that one was ranked Most Important, one Least Important, and one in the middle. Participants were again asked to briefly explain the thinking behind their

ranking.

As in Round 2, Round 3 questions were built upon participant responses from the prior round. Each explored areas of agreement and disagreement and provided an understanding of underlying assumptions, views, or facts used by participants to support their respective positions. The results of each round were analyzed. Had new values been introduced or conflicting values unresolved, the investigation could have returned to the conceptual phase (Friedman & Kahn, 2003). However, consensus was reached on the key values, participants were given a final opportunity to review and validate their responses, and the empirical investigation was brought to closure. At that point, keeping with Friedman, Kahn, and Borning (2001), the study moved to the technical investigation.

Technical Investigation

The technical investigation focused on the design effort, building into the XYZ Corp End User Policy the values identified in the previous investigation. The limit of three statements was set for a practical reason. Sustaining participant involvement was a known challenge within the Delphi process (Hasson, Keeney, & McKenna, 2000). This is why Linstone and Turoff (2002) recommended limiting the total number of rounds and why Delbecq, Van de Ven, and Gustafson (1975) recommended that each round should take no more than 30 minutes to complete. Due to the iterative nature of both Delphi and VSD, the outer limits of both iterations and questions were already stretched. Limiting the scope helped ensure adequate time for participants to explore the topic without exceeding anticipated participant time constraints and fatigue.

The specific policies chosen for the investigation came from three different sections of the policy (Table 2). Each represented an activity totally dependent upon user compliance, not enforceable through technology. The Delphi process was again employed. Drawing upon the same panel of stakeholders, the survey instrument asked participants to re-write the policy statements in a way that reflected the identified values. Subsequent rounds solicited feedback on the various statements until consensus on value sensitive language was reached.

Study Validation

As a test of VSD as a methodology for defining and aligning employee and organizational values and creating a value-sensitive security policy, this study was one of scores of studies testing VSD for different types of design efforts. In this way the study contributed to the validation of VSD as a qualitative research methodology (Tellis, 1997). However, the study was not designed to show that every organization can or should use VSD for security policy design or that the security values defined by the set of stakeholders in the study group were universal. As Patton (2001) states, "While one cannot generalize from single cases or very small samples, one can learn from them – and learn a great deal, often opening up new territory for further research…" (p. 41). However, as Patton also states, research must be credible to be useful.

As the study was comprised of multiple methodologies (VSD as the overall methodology, Burmeister's (2012) four-step process for the conceptual investigation, and Delphi Method for the empirical and technical investigations), a variety of methods were used to validate the findings. This was important because different research methods

lend themselves to different types of evaluation (Maxwell, 2005; Patton, 2001; Whittemore, Chase, & Mandle, 2001). Validity, for the purpose of this study, referred to the extent to which findings were well founded and true to life while keeping in mind that no matter how strong the evidence, validity in qualitative research is ultimately uncertain (Whittemore et al., 2001). To bring consistency to the evaluation process, the study used Maxwell (2005) as a framework. Maxwell described the purpose of evaluating the validity of qualitative research as establishing "grounds for distinguishing accounts that are credible from those that are not" (p. 106). He further posited that qualitative research did not have to reveal an ultimate truth in order to be useful. It did, however, have to sufficiently address the validity threats of bias and threats of reactivity. According to Maxwell a threat of bias occurs when the researcher selects data or data sources to support an existing preconception. Threat of bias was addressed in the methodology prior to the study by identifying and addressing the selection of data sources and threats to plausibility. Reactivity addressed the researcher's influence on participants. Reactivity was addressed after the study by scrutinizing the data selection process and analyzing how participants may have been influenced (Maxwell, 2005; Patton, 2001). Findings were closely examined for evidence that did not support the conclusions.

The Maxwell (2005) framework also took into consideration internal and external generalizability, recognizing that not every study requires both. Internal generalizability was defined as the generalizability of a conclusion within the group studied; external was the generalizability of a conclusion beyond the group studied. In this study, VSD was applied to elicit the security values specific to the study group, and therefore had to meet

criteria for internal generalizability. As a test of VSD's suitability for creating a value-sensitive policy in general, it had to meet criteria for external generalizability.

Maxwell (2005) suggested that a goal to minimize bias and reactivity was not practical, yet it was incumbent upon the researcher to recognize bias and reactivity, understand it, and explain it. He offered a number of strategies that could be employed to aid in the understanding and communication, five of which were employed in the evaluation of this study. The first strategy was to collect rich data. Rich data was defined as detailed and varied inputs such as that which comes from numerous observations. In this VSD study, rich data came from the large number of subjects, the diverse population, and numerous iterations of questioning. The second strategy was respondent validation. The iterative VSD process of gaining participant consensus before moving on was well suited for this strategy as the study participants themselves were the ones validating the findings. The third strategy was searching for discrepant evidence. Discrepant evidence came in the form of inconsistencies in data provided by study participants. The fourth strategy was quasi statistics. Quasi statistics were simple counts and percentages derived from the data to illustrate clear choices as were used in the empirical and technical investigations to identify consensus in choices. The fifth strategy was comparison. Comparison looked at responses across different segments of the respondent population (i.e. employee vs. manager; North American vs. International). Greater consistency across different groups indicated stronger study validity. Table 3 summarizes the validation framework, outlining the questions through which validation was assessed. The questions are organized by research question, whether internal or external generalizability was relevant, and the specific validity threat it addressed.

Table 3

Validation Framework

Generalizability	**Threat of Bias**		**Threat of Reactivity**
	Selection of data sources that fits researcher's preconceptions	Failure to scrutinize all evidence	Researcher influences participants
RQ1 Internal Generalizability	What evidence can be provided that the selection of questions represents the universe of stakeholders?	What steps were taken to provide consistent evaluation of all responses when incorporating them into subsequent survey rounds?	What evidence is there that the policy reflects the aligned employee and organizational values as defined by the constituent groups?
Analysis Strategy:	Comparison Respondent validation	Quasi statistics Search for discrepant evidence	Respondent validation
RQ2 External Generalizability	What characteristics of the methodology contribute to or detract from external generalizability?	What attributes of the VSD process contribute to or detract from external generalizability?	What evidence is there that the VSD process can be deployed by other organizations in creating a value-sensitive end user policy?
Analysis Strategy:	Rich Data	Comparison Search for discrepant evidence	Comparison Search for discrepant evidence

Before deciding on the Maxwell framework, two other study validation methods were considered. The first was a follow up survey of study participants, assessing if the final product of the study reflected what they considered security values. This follow up survey was incorporated into the study and the responses evaluated within the Maxwell framework. The second method considered was a survey of non-participants to see if the

resulting policy reflected their values as well. This approach was discarded, for without having participated in the formulation of a value sensitive policy, the second group may not have recognized values embedded in policy text, nor would they have a sense of whether the VSD methodology was useful in its creation. As such, the survey would not have addressed either of the research questions.

Summary

The methodology chapter described how the research questions were explored. It detailed how VSD was applied throughout the study, from the conceptual investigation through the empirical and technical investigations, and then evaluated VSD as a means of identifying organizational and employee security values and integrating them into the organization's end user security policy. The chapter described how the VSD conceptual investigation directed the selection of the study organization based on its reliance on a single policy directing a global and culturally diverse employee base. It also described how the conceptual investigation directed the selection of participants to include stakeholders representative of both the organization and its culturally diverse employees.

The Methodology chapter also detailed how VSD was used to establish the initial set of security values, how the Delphi method was incorporated into the VSD empirical and technical investigations to facilitate an asynchronous collaboration on defining shared values, and how, at its conclusion, the study yielded agreed upon value sensitive policy language. The use of the Maxwell (2005) framework for validating qualitative research was discussed and the specific questions associated with strategies to validate

the study findings were detailed. The chapter concluded with a discussion of alternative validation methods and the reasons why they were discarded.

Chapter 4

Results

Introduction

As described in the methodology section, VSD results came from three distinct investigations, with each investigation comprised of components that influenced and potentially re-opened the other two. In keeping with that model, the Data section of this chapter describes the results of each investigation component, the investigation as a whole, and the influence of each investigation on the other two. In so doing, it traces the steps in defining security values, starting with the literature of organizational values, security culture, and VSD, through to the creation of value sensitive policy statements crafted by the study participants. The Data section also includes the results of the follow up survey that captured the participant's evaluation of the VSD process and of the policy language the study yielded.

The Analysis section examines the stakeholder recruitment process, explains how participant responses were aggregated and interpreted for presentation in the subsequent survey, and draws conclusions about XYZ's experience using VSD as a methodology for identifying its security values and creating a value sensitive security policy. Two factors unique to this study are described that significantly influenced the study design. The first was that XYZ Corp is a global organization with a common end user security policy. The

second was that the researcher was a colleague to many of the participants across the regions. This section also examines the influence of those factors on the study and its findings.

The Validity section of this chapter examines each of the VSD investigations against the Maxwell framework established in the Methodology chapter (Table 3). Through this analysis, the validity of findings within the context of the study is examined and conclusions drawn about researcher bias and reactivity. Questions taken from the framework explore the role of the researcher in participant selection, selection of data sources, scrutiny of data, and influence over participant responses. Protections against bias (rich data sources, search for discrepant data, and continuous participant data validation) are also explored.

Data

Each of the VSD investigations was comprised of multiple, iterative data gathering opportunities. Combined, they provide a philosophically informed and methodical progression from the universe of values to those relevant to a set of stakeholders and their policy design effort. The data presented in this section documents the progression.

Conceptual Investigation Data

For the conceptual investigation, VSD prescribed two goals: to select a panel of participants representative of the universe of stakeholders and to establish an initial list of relevant values that serve as a starting point for the empirical investigation. A total of 44 policy makers, including at least three from each of the four regions, were asked to

participate and 15 volunteered. Among the participants were at least two from each international region, providing an equal number of participants from North America and the combined international regions. Response from the Privacy Champions, employees who regularly volunteered to participate in security- and privacy-promoting activities, was not as strong. A total of 263 Privacy Champions were asked to participate, 145 from North America and 118 from the international regions. All but two of the 29 volunteers were from North America. In total, 307 volunteers were solicited and 44 agreed to participate. As a percentage of those solicited, the greatest response came from international policy makers at 44%, followed by the North American policy makers at 29%, the North American Privacy Champions at 19%, and the international Privacy Champions at 2%. Actual numbers are detailed in Table 4.

Table 4

Participation by Role and Location

Location	**Policy Makers**		**Privacy Champions**		**Total**	
	Asked	Agreed	Asked	Agreed	Asked	Agreed
North America	28	8	145	27	173	35
International	16	7	118	2	134	9
Totals	44	15	263	29	307	44

The purpose of the second part of the conceptual investigation was to establish the initial set of security values for review in the empirical phase (Friedman, Kahn, & Borning, 2006). Because there is little research into security values, a wide net was cast for the initial list. The following search terms were applied to searches in Google Scholar, ProQuest's ABI/Inform Complete, and the ACM digital library: information

security, information security policy, organizational values, security behavior, security culture, security management, security values, Value Sensitive Design, and values. These yielded 287 peer-reviewed journal articles. Each of the 287 was then individually reviewed for the terms "security" and "values" or for text that implied a definition of security values. Articles that discussed security as a value itself were discarded, as were those that referenced security values but did not provide examples. Articles that did not use the term "values" but referenced a concept that functioned as a value within the context of the study were included. For example, Chang and Lin (2007) investigated how various attributes of organizational culture influenced information security management. What they termed cultural traits and security culture constructs were comparable to, or in some cases, the same as value statements in other works. This search yielded a total of 13 relevant articles and 56 value statements as detailed in Appendix E.

In addition to the values gleaned from the literature review values were culled from Friedman, Kahn, and Borning's (2006) detailed description of human values with ethical import (Appendix A), Kujala and Väänänen-Vainio-Mattila (2009) Category Framework of User Values (Appendix B), Dhillon and Torkzadeh's (2006) values within information systems security: Fundamental Objectives Related to IS Security (Appendix C) and Means Objectives Related to IS Security (Appendix D). The published values of the organization participating in the study (Appendix F) were also identified. After duplicate entries were removed and similar language grouped together, 84 value categories remained. Following Burmeister (2012), the 84 value categories were clustered into what became 55 themes. The themes were then regrouped, identifying themes that were examples of the same underlying key theme. This brought the list of

55 themes to a list of 11 key values (Table 5). These 11 key values were included in the initial questionnaire of the empirical investigation. The specific value categories and themes for each of the steps from initial set to key values are provided in Appendix G.

Table 5

Initial Set of Key Values

Value Number	Key Values
1	Anticipate problems and prevent them
2	Build and sustain trust
3	Create value for customers
4	Creatively address problems and opportunities
5	Do the right thing
6	Ensure information is properly accessible
7	Honor customer trust over personal convenience
8	Make work meaningful and satisfying
9	Promote personal responsibility
10	Remove obstacles and delays to necessary action
11	Respect what has been entrusted to you

Empirical Investigation Data

The goal of the empirical investigation was for participants to come to consensus on a security value for each of three policy statements. The method of working toward consensus was Delphi questionnaire. For each of three Delphi rounds, participants were given the policy statement along with a scenario that illustrated the security value (Table 2). The scenarios were taken from actual security events and were selected to highlight how security values may be in conflict with other employee values. In Delphi Round 1 (Appendix N) participants were asked to envision themselves in the scenario, and identify

up to three values they associated with upholding the policy. They were told they could choose from the initial list of 11 values established during the conceptual investigation (Table 5), and/or create their own, up to a total of three. They were also asked to explain the thinking behind their choices.

Thirty-nine participants responded to the survey. Responses were analyzed in two ways. The first was a simple vote on choices, with key values 1, 5, 7, 9, and 11 (Table 5) appearing most frequently. As show on Table 6, there was strong consensus (over 70%) on at least one key value, and relatively strong consensus (over 45%) on at least two. All respondents chose from among the 11 key values. No participant proposed a new one.

Table 6

Round 1 Top Scoring Value Statements

Policy 1	**Policy 2**	**Policy 3**
7 (74%)	1 (64%)	11 (79%)
11(74%).	11 (49%)	5 (67%)
5 (46%)	7 (46%)	9 (49%)

Note: The value statements selected for each policy, followed by the percentage of participants selecting that statement (n= 39)

In the second response analysis, the rationale given by participants for choices was categorized by theme of the security value described. The comments showed even stronger consensus. For each policy statement, at least 85% of the responses reflected a security theme in common with the others. The themes of these responses are shown in Table 7.

Table 7

Round 1 Themes in Selection Rationale

Policy 1	Policy 2	Policy 3
We are responsible for sustaining customer trusts	We are responsible for maintaining data security	We are responsible for maintaining data security
We are responsible for maintaining data security	We are responsible for following the rules	We are responsible for following the rules
We are responsible for following the rules	Employees need to plan ahead for security	We are responsible for sustaining company trust

The goal of Delphi Round 2 (Appendix P), was to bring participants closer to consensus on security values as they related to the specific policies – moving each from three disparate values to one central value. In this round, participants were again given the three policy statements and scenarios, along with three value statements identified in Round 1. Participants were asked to rank the three values from most to least important and to comment on the thinking behind their choices. Thirty-six participants responded to the survey.

Values were decided by awarding one point for each statement that was considered the most or second most important, and subtracting one point for each statement listed as least important. Participants showed strong consensus on the most important value for Policies 1, 2, and 3 (15, 15, and 17 points, respectively), somewhat less strong consensus on the second most important value for Policies 1 and 2 (11 and 13 points, respectively), and weaker consensus for the second most important value for Policy 3 (9 points). These highest-ranking values are shown in Table 8.

Table 8

Round 1 Key Theme Ratings

	Policy 1	**Policy 2**	**Policy 3**
Most Important	Respect what has been entrusted to you	Respect what has been entrusted to you	Respect what has been entrusted to you
Second Most Important	Honor customer trust over personal convenience	Honor customer trust over personal convenience	Promote personal responsibility

In addition to the ratings, comments were analyzed for common themes. From these common themes the following value statements were crafted (Table 9).

Table 9

Round 2 Security Value Statements

Security Value Statement 1	**Security Value Statement 2**	**Security Value Statement 3**
We are honor bound to follow XYZ's security policies as they are designed to safeguard the sensitive data customers have entrusted to us.	We respect the responsibility entrusted to us by XYZ and by customers by anticipating security problems and looking for ways to avoid them.	Lending XYZ information resources, including company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited.

In Delphi Round 3 (Appendix R) participants were given the three value statements from Round 2 and asked how satisfied they were that the proposed value statement addressed the security value associated with the policy. If not satisfied, they were asked to comment on what change was needed. Thirty-eight participants responded to the survey. Response was strong with satisfied or very satisfied at 82%, 87%, and 92% respectively for the three value statements (Table 10).

Table 10

Round 3 Agreed Upon Security Values

Security Value 1	Security Value 2	Security Value 3
We must honor our commitment to our customers to follow XYZ's security policies as they are designed to safeguard the sensitive data customers have entrusted to us.	We respect the responsibility entrusted to us by XYZ and our customers by anticipating security problems and proactively looking for ways to avoid them.	As employees we have a personal responsibility to do what is right for XYZ and our customers, respecting their trust over personal convenience and promoting customer security interests.

In the Round 3 comments, participants suggested wording changes to improve clarity. Because there was strong consensus and no new values were added, it was not necessary to return to the conceptual investigation. The requested wording improvements were incorporated into the statements. They were then deemed final and became the starting values for the technical investigation.

Technical Investigation Data

The goal of the technical investigation was to integrate the security values defined in the empirical investigation into the policy statements, thus creating value sensitive policies (VSPs). Delphi Round 4 (Appendix T) was the only survey where pre-constructed choices were not offered. This was done to give participants the greatest latitude in constructing the VSPs. Participants were given the three policies used in the empirical investigation along with the associated security value defined in Round 3, and asked to draft a VSP that incorporated the value into the text of the policy. They were also asked to briefly explain their thinking. Twenty-four participants responded.

Responses were evaluated for their logical connection between the value and the policy, clarity of direction to employees, and general understandability. A point system was used to rank responses. If either policy or value was not included in the draft statement, the response was rated 0 and omitted from final list. Zero to three points were awarded for clarity and understandability. To earn all three points, the VSP had to clearly articulate both policy and value, while establishing a strong, logical connection between the two. Four VSPs proposed for Policy 1 received the top score. Five VSPs received the top score for Policy 2. Eight VSPs received the top score for Policy 3. Participant comments were then analyzed to identify common themes in their proposed VSPs. VSPs with similarly themed comments were combined, resulting in five VSPs for each of the three Policies (Table 11).

Table 11

Round 4 Top Scoring Value Sensitive Policies

Policy 1	**Policy 2**	**Policy 3**
1. To honor our commitment to safeguard sensitive data, XYZ business can be conducted using XYZ equipment or non-XYZ equipment that is in compliance with the Remote Access Standard. The use of computer systems or email accounts not provided by XYZ is not allowed.	1. By not leaving XYZ information resources unsecured or visible and unattended outside XYZ's facilities, we respect the responsibility XYZ entrusts to us.	1. Respecting trust over personal convenience and promoting customer security interests, we should not lend XYZ information resources, including company issued laptops and desktop computers, to family members, friends, or non-XYZ employees.

