Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2012 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-15-2012

# Initial Validation and Empirical Development of the Construct of Computer Security Self-Efficacy (CSSE)

Marlon Clarke
*Nova Southeastern University*

Yair Levy
*Nova Southeastern University*, levyy@nova.edu

# Initial Validation and Empirical Development of the Construct of Computer Security Self-Efficacy (CSSE)

**Marlon Clarke**
Graduate School of Computer and Information Sciences, Nova Southeastern University,
Ft. Lauderdale, FL 33314, USA

**Yair Levy**[1]
Graduate School of Computer and Information Sciences, Nova Southeastern University,
Ft. Lauderdale, FL 33314, USA

## ABSTRACT

As organizations have become more dependent on networked information systems (IS) to conduct their business operations, their susceptibility to various threats to information security has also increased. Research has consistently identified the inappropriate security behavior of the users as the most significant of these threats. Various factors have been identified in prior research as contributing to these inappropriate security behaviors, however, not enough is known about the role of social factors in mediating these behaviors. This study developed a new Computer Security Self-Efficacy (CSSE) construct, identified 35 highly reliable items of CSSE in the context of individuals' use of encrypted e-mail, and identified four significant factors of CSSE. The four factors were named Performance Accomplishments and Technical Support, Goal Commitment and Resource Availability, Experience Level, and Individual Characteristics. We conclude with a discussion on limitations and recommended future research that can result from the findings of this study.

**Keywords:** Computer self-efficacy, information security abilities, user perceived computer abilities, computer security self-efficacy, use of encrypted e-mail.

[1] Corresponding author. levyy@nova.edu +1 954 262 2006

## INTRODUCTION

The increase in the use of computers and associated technologies has been phenomenal. According to Im and Baskerville (2005), this increased use has had significant impact on everyday life and business operations. As such, Information Systems (IS) are now considered critical resources that support the attainment of management objectives and manage the operations of various other infrastructures (Hamill et. al. 2005). Given the reliance on IS, organizations must develop strategies and programs to effectively secure their computer assets, while preventing IS compromise (Im and Baskerville 2005).

Prior research has concluded that the largest security threat facing organizations is the inappropriate or insecure behavior of its own IS users (Keller et al. 2005; Ramim and Levy 2006; Whitman 2003). The causes of these behaviors are not fully understood, and research is required to identify the factors responsible for the inappropriate security behavior of IS users (Teer et al. 2007). Cronan and Douglas (2006) argued the need for a better understanding of the precedents of inappropriate security behavior.

E-mail is one IS identified as being at risk due to the persistence of inappropriate security behaviors on the part of IS users (Tracy et al. 2007). It has been argued that e-mail is now the main way of communicating across businesses and has replaced traditional communication methods (Nenadic et al. 2004). As the use of and dependence on e-mail messaging has grown, issues related to the security of the e-mail messages have been largely overlooked. According to Tracy et al. (2007), early e-mail standards placed little emphasis on security, and these standards form the basis of current e-mail implementations. Thus, e-mail systems have been identified as being vulnerable and susceptible to various information security threats such as being forged, intercepted, read by unintended recipients, or altered during transmission (Garfinkel et al. 2005).

In particular, the transmission of unencrypted e-mail messages in many organizations is considered to pose serious security risks (Dong-Her and Hsiu-Sen 2004; Garfinkel 2003). Despite the critical nature of this threat, the use of encryption with e-mail messages by IS users remains infrequent (Garfinkel 2003). As organizations become more concerned about the dangers in e-mail or the leaking of proprietary corporate information, an understanding of the human factors influencing inappropriate security behavior regarding e-mail appears to be important (Nenadic et al. 2004).

Computer self-efficacy (CSE), defined as individuals' judgment of their ability to use a computer in the achievement of a job task (Compeau and Higgins 1995), has been used to explain the behavior of IS users (Compeau and Higgins 1995; Kuo and Hsu 2001; Marakas et al. 1998). Research has shown that CSE exerts a significant influence on an individual's decision to use computers to achieve various tasks (Compeau and Higgins; Kuo and Hsu 2001; Marakas et al.). One problem with using CSE, however, is its generalizability, that is "the extent to which self-efficacy perceptions are restricted to particular situations" (Compeau and Higgins 1995, p. 192). As such, Compeau and Higgins argued the need for further examination of CSE and its associations with specific domains of interest or tasks relating to computers. InfoSec represents one such computer-related task that can be performed by a group of non-specialist IS users (Aytes and Connolly 2004). Marakas et al. (2007) argued that even vigorously validated measures of CSE, when applied to unrelated studies, will have limited generalizability. As such, researchers have been advised to develop new measures, or to significantly revise and revalidate existing measures to align measures of CSE with the specific task being investigated (Bandura 2001). This research built on seminal work of Compeau and Higgins (1995) by addressing the need for the development of newly specialized CSE measures, examining the inappropriate

security behavior of IS users, and identifying factors of users' ability to hinder these inappropriate security behaviors.

