https://doi.org/10.48009/2_iis_2013_279-288

*Issues in Information Systems*

*Volume 14, Issue 2, pp.*279-288*, 2013*

# Security Survey Information Sharing: Emotional intelligence and Privacy Sensitivity

***Belinda Shipps, North Carolina A&T State University, bpshipps@ncat.edu***

## ABSTRACT

*Although information security is a vital part of organizations, there are many individuals that refuse to provide feedback or disclose information to organizations by participating in improvement and knowledge gathering efforts such as surveys.* [1] *conducted research which indicated that emotions had a significant effect on an individual's decision to disclose information. This research seeks to extend this research finding by asking the following questions. Do emotions and emotional intelligence (EQ) and privacy sensitivity regarding information security have an effect on willingness to share information? Why is it so difficult to get others to participate in security surveys when the surveys can be used to help improve security processes? Protection of valuable information has become of increasing interest to organizations as they struggle to compete with others. Organizations are becoming more aware of the growing need for continuous feedback, monitoring and change regarding information security systems to combat the constant, new and growing security threats that exist. This research proposes a conceptual model to help in examining factors relating to emotional intelligence, sensitivity to privacy concerns, social norms and expectancy that may be associated with individuals and their unwillingness to participate in providing feedback about security systems*

**Keywords:** Information security, computer security, emotional intelligence, social norms, expectancy theory, theory of planned behavior and theory of reasoned action

## INTRODUCTION

Information security plays a key role in organizations, however many individuals refuse to provide feedback or disclose information to organizations by participating in improvement and knowledge gathering efforts such as surveys. In one study by [1] emotions had a significant effect on an individual's decision to disclose information. Do emotions and emotional intelligence (EQ) and privacy sensitivity regarding information security have an effect on willingness to share information? Why is it so difficult to get others to participate in security surveys when the surveys can be used to help improve security processes? Organizations use information systems to help them efficiently and effectively share and exchange information in various ways. Loss and damage of information can be devastating to a firm. Protection of this information has become a major concern for organizations and their ability to compete with others. Organizations need continuous feedback, monitoring and change to combat the constant, new and growing security threats that exist.

Information and its protection involve complex and dynamic issues that require continuous attention due to the growing and changing global nature of information systems. The types of information exchange continue to grow as people increasingly find new ways such as cloud computing and mobile technology to share information with others. All of these forms of communication require methods and procedures to safeguard against new and existing threats.

Information protection covers a range of areas throughout an organization such as protection of software, email, databases, networks and personal data. Protection also spans a range of interchange between people such as: retail consumers and merchants, bankers and customers, suppliers and purchasing agents, stock market brokers and clients, students and academics and government and military officials.

Information or computer Security focuses on protecting information and information systems from harmful risks from authorized and unauthorized users in terms of its integrity, confidentiality and accessibility. This protection can relate to physical, technical or human controls. Part of protecting the information involves getting feedback from users of security systems in order to better understand the things that are helping and to become aware of new situations or old processes and procedures that no longer work.

Collecting information through surveys or some form of information gathering provides valuable input from employees and users who may recognize problems (real or potential) that others are not aware of. This feedback on security systems is essential to help in continual improvement, change and success of security systems [19].

Organizations are challenged with new and increasingly threatening security concerns [27]. There are many business risks associated with security such as: disclosure, identity theft, viruses that destroy information or deny services, and unauthorized individuals that access or modify information. Part of taking a preventative approach involves getting feedback from employees and others through the use of interviews, surveys and questionnaires on potential breaches and the status of the security system.

Much of previous research has focused on understanding security in relation to technology. Technology plays a significant role in providing controls and methods for minimizing risk and maximizing value. However humans also play a critical role in the security process. People have the potential to cause security breaches due to their behavior [23]. How humans or individuals think, react and behave toward security-related issues, policies and procedures can impact the overall performance of the organization as well as the security structure and strategies.