2. XYZ employees can conduct business for our customers using XYZ equipment and non-XYZ equipment that is in compliance with the Remote Access Standard. This policy allows us to honor our commitment to our customers as it helps ensure their information is safe.	2. We respect the responsibility entrusted to us by XYZ and our customers. Therefore we should anticipate security problems and proactively avoid them. As it relates to XYZ information resources, we must make all efforts to prevent theft or unauthorized access. Users must not leave XYZ information resources unsecured, visible, or unattended outside XYZ's facilities.	2. As XYZ employees, we have a personal responsibility to protect XYZ and customer security interests over personal convenience. As such, we do not permit the use of XYZ information resources, including company issued laptops and desktop computers, to family members, friends, or non-XYZ employees.
3. In order to honor our commitment to clients to protect client and cardholder data, XYZ business can only be conducted using XYZ equipment or non-XYZ equipment that meets all remote access standards.	3. To honor our responsibility to protect the data entrusted to us by XYZ and our customers, we must anticipate security problems and proactively look for ways to avoid them. Specifically, we must never leave these information resources unsecured, visible and/or unattended outside XYZ's facilities.	3. As employees we have a personal responsibility to do what is right for XYZ and our customers. Lending XYZ information resources, including company issued laptops and desktop computer to family members, friends, or non-XYZ employees is prohibited. This ensures that we respect customer trust over personal convenience and promote customer security interests.
4. XYZ provides employees with secure computer systems and email accounts that safeguards sensitive data entrusted to us. The use of computer systems or email accounts not provided by XYZ is prohibited. If one must use a non-XYZ system to conduct XYZ business, it must be done in compliance with the Remote Access Standard. Complying with this policy, honors our commitment to our customers	4. We here at XYZ respect the documents and sensitive information we have been trusted with. We do not leave papers, passwords or documents where they can be found or exploited.	4. As employees we have a personal responsibility to do what is right for XYZ and our customers, respecting their trust over personal convenience and promoting customer security interests. Be sure not to lend XYZ information resources, including company issued laptops and desktop computers to family members, friends, or non-XYZ employees.

5. To honor our commitment to customers, XYZ business can be conducted using XYZ equipment or non-XYZ equipment in compliance with the Remote Access Standard. Using computer systems or email accounts not provided by XYZ is prohibited. This helps keep sensitive data entrusted to us safe and secure.	5. We are responsible for anticipating security problems and proactively looking for ways to avoid them. Therefore, users must not leave XYZ information resources unsecured or visible and unattended outside of XYZ's facilities.	5. Lending XYZ information resources, including company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited. As employees we have a personal responsibility to do what is right for XYZ and our customers, respecting their trust over personal convenience and promoting customer security interests.

The goal of Delphi Round 5 (Appendix V) was to come to consensus on VSPs, reducing the list of five to the one that best integrated value and policy. Participants were given the same three policies and associated value statements, along with the five Round 4 VSPs. For each policy/value pair, they were asked to select the one statement that best connected the value to the policy while also providing clear direction to employees. If they did not like the choices, the opportunity to craft a replacement was offered. Twenty-seven participants responded to the survey. For each policy/value pair, two of the five choices received 30% or more of the votes (Table 12).

Table 12

Round 5 Consensus on Value Sensitive Policies

Policy 1	**Policy 2**	**Policy 3**
1. To honor our commitment to safeguard sensitive data, XYZ business can be conducted using XYZ equipment or	2. We respect the responsibility entrusted to us by XYZ and our customers. Therefore we should anticipate security problems and proactively avoid	2. As XYZ employees, we have a personal responsibility to protect XYZ and customer security interests over

non-XYZ equipment that is in compliance with the Remote Access Standard. The use of computer systems or email accounts not provided by XYZ is not allowed.	them. As it relates to XYZ information resources, we must make all efforts to prevent theft or unauthorized access. Users must not leave XYZ information resources unsecured, visible, or unattended outside XYZ's facilities.	personal convenience. As such, we do not permit the use of XYZ information resources, including company issued laptops and desktop computers, to family members, friends, or non-XYZ employees.
4. XYZ provides employees with secure computer systems and email accounts that safeguards sensitive data entrusted to us. The use of computer systems or email accounts not provided by XYZ is prohibited. If one must use a non-XYZ system to conduct XYZ business, it must be done in compliance with the Remote Access Standard. Complying with this policy, honors our commitment to our customers.	5. We are responsible for anticipating security problems and proactively looking for ways to avoid them. Therefore, users must not leave XYZ information resources unsecured or visible and unattended outside of XYZ's facilities.	5. Lending XYZ information resources, including company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited. As employees we have a personal responsibility to do what is right for XYZ and our customers, respecting their trust over personal convenience and promoting customer security interests.

Each of the two most often selected VSPs was reviewed in light of the accompanying participant comments. Comments fell into three areas: an explanation of why they liked the VSP, suggested changes to improve clarity, or suggested changes to the policy itself. Common themes were incorporated into the VSPs and presented in Round 6.

Thirty participants responded to the Delphi Round 6 survey (Appendix X). In this round, participants were asked how satisfied they were with the three final VSPs. The criteria for satisfaction was defined as a strong, logical connection between the agreed upon security value and the XYZ policy, that was easily understood and provided a clear direction to employees. For both VSP 1 and 2, 28 (93%) respondents were either

satisfied or very satisfied, with comments suggesting similar, but minor changes in wording. For VSP 3, all 30 were either satisfied or very satisfied (Table 13).

Table 13

Round 6 Final Value Sensitive Policies

VSP 1	VSP 2	VSP 3
To safeguard sensitive data, only email accounts provided by XYZ may be used to conduct XYZ business. Furthermore, XYZ business must be conducted using XYZ equipment or using non-XYZ equipment that is in compliance with the Remote Access Standard. Complying with this policy honors our commitment to customers to keep their data secure.	To protect the data entrusted to us, it must not be left visible or unattended outside XYZ's facilities or unsecured and unattended within XYZ's facilities. When working with client data, we must anticipate problems related to keeping data secure when we are not present, and proactively looking for ways to avoid them.	As XYZ employees, we have a personal responsibility to protect XYZ and customer security interests over personal convenience. For that reason, lending XYZ information resources such as company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited.

Data Summary - Study Results

From a VSD perspective, Delphi Round 6 ended the design project. Value sensitive policy statements were crafted and agreed upon with strong consensus from the study participants. No new values were added that would have required a return to the conceptual or technical investigations. However the study was also designed to test the methodology. For that reason, one more round was added asking the participants' thoughts about the VSD process (Appendix Z): how successful it was for identifying the values they associated with security and how successful it was for integrating security values into security policy. Other comments were also welcome. To refresh their

memory, the participants were given the three value statements agreed upon in Delphi Round 6, slightly modified to incorporate the wording changes suggested in the comments (Table 14). All 21 respondents stated that the VSP process was Successful or Somewhat successful integrating security values into security policy.

Table 14

Initial Policy and Corresponding Value Sensitive Policy

	Policy	**VSP**
Policy/ VSP 1	XYZ business can be conducted using XYZ equipment and from non-XYZ equipment in compliance with the Remote Access Standard. The use of computer systems or email accounts not provided by XYZ is prohibited.	To safeguard sensitive data, only email accounts provided by XYZ or other approved methods for data sharing may be used to conduct XYZ business. Furthermore, XYZ business must be conducted using XYZ equipment or using non-XYZ equipment that is in compliance with the Remote Access Standard. Complying with this policy honors our commitment to customers to keep their data secure.
Policy/ VSP 2	Users must not leave XYZ information resources unsecured or visible and unattended outside XYZ's facilities	To protect the data entrusted to us, client data and other sensitive information must not be left visible or unattended outside XYZ's facilities or unsecured and unattended within XYZ's facilities. When working with client data, we must anticipate problems related to keeping data secure when we are not present, and proactively looking for ways to avoid them.

Policy/ VSP 3	Lending XYZ information resources, including company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited.	As XYZ employees, we have a personal responsibility to protect XYZ and customer security interests over personal convenience. For that reason, lending XYZ information resources such as company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited.

Participants from each of the constituent groups expressed favor with the process, its cross-cultural participation, and the concept of VSPs in general. Two respondents, a North American Privacy Champion and a North American policy maker, additionally commented that the method might be only somewhat successful because they were given a set of security values at the start of the empirical investigation. The full list of comments is presented in Table 15.

Table 15

Follow Up Survey Comments

Question	**Comments**
How successful was the process for identifying values associated with security?	"The values were clearly identified and combined/associated with the security statement to relay the messages." "I think it was somewhat successful. I struggled with VSP1 because I think there are more than one values that can be associated with the existing policy, so it was not a one-to-one fit. The other 2 VSPs were a more clear one to one fit of Value to Policy." "Identifying these values will help all employees to better understand why specific security rules are in place" "the values and the policies were given in advance so i'm not sure about the identification of seurity values"

	"I really consider that this process permited the participation of all areas and cultures." "Values were constrained by provided choices, therefore hard to know if we would have had more success with a different approach."
How successful was the process for integrating those values into security policy?	"Good combination of values and security. They were integrated well in all three statements that are clearly understandable." "that is what we accomplished with this work" "Introducing into the policy a value to follow, makes people to proceed accordingly with their believes and not because it is required of mandatory." "Same as above. It can be difficult if there are multiple values supporting a single policy" "Given the number of evaluation rounds as well as the different views of all responders it seems quite a long procedure to find an appropriate wording. Still this evaluation process is really benefitial and needed time has to be taken."
Anything else you would like to add?	"I think the process that was taken to get to the end result was very successful. The security policy wording is very straightforward and everyone should be able to understand and comply." "Very interesting and I as a follow-up I would be interested to see how it can be applied to the industry in general." "I really like the resulting policy statements. They are clear, and personally relatable." "A very interesting study and excercise for all of us. Thank you for the oportunity to make us part of this" "I'm impressed with the process as a whole and thought it was a very good way to update the policies. By making them value sensitive, they give the employee something at stake besides a "Don't do this or else" type of mentality. Including the values seems to give more reason for adherence." "It was an interesting exercise. I understand better now about policies vs. values."

	"I would like to see such statements in XYZ's future policies to help employees understanding why security is such important. I would propose to also verify whether other company directions can be used to define according policy statements"
	"I believe this process helped clarify prior policy statements and i enjoyed being part of this process"
	"The end result is dependent on the qualification and capability of the group. With a large group, the voice of most experienced few can be overpowered. Overall, I did like the progressive approach and with few modification (giving higer value to input based on participant expertise, smaller group and better tool) can be a very effective."

Note: Responses are quoted verbatim

As will be discussed in the next section, the actual number of participants varied throughout the study (Table 16). There were originally 44 volunteers, but only 39 went through the Login Test that established access to the survey site. Participation was strong in the first three rounds. There was a noticeable drop-off in Round 4 where, coincidentally or not, all the questions were open-ended and no multiple choice answers were offered. Participation increased again for Rounds 5 and 6 but never regained the strong support seen earlier in the study. About half of the original participants completed the Follow Up survey.

Table 16

		Int'l Policy Maker	Int'l Employee	North American Policy Maker	North American Employee	Total
Recruitment		7	2	8	27	44
Login Test		- - - - - - - - - - - - -		Not available	- - - - - - -	39
Empirical Investigation	Round 1	6	2	8	23	39
	Round 2	6	2	9	19	36
	Round 3	4	3	8	23	38
Technical Investigation	Round 4	3	1	6	14	24
	Round 5	3	1	7	16	27
	Round 6	4	1	9	16	30
Follow Up		3	2	3	8	21

Analysis

Although the VSD effort was successful in that consensus was reached on VSPs, there were choices in how the methodology was applied in the study that warrants scrutiny. The VSD methodology provides for researcher discretion in how data is gathered, stakeholders identified, and competing values among stakeholders resolved. At the same time, researcher choices influence the outcome of the design effort (Pommeranz, Detweiler, Wiggers, & Jonker, 2012; Steen & van de Poel, 2012). This is a known and acknowledged VSD limitation (Borning & Muller, 2012). In this section, the methodological choices within the study are examined along with alternatives, rationale, and potential impact on the resulting security values and VSPs.

Conceptual Investigation Analysis– Identification of Initial Values

The VSD literature, combined with scholarly literature referencing information security, information security policy, organizational values, security behavior, security

culture, security management, and security values provided a robust data set from which the initial set of security values was culled. Burmeister (2012) offered a methodical approach for clustering the values and reducing them to a manageable starting point for the conceptual investigation. The Round 3 survey indicated strong consensus on the proposed security values, and there were no comments requesting values-related changes. All of these factors suggest that the conceptual investigation succeeded in providing participants with a strong starting point for the empirical investigation. As noted in the Data section, two participants commented in the follow up survey that their options were constrained by the initial set of choices. Although there was ample opportunity for participants to propose alternative value statements, these two participants chose not to do so. There was insufficient information to know why.

Conceptual Investigation Analysis - Identification and Solicitation of Stakeholders

As noted in the Methodology (Chapter 3), a successful technical design results in a global end user policy that reflects the security values of the organization's entire employee base, transcends cultural differences, and is written in simple enough language to be clearly understood by non-native English speakers. To achieve that goal, study participants had to be representative of the organization and its employees. A statistical sample was not required, but as a group, participants had to be representative of the qualities of stakeholders (Powell, 2003). To meet this standard, participants had to be solicited from among security policy makers and other employees in all four of its regions. The employee solicitation plan, made in conjunction with the XYZ Corporation Privacy Office, was to recruit the regional security policy makers to represent company

values, and to recruit members of the Privacy Champions program as representatives of non-policy making employees. There are at least two Privacy Champions in each of the 35 nations comprising the four regions. Recruitment did not work out as planned as only two international privacy champions volunteered for the study. At least one policy maker from each of the three international regions volunteered, bringing to the study some sensitivity to language and culture, but international employees were underrepresented as a category of stakeholders.

The XYZ Privacy Office offered two explanations for the poor response. One explanation was the solicitation method. XYZ Corporation has a strong Data Across Borders program based on international privacy laws, binding rules, and safe harbour agreements. That program restricted the distribution and use of group mailing lists that included international employees. By policy, XYZ could not provide the researcher with international employee names and email addresses for a direct solicitation. Recruitment was managed by the US Privacy Officer, who contacted the country Privacy Officers, who in turn contacted the local Privacy Champions. Although reminder letters went out during the recruitment period, there was no way to confirm if the international Privacy Champions received the solicitation, or were encouraged to participate as they had been in North America. The recruitment of international policy makers was handled differently. Because the researcher personally knew the international policy makers and their email addresses, direct solicitation was permitted. All had known about the study prior to the volunteer recruitment and all had a professional interest in improving the quality of security policy.

A second factor that may have influenced Privacy Champion participation was how the individuals came to be in the Privacy Champion roles. In North America, Privacy Champions volunteered for the Privacy Champion role, typically because of their interest in privacy and security. As the researcher later discovered, international Privacy Champions were assigned the responsibility in addition to their formal job duties based on availability and skill set. Interest in the role was not a factor. As such, there was no pre-existing tie between the goals of the study and the interests of those solicited.

A third factor related to participant recruitment was the influence of a prior working relationship with the researcher. The researcher knew all 44 of the solicited policy makers, a third of whom volunteered. The response from North American Privacy Champions was comparable. Of the 28 who volunteered, 36% had a prior working relationship with the researcher. Because the researcher did not have the names of solicited international Privacy Champions, there was no data from which to evaluate the influence of the researcher's prior working relationship.

Delphi Method Analysis

It was not just participant recruitment that was influenced by the geographic diversity of stakeholders. The study instrument, its distribution method, and study-related communications were also affected. As described in the Chapter 3, the span of participants' time zones made synchronous communications – in person meetings or conference calls – impractical. At the same time, local security policy prohibited Internet access, thereby precluding the use of Internet-based survey tools. The best accessible alternative was a SharePoint survey site, managed by XYZ's security organization and

hosted on the company intranet. The features of the SharePoint survey were not robust. For example, survey instructions could not be prominently displayed on the survey instrument and had to be sent via email prior to each round (see Appendices M, O, Q, S, U, W, and Y). The survey tool was not able to enforce limits on the number of responses (i.e. "pick three"). There was no flexibility in page layout or typeface, which might have improved the visual experience. Even more significantly from a Delphi Method perspective, the security that enforced participant anonymity also constrained the exchange of information among participants and between the researcher and participants.

Because many of the Privacy Champions reported directly or indirectly to a policy maker, a decision was made to keep responses anonymous. This offered participants the greatest latitude for freely expressing their thoughts. However, the survey tool had limited access granularity. With the anonymous response feature turned on, the respondent name was unavailable to both other participants and the researcher. This made it impossible for the researcher to identify and communicate with individuals who failed to respond to the weekly survey, a practice suggested by Hasson, Keeney, and McKenna (2000) and Delbecq, Van de Ven, and Gustafson (1975) to increase the response rate. Furthermore, anonymous access restricted participants from directly accessing the postings of others. Despite the instruction encouraging participants to look at other responses and change their response based on the comments of others, only one participant asked to see other comments, and then only for one round.

Anonymous submissions presented two other challenges. One was that it was not possible to validate location and role data. For example, although only two international Privacy Champions volunteered, in Round 3, three participants reported that location/role

combination. This could have been an error on the part of the respondent, or it could have been participant confusion since Privacy Champions may have been policy makers in areas other than security. The surveys tried to avoid confusion by tying the role to how the volunteer was recruited, rather than job responsibilities:

> If you were recruited for the study through the Privacy Champion Program, please select 1. All others should select 2.
>
> - 1. I am a Privacy Champion
> - 2. I am a Security/Compliance Policy Maker

As noted, this approach was not sufficient.

Continued stakeholder participation was also a factor. The Delphi method accommodated disparate time zones and work schedules. However, participants required a window of a few days for all to respond to the survey. Time was also needed between rounds for analysis of results and the preparation of the next round of questions. Including the time needed to test access to the survey site, the study took a full eight weeks. Participation varied from week to week with a marked decline in all groups as the study moved from empirical to technical investigation, and again from technical investigation to follow up (see Table 16).

The literature suggests two possible explanations for the drop in participation. The first is participant fatigue, one of the reasons why Delphi researchers suggest limiting the number of rounds (Brockhoff, 2002; Delbecq, Van de Ven, & Gustafson, 1975). The second is that holders of minority views are not adequately explored (Linstone & Turoff, 2002). Related to that within the context of the study is that Round 4 was the most difficult of the surveys, as no multiple choice options were offered. Although all participants were encouraged to participate in Round 5 regardless of participation in Round 4, some may have become disenfranchised.