## THEORETICAL BACKGROUND

Grounded in the social cognitive theory (SCT), self-efficacy theory (Bandura 1977) advocates the belief one has in his or her capability to perform a specific task. The theory is that environmental influences such as social pressures, cognitive and other personal factors such as personality and demographic characteristics, and behavior are reciprocally determined (Compeau and Higgins 1995). The SCT advances output expectations and self-efficacy as the cognitive forces that influence behavior (Bandura 1977; Compeau and Higgins 1995). Accordingly, individuals will undertake behaviors they see as having favorable outcomes (Compeau and Higgins 1995). Thus, before actually performing a behavior, individuals often evaluate their ability to perform such behavior. Self-efficacy expectations deal with beliefs about one's ability to perform a particular task (Bandura 1986). As such, it relates to judgments of what individuals can do with the skills they possess and is not focused on the actual skill itself. Bandura identified performance accomplishments, vicarious experiences, forms of verbal persuasion, and physiological responses as the four main sources of self-efficacy.

*Performance accomplishments*, or mastery experiences, pertain to situations in which people have achieved performance success (Peterson and Arnn 2005). Through repeated performance success, individuals develop a level of mastery and gain confidence in their abilities to perform a specific task. *Vicarious experiences* are situations in which people observe others perform successfully, compare themselves to that performance, and form beliefs about their own competence (Peterson and Arnn 2005). *Forms of verbal persuasion* relates to feedback from others that is judged to be authentic and a reasonable match to one's personal assessment of

capabilities (Peterson and Arnn 2005). *Physiological responses* to experiences (anxiety, stress, mood, and fatigue) are physical and emotional reactions to specific situations (Peterson and Arnn 2005). The manner in which these reactions are perceived and interpreted can influence one's level of self-efficacy.

## Computer Self-efficacy

Derived from the broader self-efficacy construct, CSE is concerned with self-efficacy in relation to computer use and was defined by Compeau and Higgins (1995) as "an individual's perception of his or her ability to use a computer in the accomplishment of a job task" (p. 193). Using an empirical study of the perception of 2000 randomly selected knowledge workers, Compeau and Higgins examined how computer use was mediated by encouragement of others, duration of use and use by others, organizational support and training, outcome expectations, affect, and anxiety. Compeau and Higgins concluded that IS users with higher CSE had higher usage of computers, enjoyed using them more, and possessed less computer related anxiety. These claims were further validated in a later study of 394 subjects (Compeau et al. 1999). For their seminal study, Compeau and Higgins (1995) developed the instrument of CSE consisting of 10 items in ascending order of difficulty; respondents were asked to state whether or not they could complete the job using a software package. If respondents could complete the task, they would then indicate their confidence in their ability using a 10-point Likert scale. The Compeau and Higgins measure has been applied in various technological contexts, and has been identified as having high reliability and validity (Levy and Green 2009). The original seminal CSE instrument was central to this research study as it was used as the foundation for the development of a new Computer Security Self-Efficacy (CSSE) instrument and construct.

## Computer Self-Efficacy and Information System Security

There has been limited research that advances CSE as a variable in the study of InfoSec related behaviors. Crossler and Belanger (2006) examined the impact of CSE on the usage of InfoSec tools, based on the level of instruction received by individuals. They concluded that an individual's level of CSE directly impacted his or her use of security tools. Phelps (2005) examined the effect of CSE on the effectiveness of InfoSec in relation to a library IS and concluded that participants with higher self-efficacy were more effective at implementing system security. Other researchers, such as Chai et al. (2006), as well as Lee, LaRose, and Rifton (2008) also identified a positive relationship between self-efficacy and information security behavior, however, they failed to develop and validate a robust specialized instrument to measure CSE in the context of InfoSec.

In reviewing measures utilized in prior studies measuring InfoSec related self-efficacy, multiple instruments were identified. Chai et al. (2006) utilized a four-item measure, adapted from the work of Bandura et al. (1996), and originally developed to measure academic self-efficacy. The adapted measure consisted of four items, and utilized a five-point response format. Chai et al., however, argued the need for future studies incorporating additional factors and a larger, more diverse population.