In order to address current and potential risk, firms' management and employees from the top down will need to understand the value or harm of their actions or lack of actions in terms of security performance and well-being of the firm. Individual workers need to understand and be made aware of their value in this process.

In many instances, success of information security systems is not based on cognitive knowledge, but the non-cognitive knowledge that an individual possesses [12]. This non-cognitive knowledge that may prevent a person from participating in surveys might include fear of job loss or disapproval from a boss or manager. It may also include lack of understanding of the value of the workers input about security systems versus the time to complete the survey. [27, p.823] state that" security is usually viewed as an inconvenience, which may deter users from practicing safe behavior".

[1] found a significant link between emotions and willingness to disclose information. In a security study by [23] non-respondents of a security survey revealed various reasons for non-participation. Non-participants indicated (23%) that they did not feel it was worth their time in relation to the value they would gain from the survey. They also indicated (23%) that they do not share any information about security policies with outside entities. This could be due to fear of disapproval by management or a lack of understanding of the value toward improving security performance.

These findings suggest a need for research that evaluates factors that affect why individuals do and do not participate in efforts to obtain feedback and input on security-based issues. This research examines factors (emotional intelligence, sensitivity to privacy concerns, social norms, and expectancy) that may help to pinpoint areas that discourage participation. This information can be used to aid in developing methods and procedures to encourage and motivate individuals, managers, employees and others to participate.

This research may also help organizations improve the performance of the organization and employees in their understanding and behavior as it relates to information security. Improving information security performance may help improve the firm trust and confidence with others who share information and interact with the organization. For example, employees may feel more comfortable in sharing sensitive information with human resource managers or health care representatives if they feel they can trust the security and privacy of the firm's information system's environment.

This research attempts to address this issue by proposing a conceptual model that explores possible factors that may affect the (un)/willingness of individuals to participate in security-based surveys. The conceptual model includes the following: sensitivity factors, emotional intelligence factors, social factors (subjective norm) and expectancy factors.

Emotions, sensitivity to privacy concerns, social norms and expectancy of the individual may have a significant impact on why individuals do not participate in information security surveys. I posit that part of participating in information system security practices involves providing feedback to help monitor, assess and improve the progress of the security system. I suggest that individuals, who do not recognize this need for constant improvement through assessment, change and adaptation, may be highly sensitive to privacy concerns relating to security information. They also maybe low responders (low in emotional intelligence) in regard to data gathering initiatives such as surveys or interview initiatives relating to security systems. Recognizing the need to give feedback and understanding how to give feedback are characteristics of people with high emotional intelligence [12]. This research seeks to understand why individuals are reluctant to participate in security research. Previous research on why people do not participate in security research indicates that some of the main reasons involve lack of understanding of the value of their feedback, voice and time.

The research question focuses on the issue of willingness to provide security feedback and completion of security questionnaires to help in assessing, understanding and improving security performance and procedures within an organization. This research study seeks to understand significant factors that contribute to the willingness of individuals to respond to security-based questionnaires.

A conceptual model is presented that garners support from principles and theories from: personality, emotional intelligence, social norms and theory of planned behavior, theory of reasoned action and expectancy theory.

In the following sections the literature, hypotheses and the conceptual model are discussed. First, the theories and literature that support the model are discussed; next the conceptual model is explained, followed by the methodology. Finally, the analysis and conclusion are discussed.

## LITERATURE REVIEW AND HYPOTHESES:

### Non-cognitive factors and behavior

In some cases, people understand the seriousness of security systems, but still do not abide by the policies, processes and procedures. Procedures such as completing security surveys to provide feedback may still be ignored even though an individual understands the risk of non-compliance. Although technology is an important consideration in managing and evaluating security systems, the human factor warrants considerable attention also. Without the receptivity and compliance of people, security policies and procedures may not prove to be very effective in controlling for security risks and threats to the organization. Cognitive knowledge about security systems and software are helpful, but non-cognitive knowledge such as emotional intelligence (EQ) may help in explaining why individuals choose to be non-respondents in security surveys and possibly hurting the success of security systems and their evaluations. "People with the highest levels of intelligence (IQs) outperform those with average IQs (High EQs) just 20% of the time", [12, p. 8]. If the importance and value of the individual input, thinking and actions toward security, policies and procedures are not conveyed to individuals, there may be an overall lack of attention and willingness to carryout existing procedures and policies. Individuals may lack concern and/or have de-valued feelings regarding their time and input associated with efforts toward continued improvement of security procedures and performance.