The second significant drop-off in participation came after Round 6. Following the guidance of Delbecq, Van de Ven, and Gustafson (1975) a follow up round was included to bring the studied issue to closure and help participants appreciate the value of their contribution. Except for the change in subject line, from "Round x…" to " Study Follow up …" there was no difference between this last round and the previous ones. An explanation for the drop-off in participation could be that as a follow up, participants felt their contribution was less important. However, there is no evidence to either support or refute this explanation.

Empirical Investigation Analysis

The goal of the empirical investigation was to establish a set of security values that XYZ and its employees and organizations associated with security behavior. As described earlier, the empirical investigation was comprised of three rounds of Delphi surveys. Between each round, the researcher analyzed responses, synthesized participant comments, and reduced the number of options until there was strong consensus on a value statement for each policy.

Throughout the empirical investigation there was strong policy maker response, important because it is the policy makers that represent organizational values. There was also a strong response from North American employees, important because they represented a broad spectrum of job categories and locations throughout the region. The low international employee response offered too small a group to draw conclusions based on role within location. Because the participants were chosen for their perspectives, and not as a statistical sample, a statistical analysis of their responses was not performed.

However, as part of the response analysis for each round, responses were grouped by theme. There were no themes uniquely attributable to any one location or role.

Throughout the investigation, there was only one response that addressed cultural diversity. Submitted by an international Privacy Champion, the comment read: “The meaning is fine, the wording "honor bound" is culturally very difficult. It to [*sic*] much sounds like military language and might even have a negative effect.” The term honor bound" was subsequently removed from the value statement, even though a North American Privacy Champion responded to the same question with “Adding the words honor bound make it a personal responsibility.”

A concern when formulating the empirical investigation study instruments was that the participant comments would address the value behind the scenario, and not the broader policy that the scenarios illustrated. The concern was not well founded. Although some comments clearly responded to the scenario, they almost always addressed the security issue raised by the policy. The extent to which policy and scenario were specifically addressed varied by round and policy.

In Round 1, Policy 1, almost all comments addressed the policy, not the scenario. Comments like these were typical: “The policy is very clear. Personal convenience is no justification for violating a company policy” and “Protecting the company and its clients information should always be the first thing that comes to mind.” For Policy 2, most comments were fairly evenly divided between policy and scenario. Whereas some participants commented on “Lee’s” actions, comments similar to this were also posted: “I chose based on the policy and not the scenario - employees need to be trustworthy.” Policy 3 comments were also fairly evenly divided. Items such as “Need to understand

that the company has entrusted you with a company asset and to keep that asset secure." and "Policies are written and communicated in order to ensure everyone operates by the same code..." were just as prevalent as comments such as these: "He should not have loaned the computer to his son." and "Petrov is not working responsibly."

In Round 2, there were even fewer references to the scenario – about 10% for each policy. By Round 3, there were no references to the scenario. Comments were mostly focused on policy wording, with a few suggesting changes to the policy itself. For example, two respondents suggested extending the policy that prohibited leaving sensitive information unattended in public facilities to include sensitive information left unattended in corporate facilities. No new values were proposed in any of the rounds of the empirical investigation.

Technical Investigation Analysis

The goal of the technical investigation was to integrate the agreed upon security values into its associated policy. As described earlier, the technical investigation was comprised of three rounds of Delphi surveys (Rounds 4, 5, and 6), plus a follow up round to gather data on the process itself. As also noted earlier, there was a drop in participation ranging from 20-40% as the survey moved to this investigation. However, the quality of responses and strength of consensus can reflect a sufficient level of inclusion (Powell, 2003). In this study, technical investigation responses were both robust and aligned.

Round 4 was the only fully open-ended survey – a possible reason why the level of participation dropped to the lowest level in the technical investigation – down by 25%

among the North American policy makers, 40% among North American Privacy Champions, and by 50% across the two international groups. No participant ever offered an explanation of his or her departure from the study and because responses were anonymous, it was not possible to seek out those who chose to leave. Participation never returned to the levels sustained in the empirical investigation. The responses that were submitted, however, were well considered, substantive, and constructive. An example for each of the policies is included in Table 17.

Table 17

Examples of Participant VSPs and Explanations

Policy	VSP	Explanation
1	"To honor our commitment to our customers, safeguard the sensitive data they entrust to us, and comply with our security policies; we must conduct XYZ business on XYZ equipment, and from non-XYZ equipment that complies with the Remote Access Standard, also the use of computer systems or emails not provided by XYZ is prohibited."	"By stating the value first the end user has a better understanding of why the statements need to exist."
2	"XYZ information resources should not be left unsecured. Employees must respect the responsibility entrusted by XYZ and it's customers by anticipating security problems and proactively looking for ways to avoid them."	"I removed the words visible and unattended, because i think that in and out of the work place, any information resources should not be left unattended, and this simplified the "what". This is a simple statement with one main point, i thought it could be first and then go into the "why" since the "what" would not be forgotten since it is not complicated."

3	"Lending XYZ information resources, including company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited. As employees we have a personal responsibility to do what is right for XYZ and our customers, respecting their trust over personal convenience and promoting customer security interests."	"Would just put them one after the other as written. The policy is needed so there is no question as to the rule, and the value is an explanation of why the policy is there."

Note: Responses are quoted verbatim

Throughout the technical investigation there were strong indications of consensus. Many of the proposed VSPs included the phrases "honor our commitment to clients," "we respect the responsibility entrusted to us," and "a personal responsibility to do what is right." A rating rubric was applied to evaluate the submissions and identify the best in terms of understandability of content, clarity of presentation, completeness of thought, and logical connection between policy and value. The highest rated submissions were presented in Round 5.

Round 5 returned to a simpler approach, a vote on the best of the Round 4 submission and an optional, open-ended explanation. Following Powell (2003), a percentage level for inclusion was established. In this case 30% of all participants rated it as their first choice. Again, there was strong consensus on the VSPs, and nothing in the comments that suggested variance in interpretation. Comments fell into one of two categories – a change to the policy itself or improved wording. No other values were proposed nor was a different approach to integrating the value into the policy. The VSPs that met the 30% threshold were similar enough to be blended into a single VSP for each policy and proposed as final in Round 6.

Round 6 also consisted of a simple vote, with the researcher following Powell (2003), establishing a percentage level for inclusion. Again, there was strong consensus, with 93% of participants either agreeing or strongly agreeing with the proposed VSP for Policies 1 and 2, and 100% agreeing or strongly agreeing with the proposed VSP for Policies 3. Comments supported the tally: "2 and 5 are both basically the same…" and "Just change the sentences. Second sentence first, first sentence last." More substantive comments were typically on clarity, "Need to remove 'these' in front of information resources, but is ok otherwise" or on requested changes to the policy, "I think the policy should be expanded…" Consistent with comments in earlier rounds, changes to policy were proposed in Round 6 as well, although it is not possible to know if the same or different participants raised them. Because the stated goal of the study was to integrate the value into the policy, the researcher took the position that for this study policy would not change. In future studies, that position is worthy of re-examination as VSD empowers stakeholders to change the end product to reflect the values of its users.

To accommodate the improvements proposed in Round 6 and give participants an opportunity to comment on the VSD process, the follow up survey was added. As noted earlier, all respondents, albeit half the number of those who participated in Round 1, considered VSD successful as a means of defining security values and integrating them into policy. According to Linstone and Turoff (1975), convergence of opinions is an indicator that consensus was reached, and data clearly shows that convergence was reached. However one respondent raised a valid point, commenting "[it is] hard to know if we would have had more success with a different approach." It is a question left to future research.

Analysis Summary

No one study can definitively establish the usefulness of a methodology. However, the study can validate that its goals were met and identify areas that bear further scrutiny. In this study, there was sustained and meaningful participation from stakeholders. Consensus was reached on security values and on the three value sensitive security policies. Comments in the follow up survey not only confirmed satisfaction with the final wording of the VSPs, but satisfaction with the idea of building values into policies and the inclusionary nature of the VSP process.

However, it can be argued that limitations in participant solicitation and data collection leave the data set incomplete. Logistical issues related to accommodating an organization with broad geographic and cultural diversity leaves open methodological questions. The Delphi methodology was able to overcome problems of time and distance that precluded face-to-face meetings or conference calls. It provided a safe venue for the open exchange of ideas. At the same time, Delphi is prone to participant fatigue, particularly when applied to VSD research that requires at least two, multi-round investigations. Also, the tool used to distribute the Delphi survey must overcome the access issue faced in this study as it is a serious limitation if the researcher cannot pursue those that fail to respond (Hasson, Keeney, & McKenna, 2000) or seek clarification and a deeper understanding of responses (Okoli & Pawlowski, 2004). A more complete analysis of empirical and technical investigations would have been possible had the Delphi data collection tool been able to accommodate both researcher access and participant-level anonymity.

Validity

The traditional means of validating a VSD project is through the iterative feedback from participants as they move through the investigations (Friedman, Kahn, & Borning, 2001). Because this study was designed to evaluate the methodology rather than the design of a finite end product, the study required validation beyond that provided by participants. Within the literature of qualitative research, Maxwell (2005) offered an established framework for examining data validity and generalizability. This framework was, as described in Chapter 3, adapted for this study.

The Maxwell framework provides strategies for examining bias and reactivity as threats to internal and external generalizability. This is particularly useful because VSD and Delphi methods are, by design, researcher controlled and influenced. It is also useful because of the relevance of internal generalizability to the first research question and external generalizability to the second. Under the framework, bias is a threat to validity when the selection of data sources and scrutiny of evidence are conducted in a manner that reflects the researcher's preconceptions. Scrutiny for both internal and external validity comes through an examination of bias and influence in the participant selection processes, in the process by which responses were evaluated, through rigorous respondent validation, and through a diligent search for discrepant evidence. These activities are explored through four questions.

Were participants selected to fit the researcher's preconceptions?

The goal of stakeholder recruitment was to generate a broad range of knowledgeable opinions from both policy writers and employees (Linstone & Turoff,

2002; Okoli & Pawlowski, 2004). Rather than hand select potential participants from the organization at large, a practice that might inadvertently lead to selection bias, participants were solicited from two global, pre-established, expert groups. During the recruitment period, the researcher avoided one-on-one communication with potential subjects. Questions were submitted via email and responses were aggregated and sent to the constituent groups as an FAQ. All who volunteered for the study were accepted.

Were data sources selected to fit the researcher's preconceptions?

The VSD literature offered the researcher little guidance on how to identify and evaluate relevant values during the conceptual investigation. It had been defined by Friedman, Kahn, and Borning (2001) as "thoughtful consideration of how stakeholders might be socially impacted by one's technological designs" (p.3), the implication being that it is the researcher who performs the thoughtfulness. How VSD researchers have conducted the investigation has varied considerably. Regardless of the process disparities among conceptual investigations, the VSD literature was consistent in placing responsibility for establishing the initial value set with the researcher. By its very definition, the method opens itself to threat of bias.

As a test of bias in the conceptual investigation, the Maxwell framework asked what steps were taken to provide consistent evaluation of all responses. Strategies to minimize bias came from the collection of detailed and varied data, use of an established method for reducing the initial set of values to a workable number, and involving respondents in validating the selection. To establish the rich data set, all known data sources were included in the investigation. The 287 studies that provided background for

the study (the literature of organizational culture, organizational values, employee values, security culture, security behavior, and VSD) were searched for the terms "security" and "values." In addition, the XYZ Corporate Values were included. The research yielded an initial data set of 56 value statements. To address the threat of bias in culling the list down to a workable starting point for the empirical investigation, the Burmeister (2012) methodology was followed. This yielded 11 security values based on rich sources and a formal selection methodology and provided an informed and workable starting point for the empirical investigation. In the first round of the empirical investigation, participants were asked to identify security values from the 11 or submit their own, providing an opportunity for any value overlooked by the researcher to be included in the study.

Were all stakeholder responses given full and equal scrutiny?

To minimize bias in the process of whittling hundreds of responses down to a single value or value sensitive policy, a rigorous process was followed. Responses and comments were exported out to duplicate worksheets – one that included respondent role and location, and one that included only responses. The version without demographic information was used for scrutiny. Both responses and comments were included in the review so that the analysis included a search for discrepant evidence. The results from that analysis were reduced to key themes, and then key themes were tabulated. Those with the strongest participant support were presented to the group in the next round for validation and/or modification. This three-step evaluation minimized bias related to the role or location of respondent, as well as bias related to spelling and grammar or eloquence of argument.

To what extent did the researcher influence participant responses?

There is a paradox in qualitative research in that subjective awareness is what brings the researcher to the problem, yet at the same time diminishes objectivity that can influence data collection and analysis (Ahern, 1999). From a VSD perspective, Borning and Muller (2012) suggested strong representation across stakeholders' groups as a means of countering the threat of researcher influence. This was consistent with Maxwell who suggested that researcher influence is detected through a search for discrepant evidence, comparison of data across constituent groups, and respondent validation.

In analyzing the rounds of responses, the researcher evaluated both the respondents' choices and rationale. Although the goal was to identify common themes, a diligent review of all responses was conducted to look for varying perspectives. Iteration in Delphi rounds was used as a means of working through the differences and bringing participants to consensus. In this way, discrepant data was brought to the participants to resolve. As part of the analysis for each round, responses were categorized by role and location of respondent. Only one question in one round suggested the possibility of regional trend, but there was insufficient evidence to draw a definitive conclusion. In Round 1, value 2, one of the value choices, "We are responsible for following the rules", was selected by only one international participant (13%), where as it was selected by 23% of the North Americans. However, there were too few international participants to draw inferences from that statistic. Furthermore, there were no other questions in the survey that yielded a skewed response.

Respondent validation was incorporated into each round of empirical and technical investigations. This included the option for participants to provide alternatives if the

options offered were insufficient. None were offered. Furthermore, the comments offered by participants in each round were a rich source of information about how the questions were interpreted, providing further response validation in each round.

Validity Summary

In the opening section on validity, Maxwell (2005) asked a simple question, "How might you be wrong?" (p.105). The toolset he offered, adapted for this study as the Maxwell framework, looked to both the data and the data collection practices for evidence of credibility. The strength of the study's conclusions lay in its rich data, the rigorous search for discrepant data, and iterative participant validation. Its weakness in its conclusions lay in the fact that only three of the four solicited constituent groups were well represented.

Summary

In this chapter, study results were examined from three perspectives. First was a look at the data – how the initial review of 287 journal articles were systematically assessed, yielding a set of 11 value statements, and how the study participants culled from these 11 a single key value statement for each of the three security scenarios. The Data section demonstrated how participants were solicited and how the volunteers that came from that solicitation represented, or failed to represent, the diversity of the organization. The Analysis section examined the methodology followed to constrain opportunities for researcher bias and acknowledge the limits of those constraints. The Analysis section also described the influences on data gathering decisions, including

options for survey tools, communications, and privacy requirements unique to the population studied. The Validity section examined the study's claims of generalizability of findings by examining opportunities for researcher bias and influence. Through a set of questions established by Maxwell (2005), bias in participant selection, the establishment of the initial value set, and the tabulation of each round of survey responses were scrutinized. Despite the many opportunities for research bias and the threat of reactivity, the continuous confirmation of choices by participants, consistent across role and location, was found to be a validation of the resulting value sensitive policies and the VSD method used to define them.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Introduction

Chapter 5 returns to the two research questions, drawing inferences from the results on security values and value sensitive policies as a means of aligning organizational and employees, and thus promoting security culture. The chapter also discusses limits around those conclusions, particularly in security practice, and suggests opportunities for future research. The chapter concludes with a summary of the study.

Conclusions

This study began with two questions: What values do employees and organizations associate with security behavior? Can VSD be used to create a security policy that reflects both organization and employee values? Starting with the second research question helps understand conclusions related to each. VSD can be used to create a security policy that reflects the values of both the organization and its employees. This was clear from the data that evolved over the three investigations and was corroborated by study participants. In their own words, reflecting the total body of comments: “I'm impressed with the process as a whole and thought it was a very good way to update the policies,” said one. “I really like the resulting policy statements,” said another. “They

are clear, and personally relatable. I really consider that this process permitted the participation of all areas and cultures."

And what are those values, RQ1 asks? Through the VSP process, three values emerged: trust, commitment, and personal responsibility. Interestingly, the value statements that evolved were not isolated values, but rather the pairing of trust and one other value.

1. We must honor our commitment to our customers to follow XYZ's security policies as they are designed to safeguard the sensitive data customers have entrusted to us - a combination of trust and commitment
2. We respect the responsibility entrusted to us by XYZ and our customers by anticipating security problems and proactively looking for ways to avoid them - a combination of trust and personal responsibility
3. As employees we have a personal responsibility to do what is right for XYZ and our customers, respecting their trust over personal convenience and promoting customer security interests - also a combination trust and personal responsibility

In the estimation of these participants, security values are a combination of respect for what has been entrusted to them and a personal commitment to a course of action that supports that trust. The dual nature of the values uncovered in this study has interesting implications for security culture as the literature of security culture describes it as a combination of values and action. This speaks to the underlying thesis of this study - that when employee and organizational values are aligned, employees will automatically behave in a manner that was consistent with those values. The results of this study alter that a bit. Rather than values being a catalyst for action, it shows that action is part of

the value itself. If this is true, it provides a compelling reason to integrate values and policy.

Implications

This study showed that VSD can be used to create security policies that reflect the values of the organization and its employees. It showed that consensus can be reached in a culturally diverse organization, and in an organization where security has a high profile. At the same time, there are aspects of the methodology that must be refined before the method could be deployed in practice. These include the length of time needed to develop VSPs for an entire policy document and the skillset needed to run a VSP project.

In this study, it took six rounds of surveys and eight weeks of continued involvement for participants to evolve VSPs for three policy statements. Participant fatigue became evident at week five. As is, the method is not practical for an organization that wants to use the method to develop its entire end user policy – a document of perhaps 20 or 30 policy statements. Beyond survey fatigue, employee travel, vacation, illness, and other work commitments will interfere with full participation. This is a problem because Delphi is heavily dependent upon the same participants committed to the study, maintaining involvement until the process is completed (Buck, Gross, Hakim, & Weinblatt, 1993). From a practical perspective, researchers will have to look for data collection methods that are more efficient, or have a deeper understanding of potential participation drop off so that problems can be circumvented.

VSD is heavily dependent upon a trained facilitator. That person is responsible for identifying the initial value set introduced in the empirical investigation and for aggregating and finding commonalities among each round of responses. The skillset for the role includes knowledge of security sufficient to understand the policies and their implications. It also requires knowledge of the research methods that can used to establish the initial set of values, create and validate survey questions, and move the study group through the VSD process. It is the facilitator's responsibility to identify logistical obstacles and modify the methodology to overcome them. These can be the identification of representative stakeholders, time zone issues, privacy constraints, or data collection limits, such as those encountered in the course of this study. Others unique to the organization will be left to the facilitator to resolve. These are not insurmountable obstacles, but they are important considerations for an organization that wants to use the method presented here to establish their own value sensitive policies.