In another study, Lee et al. (2008) developed a five-item measure that evaluated individuals' confidence to run an anti-virus program, install personal firewalls, update virus definitions, update patches, and screen e-mail on a seven-point scale. Lee et al. conceded that the model needed additional refinement and validation. Further, Phelps (2005) developed a measure for self-efficacy in the context of InfoSec comprising 20 questions and a responses scale of 0 to 100. Phelps recommended that further research should be conducted aimed at enhancing the

instrument to ensure construct validity, and to further examine factors that influence InfoSec. This study attempted to fulfill that need through the development and validation of the CSSE measurement instrument related to the use of encryption with e-mail messages in an organizational setting.

## RESEARCH MODEL AND RESEARCH QUESTIONS

This study utilized a mixed method approach to develop, validate, and test the reliability of a newly developed CSSE construct, in relation to the use of encryption with e-mail messages. According to Creswell and Plano-Clark (2007), using a mixed method approach allows for greater overall strength of a study than using qualitative or quantitative methods individually. First, a qualitative phase was performed to maximize all validities and to develop a theoretical framework. Next, a quantitative phase was utilized to explore the theoretical framework, verify the validities of the constructs, and to further refine the concepts and establish statistical validities.

The main research question that this study addressed was: What are the items of a Computer Security Self-Efficacy (CSSE) construct that demonstrate validity and reliability of such a measure? In answering this question, this study developed and examined a new CSSE construct, which was grounded in the social cognitive theory (SCT) (Bandura 1977; Barling and Beattie 1983; Compeau and Higgins 1995) and IS literature (Aytes and Connolly 2004; Dhillon and Backhouse 2001; Goodhue and Straub 1991; Lucas 1975; Straub 1989). The specific research questions that this study addressed were:

RQ1: What are the CSSE items, in the context of individuals' use of encrypted e-mail, as indicated by literature and a focus group?

RQ2: What is the validity of the proposed CSSE items, in the context of individuals' use of encrypted e-mail, as indicated by an expert panel?

RQ3: What are the significant factors of CSSE in the context of individuals' use of encrypted e-mail?

RQ4: What are the CSSE items that provide high reliability in the context of individuals' use of encrypted e-mail?

## Research Methodology

Through a review of existing literature, an initial list of CSSE items was developed. The initial list of items was developed based on a review of existing literature (Bandura 1977; Compeau and Higgins 1995; Compeau et al. 1999; Crossler and Bellanger 2006; Gist and Mitchell 1989; Hill et al. 1987; Marakas et al. 1998; Torkzadeh et al. 2006). There were 32 initial CSSE items identified from the literature review.

### *Qualitative Phase*

Subsequent to the development of the initial pool of CSSE item from literature, a qualitative first phase was performed using focus groups and an expert panel.

***Focus Group:*** To augment the initial list of items identified from the literature review, a qualitative questionnaire was developed in accordance with the methodology of Keeney (1999). Invitations were sent to two groups of participants, IS users pursuing business studies and entry-level technical employees; 10 individuals from each group participated in focus group study. The focus group study resulted in five additional items of CSSE which were added to the initial list of items. This yielded a list of 37 CSSE items, which addressed the first research question of this study.

The 37 CSSE items obtained from the literature review and the focus group study were next used to develop a preliminary CSSE survey instrument. The instrument asked respondents to assess their current capabilities related to the sending of encrypted e-mail messages by responding to a series of multiple choice questions. The instrument utilized a 10-point Likert scale allowing responses on a confidence scale of 1 to 10, with 1 indicated the lowest confidence and 10 the highest confidence that the individual could send encrypted e-mail messages given various scenarios. Participants in the main survey were asked to respond to the question: *"I believe I have the ability to send an encrypted e-mail message…"* given various scenarios.

***Expert Panel:*** The preliminary survey instrument was put through a qualitative review by an experts panel of three IS faculty members and three IS professionals who evaluated the instrument, the clarity of the items, and the precision of the instruments. Feedback from the expert panel was used to adjust the instrument resulting in a finalized survey instrument containing 36 items (Appendix A). The results of the expert panel were appropriate in making a determination of the instrument's validity and addressed the second research question for this study.