There are constant new threats and risks that occur in information security systems. Many individuals are aware of these risks, but are not motivated to participate in the security processes that include providing feedback on the security systems through surveys and other feedback methods.

[24] indicate from their study that cognitive intelligence (IQ) alone was not a good predictor of behavior. Other researchers have also supported the idea that intelligence/cognitive alone is not a good indicator of success. Consideration of EQ may help in understanding individual decision-making. David Wechsler defines intelligence as "the aggregate or global capacity of the individual to act purposefully, to think rationally, and to deal effectively with his environment [32, p. 7].

This research explores: emotional intelligence, sensitivity, subjective norms and expectancy theory. I suggest that looking at the individual, important others and their emotions, sensitivity and behavior toward security issues may play a role in their decision not to participate.

### Emotional Intelligence

Emotion and the sensitivity of information can affect an individual's willingness to disclose information [1] [7]. Recognizing or being aware of the need to give feedback and understanding how to give feedback are characteristics of people with high emotional intelligence [12]. [28] defined emotional intelligence as a type of social intelligence where an individual is aware of their own emotions and can distinguish between them and is able to manage and guide them in their thinking and decisions. Emotional Intelligence can help to initiate and orchestrate change, attitude and behavior toward security in the firm and the need for continual change. I focus on the emotions associated with: a) self-actualization and the b) ability to change and make things better through individual efforts

In the past, much of information security research and analysis has been focused on technical solutions and not the human element. In this research I focus on the human factor in understanding information security issues and why individuals do not participate in information-sharing efforts such as security surveys.

This research can be valuable to organizations as well as researchers in understanding how to motivate individuals to participate in security information gathering initiatives such as research or organizational surveys. This can be helpful by shedding light on the value of the individual's contribution to organizational development and improvement efforts associated with information security. This research can help to recognize barriers to participation and information sharing.

**Raising expectations by raising emotional Intelligence**

I suggest that raising (emotional intelligence (EQ)) self-awareness in terms of individual value and raising emotional intelligence in regard to the individual's feelings toward sharing (sensitive) information about security threats and controls will motivate individuals to decide to participate in surveys. Unlike IQ, emotional intelligence is flexible and can be raised to help individuals and organizations better understand their emotions (such as fear of disapproval or fear of losing their jobs) to be successful [12, 21]. Raising emotional intelligence can help improve success of individuals and the organization as a whole [12].

**Hypotheses**

In this section I explain the Emotional Intelligence and participation model (EIPM). The EIPM conceptual model addresses the association between independent variables: emotional intelligence, sensitivity, expectancy and social norms and a continuous dependent variable for participation.

Ng [27] argues that users can make better decisions toward supporting preventative behavior (such as security surveys or security awareness programs) when they are made aware of possible threats (perceived susceptibility) and the benefits of security control effectiveness (perceived benefits). When they evaluate their emotions, they can learn to manage their emotions better so they can make conscious decisions to perform the suitable, preventive behavior.

**H1:** There is a positive association between emotional intelligence (awareness) and participation in security questionnaires