Recommendations for Future Research

The goal of this study was to determine if VSD is an effective method for defining organizational and employee security values and integrating them into the organization's end user security policy. By all participant accounts, the research goal was met. In so doing, the study filled a gap in the literature and practice of security culture by showing how security values can be defined and how employee and organizational values can be aligned and communicated. Yet each organization that plans to implement such a program will run into unique challenges that further research can help address. Further research can also help validate the results of this study. No one study can test all

components of the methodology, but all components should be validated as it is tempting to give the results broader applicability than the methodology supports. The six areas discussed in this section are by no means a definitive list of work to be done to more deeply understand security values and the role they play in security culture. Rather they serve to illustrate the complexity of design choices and frame methodological issues for future studies.

Although VSD is arguably the most widely reviewed method of instilling values into design (Manders-Huits**,** 2011), it is by no means the only one. Burgemeestre, Hulstijn, and Tan (2013) and Rotondo and Freier (2010) are among those to evaluate alternatives. VSD was selected for this study because it incorporated both values definition and alignment. However as described in Chapter 2, there are numerous ways to establish the initial set of values introduced in the empirical investigation. There are also numerous ways to work with participants to elicit relevant values. Future research can explore these two questions separately. Furthermore, separately exploring dimensions of security values and ways of aligning employee and organizational values may address the hefty time commitment VSD requires.

Participant selection is one area that would benefit from further exploration and experimentation. There are quantitative and other qualitative methods to identify organizational and employee values. Selecting employees who have shown no particular interest in security may present a different set of employee values than those that come from a group like the Privacy Champions. More work is needed in representing cultural diversity of participants as well. In this study, an assumption was made that participation from all four regions would address the cultural diversity of the

organization. However, that was likely not so as the regions themselves were culturally diverse. For example, there were two APAC participants, one in Singapore, of Australian heritage, and one in Sydney of Malaysian heritage. APAC staff however, is based in China, India, and South Korea, as well as in Australia, and Singapore. Each of these areas has unique cultural mores that may inform what employees and organizations consider security values. The same questions can be raised for each of the other regions and the many nations they comprise.

The choice of methodology made to accommodate cultural and geographic diversity is another area worthy of future exploration. In this study, all participants were either involved in creating security policy or promoting security awareness. The organization itself had a mature security program and published organizational values. It would be useful to compare results of this study with those from a fledgling company that had not yet established strong messages around security or values.

As noted in the Methodology (Chapter 3), logistical issues specific to XYZ Corp drove many of the operational decisions. Understanding the extent to which these operational issues influenced results is important for both research and practice. For example, the geographic diversity in this study operationalized as a requirement for asynchronous communications. The data collection method selected to overcome the breadth of participant time zones also limited participant interaction and exchange of ideas. A different study site will have its own requirements, providing an opportunity to test different tools for data collection. Along these same lines, three policy statements were sufficient to test VSD as a means of integrating employee and organizational values into an end user policy. However, end user policies can be comprised of 20 or more

policy statements. The logistics of bringing disparate stakeholder cohorts to agreement on the full complement of policy statements presents a research challenge in its own right.

The methodology employed in the empirical investigation raises another question - did the scenarios help participants understand the security values or did they limit creative thinking? The scenarios, taken from actual incidents at XYZ Corp, were designed to help participants understand conflicting values that drive behavior. In each case, a well-meaning employee made a values-based decision that was unintentionally in conflict with the security policy. It is possible that other scenarios or other methods of eliciting stakeholder values would generate different values. The extent to which the scenarios informed participant responses is unknown. Along the same lines, this study, for the most part, presented options through multiple-choice questions on the Delphi instrument. It would be useful to know whether open-ended questions would yield the same results. If results differed, the question would be raised if the values identified in this study were incorrect, or if the values elicited through equally rigorous methods could be equally valid.

Study leadership should also be explored. In this study, the researcher was well known to the organization and many of the study participants. Unintentional researcher bias and its influence on results may be less of a factor when someone from outside the organization leads the study. Along the same lines, it would be useful to know how the initial set of values differs when established by persons or groups other than the principle researcher.

Part of establishing a body of knowledge around security values and its influence

on security culture is validating findings through different approaches. This is achieved through studies in other types of organizations, different types of stakeholders, other implementations of VSD, and other means of defining and aligning employee and organizational values. Each study will have its logistical considerations, limitations, and constraints that influence the outcome, but each will also help build a better understanding of employee and organizational security values and how they can be aligned to promote security culture. Yet coming to a deeper understanding of security values and values alignment is only a first step in understanding the role of security values in security culture. The step that follows is a return to the seminal question – will aligned employee and organizational values promote the automatic and habitual security promoting behaviors associated with security culture? This study lays the groundwork for that research and establishes a foundation upon which this larger question can be explored.

Summary

The security literature presents strong evidence that employee behavior continues to be a critical component of the organization's security program and that establishing a culture of security is an effective means of promoting habitual and consistent security practices. Security culture research suggest that if employee and organizational values can be aligned, not only will the organization influence employees toward security culture, the employees will influence one another and strengthen the culture. However, there is little research on how an organization defines its security values as well as those of its employees, and once defined, how the values are aligned and communicated.

Value Sensitive Design has evolved as a theoretically grounded approach to identifying stakeholder values and building them into technology design. This study tested VSD as a method of identifying security values within an organization and incorporating them into the end user policy.

The study was conducted at a global financial services organization, following VSD's iterative, tripartite, methodology to identify the security-related, human value requirements of stakeholders, address competing values, and test for consensus throughout the design process. The conceptual investigation began with the researcher's exploration of an initial set of values associated with information security, culling 287 articles from the VSD, information security, and security culture literature, plus the studied organization's published value statements to establish a starting point for participants. From these sources, an initial set of 86 values was established, and then following Burmeister's (2012) methodology, reduced to that to the 11 key values that became the starting point for the empirical investigation. The empirical and technical investigations employed an online, Delphi process, guiding participants toward agreement on security values and then the expression of those values within three policy statements.

Participants were solicited from the organization's security policy makers and from its Privacy Champion program, employees who volunteered to assist with security and privacy related activities. Policy makers were solicited because organizations express their values thru policy; Privacy Champions were solicited as representatives of the employee population. Although all four of the organization's global regions were

represented, only two of the 39 participants were from among the international Privacy Champions.

The goal of the empirical investigation was to come to consensus on the security values relevant to the three policy statements. Participants were given three policy statements from the XYZ Corp End User Policy, along with scenarios taken from actual security incidents, selected to highlight how security values may be in conflict with other employee values, and the list of 11 key values evolved during the conceptual investigation. Over the course of three Delphi Rounds (three weeks), participation remained strong and consensus was reached on a value statement for each policy:

1. We must honor our commitment to our customers to follow XYZ's security policies as they are designed to safeguard the sensitive data customers have entrusted to us.
2. We respect the responsibility entrusted to us by XYZ and our customers by anticipating security problems and proactively looking for ways to avoid them.
3. As employees we have a personal responsibility to do what is right for XYZ and our customers, respecting their trust over personal convenience and promoting customer security interests.

The common theme across the three was that security values are a combination of two values: trust and one other value. Each of the three VSP included respect for what has been entrusted to them and a personal commitment to a course of action that supports that trust.

The goal of the technical investigation was to integrate the values defined in the empirical investigation into the policy statements, thus creating value sensitive policies

(VSPs). Participants were given the three policy statements from the empirical investigation, along with their three corresponding value statements. Within the three weeks (thee Delphi Rounds) of the technical investigation, participation varied from 60% to 80% of empirical investigation participation. Those who remained reached strong consensus on VSPs, bringing the technical investigation to a close. Because no new values were added that would have required a return to the conceptual or technical investigations, had the study been simply a VSD project, it would have concluded at that point. However, the purpose of the study was to test VSD as means aligning employee and organizational values and incorporating them into a VSP. One further survey was required to solicit participant feedback on those two questions. In the final survey all participants responded that they were satisfied or very satisfied with the VSP they had evolved, and comments about the process were equally favorable. The three final VSPs were the following:

1. To safeguard sensitive data, only email accounts provided by XYZ or other approved methods for data sharing may be used to conduct XYZ business. Furthermore, XYZ business must be conducted using XYZ equipment or using non-XYZ equipment that is in compliance with the Remote Access Standard. Complying with this policy honors our commitment to customers to keep their data secure.
2. To protect the data entrusted to us, client data and other sensitive information must not be left visible or unattended outside XYZ's facilities or unsecured and unattended within XYZ's facilities. When working with client data, we must

anticipate problems related to keeping data secure when we are not present, and proactively looking for ways to avoid them.

3. As XYZ employees, we have a personal responsibility to protect XYZ and customer security interests over personal convenience. For that reason, lending XYZ information resources such as company issued laptops and desktop computers to family members, friends, or non- XYZ employees is prohibited.

Because the study was designed to evaluate the methodology and not just create a value sensitive end product, the study required validation beyond the survey that ended the technical investigation. A validation framework was created, based on Maxwell (2005) that provided strategies for examining bias and reactivity as threats to internal and external generalizability. The strength of the study was found to be in its rich data, rigorous search for discrepant data, and iterative participant validation. The weakness in its conclusions lay in the fact that only three of the four solicited constituent groups were well represented.

As seminal research in building security culture through security values, it is important to acknowledge its limits. Stakeholders participated in the VSD process, identified security values, and crafted security policies that included both the agreed upon value and the behavior associated with it. These results affirmed the two research questions. However, this line of research is in its infancy. Future research is necessary to validate these results and explore methodologies that may be more efficient or more suitable to other organizations. Once a more robust body of knowledge exists, practical application must be explored. Research must return to test the thesis upon which this study was built – that aligning employee and organizational security values contributes to

security culture, promoting the habitual and self-perpetuating security behavior associated with it.

Appendices

Appendix A: Human Values (with Ethical Import) Often Implicated in System Design

Human Value	Definition	Sample Literature
Human Welfare	Refers to people's physical, material, and psychological well-being	Leveson (1991); Friedman, Kahn, and Hagman (2003); Neumann (1995); Turiel (1983, 1998)
Ownership and Property	Refers to a right to possess an object (or information), use it, manage it, derive income from it, and bequeath it	Becker (1977); Friedman (1997b); Herskovits (1952); Lipinski and Britz (2000)
Privacy	Refers to a claim, an entitlement, or a right of an individual to determine what information about himself or herself can be communicated to others	Agre and Rotenberg (1998); Bellotti (1998); Boyle, Edwards, and Greenberg (2000); Friedman (1997b); Fuchs (1999); Jancke, Venolia, Grudin, Cadiz, and Gupta (2001); Palen and Dourish (2003); Nissenbaum (1998); Phillips (1998); Schoeman (1984); Svensson, Hook, Laaksolahti, and Waern (2001)
Freedom from Bias	Refers to systematic unfairness perpetrated on individuals or groups, including preexisting social bias, technical bias, and emergent social bias	Friedman and Nissenbaum (1996); cf. Nass and Gong (2000); Reeves and Nass (1996)
Universal Usability	Refers to making all people successful users of information technology	Aberg and Shahmehri (2001); Shneiderman (1999, 2000); Cooper and Rejmer (2001); Jacko, Dixon, Rosa, Scott, and Pappas (1999); Stephanidis (2001)
Trust	Refers to expectations that exist between people who can experience goodwill, extend goodwill toward others, feel vulnerable, and experience betrayal	Baier (1986); Camp (2000); Dieberger, Hook, Svensson, and Lonnqvist (2001); Egger (2000); Fogg and Tseng (1999); Friedman, Kahn, and Howe (2000); Kahn and Turiel (1988); Mayer, Davis, and Schoorman (1995); Olson

		and Olson (2000); Nissenbaum (2001); Rocco (1998)
Autonomy	Refers to people's ability to decide, plan, and act in ways that they believe will help them to achieve their goals	Friedman and Nissenbaum (1997); Hill (1991); Isaacs, Tang, and Morris (1996); Suchman (1994); Winograd (1994)
Informed Consent	Refers to garnering people's agreement, encompassing criteria of disclosure and comprehension (for "informed") and voluntariness, competence, and agreement (for "consent")	Faden and Beauchamp (1986); Friedman, Millett, and Felten (2000); The Belmont Report (1978)
Accountability	Refers to the properties that ensures that the actions of a person, people, or institution may be traced uniquely to the person, people, or institution	Friedman and Kahn (1992); Friedman and Millet (1995); Reeves and Nass (1996)
Courtesy*	Refers to treating people with politeness and consideration	Bennett and Delatree (1978); Wynne and Ryan (1993)
Identity	Refers to people's understanding of who they are over time, embracing both continuity and discontinuity over time	Bers, Gonzalo-Heydrich, and DeMaso (2001); Rosenberg (1997); Schiano and White (1998); Turkle (1996)
Calmness	Refers to a peaceful and composed psychological state	Friedman and Kahn (2003); Weiser and Brown (1997)
Environmental Sustainability	Refers to sustaining ecosystems such that they meet the needs of the present without compromising future generations	United Nations (1992); World Commission on Environment and Development (1987); Hart (1999); Moldan, Billharz, and Matravers (1997); Northwest Environment Watch (2002)

Note: From "Value sensitive design and information systems,' by B. Friedman, P. H. Kahn, and A. Borning, 2006, in *Human-Computer Interaction and Management Information Systems: Foundations*, p. 364. Copyright 2006 by ME Sharpe.

*All but Courtesy were included in the original Friedman & Kahn (2003) list of 12 human values with ethical import. Courtesy was added in 2006, referenced in the Note.

Appendix B: A Category Framework of User Values

Category of Values	Description	Product Benefit Examples
Social values (Alderfer 1972; Maslow 1970, Sheth et al. 1991)	Relatedness, social, and external esteem, status, power, control and dominance, achievement, conformity, equality, helpfulness, honesty and loyalty	Increase in social associations between family or other social groups, increase in respect, influence, power, social achievement and conformity, e.g. in communication or task management
Emotional/ hedonistic values (Holbrook 2005; Schwartz 1992; Sheth et al. 1991)	Aroused feelings or affective states, pleasure, fun, sensory enjoyment	Features arousing positive feelings, pleasure and enjoyment, increase in emotional experiences, support in handling experiences and emotions and saving emotional occasions; e.g. mobile TV
Stimulation and epistemic values (Schwartz 1992; Sheth et al. 1991)	Excitement, experienced curiosity, novelty and gained knowledge	Increase in excitement; e.g. in adventure gaming
Growth and self-actualization values (Alderfer 1972; Maslow 1970; Rokeach 1973, Schwartz 1992)	Self-actualization, creating, independent thought and action	Support in creating new things and achieving internal esteem; e.g. a multimedia authoring system; personal web site creation
Traditional values (Schwartz 1992)	Respect, commitment, and acceptance of the customs and ideas that traditional culture or religion impose on the self	Support in users' tasks in maintaining their customs and ideas; e.g. traditional industrial design of product appearance; religious content
Safety values (Maslow 1970; Schwartz 1992)	Security, social order, healthy, comfort, freedom from fear	Protection and alarms, ease of use, familiarity of functions and appearance; e.g. mobile communication or surveillance

Universal values (Schwartz 1992)	Understanding, appreciation, tolerance, and protection for the welfare of all people and for nature	Ecological soundness, improving equality; e.g. recyclability of products; flea market web sites; donation web sites

Note: From "Value of information systems and products: Understanding the users' perspective and values" by S. Kujala and K. Väänänen-Vainio-Mattila, 2009, *Journal of Information Technology Theory and Application (JITTA), 9*, p. 32.

Appendix C: Fundamental Objectives Related to IS Security

Overall objective: Maximize IS security

- Enhance management development practices
  - Develop a management team that leads by example
  - Ensure individual comfort level of computers/software
  - Increase confidence in using computers
  - Create legitimate opportunities for financial gain
  - Provide employees with adequate IT training
  - Develop capability level of IT staff
- Provide adequate human resource management practices
  - Provide necessary job resources
  - Create an environment that promotes contribution
  - Encourage high levels of group morale
  - Enhance individual/group pride in the organization
  - Create an environment of employee motivation
  - Create an organizational code of ethics
- Develop and sustain an ethical environment
  - Develop an understood value system in the organization/whistle blowing
  - Develop coworker and organizational ethical relationships
  - Instill value-based work ethics
  - Instill professional work ethics
  - Create an environment that promotes organizational loyalty
  - Stress individuals treating others as they would like to be treated
- Promote individual work ethic
  - Maximize employee integrity in the company
  - Minimize urgency of personal gain
  - Create a desire to not jeopardize the position of the company
  - Create an environment that promotes company profitability rather than personal
  - Minimize temptation to use information for personal benefit
- Maximize data integrity
  - Minimize unauthorized changes
  - Ensure data integrity
- Enhance integrity of business processes
  - Understand the expected use of all available information
  - Develop understanding of procedures and codes of conduct
  - Ensure that appropriate organizational controls (formal and informal) are in place
- Maximizing privacy
  - Emphasize importance of personal privacy
  - Emphasize importance of rules against disclosure

Maximize access control	Maximize organizational integrity
Create user passwords	Create an environment of managerial support and solidarity
Provide several levels of user access	Create environment of positive management interaction
Ensure physical security	Create an environment that promotes respect
Minimize unauthorized access to information	Create an environment that promotes individual reliability
	Create environment of positive peer interaction

Note: From "Value-focused assessment of information system security in organizations" by G. Dhillon & G. Torkzadeh, 2006, *Information Systems Journal, 16(3),* p. 306.

Appendix D: Means Objectives Related to IS Security

- Increase trust
  - Display employer trust in employees
  - Develop an environment that promotes a sense of organizational responsibility
  - Maximize loyalty
- Provide open communication
  - Minimize curiosity because of lack of information
  - Create an open-door environment within all levels of the organization
  - Stress IT department interactiveness
  - Develop open communication with IT department
  - Limit 'arm's length' management
- Maximize awareness
  - Create an environment that promotes awareness
  - Develop awareness of balance between technical and social aspects of IS security
  - Ensure explicit understanding of organizational culture by individuals
  - Educate employees to be aware about suspicious individuals and activities
- Optimize work allocation practices
  - Distribute workload optimally
  - Monitor and adjust unoccupied time
  - Develop understanding of organizational and information use procedures
- Establish ownership of information
  - Promote ownership in the organization
  - Emphasize importance in confidentiality
  - Emphasize the understanding of the value of information
  - Create a contract of confidentiality
- Ensure availability of information
  - Ensure adequate procedures for availability of correct information
- Promote responsibility and accountability
  - Clarify delegation of responsibilities
  - Maximize level of commitment to organization
  - Create an environment that promotes accountability
- Understand work situation
  - Minimize need to have leverage on others
  - Minimize desire to seek revenge on others
  - Minimize creation of disgruntled employees
- Maximize fulfillment of personal needs
  - Appreciate personal needs for job enhancement
  - Facilitate attainment of self-actualization needs
- Understand individual characteristics
  - Understand particular individual characteristics and demographics to subvert controls
  - Interpret individual lifestyles
- Enhance understanding of personal financial situation
  - Understand the needs of different level of financial status
  - Eliminate the personal benefit of sharing information with competitors

Clarify centralization/decentralization issues	Ensure censure
Ensure a right balance between centralization and decentralization	Introduce a fear of being exposed or ridiculed
	Instill a fear of consequences
Ensure legal and procedural compliance	Instill a fear of losing your job
Minimize the disregard for laws	Instill excommunication fear
Decrease the level of employer's tolerance for misuse of information	Understand personal beliefs
Develop understanding of legalities and regulations	Celebrate and understand the manner in which one was raised
Develop mechanisms for an information audit trail	Minimize the need for greed in the organization
	Instill ethical and moral values

Note: From "Value-focused assessment of information system security in organizations" by G. Dhillon & G. Torkzadeh, 2006, *Information Systems Journal, 16(3),* p. 307.