***Quantitative Main Study***

The quantitative phase of the study involved the distribution of the survey instruments by e-mail to collect data from attendees of business and medical schools in a large university located in the southeastern United States. Data was collected over a three-week period using a Web-based survey, allowing us to minimize issues relating to data accuracy and to eliminate issues related to missing data. Pre-analysis data screening was then performed to identify and address irregularities or problems with the collected data. This resulted in 292 usable responses (See Table 1).

| Item | Frequency | Percentage (%) |
|---|---|---|
| **Prior Use of Encryption** | | |
| *Yes* | 87 | 29.8 |
| *No* | 205 | 70.2 |
| **Current Use of Encryption** | | |
| *Yes* | 40 | 13.7 |
| *No* | 252 | 86.3 |
| **Expertise in Using Encryption** | | |
| *Expert* | 11 | 3.8 |
| *Average* | 66 | 22.6 |
| *Novice* | 215 | 73.6 |
| **Use Social networking** | | |
| *Yes* | 246 | 84.2 |
| *No* | 46 | 15.8 |
| **Gender** | | |
| *Male* | 110 | 37.7 |
| *Female* | 182 | 62.3 |
| **Age** | | |
| *Less than 20* | 1 | 0.3 |
| *20 to 29* | 125 | 42.8 |
| *30 to 39* | 84 | 28.8 |
| *40 to 49* | 59 | 20.2 |
| *50 to 59* | 19 | 6.5 |
| *Over 60* | 4 | 1.4 |
| **Academic level** | | |
| *Graduate* | 270 | 92.5 |
| *Junior* | 9 | 3.1 |
| *Senior* | 8 | 2.7 |
| *Sophomore* | 5 | 1.7 |
| **Major** | | |
| *Business* | 146 | 50 |
| *Health Professions* | 96 | 32.9 |
| *Other* | 25 | 8.6 |
| *Computer Sciences and Info Syst.* | 22 | 7.5 |
| *Education* | 3 | 1 |

| ***Years of Computer Use*** | **Minumum** | **Maximum** | **Mean** | **Std Deviation** |
|---|---|---|---|---|
| | 7 | 30 | 17.32 | 5.318 |

**Table 1.** Descriptive of Study Participants

To determine the number of factors to be retained, first the Kaiser criterion was utilized. The Kaiser criterion dictates that only factors with eigenvalues greater than one should be retained as common factors (Child 2006). Factors with eigenvalues values of below one were considered for elimination. Next, the scree test was performed using Principal Component Analysis (PCA). The scree test involves the graphical representation of the eigenvalues and identification of the break point where the curve flattens (Costello and Osbourne 2005). The data points above the break indicate the number of factors to be retained. Based on the Kaiser

criterion and the scree test, the number of factors to be retained was four. Next, a second PCA with Varimax rotation was performed, forcing the number of factors to four. An analysis of the PCA factor loading of each item with its principal component, and with other components was performed, identifying items with high and medium loadings (Appendix B). A review of the loadings on each factor was undertaken to make a determination of the specific factors of CSSE and their associated items. Four factors emerged: Performance Accomplishments and Technical Support, Goal Commitment and Resource Availability, Experience Level, and Individual Characteristics (Appendix C). This result answered the third research question of this study.

Next, the Cronbach's Alpha of the principal factors was evaluated. In performing this analysis, the overall Cronbach's Alpha reliability coefficient of each CSSE factor was calculated to test the reliability of each of the four factors, which were identified as possessing high reliability (.953, .951, .869, & .913). The Cronbach's Alpha for each individual factor was then calculated with each other item deleted from its associated factor individually. Based on the 'Cronbach Alpha if item is deleted,' one items deemed not reliable was deleted, leaving a list of highly reliable items. The results in this section, 35 items of CSSE (Appendix B) with high calculated reliability coefficients, provided an answer to the fourth research question.

## CONCLUSIONS

### Summary of Key Research Findings

Four main factors of CSSE were identified; Performance Accomplishments and Technical Support, Goal Commitment and Resource Availability, Experience Level, and Individual Characteristics. The Cronbach's Alpha of the four factors was very high, indicating high reliability for all four factors. The Performance Accomplishments and Technical Support factor was found to explain the largest variance in the data collected, just under 29%. This factor

included the CSE characteristics of performance accomplishment and situational support found in literature (Bandura 1977; 1986). Bandura (1977) identified performance accomplishment as the most crucial source of self-efficacy beliefs. Thus, one conclusion drawn from this study is that prior success using encryption, and access to readily available support should likely result in high CSSE and users who are more likely to use e-mail encryption.

Goal Commitment and Resource Availability, the second significant factor, represented a combination of the existing goal commitment, time, and persuasion characteristics identified in prior literature (Compeau and Higgins 1995; Marakas et al. 1998). These characteristics from literature were supplemented with the newly identified characteristic of resource availability. Resource availability was identified in the qualitative phase as an item that individuals considered important when assessing their ability to send encrypted e-mail messages. This factor explained over 20% of the variance in the collected data.