**Sensitivity of information – level of sensitivity and recognizing barriers**

Some individuals are more sensitive in terms of privacy and negative outcomes about sharing certain types of information [8]. This can create barriers to information sharing. However, if these barriers are identified, management can address barriers in order to encourage participation in information sharing initiatives such as security-based surveys. Previous research [6] indicates that employees in general tend to shy away from sharing information for many reasons such as: fear of reporting inaccurate information, worry and fear over saying the wrong thing, fear of criticism, fear of security and confidential breaches, or feeling that their contributions are not valued. This is especially true when the information is considered more private and sensitive in terms of risk or negative outcomes [8]. Individuals may not see the value or benefits of sharing or they may be fearful that they will get into trouble for sharing information. For example, some people with personalities that are more agreeable or more outgoing may feel that sharing sensitive information through completion of information-security surveys will help everyone by providing a safer environment. Security-based information has a certain level of privacy and trust associated with it that can make people fearful in sharing information. The feelings regarding sharing private or sensitive information may be perceived as having desirable or undesirable results. For example, information-security-based information may be viewed as very private information that may cause serious problems if it falls into the wrong hands. In this situation, individuals may be more fearful (sensitive) that they may give out too much private/sensitive information or that access to their shared responses may not be secure and unauthorized people may see the information and penalize them for sharing security-based information. I look at sensitivity in terms of five dimensions of personality.

Costa & McCrae [16]

| **Personality dimension** | **High level** | **Low level** |
|---|---|---|
| Neuroticism | sensitive, nervous | secure, confident |
| Extraversion | outgoing, energetic | shy, withdrawn |
| Openness to experience | inventive, curious | cautious, conservative |
| Agreeableness | friendly, compassionate | competitive, outspoken |
| Conscientiousness | efficient, organized | easy-going, careless |

**Sensitivity**

In the next section I discuss five dimensions of the five factor model and associated hypotheses that are used to measure sensitivity. The five factor model was used because of its validity and support from other research as a strong measure of personality. This construct is a measure of an individual's sensitivity toward participating in security surveys. In developing the sensitivity construct I borrow from Goldberg's Five Factor Model developed by [26]. There are 12 scales with four branches of abilities which consist of a) perceiving, b) assimilating, c) understanding d) managing emotions.

**Extroversion**

Extroversion is characterized as sociable and outgoing behavior. Extroverts tend to be more talkative and engaging as opposed to introverts who tend to be more shy and withdrawn. They tend to enjoy more social interaction and involvement and therefore may be more willing to engage in sharing sensitive information about security systems. Previous research suggests that extroversion can affect an individual's social norms [3]. Extroverts may identify and relate more to the organization and their mission and therefore, be more verbal about expressing their opinion. Extroverts may more readily recognize their value to the organization and therefore the individual value they bring by participating in initiatives such as security surveys. I suggest that extroverts thus have a low level of sensitivity to security-based information sharing

**H2:** There is a positive association between extroversion and the level of sharing/participating in sensitive, security-based information sharing such as surveys (low sensitivity to security-based information sharing)

**Agreeableness**

Individuals with the agreeableness trait are friendly and congenial. "Agreeableness or sociability refers to friendly, considerate and modest behavior." [18, p. 100]. Individuals that are agreeable tend to be kind, trusting, cooperative, and generous [20].

Agreeable individuals are warm and friendly but tend to be hesitant or concerned about destructive attitudes and behavior [13]. This concern suggests that individuals with the agreeableness trait may be reluctant to participate in security-based information sharing because of possible fears or concerns regarding the possibility of unauthorized access or use of the sensitive, security-based information that they provide.

**H3:** There is a negative association between agreeableness and the level of sharing/participating in sensitive, security-based information sharing such as surveys (high sensitivity to security-based information sharing)

**Neuroticism**

Neuroticism also referred to as emotional instability is defined as a trait associated with depression, anxiety, instability, fear and impulsiveness [20]. Individuals with this trait tend to be pessimistic and fearful and may experience work-related problems [22].

I argue that individuals with the neuroticism trait tend to be more fearful and apprehensive of situations and may be more uncomfortable and nervous in sharing security-based information associated with surveys or other forms of data gathering. Security-based information tends to have a high level of sensitivity and privacy associated with it.