Appendix E: Values in Security Literature

Source	Value Statements
Adams, Thomson, Brown, Sartori, Taylor, & Waldherr, S. (2008)	Trust
Ågerfalk, Karlsson, & Hjalmarsson, (2001)	Trust
Batteau (2011	Trust
Cazier, Shao, & St. Louis (2007)	Trust
Cazier, Shao, & St Louis (2006)	Trust
Chang, & Lin (2007).	Consistency: Order, rules and regulations, uniformity, and efficiency Effectiveness: Competitiveness, goal achievement, production, effectiveness, and benefit-oriented measures Innovativeness: Creativity, entrepreneurship, adaptability, and dynamism Cooperativeness: Cooperation, information sharing, trust, empowerment, and team work
Hedström, Kolkowska, Karlsson, & Allen (2011)	Accountability, integrity, confidentiality, productivity, easy availability, privacy, efficiency
Helokunnas & Kuusisto, (2003)	Confidentiality, integrity and availability have to be in balance.
Killingsworth (2012).	Honesty, integrity, respect, teamwork, loyalty, citizenship, and accountability

Koch, Proynova, Paech, & Wetter (2013)	Safety, harmony and stability of society, of relationship, and of self
Kolkowska, (2006).	Clear overall rules and policies, limited control, maximal freedom and flexibility, maximal awareness. Trust, Privacy, maximal information and system availability. Cooperation. Openness of information, maximal information integrity
Laeequddin & Sardana (2010).	Trust
Lee, Soutar, & Louviere (2007)	Obey rules and regulations. Check who is at my door before opening it.

Appendix F: XYZ Corporate Values

1. Put customers first. Create value for our customers in everything we do.

2. Empower our people. Encourage and support each other to learn and grow in our careers.

3. Act with integrity. Build relationships based on honesty, trust, and respect with our customers, colleagues and communities.

4. Deliver excellence. Innovate and challenge the status quo to achieve exceptional results.

5. Enjoy the journey. Take pride in our work and succeed together as part of a diverse global team.

Appendix G: Four Step Process – From Initial Set to Key Values

1a. Initial Set of Values	1b. Value Categories	2. Categories Clustered Into Themes	3. Subsidiary Values Removed	4. Key Values Within Themes
Trust	Accountability	Access control	Accountability	Anticipate problems and prevent them
Trust	Adaptability	Accountability	Adaptability	Build and sustain trust
Trust	Autonomy	Achievement	Autonomy	Create value for customers
Trust	Availability of information	Adaptability	Availability	Creatively address problems and opportunities
Trust	Balance between centralization and decentralization	Autonomy	Awareness	Do the right thing
Consistency: Order, rules and regulations, uniformity, and efficiency Effectiveness: Competitiveness, goal achievement, production, effectiveness, and benefit-oriented measures Innovativeness: Creativity, entrepreneurship, adaptability, and dynamism Cooperativeness: Cooperation, information sharing, trust, empowerment, and team work	Balance between confidentiality, integrity and availability	Availability	Balance	Ensure information is properly accessible

Accountability, integrity, confidentiality, productivity, easy availability, privacy, efficiency	Benefit-oriented measures	Awareness	Incent/ensure compliance	Honor customer trust over personal convenience
Confidentiality, integrity and availability have to be in balance.	Calmness	Balance	Calm	Make work meaningful and satisfying
Honesty, integrity, respect, teamwork, loyalty, citizenship, and accountability	Check who is at my door before opening it.	Calm	Citizenship	Promote personal responsibility
Safety, harmony and stability of society, of relationship, and of self	Citizenship	Citizenship	Strong governance	Remove obstacles and delays to necessary action
Clear overall rules and policies, limited control, maximal freedom and flexibility, maximal awareness. Trust, Privacy, maximal information and system availability. Cooperation. Openness of information, maximal information integrity	Clear overall rules and policies	Competitiveness	Competitiveness	Respect what has been entrusted to you
Trust	Competitiveness	Confidentiality	Confidentiality	

Obey rules and regulations. Check who is at my door before opening it.	Confidentiality	Consistency	Consistency
	Consistency	Control	Cooperation
	Cooperation	Cooperation	Courtesy
	Courtesy	Courtesy	Customer value
	Create value for our customers	Creativity	Creativity
	Creativity	Customer value	Excellence
	Deliver excellence	Dynamism	Respect
	Develop and sustain an ethical environment	Effectiveness	Dynamism
	Dynamism	Efficiency	Effectiveness
	Effectiveness	Empowerment	Efficiency
	Efficiency	Encouragement	Pleasure
	Emotional/ hedonistic values	Enjoyment	Empowerment
	Empowerment	Entrepreneurship	Encouragement
	Encourage and support others	Excellence	Informed consent
	Enhance integrity of business processes	Flexibility	Personnel fulfillment
	Enhance management development practices	Freedom	Enjoyment

Enhance understanding of personal financial s**ituation**	Harmony	Punish noncompliance
Enjoy the journey	Honesty	Entrepreneurship
Ensure availability of information	Human welfare	Sustainability
Ensure censure	Incent/ensure compliance	Flexibility
Ensure legal and procedural compliance	Informed consent	Freedom
Entrepreneurship	Innovation	Achievement
Environmental sustainability	Integrity	Self-actualization
Establish ownership of information	Loyalty	Harmony
Freedom from Bias	Obedience	Honesty
Goal achievement	Personnel fulfillment	Human welfare
Growth and self-actualization values	Pleasure	Obedience
Harmony of self, society, or a relationship	Pride in work	Innovation
Honesty	Privacy	Integrity
Human welfare	Production	Control
Identity	Productivity	Loyalty

Improve authority structures	Punish noncompliance	Access control
Information sharing	Respect	Pride in work
Informed consent	Safety values	Privacy
Innovativeness	Self-actualization	Production
Integrity	Social values	Productivity
Limited control	Stability	Work ethic
Loyalty	Strong governance	Safety values
Maximal awareness	Sustainability	Social values
Maximal flexibility	Team work	Stability
Maximal freedom	Trust	Team work
Maximal information integrity	Usability	Trust
Maximize access control	Work ethic	Usability
Maximize awareness	Awareness	
Maximize data integrity	Obedience	
Maximize fulfillment of personal needs	Access control	
Maximize organizational integrity	Efficiency	
Obey rules and regulations	Informed consent	

Openness of information	Incent/ensure compliance
Optimize work allocation practices	Pride in work
Ownership and Property	Privacy
Pride in work	Production
Privacy	Productivity
Production	Work ethic
Productivity	Accountability
Promote individual work ethic	Personnel fulfillment
Promote responsibility and accountability	Incent/ensure compliance
Provide adequate HR management practices	Respect
Provide open communication	Strong governance
Respect	Safety values
Rules and order	Social values
Safety	Stability
Social values	Personnel fulfillment
Stability	Team work
Stimulation and epistemic values	Respect
Team work	Trust

Traditional values	Incent/ensure compliance
Trust	Incent/ensure compliance
Understand individual characteristics	Incent/ensure compliance
Understand personal beliefs	Consistency
Understand work situation	Usability
Uniformity	Respect
Universal usability	Usability
Universal values	Respect

Appendix H: Communiqué to Solicit Manager Participants

Dear Privacy and Security Policy Makers:

I am inviting you to participate in a dissertation study I am conducting toward the completion of a doctoral degree in Information Systems/Information Security at Nova Southeastern University in Fort Lauderdale, Florida. The purpose of the study is to test a methodology called Value Sensitive Design for defining an organization's collective security values and creating an end user security policy that reflects those values.

How do I say Yes?
If you would like to participate, email me [LINK] and I will put you on the list.

Why are you asking me? Are others being asked?
You are invited to participate because you have been involved in creating and/or writing security or privacy policy or standards at XYZ Corp. I am also inviting members of the global Privacy Champions program. They will represent users and communicators of policy as you represent the creators.

What's involved?
Each Monday starting February 17th and continuing for 6-8 weeks, you will be sent a link to a brief SharePoint questionnaire that asks about security values. Each questionnaire will take about 10 minutes to complete. The questionnaire is due back no later than the immediately following Wednesday, 5 PM local time. Responses will be pooled together, analyzed, and then returned to the group for follow up the next week. After consensus is reached on what constitutes security values (two or three rounds of questionnaires) you will be asked to respond to a second set of questionnaires designed to incorporate the agreed upon values into policy statements.

You do not need to know anything about security values or writing policy to participate.

Will my responses be kept private?
Responses are anonymous – no one will know who says. However, all responses will be posted so that participants can get ideas from one another. In addition, I will keep a list of all volunteer participants so that I can send study–related notices and reminders.

For research purposes, each survey will ask your regional affiliation (International or North America) and whether or not your job includes creating security policy. This is done to ensure that all the regions participate and that volunteers include both policy makers like you and employees who do not create policy, but are involved in security policy awareness.

Are there any benefits for taking part in this research study?
There are no direct benefits for participating. However, you may find it fun to help define our corporate understanding of security values and see how they are translated into a new kind of end user policy language. Once the research is completed, you may request a study summary.

What if I do not want to participate?
Participation is strictly voluntary. If you want to volunteer, or if you have questions, please send me a note by Thursday of this week, close of business local time. I will aggregate all questions into an FAQ and send it out to all who contact me. I will need to know by Tuesday, February 11th if you plan on participating

[Signature]
[Contact information]

Appendix I: Communiqué to Solicit Employee Participants

Dear Privacy Champions:

I am writing to you to ask you to participate in a study on security values, part of the work I am doing towards a doctoral degree in information systems/information security at Nova Southeastern University in Fort Lauderdale, Florida. The purpose of the study is to test a method of writing an End User Policy that reflects security values shared by management and employees. The study involves responding to a series of short, online (SharePoint) questionnaires, designed to work toward a common set of security values, and then policy language that reflects the agreed upon values.

Each Monday, beginning February 17th and continuing for about 8 weeks, you will be sent a link to a brief questionnaire related to three specific end user security policy statements. The questionnaire will take 10-15 minutes to complete and will be due back Wednesday, close of business local time. You will be able to see the responses others post as they will be able to see yours, but all responses are anonymous. No one will know who said what.

Participation in the study is strictly voluntary. However, reliable results can only be achieved if participants complete the entire series of questionnaires.

An FAQ is attached, but please feel free to contact me directly if you have questions.

If you would like to volunteer, please send me a note by Monday, February 10th, close of business local time. Those who volunteer will get more detailed information sometime next week.

Thank you.

[Signature]
[Contact information]

Appendix J: FAQ for Employee Participants

Dear Privacy Champions:

You are invited to participate in a dissertation study I am conducting toward the completion of a doctoral degree in Information Systems/Information Security. The purpose of the study is to test a methodology called Value Sensitive Design as a means of identifying an organization's security values and creating an end user security policy that reflects those values.

If you would like to participate, email me [LINK] by Monday, Feb 10th and I will put you on the list.

Why are you asking me?
You are invited to participate because you have been involved in promoting security and privacy awareness through the XYZ Corp Privacy Champions program.

What's involved?
Each Monday starting in mid-February and continuing for 6-8 weeks, you will be sent a link to a brief SharePoint questionnaire that asks about security values. Each questionnaire will take about 10 minutes to complete and are due back no later than the immediately following Wednesday, 5 PM local time. Responses will be pooled together, analyzed, and then returned to the group for follow up the next week. After consensus is reached on what constitutes security values (two or three rounds of questionnaires) you will be asked to respond to a second set of questionnaires designed to incorporate the agreed upon values into policy statements.

You do not need to know anything about security values or writing policy to participate.

Will my responses be kept private?
Responses are anonymous – no one will know who says. However, all responses will be posted so that participants can get ideas from one another. In addition, I will keep a list of participants so that I can send study–related notices and reminders.

For research purposes, each survey will ask your regional affiliation (International or North America) and whether or not your job includes creating security policy. This is done to ensure that all the regions participate and that volunteers include employees like you who do not create policy, but are involved in security policy awareness as well as those who are responsible for creating security policy documents.

Are there any benefits for taking part in this research study?
There are no direct benefits for participating. However, you may find it fun to help define our corporate understanding of security values and see how they are translated into a new kind of end user policy language. Once the research is completed, you may request a study summary.

What if I do not want to participate?
If you do not want to participate, ignore this request. Participation is strictly voluntary. If you have any questions about the study or participating in it, please contact me [email link].

[Signature]
[Contact information]

Appendix K: Communiqué to Delphi Pre-test Group

Dear XX:

I am writing to you to ask you to help me with a study I am conducting on security values, part of the work I am doing towards a doctoral degree in information systems/information security at Nova Southeastern University in Fort Lauderdale, Florida. The purpose of the study is to test a method for creating an end user policy that reflects security values shared by both management and employees. The study involves responding to a series of short, online (SharePoint) questionnaires, designed to work toward a common set of security values, and then policy language that reflects the agreed upon values.

What I would like you to do for the first round of the study, and possibly other rounds, is preview the questions that will go to study participants. This will help ensure that the instructions and questions are clear and that the SharePoint site is working correctly.

Please do not volunteer if you are a Privacy Champion, as Privacy Champions will be asked to participate in the preview itself.

Participation in the study is strictly voluntary. If you can, please let me know by Wednesday so that I can get you the draft of Questionnaire 1.

Thank you!

[Signature]
[Contact information]

Appendix L: Access Test

Dear Privacy Champions and Security/Compliance policy makers:

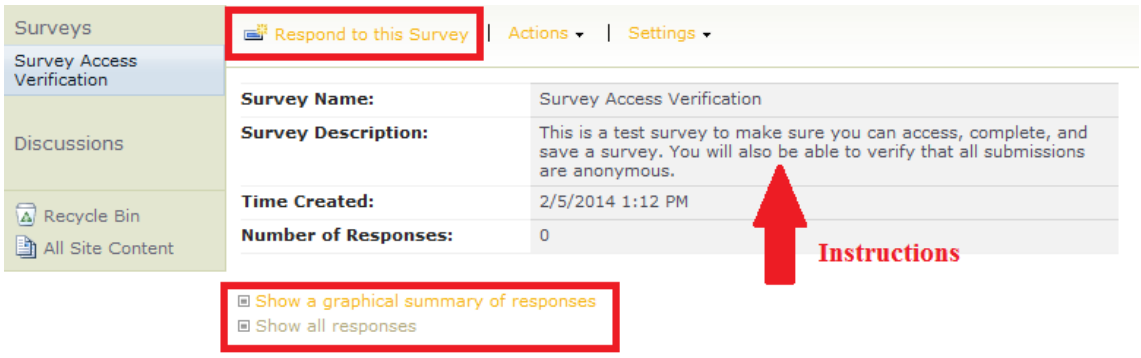
Thank you for agreeing to participate in this dissertation study. Before we officially begin next week, here is a **LINK** to test your access to the survey site. Please make sure you can open a survey, respond to it, and submit it. If you have any problems with access, please contact me.

FYI – The surveys are anonymous, but you are encouraged throughout the study to look at how others have responded. Click either of the Show… links. You may edit your entry (not someone else's) up until the cutoff date, but finding yours among a few dozen others may not be easy. One trick is note the time when you click FINISH as each entry in Show all responses is time stamped.

For those new to SharePoint surveys:

1. The study surveys are hosted on a SharePoint managed by ISCD. If you are not already logged onto the 1dc network, you will be asked to do so before getting to the survey.

2. The **LINK** you will get to SharePoint Survey site. To get started, read the instructions and then click on Respond to this Survey. When you have completed the two sample questions, click FINISH.



Again, my thanks for your participation.

[Signature]
[Contact information]

Appendix M: Empirical Investigation: Round 1 Letter

Dear Privacy Champions and security/compliance policy makers:

The method we are testing, Value Sensitive Design, is made up of three "investigations" – conceptual, empirical, and technical. You are entering the study at the empirical investigation. In the conceptual investigation completed earlier this year, a study was done to come with a starting point for your work in identifying security values. Here is the list that came from that investigation. You will see this again on the survey itself:

1. Anticipate problems and prevent them
2. Build and sustain trust
3. Create value for customers
4. Creatively address problems and opportunities
5. Do the right thing
6. Ensure information is properly accessible
7. Honor customer trust over personal convenience
8. Make work meaningful and satisfying
9. Promote personal responsibility
10. Remove obstacles and delays to necessary action
11. Respect what has been entrusted to you

The goal of the empirical investigation is for the study group to come to consensus on security values as they relate to specific policies. In this first survey you will be given three policy statements from the End User security policy. Following each statement is a scenario that illustrates conflicting values that may influence whether an employee complies with the policy. Envision yourself in the scenario, and then identify three values that you associate with upholding the policy. You can choose from the initial list, and/or create your own, up to a total of three.

After each selection of values, you will be asked to explain why you chose the values you did. The purpose of this question is to better understand how you interpret the value statements. This information will be used in preparing the next round of surveys.

IMPORTANT NOTES:

- All questions are required.
- SharePoint does not stop you from selecting more than three values. Please stick to the limit of three.
- When you have completed the survey, click FINISH.

Here is the link to the first survey: **LINK**. If you have any questions or run into difficulty, please contact me.

[Signature]
[Contact information]

Appendix N: Empirical Investigation: Round 1 Survey Instrument

Listed below are three policy statements from the XYZ Corp's End User security policy. Following each statement is a scenario that illustrates conflicting values that may influence whether the policy is followed. Envision yourself in the scenario, and identify up to three values that you associate with upholding the policy. You can choose from the initial list of 11, and/or create your own, up to a total of three.

Policy 1: XYZ business can be conducted using XYZ equipment and from non-XYZ equipment in compliance with the Remote Access Standard. The use of computer systems or email accounts not provided by XYZ is prohibited

Scenario 1: Maria is working on a report for an important customer that must be presented on Monday. It is late on Friday and she hasn't made nearly the progress she had planned. She emails sensitive account information to her home email address so that she can prepare the report at home. What Maria doesn't realize is that XYZ has contractual agreement with the customer to keep the customer's data within a secure environment – and Maria's home mail file is not secure.