The third factor identified was Experience Level, and consisted of the characteristics of skill level identified in prior literature (Bandura 1977; Marakas et al. 1998). The conclusion, therefore, is that an individual's experience level will impact their CSSE level. The experience level factor explained just over 10% of the variance in the data collected.

The final factor, Individual Characteristics, represented a collaboration of two characteristics identified in prior literature, namely age and gender (Bandura, 1986; Marakas et al., 1998). Of interest is the fact that age appears to impact CSSE, irrespective of whether the respondent is younger or older. This factor, although important, explained only 9% of the variance in the data, the least of all the factors identified.

## Implications

This study has several implications for the field of IS. First, this study contributes to the body of knowledge regarding the use of e-mail encryption. Prior seminal research, such as Compeau and Higgins (1995), Kuo and Hsu (2001), as well as Marakas et al. (1998) has confirmed the effectiveness of CSE in influencing an individual's decision to use computers to achieve various tasks. By extending CSE research into the area of e-mail encryption, this study has provided new information that may contribute to a better understanding of the precedents of inappropriate InfoSec behavior of IS users. Consequently, we hope that this work will provide fertile ground for future research aimed at understanding the precedents of encryption with e-mail specifically, and InfoSec behavior more generally. This study is also significant as it holds implications for the InfoSec industry. Prior research has argued for a better understanding of the precedents of inappropriate user security behavior as this can aid in the development of strategies to influence these behaviors. Understanding what IS users consider important in using encryption to send e-mail should assist computer security professionals working to increase the use of encryption mechanisms and potentially other InfoSec mechanisms. Thus, this study may have implications for the development of strategies to promote positive InfoSec behaviors.

## Limitations and Recommendations for Future Research

This study had three main limitations. The first limitation was that the study measured data from only one institution and therefore caution should be exercised when generalizing the results. Further studies may be required using other populations to enhance the generalizability of the results. Another limitation is that invitations to participate in the study were sent by e-mail. Thus it is possible that users who infrequently checked their e-mail messages may not have received the invitation. The third limitation related to the fact that, although this study examined

CSSE in relation to computer security, only one InfoSec behavior was examined. Consequently, future research may be required to examine CSSE in relation to other user-related InfoSec behaviors. Research of this nature will serve to enhance the generalizability of this study. Finally, future research should attempt to evaluate the predictive nature of CSSE in the context of other valid IS constructs, using other populations to enhance generalizability.

## REFERENCES

Aytes, K., and Connolly, T. 2004. "Computer Security and Risky Computing Practices: A Rational Choice Perspective," *Journal of Organizational and End User Computing,* (16:3), July/September, pp. 22-40.

Bandura, A. 1977. "Self-efficacy: Towards a Unifying Theory of Behavioral Change," *Psychological Review*, (84:2), February, pp. 191-215.

Bandura, A. 1986. *Social Foundations of Thought and Action*, Englewood Cliffs, NJ: Prentice Hall.

Bandura, A., Barbaranelli, C., Caprara, G. V., and Pastorelli, C. 1996. "Multifaceted Impact of Self-efficacy Beliefs on Academic Functioning," *Child Development*, (67:3), pp. 1206-1222.

Barling, J., and Beattie, R. 1983. "Self-efficacy Beliefs and Sales Performance," *Journal of Organizational Behavior Management,* (*5*), pp. 41-51.

Brown, I., and Snow, R. 1999. "A Proxy Approach to E-mail Security," *Software Practice and Experience*, (29:12), pp. 1049-1060.

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H., and Upadhyaya, S. 2006. "Role of Perceived Importance of Information Security: An Exploratory Study of Middle School Children's Information Security Behavior," *Issues in Informing Science and Information Technology*, (3*)*, pp. 127-135.

Child, D. 2006. *The Essentials of Factor Analysis,* New York, NY: Continuum International Publishing Group.

Compeau, D. R., and Higgins, C. A. 1995. "Computer Self-efficacy: Development of a Measure and Initial Test. *MIS Quarterly*, (19:2), pp. 189-211.

Compeau, D. R., Higgins, C. A., and Huff, S. 1999. "Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study," *MIS Quarterly,* (23:2), pp. 145-158.

Cooper, D. R., and Schindler, P. S. 2006. *Business Research Methods* (9th ed.), New York: McGraw-Hill.