**H4:** There is a negative association between neuroticism and the level of sharing/participating in sensitive, security-based information sharing such as surveys (high sensitivity to security-based information sharing)

**Conscientiousness**

Conscientiousness is defined as a trait that relates to the level of fortitude, determination and willpower of an individual. Individuals with this trait tend to be thorough, organized and precise [20]. These individuals tend to be more risk-averse, cautious and concerned about unsafe situations [13]. These individuals are detail-oriented and thorough and may view participation in security-based information sharing as harmful. Therefore I suggest that conscientious individuals may be less willing to share security-based information which tends to be private and sensitive.

**H5:** There is a negative association between conscientiousness and the level of sharing/participating in sensitive, security-based information sharing such as surveys (high sensitivity to security-based information sharing)

**Openness**

Openness is defined as a trait that is associated with a high level of liberalism, open-mindedness, curiosity, creativity and progressiveness [11]. I argue that individuals with a high level of openness tend to be creative, analytical and logical in their

thinking. I argue that they are able to recognize and weigh the potential risks and benefits associated with sharing sensitive and private information such as security-based information and therefore may be more willing to share or participate in information sharing initiatives such as surveys. I argue that they are more willing to share and therefore less sensitive to sharing information because of their ability to rationally consider both sides and not let fearful emotions dissuade them from participating

**H6:** There is a positive association between openness and the level of sharing/participating in sensitive, security-based information sharing such as surveys (low sensitivity to security-based information sharing)

## EIPM CONCEPTUAL MODEL

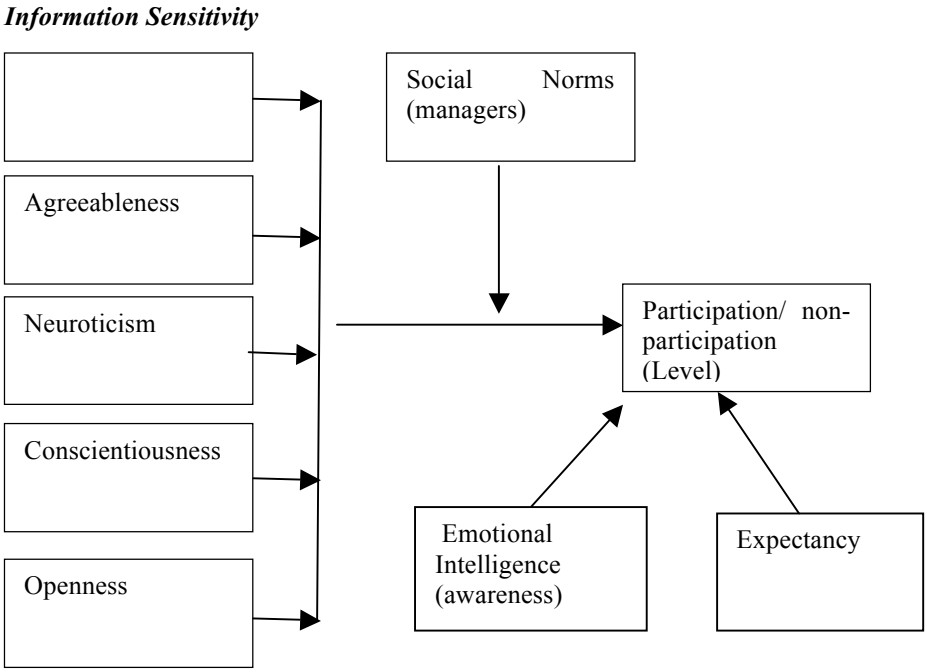


**Figure 1** Security Survey Model

### Participation

### Expectancy Theory emotions and participation

Expectancy theory has been used in previous studies to help understand organizations and the attitudes and behaviors of people associated with the organization. This theory has been used to help understand the motivation of workers and their behavior and why individuals select one behavior over another. In a study by [24], when ability and role perception measures were combined with measures of expectancy, there was a significant difference in behavior. Expectancy theory suggests that individuals make choices based upon whether the results will be beneficial/desirable or undesirable [8]. This is especially true when the information is associated with privacy and sensitivity [8]. This theory can help understand individual motivations and expectations toward security-based information sharing and their decision to participate or not in information sharing such as surveys.