What three values do you associate with upholding the above policy statement? You may choose from the list or add your own. Multiple values entered into the Specify box should be separated with a semi-colon (;)

- ☐ 1. Anticipate problems and prevent them
- ☐ 2. Build and sustain trust
- ☐ 3. Create value for customers
- ☐ 4. Creatively address problems and opportunities
- ☐ 5. Do the right thing
- ☐ 6. Ensure information is properly accessible
- ☐ 7. Honor customer trust over personal convenience
- ☐ 8. Make work meaningful and satisfying
- ☐ 9. Promote personal responsibility
- ☐ 10. Remove obstacles and delays to necessary action
- ☐ 11. Respect what has been entrusted to you
- ☐ Specify your own value _____
  _____

Value 1: Briefly explain the thinking behind your choices.

_____

_____

_____

Policy 2: Users must not leave XYZ information resources unsecured or visible and unattended outside XYZ's facilities.

Scenario 2: Tomorrow was going to be a busy day. More than 500 customers were being sent a special mailing to introduce a new service that detailed monthly account activity and suggested personalized marketing strategies. Concerned that they wouldn't finish on time for tomorrow's 3 pm mail pick up, Lee decided to get started today. He printed out all the reports and laid them out in a nearby conference room so they would be ready for stuffing and sorting in the morning.

What three values do you associate with upholding the above policy statement? You may choose from the list or add your own. Multiple values entered into the Specify box should be separated with a semi-colon (;)

- ☐ 1. Anticipate problems and prevent them
- ☐ 2. Build and sustain trust
- ☐ 3. Create value for customers
- ☐ 4. Creatively address problems and opportunities
- ☐ 5. Do the right thing
- ☐ 6. Ensure information is properly accessible
- ☐ 7. Honor customer trust over personal convenience
- ☐ 8. Make work meaningful and satisfying
- ☐ 9. Promote personal responsibility
- ☐ 10. Remove obstacles and delays to necessary action
- ☐ 11. Respect what has been entrusted to you
- ☐ Specify your own value _____
  _____

Value 2: Briefly explain the thinking behind your choices.

_____
_____
_____

Policy 3: Lending XYZ information resources, including company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited.

Scenario: All was in a panic when Petrov came last night. Both boys had papers due for school and were fighting over the use of the family computer. Luckily, Petrov brought his laptop home that night and could lend it to his older son.

Values: What three values do you associate with upholding the above policy statement? You may choose from the list or add your own. Multiple values entered into the Specify box should be separated with a semi-colon (;)

- ☐ 1. Anticipate problems and prevent them
- ☐ 2. Build and sustain trust
- ☐ 3. Create value for customers
- ☐ 4. Creatively address problems and opportunities
- ☐ 5. Do the right thing
- ☐ 6. Ensure information is properly accessible
- ☐ 7. Honor customer trust over personal convenience
- ☐ 8. Make work meaningful and satisfying
- ☐ 9. Promote personal responsibility
- ☐ 10. Remove obstacles and delays to necessary action
- ☐ 11. Respect what has been entrusted to you
- ☐ Specify your own value _____
  _____

Value 3: Briefly explain the thinking behind your choices.

_____
_____

Please identify your geographic affiliation.

- O North America
- O International

If you were recruited for the study through the Privacy Champion Program, please select 1. All others should select 2.

- O 1. I am a Privacy Champion
- O 2. I am a Security/Compliance Policy Maker

Appendix O: Empirical Investigation: Round 2 Letter

Dear Privacy Champions and security/compliance policy makers:

Kudos on your first round of responses! Your insightful comments reflected the complexity of these issues.

The goal of Round 2 is to bring us closer to consensus on security values as they relate to specific policies. In this second survey, you are given the same policy statements and scenarios as last week, along with the three Round 1 values most frequently identified and the underlying theme most often noted in your comments. Please rank the three values, so that that only one value is ranked **Most Important**, only one is **Least Important**, and only one is **In the middle**. As in the previous round, you will be asked to comment on the thinking behind your choices.

Here is the link: **LINK** If you have any questions or run into difficulty, please contact me.

IMPORTANT NOTES:

- SharePoint does not have the logic to prevent you from giving each value the same ranking. Within each scenario, please give each value a different ranking.
- You are encouraged to look at other responses and change your response based on the comments of others. Just remember to note your response number or time stamp so that you can find your original entry.
- Round 2 closes Wednesday, 6 PM US Mountain Time

[Signature]
[Contact information]

Appendix P: Empirical Investigation: Round 2 Survey Instrument

In this second survey, you are given the same policy statements and scenarios as last week, along with the three Round 1 values most frequently identified, and the underlying theme most often referenced in the comments. Please give each of the three values a unique ranking. Only one value should be Most Important, one Least Important, and one in the middle.

Policy 1: XYZ business can be conducted using XYZ equipment and from non-XYZ equipment in compliance with the Remote Access Standard. The use of computer systems or email accounts not provided by XYZ is prohibited.

Scenario 1: Maria is working on a report for an important customer that must be presented on Monday. It is late on Friday and she hasn't made nearly the progress she had planned. She emails sensitive account information to her home email address so that she can prepare the report at home. What Maria doesn't realize is that XYZ has contractual agreement with the customer to keep the customer's data within a secure environment – and Maria's home mail file is not secure.

Below are listed the most frequently selected values associated with this policy statement. The most frequently referenced underlying theme was responsibility for sustaining customer trust.

Please rank them according to your values associated with information security. Give each of the three a different ranking.

	Most Important	**In the middle**	**Least Important**
Do the right thing	O	O	O
Honor customer trust over personal convenience	O	O	O
Respect what has been entrusted to you	O	O	O

Value 1: Briefly explain the thinking behind your ranking.

_____

_____

_____

Policy 2: Users must not leave XYZ information resources unsecured or visible and unattended outside XYZ's facilities.

Scenario 2: Tomorrow was going to be a busy day. More than 500 customers were being sent a special mailing to introduce a new service that detailed monthly account activity and suggested personalized marketing strategies. Concerned that they wouldn't finish on time for tomorrow's 3 pm mail pick up, Lee decided to get started today. He printed out all the reports and laid them out in a nearby conference room so they would be ready for stuffing and sorting in the morning.

Below are listed the most frequently selected values associated with this policy statement. The most frequently referenced underlying theme was employee responsibility for maintaining information security.

Please rank them according to your values associated with information security. Give each of the three a different ranking.

	Most Important	**In the middle**	**Least Important**
Anticipate problems and prevent them	O	O	O
Honor customer trust over personal convenience	O	O	O
Respect what has been entrusted to you	O	O	O

Value 2: Briefly explain the thinking behind your ranking.

_____
_____
_____

Policy 3: Lending XYZ information resources, including company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited.

Scenario 3: All was in a panic when Petrov came last night. Both boys had papers due for school and were fighting over the use of the family computer. Luckily, Petrov brought his laptop home that night and could lend it to his older son.

Below are listed the most frequently selected values associated with this policy

statement. There was a tie for most frequently referenced underlying theme: Responsibility for following the rules and Responsibility for sustaining company trust.

Please rank them according to your values associated with information security. Give each of the three a different ranking.

	Most Important	**In the middle**	**Least Important**
Do the right thing	O	O	O
Promote personal responsibility	O	O	O
Respect what has been entrusted to you	O	O	O

Value 3: Briefly explain the thinking behind your ranking.

_____
_____
_____

Please identify your geographic affiliation.
O North America
O International

What is your role as it relates to Information Security policy? If you were recruited for the study through the Privacy Champion Program, please select 1. All others should select 2.
O 1. I am a Privacy Champion
O 2. I am a Security/Compliance Policy Maker

Appendix Q: Empirical Investigation: Round 3 Letter

Dear Privacy Champions and security/compliance policy makers:

You continue to do an amazing job on honing in on our security values and working toward consensus on the values related to specific policies.

In Round 3, for each policy your responses have been blended into a single, proposed security value statement. You are asked how satisfied you are that the proposed statement addresses the security value associated with the policy.

If you are not satisfied, you are also asked comment on what needs to change.

Here is the link: **LINK** If you have any questions or run into difficulty, please contact me.

NOTE: Round 3 closes **Wednesday, 6 PM US Mountain Time.**

[Signature]
[Contact information]

Appendix R: Empirical Investigation: Round 3 Survey Instrument

For the past two weeks, we have been working toward consensus on the security values related to specific policies. Your responses have been blended into a single, proposed security value statement for each policy. In Round 3, you are asked how satisfied are you that the proposed statement addresses the security value associated with the policy. If you are not satisfied, please comment on what has to change is needed.

Policy 1: XYZ business can be conducted using XYZ equipment and from non-XYZ equipment in compliance with the Remote Access Standard. The use of computer systems or email accounts not provided by XYZ is prohibited.

Proposed security value: We are honor bound to follow XYZ's security policies as they are designed to safeguard the sensitive data customers have entrusted to us.

How satisfied are you that the statement addresses the security value associate with the policy?

O Very satisfied
O Satisfied
O Dissatisfied
O Very dissatisfied

If you were not satisfied with the value statement for Policy 1, what needs to change?

_____
_____
_____

Policy 2: Users must not leave XYZ information resources unsecured or visible and unattended outside XYZ's facilities.

Proposed security value: We respect the responsibility entrusted to us by XYZ and by customers by anticipating security problems and looking for ways to avoid them.

How satisfied are you that the statement addresses the security value associate with the policy?

O Very satisfied
O Satisfied
O Dissatisfied
O Very dissatisfied

If you were not satisfied with the value statement for Policy 2, what needs to change?

_____
_____
_____

Policy 3: Lending XYZ information resources, including company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited.

Proposed security value: As employees we have a personal responsibility to do what is right for our customers, promoting their security interests and respecting their trust over personal convenience.

How satisfied are you that the statement addresses the security value associate with the policy?

O Very satisfied
O Satisfied
O Dissatisfied
O Very dissatisfied

If you were not satisfied with the value statement for Policy 3, what needs to change?

_____
_____
_____

Please identify your geographic affiliation.
O North America
O International

What is your role as it relates to Information Security policy? If you were recruited for the study through the Privacy Champion Program, please select 1. All others should select 2.
O 1. I am a Privacy Champion
O 2. I am a Security/Compliance Policy Maker

Appendix S: Technical Investigation: Round 4 Letter

Dear Privacy Champions and security/compliance policy makers:

You have reached the turning point of the study. The empirical investigation (where security values are fleshed out) has ended. The technical investigation (where the values are blended into a new kind of policy statement) begins. Now you know why you – policy makers and policy communicators – were specifically selected for this study. You know how to write security policy and you know how to communicate it in ways users can understand.

Your goal this week is to rewrite the three XYZ policies, changing them from traditional policy statements –"Users must.. " or "It is prohibited to…" to value sensitive policies.

When you open the survey you will see the XYZ security policy followed by the security value you have collectively defined. Blend the two together, creating a new, value sensitive security policy.

> Example: If the traditional policy states: **Employees must wear red on rainy days** and the value states: **As employees we have a responsibility to look cheerful** your value sensitive policy statement will incorporate both the action that the employees must take (wear red on Mondays) AND the value (to look cheerful).

When you have written the policy, briefly describe your thinking.

Here is the **LINK.** If you have any questions or run into difficulty, please contact me.

IMPORTANT NOTE: Round 4 closes Wednesday, 6 PM US Mountain Time

[Signature]
[Contact information]

Appendix T: Technical Investigation: Round 4 Survey Instrument

When you open the survey you will see both the XYZ policy and the agreed upon security value associated with it. Please draft a value sensitive policy statement that incorporates the value statement into the text of the policy. Then, briefly explain your thinking.

Policy 1: XYZ business can be conducted using XYZ equipment and from non-XYZ equipment in compliance with the Remote Access Standard. The use of computer systems or email accounts not provided by XYZ is prohibited.

Security value: We must honor our commitment to our customers to follow XYZ's security policies as they are designed to safeguard the sensitive data customers have entrusted to us.

Please draft a value sensitive policy statement that incorporates the security value into the text of the policy.

_____
_____
_____

Value sensitive policy 1: Briefly explain your thinking.

_____
_____
_____

Policy 2: Users must not leave XYZ information resources unsecured or visible and unattended outside XYZ's facilities.

Security value: We respect the responsibility entrusted to us by XYZ and our customers by anticipating security problems and proactively looking for ways to avoid them.

Please draft a value sensitive policy statement that incorporates the security value into the text of the policy.

_____
_____
_____

Value sensitive policy 2: Briefly explain your thinking.

_____
_____
_____

Policy 3: Lending XYZ information resources, including company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited.

Proposed security value: As employees we have a personal responsibility to do what is right for XYZ and our customers, respecting their trust over personal convenience and promoting customer security interests.

Please draft a value sensitive policy statement that incorporates the security value into the text of the policy.

_____
_____
_____

Value sensitive policy 3: Briefly explain your thinking.

_____
_____
_____

Please identify your geographic affiliation.
O North America
O International

What is your role as it relates to Information Security policy? If you were recruited for the study through the Privacy Champion Program, please select 1. All others should select 2.
O 1. I am a Privacy Champion
O 2. I am a Security/Compliance Policy Maker

Appendix U: Technical Investigation: Round 5 Letter

Dear Privacy Champions and security/compliance policy makers:

Round 5 brings us close to accomplishing the task of creating value sensitive security policy statements. In this survey you will be given the same three policies and associated value statements, along with the five Round 4 value sensitive policy statements that best met the criteria below:

- A strong, logical connection between the value and the policy
- Easily understood
- Clear direction to employees

For each policy/value pair, you will be asked to select the statement that best connects the value to the policy while also providing clear direction to employees. If you think the best is not good enough, space is provided to explain the improvement you think is needed.

Here is the link: **LINK.** If you have any questions or run into difficulty, please contact me.

IMPORTANT NOTE: Round 3 closes Wednesday, 6 PM US Mountain Time

[Signature]
[Contact information]

Appendix V: Technical Investigation: Round 5 Survey Instrument

When you open the survey you will see both the XYZ policy and the agreed upon security value associated with it. For each policy/value pair, select the statement that best connects the value to the policy while also providing clear direction to employees. If you think the best is not good enough, briefly explain the improvement you think is needed.

Policy 1: XYZ business can be conducted using XYZ equipment and from non-XYZ equipment in compliance with the Remote Access Standard. The use of computer systems or email accounts not provided by XYZ is prohibited.

Security value: We must honor our commitment to our customers to follow XYZ's security policies as they are designed to safeguard the sensitive data customers have entrusted to us.

Select the statement that best connects the value to the policy while also providing clear direction to employees:

1. To honor our commitment to safeguard sensitive data, XYZ business can be conducted using XYZ equipment or non-XYZ equipment that is in compliance with the Remote Access Standard. The use of computer systems or email accounts not provided by XYZ is not allowed.

2. XYZ employees can conduct business for our customers using XYZ equipment and non-XYZ equipment that is in compliance with the Remote Access Standard. This policy allows us to honor our commitment to our customers as it helps ensure their information is safe.

3. In order to honor our commitment to clients to protect client and cardholder data, XYZ business can only be conducted using XYZ equipment or non-XYZ equipment that meets all remote access standards.

4. XYZ provides employees with secure computer systems and email accounts that safeguards sensitive data entrusted to us. The use of computer systems or email accounts not provided by XYZ is prohibited. If one must use a non-XYZ system to conduct XYZ business, it must be done in compliance with the Remote Access Standard. Complying with this policy, honors our commitment to our customers.

5. To honor our commitment to customers, XYZ business can be conducted using XYZ equipment or non-XYZ equipment in compliance with the Remote Access Standard. Using computer systems or email accounts not provided by XYZ is prohibited. This helps keep sensitive data entrusted to us safe and secure.

O Statement 1
O Statement 2
O Statement 3
O Statement 4
O Statement 5

Value sensitive policy 1: If the best is not good enough what needs to be improved?

_____
_____
_____

Policy 2: Users must not leave XYZ information resources unsecured or visible and unattended outside XYZ's facilities.

Security value: We respect the responsibility entrusted to us by XYZ and our customers by anticipating security problems and proactively looking for ways to avoid them.

Select the statement that best connects the value to the policy while also providing clear direction to employees:

1. By not leaving XYZ information resources unsecured or visible and unattended outside XYZ's facilities, we respect the responsibility XYZ entrusts to us.

2. We respect the responsibility entrusted to us by XYZ and our customers. Therefore we should anticipate security problems and proactively avoid them. As it relates to XYZ information resources, we must make all efforts to prevent theft or unauthorized access. Users must not leave XYZ information resources unsecured, visible, or unattended outside XYZ's facilities.

3. To honor our responsibility to protect the data entrusted to us by XYZ and our customers, we must anticipate security problems and proactively look for ways to avoid them. Specifically, we must never leave these information resources unsecured, visible and/or unattended outside XYZ's facilities.

4. We here at XYZ respect the documents and sensitive information we have been trusted with. We do not leave papers, passwords or documents where they can be found or exploited.

5. We are responsible for anticipating security problems and proactively looking for ways to avoid them. Therefore, users must not leave XYZ information resources unsecured or visible and unattended outside of XYZ's facilities.
O Statement 1
O Statement 2
O Statement 3
O Statement 4
O Statement 5

Value sensitive policy 2: If the best is not good enough what needs to be improved?
_____
_____
_____

Policy 3: Lending XYZ information resources, including company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited.

Proposed security value: As employees we have a personal responsibility to do what is right for XYZ and our customers, respecting their trust over personal convenience and promoting customer security interests.

Select the statement that best connects the value to the policy while also providing clear direction to employees:

1. Respecting trust over personal convenience and promoting customer security interests, we should not lend XYZ information resources, including company issued laptops and desktop computers, to family members, friends, or non-XYZ employees.

2. As XYZ employees, we have a personal responsibility to protect XYZ and customer security interests over personal convenience. As such, we do not permit the use of XYZ information resources, including company issued laptops and desktop computers, to family members, friends, or non-XYZ employees.

3. As employees we have a personal responsibility to do what is right for XYZ and our customers. Lending XYZ information resources, including company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited. This ensures that we respect customer trust over personal convenience and promote customer security interests.

4. As employees we have a personal responsibility to do what is right for XYZ and our customers, respecting their trust over personal convenience and promoting customer security interests. Be sure not to lend XYZ information resources, including company issued laptops and desktop computers to family members, friends, or non-XYZ employees.

5. Lending XYZ information resources, including company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited. As employees we have a personal responsibility to do what is right for XYZ and our customers, respecting their trust over personal convenience and promoting customer security interests.

- O Statement 1
- O Statement 2
- O Statement 3
- O Statement 4
- O Statement 5

Value sensitive policy 3: If the best is not good enough what needs to be improved?

_____
_____
_____

Please identify your geographic affiliation.
O North America
O International

What is your role as it relates to Information Security policy? If you were recruited for the study through the Privacy Champion Program, please select 1. All others should select 2.
O 1. I am a Privacy Champion
O 2. I am a Security/Compliance Policy Maker

Appendix W: Technical Investigation: Round 6 Letter

Dear Privacy Champions and security/compliance policy makers:

For the past two weeks, we have been working to integrate the previously agreed upon security values into the three XYZ End User Policy statements. In this survey, responses from prior rounds have been blended into a single, value sensitive policy (VSP) statement for each of the original policies. You are asked how satisfied you are with the final language.