Costello, A., and Osborne, J. 2005. "Best Practices in Exploratory Factor Analysis: Four Recommendations for Getting the Most from your Analysis," *Practical Assessment Research & Evaluation,* (10:7)

Creswell, J. W., and Plano Clark, V. 2007. *Designing and Conducting Mixed Methods Research,* Thousand Oaks, CA: Sage.

Crossler, R., and Belanger, F. 2006. "The Effect of Computer Self-efficacy on Security Training Effectiveness," *Proceedings of the InfoSecD Conference'06*, Kennesaw, GA.

Dhillon, G., and Backhouse, J. 2001. "Current Directions in IS Security Research: Towards Socio-organizational Perspectives," *Information Systems Journal,* (11:2), pp. 127-153.

Dong-Her, S., and Hsiu-Sen, C. 2004. "E-mail Viruses: How Organizations Can Protect their E-mail," *Online Information Review,* (28:5), pp. 356-66.

Garfinkel, S. 2003. "Enabling E-mail Confidentiality through the use of Opportunistic Encryption," *Proceedings of the 2003 Annual National Conference on Digital Government Research,* Boston, MA.

Gist, M. E., and Mitchell, T. R. 1992. "Self-efficacy: A Theoretical Analysis of its Determinants and Malleability," *Academy of Management Review,* (17), pp. 183-211.

Goodhue, D. L., and Straub, D. W. 1991. "Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security," *Information & Management*, (20), pp. 13-27.

Hamill, J. T., Dekro, R. F., and Kloeber, J. M. 2005. "Evaluating Information Assurance Strategies," *Decision Support Systems*, (39), pp. 463-484.

Hill, T., Smith, N. D., and Mann, M. F. 1987. "Role of Efficacy Expectations in Predicting the Decision to use Advanced Technologies: The Case of Computers," *Journal of Applied Psychology*, (72:2), pp. 307-313.

Im, G. P., and Baskerville, R. L. 2005. "Information System Threat Categories: The Enduring Problem of Human Error," *The DATA BASE for Advances in Information Systems*, (36:4), pp. 68–79.

Keeney, R. L. 1999. "The Value of Internet Commerce to the Consumer," *Management Science*, (45:4), pp. 533-542.

Keller, S., Powell, A., Horstman, B., Predmore, C., and Crawford, M. 2005. "Information Security Threats and Practices in Small Businesses," *Information Systems Management*, (22:2), pp. 7-19.

Kuo, F., and Hsu, M. 2001. "Development and Validation of Ethical Computer Self-efficacy: The Case of Softlifting," *Journal of Business Ethics*, (32:4), pp. 299-315.

Lee, D., LaRose, R., and Rifton, N. 2008. "Keeping our Network Safe: A Model of Online Protection Behavior," *Behavior & Information Technology*, (27:5), pp. 445-454.

Levy, Y. 2006. *Assessing the Value of E-learning Systems*, Hershey, PA: Information Science Publishers.

Levy, Y., and Green, B. 2009. "An Empirical Study of Computer Self-efficacy and the Technology Acceptance Model in the Military: A Case of a US Navy Combat Information System," *Journal of Organizational and End User Computing,* (21:3), pp. 1-23.

Lucas, H. C. 1975. "Performance and the Use of an Information System," *Management Science,* (21:8), pp. 908-919.

Marakas, G., Johnson, R., and Clay, F. 2007. "The Evolving Nature of the Computer Self-efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time," *Journal for the Association of Information Systems,* (8:1), pp. 16-46.

Marakas, G. M., Yi, M. Y., and Johnson, R. D. 1998. "The Multi-level and Multifaceted Character of Computer Self-efficacy: Towards Clarification of the Construct and an Integrated Framework for Research," *Information Systems Research*, (9:2), pp. 126-163.

Nenadic, A., Zhang, N., and Barton, S. 2004. "Fair and Certified E-mail Delivery," *Proceedings of the 19th ACM Symposium on Applied Computing, 2004*. Nicosia, Cypress.

Peterson, T. O., and Arnn, R. B. 2005. "Self-efficacy: The Foundation of Human Performance," *Performance Improvement Quarterly*, (18:2), pp. 5-18.

Phelps, D. 2005. "*Information System Security: Self-efficacy and Security Effectiveness in Florida Libraries,"* Retrieved from ProQuest Dissertations & Theses. (ATT 3183102).

Ramim, M., and Levy, Y. 2006. "Securing E-learning Systems: A Case of Insider Cyber Attacks and Novice IT Management in a Small University," *Journal of Cases on Information Technology,* (8:4), pp. 24-34.