Expectancy theory of motivation describes how individuals decide on which behavior to adopt and how to accomplish the outcome they want. [31] studied the motivation associated with making decisions and developed three variables to help in understanding expectancy: a) Valence b) Expectancy c) Instrumentality. They are used to explain choosing one element instead of another: effort-performance expectancy (E>P expectancy) and performance-outcome expectancy (P> O expectancy). Expectancy is the belief that an individual's effort (E) will result in achievement of desired performance (P)

goals. Expectancy perception relate to: self-efficacy, goal difficulty and control. Expectancy theory looks at the mental processes associated with making a decision.

Previous research indicates that in regards to information associated with privacy such as medical or information security, individuals will evaluate the severity and risk involved in the decision [4]. Part of this assessment of risk has been associated with emotions [25]. Previous research indicates that emotions can alter perceptions and decision-making [15]. [4] found that emotions play a significant role in disclosing or sharing sensitive information. In this research, I focus specifically on information sharing associated with participating in obtaining data relating to information-security based questionnaires and interviews.

I argue that individual emotions play a role in disclosing or sharing information-security specifically in relation to participating in surveys or interviews. I suggest that human factors such as emotions are important considerations in developing, managing and improving information security within organizations. The emotions of an individual or employee play a role in expectations and decision-making.

Employees can have a major impact on the security of the information within an organization. Employees have access to very sensitive and private information and can pose a huge threat to the safety and security of the information [5]. Employees may be aware but unwilling to share information about real or potential security holes and breaches within the system that have not been addressed. Therefore, employee feedback and information sharing can be important to the success of the information security within an organization. The emotions and perceptions toward security systems may affect the choice to participate or not in sharing information.

In this research I focus on individuals and their emotions and sensitivity toward sharing information and the expected outcomes or results associated with sharing security-based information through questionnaires and interviews.

I suggest that emotions play a role in an individual's behavior and perception of expected outcomes that result from sharing sensitive, information-security-based information. I argue that in regard to information security, social influence, certain sensitivity to information, individual expectations and emotions will motivate individuals to make decisions to participate or not in information sharing initiatives.

Participation is used as a construct that measures the level of willingness to participate in information sharing of security-based information. Possible factors in the models that affect participation: Emotional Intelligence, sensitivity to private information, social norms and expectancy.

Individuals may choose not to participate in information security surveys if they do not feel they will achieve their expected outcome. For example, if they feel anxious or fearful about participating because they think their boss will disapprove of their participation in information sharing through security survey participation, they may decline because they expect a negative response or disapproval from their boss. However, individuals may be motivated to participate if they expect their boss to look favorably upon the behavior and the boss gives them high praise and rewards for their contribution.

**H7:** There is a positive association between individual expectations and employee participating/sharing security-based information.

**Social Norms/Social Influence and Managers**

An individual's actions may be influenced by the social norms in the work environment that are associated with other people and their opinions. Social influence or social norms relate to an individual's feelings based on their perceptions of significant others' opinions on what the individual should do. I suggest that non-participants in surveys may be influenced in their intentions to participate if other important co-workers or other significant others think participating is unacceptable, a waste of time and/or has no value. Social influence has been used in previous research relating to technology acceptance [30].

Theory of Reasoned Action (TRA) and the theory of planned behavior (TPB) both provide support for social norms/subjective norms [2, 17]. TRA suggests that actual behavior relates to an individual's behavioral intentions. Behavioral intentions are influenced by: (a) individual attitude regarding the behavior; and (b) social norms, which are defined as individual perceptions of social demands or pressures. This relates to how important others think and feel about change and the adopting behavior such as completing survey questionnaires to provide feedback that could result in changes in information security systems. I suggest that when individuals are influenced by social norms and attitudes of important

others who do not think surveys are important to complete, people are less likely to complete information security questionnaires.