- Is there a strong, logical connection between the agreed upon security value and the XYZ policy?
- Is it easily understood?
- Does it provide a clear direction to employees?

If you are not satisfied, you are also asked comment on what needs to change.

IMPORTANT NOTES:

1. Everyone on this distribution is encouraged to weigh in on the VSPs – even if you missed earlier rounds.
2. The study is testing the method we followed to create a VSP. You may disagree with the original XYZ policy statement and still be satisfied with the proposed VSP.

Here is the link: **LINK.** If you have any questions or run into difficulty, please contact me.

NOTE: Round 3 closes **Wednesday, 6 PM US Mountain Time**

[Signature]
[Contact information]

Appendix X: Technical Investigation: Round 6 Survey Instrument

For the past two weeks, we have been working to integrate the previously agreed upon security values into the three XYZ End User Policy statements. In this survey, responses from prior rounds have been blended into a single, value sensitive policy (VSP) statement for each of the original policies. You are asked how satisfied you are with the final language.

- Is there a strong, logical connection between the agreed upon security value and the XYZ policy?
- Is it easily understood?
- Does it provide a clear direction to employees?

Policy 1: XYZ business can be conducted using XYZ equipment and from non-XYZ equipment in compliance with the Remote Access Standard. The use of computer systems or email accounts not provided by XYZ is prohibited. Security value: We must honor our commitment to our customers to follow XYZ's security policies as they are designed to safeguard the sensitive data customers have entrusted to us.

How satisfied are you that the proposed VSP, below:

- Makes a strong, logical connection between the value and the policy
- Is easily understood
- Provides a clear direction to employees

PROPOSED VSP: To safeguard sensitive data, only email accounts provided by XYZ may be used to conduct XYZ business. Furthermore, XYZ business must be conducted using XYZ equipment or using non-XYZ equipment that is in compliance with the Remote Access Standard. Complying with this policy honors our commitment to customers to keep their data secure.

O Very satisfied
O Satisfied
O Dissatisfied
O Very dissatisfied

VSP 1: If you are not satisfied with the value sensitive policy, what needs to change?

_____
_____
_____

Policy 2: Users must not leave XYZ information resources unsecured or visible and unattended outside XYZ's facilities.

Security value: We respect the responsibility entrusted to us by XYZ and our customers by anticipating security problems and proactively looking for ways to avoid them.

How satisfied are you that the proposed VSP, below:

- Makes a strong, logical connection between the value and the policy
- Is easily understood
- Provides a clear direction to employees

PROPOSED VSP: To protect the data entrusted to us, it must not be left visible or unattended outside XYZ's facilities or unsecured and unattended within XYZ's facilities. When working with client data, we must anticipate problems related to keeping data secure when we are not present, and proactively looking for ways to avoid them.

O Very satisfied
O Satisfied
O Dissatisfied
O Very dissatisfied

VSP 2: If you are not satisfied with the value sensitive policy, what needs to change?

_____
_____
_____

Policy 3: Lending XYZ information resources, including company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited.

Proposed security value: As employees we have a personal responsibility to do what is right for XYZ and our customers, respecting their trust over personal convenience and promoting customer security interests.

How satisfied are you that the proposed VSP, below:

- Makes a strong, logical connection between the value and the policy
- Is easily understood
- Provides a clear direction to employees

PROPOSED VSP: As XYZ employees, we have a personal responsibility to protect XYZ and customer security interests over personal convenience. For that reason, lending XYZ information resources such as company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited.

O Very satisfied
O Satisfied
O Dissatisfied
O Very dissatisfied

VSP 3: If you are not satisfied with the value sensitive policy, what needs to change?

_____
_____
_____

Please identify your geographic affiliation.
O North America
O International

What is your role as it relates to Information Security policy? If you were recruited for the study through the Privacy Champion Program, please select 1. All others should select 2.
O 1. I am a Privacy Champion
O 2. I am a Security/Compliance Policy Maker

Appendix Y: Security Values Study Follow Up Letter

Privacy Champions and security/compliance policy makers:

I'd like to share with you the results of your work and some thoughts about the process, and in return ask for your thoughts as well. If you remember, the initial study recruitment letter described the study as a test of Value Sensitive Design, a process for defining an organization's collective security values and creating an end user security policy that reflects those values. Over the past six weeks, you explored the security values associated with three XYZ end user policies, and then worked to integrate the values into the policy. Aside from some of you who wanted to change the policy (outside the scope of the study), you reached strong consensus on both the values (Rounds 1-3) and the value sensitive policy statements (Rounds 4-6). Here are the three final statements:

VSP 1: To safeguard sensitive data, only email accounts provided by XYZ or other approved methods for data sharing may be used to conduct XYZ business. Furthermore, XYZ business must be conducted using XYZ equipment or using non-XYZ equipment that is in compliance with the Remote Access Standard. Complying with this policy honors our commitment to customers to keep their data secure.

VSP 2: To protect the data entrusted to us, client data and other sensitive information must not be left visible or unattended outside XYZ's facilities or unsecured and unattended within XYZ's facilities. When working with client data, we must anticipate problems related to keeping data secure when we are not present, and proactively looking for ways to avoid them.

VSP 3: As XYZ employees, we have a personal responsibility to protect XYZ and customer security interests over personal convenience. For that reason, lending XYZ information resources such as company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited.

The study had two research questions.
RQ 1: What values do employees and organizations associate with security behavior?
RQ 2: Can VSD be used to create a security policy that reflects both organization and employee values?

This last survey asks your thoughts about the VSD process: How successful was the process for identifying the values you associate with security and how successful was it for integrating security values into security policy. Other comments are also welcome.

Here is the link: **LINK** If you have any questions or run into difficulty, please contact me.

NOTE: This follow up survey closes Wednesday, 6 PM US Mountain Time.

[Signature]
[Contact information]

Appendix Z: Security Values Study Follow Up Survey

The initial study recruitment letter described the purpose of the study as a test of Value Sensitive Design as a process for defining an organization's collective security values and creating an end user security policy that reflects those values. Over the past six weeks, you explored the security values associated with three XYZ end user policies, and then worked to integrate the values into the policy. Here are the three final statements:

VSP 1: To safeguard sensitive data, only email accounts provided by XYZ or other approved methods for data sharing may be used to conduct XYZ business. Furthermore, XYZ business must be conducted using XYZ equipment or using non-XYZ equipment that is in compliance with the Remote Access Standard. Complying with this policy honors our commitment to customers to keep their data secure.

VSP 2: To protect the data entrusted to us, client data and other sensitive information must not be left visible or unattended outside XYZ's facilities or unsecured and unattended within XYZ's facilities. When working with client data, we must anticipate problems related to keeping data secure when we are not present, and proactively looking for ways to avoid them.

VSP 3: As XYZ employees, we have a personal responsibility to protect XYZ and customer security interests over personal convenience. For that reason, lending XYZ information resources such as company issued laptops and desktop computers to family members, friends, or non-XYZ employees is prohibited.

The study had two research questions.
RQ 1: What values do employees and organizations associate with security behavior?
RQ 2: Can VSD be used to create a security policy that reflects both organization and employee values?

This last survey asks your thoughts about the VSD process: How successful was the process for identifying the values you associate with security and how successful was it for integrating security values into security policy. Other comments are also welcome.

1a. How successful was the process for identifying values associated with security?
O Successful
O Somewhat successful
O Somewhat not successful
O Not successful

1b. Comments?
_____
_____
_____

2a. How successful was the process for integrating those values into security policy?
O Successful
O Somewhat successful
O Somewhat not successful
O Not successful

2b. Comments?
_____
_____
_____

3. Anything else you would like to add?
_____
_____
_____

Please identify your geographic affiliation.
O North America
O International

What is your role as it relates to Information Security policy? If you were recruited for the study through the Privacy Champion Program, please select 1. All others should select 2.
O 1. I am a Privacy Champion
O 2. I am a Security/Compliance Policy Maker

Appendix AA: Institutional Review Board Approval

NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board

MEMORANDUM

To: Dianne Solomon

From: Ling Wang, Ph.D
Institutional Review Board

Date: Jan. 27, 2014

Re: *Employee and Organization Security Value Alignment through Value Sensitive Security Policy Design*

IRB Approval Number: wang01151401

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms these must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
2) ADVERSE REACTIONS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2020 respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Protocol File

Appendix BB: Permission to Use Corporate End User Policy

From: [redacted]
Sent: Sunday, May 05, 2013 1:31 PM
To: Solomon, Dianne B
Subject: RE: Sanitized EUP

Hi Dianne – Please use this email as my approval for your use of the sanitized version of that you provided to me on May 3, 2013.
Thanks -

[redacted]
Vice President Enterprise Security Risk and Compliance
O [redacted] F [redacted] M [redacted]
[redacted].com

From: Solomon, Dianne B
Sent: Friday, May 03, 2013 2:35 PM
To: [redacted]
Subject: Sanitized EUP

Hi [redacted]. This is the sanitized version of the EUP that my advisor said should be published as an appendix to the dissertation.

Please keep in mind that there is a page within the final where the student thanks those who have contributed to the reaching the milestone. I would want to thank [redacted] in that section. It is possible that someone could assume the policy is [redacted]. On the other hand, that is likely to be late 2014 or early 2015 so it would not be the current EUP.
That said, I would only agree to its publication with your approval. Thanks.

Dianne Blitstein Solomon, CIPP, CIPP/IT | Director, [redacted]
(O) [redacted] | (M) [redacted] | (Int'l) +1. [redacted] | GMT -5
Suspect an information security incident? Please call [redacted]

Appendix CC: Permission to Conduct Dissertation Study at XYZ Corp

Solomon, Dianne B

From: [redacted]
Sent: Monday, December 02, 2013 11:36 PM
To: Solomon, Dianne B
Subject: RE: Dissertation Research Approval Requested

I approve.

Thank you,
[redacted]

[redacted]
Chief Information Security Officer
CISSP, CRISC, CEH

[redacted]
Information Security & Cyber Defense
[redacted]

O (303) [redacted]
M (303) [redacted]

From: Solomon, Dianne B
Sent: Monday, December 02, 2013 2:58 PM
To: [redacted]
Subject: Dissertation Research Approval Requested

Hi [redacted]. As you probably know, I've been working on a doctorate in Information Security. [redacted] and [redacted] have been tremendously supportive, including their permission to solicit volunteers for the study from within the former ESRC and the Privacy Champions program. If all goes well, the study will start in 1Q2014.

[redacted] gave her approval contingent [redacted] Just to keep all the ends neatly tied, I'd like to have your authorization as well.

If you are Ok with the plan, all I need is a reply with "Approved". If you have concerns, we can hash them out.

Thank you all for your continuing support of this effort.

- Dianne

References

Adams, B. D., Thomson, M. H., Brown, A., Sartori, J. A., Taylor, T., & Waldherr, S. (2008). *Organizational trust in the Canadian forces* (DRDC Toronto No. CR-2008-038). Toronto, Ontario: Retrieved December 23, 2013 from http://cradpdf.drdc-rddc.gc.ca/PDFS/unc94/p529834_a1b.pdf

Ågerfalk, P. J., Karlsson, F., & Hjalmarsson, A. (2002). Exploring the explanatory power of actability: The case of internet-based software artefacts. *Working Conference Organizational Semiotics: Evolving a Science of Information Systems, Montreal, Canada, 94*, 1-20. doi: 10.1007/978-0-387-35611-2_1

Agle, B. R., & Caldwell, C. B. (1999). Understanding research on business values. *Business & Society, 38*(3), 326-387. doi: 10.1177/000765039903800305

Ahern, K. J. (1999). Ten tips for reflexive bracketing. *Qualitative Health Research. 9*(3), 407-411. doi: 10.1177/104973239900900309

Alavi, R., Islam, S., Jahankhani, H., & Al-Nemrat, A. (2013). Analyzing human factors for an effective information security management system. *International Journal of Secure Software Engineering (IJSSE), 4*(1), 50-74. doi: 10.4018/jsse.2013010104

Albrechtslund, A. (2007). Ethics and technology design. *Ethics and Information Technology, 9*(1), 63-72. doi: 10.1007/s10676-006-9129-8

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture: A behaviour compliance conceptual framework. *Proceedings of the 8th Australasian Information Security Conference (AISC 2010), Brisbane, Australia, 105*, 47-55.

Alsheikh, T., Rode, J. A., & Lindley, S. E. (2011). (Whose) value-sensitive design: A study of long-distance relationships in an Arabic cultural context. *Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work*, 75-84. doi: 10.1145/1958824.1958836

Amos, E. A. & Weathington, B. L. (2008). An analysis of the relation between employee-organization value congruence and employee attitudes. *The Journal of Psychology, 142*(6), 615-631. doi: 10.3200/JRLP.142.6.615-632

Ashenden, D. & Lawrence, D. (2013). Can we sell security like soap?: A new approach to behaviour change. *2013 Workshop on New Security Paradigms, Banff, Alberta, Canada*, 87-94. doi: 10.1145/2535813.2535823

Baggett, W. O. (2003). Creating a culture of security. *The Internal Auditor, 60*(3), 37-41.

Batteau, A. W. (2011). Creating a culture of enterprise cybersecurity. *International Journal of Business Anthropology, 2*(2), 36-47.

Borning, A., Friedman, B., Davis, J., & Lin, P. (2005). Informing public deliberation: Value sensitive design of indicators for a large-scale urban simulation. *ECSCW 2005: Proceedings of the Ninth European Conference on Computer-Supported Cooperative Work, Paris, France,* 449-468. doi: 10.1007/1-4020-4023-7

Borning, A. & Muller, M. (2012). Next steps for value sensitive design. *CHI 2012: ACM Annual Conference on Human Factors in Computing Systems, Austin, Texas, USA*, 1125-1134. doi: 10.1145/2207676.2208560

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164. doi: 10.1057/ejis.2009.8

Brady, J. W. (2011). Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers. *2011 44th Hawaii International Conference on System Sciences, Kauai, Hawaii USA*, 1-10. doi: 10.1109/HICSS.2011.368

Brey, P. A. E. (2012). Anticipatory technology ethics for emerging IT. *NanoEthics, 6*(1), 1-13. doi: 10.1007/s11569-012-0141-7

Brockhoff, K. (2002). The performance of forecasting groups in computer dialogue and face-to-face discussion. In H.A. Linstone & M.E. Turoff (Eds.), *The Delphi method: Techniques and applications* (pp. 285-311). Retrieved April 20, 2014 from http://is.njit.edu/pubs/delphibook/

Buck, A. J., Gross, M., Hakim, S., & Weinblatt, J. (1993). Using the Delphi process to analyse social policy implementation: A post hoc case from vocational rehabilitation. *Policy Sciences, 26*(4), 271-288. doi: 10.1007/BF00999473

Buffett, W. (2010, July 26). Memo to Berkshire Hathaway Managers. [Shareholder Letters]. Retrieved August 5, 2014 from www.berkshirehathaway.com/letters/2010ltr.pdf

Burgemeestre, B., Hulstijn, J., & Tan, Y. (2013). Value-based argumentation for designing and auditing security measures. *Ethics and Information Technology, 15*(3), 153-171. doi: 10.1007/s10676-013-9325-2

Burmeister, O. K. (2012). What seniors value about online community. *The Journal of Community Informatics, 8*(1), 1-15. Retrieved October 18, 2013 from http://ci-journal.net/index.php/ciej/article/view/545

Burmeister, O. K. (2013). Achieving the goal of a global computing code of ethics through an international-localisation hybrid. *Ethical Space: The International Journal of Communication Ethics, 10*(4), 25-37.

Cazier, J. A., Shao, B., & St Louis, R. D. (2006). E-business differentiation through value-based trust. *Information & Management, 43*(6), 718-727. doi: 10.1016/j.im.2006.03.006

Cazier, J. A., Shao, B. B. M., & St. Louis, R. D. (2007). Sharing information and building trust through value congruence *Information Systems Frontiers, 9*(5), 515–529. doi: 10.1007/s10796-007-9051-6

Chang, S. E. & Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438-458. doi: 10.1108/02635570710734316

Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). Knowing is doing. *Information Management & Computer Security, 16*(5), 484-501. doi:10.1108/09685220810920558

Cline, M. & Jensen, B. K. (2004). Information security: An organizational change perspective. *Proceedings of the Tenth Americas Conference on Information Systems, New York, New York,* 4514-4520.

Corriss, L. (2010). Information security governance: Integrating security into the organizational culture. *2010 Workshop on Governance of Technology, Information and Policies, Austin, Texas, USA.*, 35-41. doi: 10.1145/1920320.1920326

Cummings, M. L. (2006). Integrating ethics in design through the value-sensitive design approach. *Science and Engineering Ethics, 12*(4), 701-715. doi: 10.1007/s11948-006-0065-0

Da Veiga, A. & Eloff, J. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361. doi: 10.1080/10580530701586136

Da Veiga, A. & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207. doi: 10.1016/j.cose.2009.09.002

Davis, J.L.N. (2006). *Value sensitive design of interactions with UrbanSim indicators (Doctoral dissertation)*. Available from ProQuest Dissertations & Theses. (Accession No. 0809542)

Delbecq, A. L., Van de Ven, A. H., & Gustafson, D. H. (1975). *Group techniques for program planning: A guide to nominal group and Delphi processes*. Glenville, IL: Scott, Foresman and Company.

Denning, T., Borning, A., Friedman, B., Gill, B. T., Kohno, T., & Maisel, W. H. (2010). Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. *Proceedings of the 28th International Conference on Human Factors in Computing Systems, Atlanta, Georgia, USA, 917-926*. doi: 10.1145/1753326.1753462

Dhillon, G. & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*(3), 293–314. doi:10.1111/j.1365-2575.2006.00219.x

Doherty, N. F., Anastasakis, L., & Fulford, H. (2011). Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. *International Journal of Information Management, 31*(3), 201-209. doi: 10.1016/j.ijinfomgt.2010.06.001

Edwards, W. K., Poole, E. S., & Stoll, J. (2008). Security automation considered harmful? *2007 Workshop on New Security Paradigms, North Conway, New Hampshire, USA*, 33-42. doi: 10.1145/1600176.1600182

Employee. (2011). In *American Heritage Dictionary of the English Language* (on line edition). Retrieved March 27, 2013 from http://ahdictionary.com

Enz, C. A. (1986). *Power and shared values in the corporate culture*. Ann Arbor, MI: UMI Research Press.

Epstein, D. A., Borning, A., & Fogarty, J. (2013). Fine-grained sharing of sensed physical activity: A value sensitive approach. *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Zurich, Switzerland*, 489-498. doi: 10.1145/2493432.2493433

Faily, S. & Fléchais, I. (2010). Designing and aligning e-Science security culture with design. *Information Management & Computer Security, 18*(5), 339-349. doi: 10.1108/09685221011095254

Ferris, B., Watkins, K., & Borning, A. (2009). OneBusAway: A transit traveller information system. *International ICST Conference on Mobile Computing, Applications, and Services (MobiCASE 2009)*, *San Diego, California, USA*, 92-106. doi:10.1007/978-3-642-12607-9_7

Filho, E. L., Hashimoto, G. T., Rosa, P. F., de Souza, J. H. P., & Chaves, A. T. (2011). The impact of corporate culture in security policies – A methodology. *ICNS 2011, The Seventh International Conference on Networking and Services, Venice/Mestre, Italy*, 98-103.