Stanton, J., Stam, K., Mastrangelo, P., and Jolton, J. 2005. "Analysis of End User Behavior," *Computers & Security,* (24), pp. 124-133.

Straub, D. 1989. "Validating Instruments in MIS Research," *MIS Quarterly,* (13:2), pp. 147-169.

Teer, F. P., Kruck, S. E., and Kruck, G. P. 2007. "Empirical Study of Students' Computer Security Practices / Perceptions," *The Journal of Computer Information Systems*, (47:3), pp. 105-110.

Torkzadeh, G., Chang, J., and Demirhan, D. 2006. "A Contingency Model of Computer and Internet Self-efficacy," *Information and Management,* (42), pp. 541-550.

Tracy, M., Jansen, W., Scarfone, K., and Butterfield, J. 2007. *Guidelines on Electronic Mail Security.* Gaithsburg, MD: National Institute of Standards and Technology

Whitman, M. 2003. "Enemy at the Gate: Threats to Information Security," *Communications of the ACM,* (46:8), pp. 91-95.

## APPENDIX A - FINAL SURVEY INSTRUMENT

**E-Mail Encryption:** E-mail encryption describes a technique used to obscure electronic messages in transmission from all but the intended recipients (Brown & Snow, 1999). Encryption prevents messages from being read by anyone other than the intended recipient, guarantees that the message sent was not modified during transmission, ensures that a sender is who they claim to be, and verifies the authenticity of the sender. General e-mail does not allow for encryption and so third party plug-in applications are needed to allow for interoperability with popular e-mail clients such as Microsoft Outlook, Eudora, and Netscape Communicator.

---

*Please indicate your confidence in your ability to complete the task specified given each condition by checking a number 1 – 10 after questions 1to 36. Additionally, please provide the requested demographic information for questions 37 to 45.*

---

| | NOT CONFIDENT O | | | | | MODERATELY CONFIDENT O | | | | TOTALLY CONFIDENT O |
|---|---|---|---|---|---|---|---|---|---|---|
| **1. I believe I have the ability to send an encrypted e-mail message because of my current training.** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
| **2. I believe I have the ability to send an encrypted e-mail message if I was adequately trained beforehand.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **3. I believe I have the ability to send an encrypted e-mail message if I received no training on how to do so.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **4. I believe I have the ability to send an encrypted e-mail message if learning to use it was easy.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **5. I believe I have the ability to send an encrypted e-mail message successfully given my current experiences.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **6. I believe I have the ability to send an encrypted e-mail message if I knew what was expected of me.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **7. I believe I have the ability to send an encrypted e-mail message if it is similar to applications I have used before.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **8. I believe I have the ability to send an encrypted e-mail message I had seen e-mail being encrypted before.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **9. I believe I have the ability to send an encrypted e-mail message if I had successfully sent encrypted e-mail before.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **10. I believe I have the ability to send an encrypted e-mail message if the task is not too difficult.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **11. I believe I have the ability to send an encrypted e-mail message if it does not require too much effort.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **12. I believe I have the ability to send an encrypted e-mail message if someone who had done it before assisted me.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **13. I believe I have the ability to send an encrypted e-mail message if someone encourages me to use it.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **14. I believe I have the ability to send an encrypted e-mail message if someone else helped get me started.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **15. I believe I have the ability to send an encrypted e-mail message if someone is there to assist me.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **16. I believe I have the ability to send an encrypted e-mail message if I could get help should I get stuck.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **17. I believe I have the ability to send an encrypted e-mail message if I had just the built in help facility for assistance.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **18. I believe I have the ability to send an encrypted e-mail message if the steps were clearly documented for me.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **19. I believe I have the ability to send an encrypted e-mail message if I had the user guide available.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **20. I believe I have the ability to send an encrypted e-mail message if I tried very hard to do so.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **21. I believe I have the ability to send an encrypted e-mail message if I was older.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **22. I believe I have the ability to send an encrypted e-mail message if I was younger.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **23. I believe I have the ability to send an encrypted e-mail message because of my gender.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **24. I believe I have the ability to send an encrypted e-mail message if I had a lot of time to complete the task.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **25. I believe I have the ability to send an encrypted e-mail message if I had used encryption software in another task before.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **26. I believe I have the ability to send an encrypted e-mail message if the software provided accurate feedback for each task completed.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **27. I believe I have the ability to send an encrypted e-mail message if I was knowledgeable in the use of encrypted e-mail.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **28. I believe I have the ability to send an encrypted e-mail message with no knowledge in the use of encrypted e-mail.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **29. I believe I have the ability to send an encrypted e-mail message because information security is important to me.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **30. I believe I have the ability to send an encrypted e-mail message because I am comfortable using a computer.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **31. I believe I have the ability to send an encrypted e-mail message if the software is not very expensive.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **32. I believe I have the ability to send an encrypted e-mail message if I had no other choice.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **33.I believe I have the ability to send an encrypted e-mail message if encryption software is used by others.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **34. I believe I have the ability to send an encrypted e-mail message if I had to use a mobile device to encrypt.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **35. I believe I have the ability to send an encrypted e-mail message if I consider it beneficial to me.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **36. I believe I have the ability to send an encrypted e-mail message if I had access to the appropriate encryption software.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