As managers are able to gather information about employees and their concerns and fears regarding sharing information, they can develop strategies and procedures to "raise the emotional intelligence" of individuals through focused training and development initiatives which address the various emotional concerns with the goal of reducing the concerns and encouraging /raising feelings of individual value and importance in information sharing efforts such as completion of information-security based questionnaires and interviews. In this research I relate information sharing to sharing information through participation in information-security based interviews and questionnaires.

**Social Influence/Subjective norms**

The terms social norms or subjective norms have been used interchangeably [29]. It is defined as an individual's beliefs regarding the degree in which others wish for them to perform a behavior [17, 14]. It relates to the expectations of others for an individual. Norms relate to socially acceptable behaviors by others such as managers or a group in a department in an organization [14]. Social influence relates to social pressures that are imposed by significant others to perform in a certain manner. Previous research indicates that social pressure can impact an individual's decisions [30]. Previous research also shows that women and older workers tend to be more susceptible to the opinions of others [30]. Social influence can impact an individual's behavior through three elements: a) compliance b) internalization c) identification [30]. Internalization and identification relate to an individual changing their decision or behavior due to social pressure.

**H8:** There is a moderating positive association between manager's positive feelings about participation in security surveys and employee's emotions toward participating/sharing security-based information.

## METHODOLOGY

The methodology will consist of qualitative and quantitative analysis. Initially, interviews will be conducted with individuals working in information security system settings in order to help in developing the survey instrument. After analyzing the data from the interviews, this information will be used to supplement and support the survey instrument. Emotional intelligence will be measured by using the Bar-on EQI scale. This scale is a self-report inventory with 133 items. I plan to focus on the dimension for intrapersonal intelligence because of the focus on self-awareness. This scale was selected because of previous research that supports the reliability and validity of the scale. A high score on the intrapersonal scale is associated with individuals who feel good about themselves and have a positive outlook about their lives and the things that they do [9, p. 44]. Measure of managers' social norms will be based on a previous measure by [30]. The expectancy measure will look at an individual's expectations regarding their actions and receiving a reward [31].

I plan to measure sensitivity by using a Five Factor model questionnaire with multi-item measures. After the survey data is collected, Structural Equation Modeling (SEM) will be used for data analysis in order to help validate the model and evaluate the hypotheses. Respondents will be selected from a mix of private and public organizations. The respondents will consist of various managers and employees who work in information security system settings.

## CONCLUSIONS

In conclusion, the human element and their emotions, sensitivity toward privacy, expectations and social influences are key elements in information security systems. People and their engagement and participation in the information security process are critical to the success of information security systems. In order to insure the continued improvement of information security systems it is important to get feedback from the users of the systems [19]. This input can help in establishing better security procedures. It may help in creating new measures and eliminating obsolete measures. Information systems and the security of these systems is a vital part of the success of organizations. [1] indicate that emotions are an important consideration in deciding to disclose sensitive information. Evaluating the individual and their emotions, sensitivity to information privacy and expectations as well as their social norms in relation to participating in security surveys may help to increase the participation and success of the security systems. This research can help by providing a model that can be used

in evaluating why individuals do not participate and finding solutions to the problems associated with non-participation so that the valuable input from users can be used to make security systems better and safer.