Flanagan, M., Howe, D. C., & Nissenbaum, H. (2005). Values at play: Design tradeoffs in socially oriented game design. *Conference on Human Factors in Computing Systems, Portland, Oregon, USA*, 751-760. doi: 10.1145/1054972.1055076

Flanagan, M., Nissenbaum, H., Belman, J., & Diamond, J. (2007). A method for discovering values in digital games. *Proceedings of Digital Games Research Association (DiGRA) Conference, Tokyo, Japan*, 752-760.

Friedman, B. (1996). Value-sensitive design. *Interactions, 3*(6), 16-23.

Friedman, B., Freier, N. G., Kahn Jr., P. H., Lin, P., & Sodeman, R. (2008). Office window of the future? Field-based analyses of a new use of a large display. *International Journal of Human-Computer Studies, 66*(6), 452-465. doi: 10.1016/j.ijhcs.2007.12.005

Friedman, B., Howe, D. C., & Felten, E. (2002). Informed consent in the Mozilla browser: Implementing value-sensitive design. *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on System Sciences, Big Island, Hawaii, USA*, 1-10. doi: 10.1109/HICSS.2002.994366

Friedman, B. & Kahn, P. H. (2003). Human values, ethics, and design. In J. A. Jacko & A. Sears (Eds.), *Human-Computer Interaction Handbook* (pp. 1177–1201). Hillsdale, New Jersey: Lawrence Erlbaum Associates.

Friedman, B., Kahn, P. H., & Borning, A. (2001). *Value sensitive design: Theory and methods* (UW CSE Technical Report 02-12-01). Retrieved January 19. 2013 from University of Washington: http://www.urbansim.org/pub/Research/ResearchPapers/vsd-theory-methods-tr.pdf

Friedman, B., Kahn, P. H., & Borning, A. (2006). Value sensitive design and information systems In P. Zhang & D. Galletta (Eds.), *Human-Computer Interaction and Management Information Systems: Foundations* (pp. 348-372). Armonk, NY: ME Sharpe. doi: 10.1002/9780470281819

Friedman, B., Kahn Jr, P. H., Hagman, J., Severson, R. L., & Gill, B. (2006). The watcher and the watched: Social judgments about privacy in a public place. *Human-Computer Interaction, 21*(2), 235-272.

Friedman, B., Smith, I., Kahn, P. H., Consolvo, S., & Selawski, J. (2006). Development of a privacy addendum for open source licenses: Value sensitive design in industry. *UbiComp 2006: Ubiquitous Computing, Orange County, CA, USA,* 194-211. doi: 10.1007/11853565_12

Furnell, S. & Thomson, K. L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security, 2009*(2), 5-10. doi: 10.1016/S1361-3723(09)70019-3

Ghernouti-Helie, S., Tashi, I., & Simms, D. (2010). A multi-stage methodology for ensuring appropriate security culture and governance. *2010 International Conference on Availability, Reliability and Security, Krakow, Poland*, 353-360. doi: 10.1109/ARES.2010.118

Goldman, K., Gross, P., Heeren, C., Herman, G., Kaczmarczyk, L., Loui, M. C., & Zilles, C. (2008). Identifying important and difficult concepts in introductory computing courses using a Delphi process. *ACM SIGCSE Bulletin, 40*(1), 256-260.

Gundu, T. & Flowerday, S. V. (2013). Ignorance to awareness: Towards an information security awareness process. *South African Institute of Electrical Engineers: Africa Research Journal, 104*(2), 33-43.

Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing, 32*(4), 1008-1015. doi: 10.1046/j.1365-2648.2000.t01-1-01567.x

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems, 20*(4), 373–384. doi: 10.1016/j.jsis.2011.06.001

Helokunnas, T. & Kuusisto, R. (2003). Information security culture in a value net. *IEMC'03 Proceedings: Managing Technologically Driven Organizations: The Human Side of Innovation and Change, Albany, NY, USA*, 190-194. doi: 10.1109/IEMC.2003.1252258

Kalliath, T. J., Bluedorn, A. C., & Strube, M. J. (1999). A test of value congruence effects. *Journal of Organizational Behavior, 20*(7), 1175-1198. doi: 10.1002/(SICI)1099-1379(199912)20:7<1175::AID-JOB960>3.0.CO;2-5

Killingsworth, S. (2012). Modeling the message: Communicating compliance through organizational values and culture. *Georgetown Journal of Legal Ethics, 25*(4), 961-987.

Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. *The Scientific World Journal* [On line edition], 1-12. Retrieved June 12, 2014 from http://downloads.hindawi.com/journals/tswj/aip/463870.pdf doi: 10.1155/2014/463870

Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from "Shadow Security": Why understanding non-compliant behaviors provides the basis for effective security. *USEC '14 Workshop on Usable Security, San Diego, CA, USA*, 1-10. doi: 10.14722/usec.2014.23<007>

Kissel, R. (Ed.). (2013). *Glossary of key information security terms* (NISTIR 7298, Revision 2). U.S. Department of Commerce, National Institute of Standards and Technology. Retrieved November 2, 2013 from http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: Management's effect on culture and policy. *Information Management & Computer Security, 14*(1), 24–36 doi: 10.1108/09685220610648355

Koch, S. H., Proynova, R., Paech, B., & Wetter, T. (2013). How to approximate users' values while preserving privacy: Experiences with using attitudes towards work tasks as proxies for personal value elicitation. *Ethics and Information Technology, 15*(1), 45-61. doi: 10.1007/s10676-012-9309-7

Koepfler, J. A., Shilton, K., & Fleischmann, K. R. (2013). A stake in the issue of homelessness: Identifying values of interest for design in online communities. *6th International Conference on Communities and Technologies, Munich, Germany*, 36-45. doi: 10.1145/2482991.2482994

Kolkowska, E. (2006). Values for information system security in an academic environment: A pilot study. *12th Americas Conference on Information Systems (AMCIS), Acapulco, México. Paper 411*, 3411-3418. Retrieved December 23, 2013 from http://aisel.aisnet.org/amcis2006/411

Kolkowska, E. (2011). Security subculture in an organization – Exploring value conflicts. *Proceedings of the 19th European Conference on Information Systems – ICT and Sustainable Service Development, Helsinki, Finland.* Paper 237. Retrieved December 23, 2013 from http://aisel.aisnet.org/ecis2011/237.

Krishnan, V. R. (2002). Transformational leadership and value system congruence. *International Journal of Value-Based Management, 15*, 19-33. doi: 10.1023/A:1013029427977

Kujala, S., & Väänänen-Vainio-Mattila, K. (2009). Value of information systems and products: Understanding the users' perspective and values. *Journal of Information Technology Theory and Application (JITTA), 9*(4), 23-39.

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security, 18*(1), 4-13. doi: 10.1108/09685221011035223

Laeequddin, M. & Sardana, G. D. (2010). What breaks trust in customer supplier relationship? *Management Decision, 48*(3), 353-365. doi: 10.1108/00251741011037738

Lamm, E., Gordon, J. R., & Purser, R. E. (2010). The role of value congruence in organizational change. *Organization Development Journal, 28*(2), 49-64.

Le Dantec, C. A., Poole, E. S., & Wyche, S. P. (2009). Values as lived experience: Evolving value sensitive design in support of value discovery. *Proceedings of the 27th International Conference on Human Factors in Computing Systems, Boson, Massachusetts, USA,* 1141-1150. doi: 10.1145/1518701.1518875

Leach, J. (2003). Improving user security behavior. *Computers & Security, 22*(8), 685-692. doi: 10.1016/S0167-4048(03)00007-5

Lee, J. A., Soutar, G. N., & Louviere, J. (2007). Measuring values using best-worst scaling: The LOV example. *Psychology and Marketing, 24*(12), 1043-1058. doi: 10.1002/

Linstone, H. A. & Turoff, M. E. (2002). *The Delphi method: Techniques and applications*. Retrieved August 8, 2013 from http://is.njit.edu/pubs/delphibook

Lopes, I. M. & de Sá-Soares, F. (2012). Information security policies: A content analysis. *The 16th Pacific Asia Conference on Information Systems (PACIS), Ho Chi Minh City, Vietnam*, Paper 146. Retrieved September 1, 2013 from http://aisel.aisnet.org/pacis2012/146

Manager. (2011). In *American Heritage Dictionary of the English Language* (on line edition). Retrieved March 27, 2013 from http://ahdictionary.com

Manders-Huits, N. (2011). What values in design? The challenge of incorporating moral values into design. *Science and Engineering Ethics, 17*(2), 271-287. doi: 10.1007/s11948-010-9198-2

Maurer, S. D. (2006). Using situational interviews to assess engineering applicant fit to work group, job, and organizational requirements. *Engineering Management Journal, 18*(3), 27-35.

Maxwell, J. A. (2005). *Qualitative research design. An interactive approach, 2nd Ed.* Thousand Oaks, CA: SAGE Publications.

Meglino, B. M., Ravlin, E. C., & Adkins, C. L. (1989). A work values approach to corporate culture: A field test of the value congruence process and its relationship to individual outcomes. *Journal of Applied Psychology, 74*(3), 424-432. doi: 10.1037//0021-9010.74.3.424

Miller, J. K., Friedman, B., Jancke, G., & Gill, B. (2007). Value tensions in design: The value sensitive design, development, and appropriation of a corporation's groupware system. *Proceedings of the 2007 International ACM Conference on Supporting Group Work, Sanibel, Florida, USA, 4*(07), 281-290. doi: 10.1145/1316624.1316668

Mishra, S. & Dhillon, G. (2006). Information systems security governance research: A behavioral perspective. *1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference, New York, USA*, 18-26.

Mulligan, D. K. & King, J. (2012). Bridging the gap between privacy and design. *University of Pennsylvania Journal of Constitutional Law, 14*(4), 989-1034.

Nathan, L. P., Friedman, B., Klasnja, P., Kane, S. K., & Miller, J. (2008). Envisioning systemic effects on persons and society throughout interactive system design. *Proceedings of the 7th ACM conference on Designing interactive systems, Cape Town, South Africa*, 1-10. doi: 10.1145/1394445.1394446

Okoli, C. & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & Management, 42*(1), 15-29. doi: 10.1016/j.im.2003.11.002

Oosterlaken, I. (2014). Applying value sensitive design (VSD) to wind turbines and wind parks: An exploration. *Science and Engineering Ethics*. Advance online publication. doi: 10.1007/s11948-014-9536-x

Ostroff, C., Shin, Y., & Kinicki, A. J. (2005). Multiple perspectives of congruence: Relationships between value congruence and employee attitudes. *Journal of Organizational Behavior, 26*(6), 591-623. doi: 10.1002/job.333

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176. doi: 10.1016/j.cose.2013.12.003

Pieters, W., Padget, J., Dechesne, F., Dignum, V., & Aldewereld, H. (2013). Obligations to enforce prohibitions: On the adequacy of security policies. *Proceedings of the 6th International Conference on Security of Information and Networks, Aksaray, Turkey*, 54-61. doi: 10.1145/2523514.2523526

Patton, M. Q. (2001). *Qualitative research & evaluation methods, 3rd Ed.* Thousand Oaks, CA: SAGE Publications.

Pommeranz, A., Detweiler, C., Wiggers, P., & Jonker, C. (2012). Elicitation of situated values: Need for tools to help stakeholders and designers to reflect and communicate. *Ethics and Information Technology, 14*(4), 285-303. doi: 10.1007/s10676-011-9282-6

Posner, B. Z. (2010). Another look at the impact of personal and organizational values congruency. *Journal of Business Ethics, 97*(4), 535-541. doi: 10.1007/s10551-010-0530-1

Powell, C. (2003). The Delphi technique: Myths and realities. *Journal of Advanced Nursing, 41*(4), 376-382. doi: 10.1046/j.1365-2648.2003.02537.x

PwC. (2013). *The Global State of Information Security Survey.* Retrieved February 17, 2013 from the PwC Website: www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml#

Ramachandran, S. & Rao, S. V. (2006). Security cultures in organizations: A theoretical model. *Proceedings of the Twelfth Americas Conference on Information Systems, Acapulco, Mexico*, 3460-3464.

Richardson, R. (2012). *2010/2011 15th Annual Computer Crime and Security Survey*. Retrieved from http://reports.informationweek.com/abstract/21/7377/Security/research-2010-2011-csi-survey.html

Rokeach, M. (1973). *The nature of human values*. New York: Free Press.

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

Rotondo, A. & Freier, N. G. (2010). The problem of defining values for design: A lack of common ground between industry and academia? *CHI '10 Extended Abstracts on Human Factors in Computing Systems, Atlanta, Georgia,* 4183-4188. doi: 10.1145/1753846.1754123

Rowe, G. & Wright, G. (1999). The Delphi technique as a forecasting tool: Issues and analysis. *International Journal of Forecasting, 15*(4), 353-375. doi: 10.1016/S0169-2070(99)00018-7

Schein, E. (1990). Organizational culture. *American Psychologist, 45*(2), 109-119. doi: 10.1037/0003-066X.45.2.109

Schein, E. (1999). *The corporate culture survival guide.* San Francisco, CA: Jossey-Bass.

Schlienger, T. & Teufel, S. (2003). Analyzing information security culture: Increased trust by an appropriate information security culture. *14th International Workshop on Database and Expert Systems Applications, Prague, Czech Republic*, 405-409. doi: 10.1109/DEXA.2003.1232055

Shneiderman, B., Plaisant, C., Cohen, M., & Jacobs, S. (2009). *Designing the user interface. Strategies tor effective human-computer interaction* (5th ed.). Boston, MA: Addison Wesley.

Smith, W. J., Wokutch, R. E., Harrington, K. V., & Dennis, B. S. (2001). An examination of the influence of diversity and stakeholder role on corporate social orientation. *Business & Society, 40*(3), 266-294. doi: 10.1177/000765030104000303

Stark, L. & Tierney, M. (2013). Lockbox: Mobility, privacy and values in cloud storage. *Ethics and Information Technology, 16*(1), 1-13. doi: 10.1007/s10676-013-9328-z

Steen, M. & van de Poel, I. (2012). Making values explicit during the design process. *Technology and Society Magazine, IEEE, 31*(4), 63-72. doi: 10.1109/MTS.2012.2225671

Stevens, B. (1999). Communicating ethical values: A study of employee perceptions. *Journal of Business Ethics, 20*(2), 113-120.

Stevens, B. (2008). Corporate ethical codes: Effective instruments for influencing behavior. *Journal of Business Ethics, 78*(4), 601-609. doi: http://dx.doi.org/10.1007/s10551-007-9370-z

Strugatch, W. (2011). Turning values into valuation: Can corporate social responsibility survive hard times and emerge intact? *Journal of Management Development, 30*(1), 44-48. doi: http://dx.doi.org/10.1108/02621711111098352

Suar, D. & Khuntia, R. (2010). Influence of personal values and value congruence on unethical practices and work behavior. *Journal of Business Ethics, 97*(3), 443-460. doi: 10.1007/s10551-010-0517-y

Tejay, G. & Dhillon, G. (2005). Developing measures of information security culture. *The Fourth Workshop on e-Business (WeB 2005), Las Vegas, Nevada, USA*.

Tellis, W. (1997). Application of a case study methodology. *The Qualitative Report, 3*(3), 1-18.

Thomson, K. L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security, 2006*(10), 7-11. doi: 10.1016/S1361-3723(06)70430-4

Timmermans, J., Zhao, Y., & van den Hoven, J. (2011). Ethics and nanopharmacy: Value sensitive design of new drugs. [Case study]. *NanoEthics, 5*(3), 269–283. doi: 10.1007/s11569-011-0135-x

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Process-variance models in information security awareness research. *Information Management & Computer Security, 16*(3), 271-287. doi: 10.1108/09685220810893216

Tsohou, A., Kokolakis, S., Lambrinoudakis, C., & Gritzalis, S. (2010). A security standards' framework to facilitate best practices' awareness and conformity. *Information Management & Computer Security, 18*(5), 350-365. doi: 10.1108/09685221011095263

Van Niekerk, J. F. & von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, 29*(4), 476-486. doi: 10.1016/j.cose.2009.10.005

Voida, A., Dombrowski, L., Hayes, G. R., & Mazmanian, M. (2014). Shared values/conflicting logics: working around e-government systems. *Proceedings of the 32nd annual ACM conference on Human factors in computing systems, Toronto, Ontario, Canada ,*3583-3592. doi: 10.1145/2556288.2556971

von Solms, R. & von Solms, B. (2004). From policies to culture. *Computers & Security, 23*(4), 275-279. doi: 10.1016/j.cose.2004.01.013

Vroom, C. & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198. doi: 10.1016/j.cose.2004.01.012

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security, 17*(1), 4-19. doi: 10.1108/09685220910944722

White, K. J. & Ruh, R. A. (1973). Effects of personal values on the relationship between participation and job attitudes. *Administrative Science Quarterly, 18*(4), 506-514.

Whittemore, R., Chase, S. K., & Mandle, C. L. (2001). Validity in qualitative research. *Qualitative Health Research, 11*(4), 522-537. doi: 10.1177/104973201129119299

Williams, P. A. (2009). What does security culture look like for small organizations? *Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia*, 48-54.

Winschiers-Theophilus, H. & Bidwell, N. J. (2013). Toward an Afro-centric indigenous HCI paradigm. *International Journal of Human-Computer Interaction, 29*(4), 243-255. doi: 10.1080/10447318.2013.765763

Wright, D. (2011). A framework for the ethical impact assessment of information technology. *Ethics and Information Technology, 13*(3), 199-226. doi: 10.1007/s10676-010-9242-6

Yetim, F. (2011a). Bringing discourse ethics to Value Sensitive Design: Pathways to toward a deliberative future. *AIS Transactions on Human-Computer Interaction, 3*(2), 133-155.

Yetim, F. (2011b). Focusing on values in information systems development: A critical review of three methodological frameworks. *Proceedings of the 10th International Conference on Wirtschaftsinformatik, Zürich, Switzerland*, 1197-1204.

Yetim, F. (2011c). A set of critical heuristics for value sensitive designers and users of persuasive systems. *19th European Conference on Information Systems, Helsinki, Finland*, Paper 185. Retrieved December 30, 2013 from http://aisel.aisnet.org/ecis2011/185

Yoo, D., Huldtgren, A., Woelfer, J. P., Hendry, D. G., & Friedman, B. (2013). A value sensitive action-reflection model: Evolving a co-design space with stakeholder and designer prompts. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Paris, France*, 419-428. doi: 10.1145/2470654.2470715

Young, M. & Post, J. E. (1993). Managing to communicate, communicating to manage: How leading companies communicate with employees. *Organizational Dynamics, 22*(1), 31-43. doi: 10.1016/0090-2616(93)90080-K