## REFERENCES

1. Agarwal, R., & Anderson, C. (2008). *The Complexity of Consumers' Willingness to Disclose Personal Information: Unraveling Health Information Privacy Concerns.* Paper presented at the eHealth Initiatives Conference, Washington, DC.
2. Ajzen, I. (1991). Theory of Planned Behavior. *Organizational Behavior and Human Decision processes, 50*(1991), 179-211.
3. Ajzen, I., & Fishbein, M. (1980). *Understanding Attitudes and predicting social behavior*. Englewood Cliffs, NJ.
4. Anderson, C., & Agarwal, R. (2011). The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information, *Information Systems Research 22*(3), 469-490.
5. Ansanelli, J. (2005). Employees, The biggest threat to network security, *NetworkWorld, February*. Retrieved from http://www.networkworld.com
6. Ardichvili, A., Vaughn, P., & Wentling, T. (2003). Motivation and barriers to participation in virtual knowledge-sharing communities of practice. *Journal of Knowledge Management, 7*(1), 64-77.
7. Baddeley, M. (2011). *Information Security: Lessons from Behavioural Economics*. Cambridge Working Paper in Economics. Cambridge University.
8. Bansal, G., Zahedi, M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138-150.
9. Bar-On, R. (1997). *Bar-On Emotional Quotient Inventory: technical manual*. Toronto, ON: Multi-Health Systems.
10. Barrick, M. R., & Mount, M. K. (1991). The Big five personality dimensions and job performance: a meta-analysis *Personnel Psychology, 44*(1), 1-26.
11. Barrick, M. R., Mount, M. K., & Strauss, J. P. (1993). Conscientiousness and performance of sales representatives: test of the mediating effects of goal setting. *Journal of Applied Psychology 78*(1), 715-722.
12. Bradberry, T., & Greaves, J. (2009). *Emotional Intelligence 2.0*. San Diego, CA: Talent Smart.
13. Chauvin, B., Hermand, D. E., & Mullet, E. (2007). Risk perception and personality facets. *Risk Analysis 27*(1), 171-185.
14. Cialdini, R. B., & Goldstein, D. (2004). Annual Review Psychology *Social Influence: Conformity and Compliance, 55*(1), 591-621.
15. Cosmides, L., & Tooby, J. (2000). Evolution of adaptations for decoupling and Meta-representation University of California-Santa Barbera: Center for Evolutionary psychology.
16. Costa, P. T., & McCrae, R. (1992). *Revised NEO personality inventory (NEO PI-R) and NEO five-factor Inventory (NEO-FFI) professional manual*: Odessa.
17. Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research,* Reading, MA: Addison-Wesley.
18. Furnham, A., Dissou, G., Sloan, S., & Chamorro-Premuzic, T. (2007). Personality and intelligence in business people: a study of two personality and two intelligence measures. *Journal of Business and Psychology, 22*(1), 99-109.
19. Gil-Garcı´a, J. R. n., & PardoT, T. (2005). E-government Success Factors: Mapping Practical Tools to Theoretical Foundations, *Government Information Quarterly, 22* (1), 187–216.
20. Goldberg, L. R. (1992). The development of the markers for the big-five factor structure. *Psychological Assessment, 4*(1), 26-42.
21. Goleman, D. (1998). *Working with Emotional Intelligence* New York: Bantam Books.
22. Judge, T. A., Heller, D., & Mount, M. K. (2002). Five-factor model of personality and job satisfaction: a meta-analysis. *Journal of Applied Psychology 87*(3), 530-541.
23. Kotulic, A., & Guynes- Clark, J. (2004). Why there aren't More Information Security Research Studies. *Information & Management, 41*(1), 597-607.
24. Lawler III, E., & Suttle, J. L. (1973). Expectancy Theory and Job Behavior. *Organization Behavior and Human Performance 9*(1), 482-503.
25. Lowenstein, G., Weber, E., See, C. H., & Welch, E. (2001). Risk as feelings *Psychological Bulletin, 127*(1), 267-286.

26. Mayer, J., Caruso, D., & Salovey, P. (1999). Emotional Intelligence meets Traditional Standards for an Intelligence *Intelligence, 27*(1), 267-298.
27. Ng, B.-Y., Kankanhali, A., & Xu, Y. (2009). Studying Users' Computer Security Behavior: A Health Belief Perspective Decision *Support systems, 46*(1), 815-825.
28. Salvoney, P., & Mayer, J. D. (1990). Imagination, Cognition and personality *Emotional Intelligence, 9*(1), 185-211.
29. Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Towards a Conceptual Model of Utilization *MIS Quarterly 15*(1), 125-143.
30. Venkatesh, V., Davis, F.D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science, 46*(1), 186-204.
31. Vroom, V. H. (1964). *Work and motivation* New York: Wiley.
32. Wechsler, D. (1958). *The Measurement and Appraisal of Adult Intelligence* Baltimore, MD: US: Williams & Wilkins Co.