**37. What is the number of years you have been using a computer: _____**

**38. Have you used encryption before □ Yes □ No**

**39. Do you currently use encryption □ Yes □ No**

**40. If you use encryption, how do you rate yourself □ Expert □ Average □ Novice**

**41. Do you use social networking tools (Facebook, Twitter, etc.) □ Yes □ No**

**42. What is your gender: □ Male □ Female**

**What is your age: □ < 20 □ 20-29 □ 30-39 □ 40-49 □ 50-59 □ 60 and over**

**What is your Academic Level: □ Sophomore □ Junior □ Senior □ Graduate**

**What is your Major: □ Business □ Health Professions □ Computer and Information Sciences □ Education □ Other**

## APPENDIX B - FACTORS ANALYSIS (PCA) WITH RELIABILITY ANALYSIS

| Factor Name | | Components | | | | Factors Alpha if Item is Deleted |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | |
| Performance Accomplishments and Technical Support | Q12 | .883 | .138 | -.008 | -.007 | 0.949 |
| | Q18 | .857 | .144 | -.043 | .064 | 0.949 |
| | Q15 | .844 | .103 | .010 | .126 | 0.949 |
| | Q16 | .834 | .182 | .028 | .180 | 0.948 |
| | Q27 | .797 | .105 | .003 | .089 | 0.95 |
| | Q9 | .792 | .114 | .119 | .025 | 0.95 |
| | Q11 | .757 | .290 | .097 | .111 | 0.949 |
| | Q19 | .750 | .206 | .045 | .149 | 0.95 |
| | Q4 | .732 | .187 | .073 | -.053 | 0.95 |
| | Q10 | .722 | .291 | .153 | .036 | 0.95 |
| | Q17 | .702 | .226 | .144 | .152 | 0.95 |
| | Q14 | .669 | .362 | .163 | .192 | 0.95 |
| | Q25 | .657 | .244 | .097 | .329 | 0.951 |
| | Q26 | .596 | .166 | .190 | .363 | 0.952 |
| | Q7 | .572 | .262 | .345 | .033 | 0.952 |
| | Q8 | .555 | .301 | .367 | .013 | 0.952 |
| | Q2 | .527 | .216 | .204 | -.048 | 0.954 |
| Goal Commitment and Resource Availability | Q35 | .282 | .838 | .138 | .149 | 0.942 |
| | Q33 | .224 | .814 | .258 | .198 | 0.942 |
| | Q32 | .300 | .810 | .052 | .152 | 0.944 |
| | Q31 | .204 | .789 | .144 | .242 | 0.945 |
| | Q30 | .289 | .788 | .217 | .141 | 0.944 |
| | Q29 | .136 | .772 | .315 | .162 | 0.946 |
| | Q34 | .192 | .676 | .321 | .204 | 0.947 |
| | Q36 | .451 | .637 | .063 | .119 | 0.948 |
| | Q24 | .268 | .545 | .152 | .519 | 0.948 |
| | Q13 | .446 | .532 | .288 | .210 | 0.948 |
| | Q20 | .363 | .527 | .290 | .307 | 0.948 |
| Experience Level | Q5 | .132 | .230 | .823 | .221 | 0.805 |
| | Q1 | .046 | .212 | .819 | .202 | 0.814 |
| | Q3 | .147 | .217 | .762 | .142 | 0.837 |
| | Q28 | .059 | .451 | .594 | .250 | 0.87 |
| Individual Characteristics | Q23 | .129 | .305 | .141 | .841 | 0.884 |
| | Q22 | .104 | .304 | .309 | .767 | 0.881 |
| | Q21 | .095 | .328 | .352 | .756 | 0.861 |
| Cronbach Alpha | | 0.953 | 0.951 | 0.869 | 0.913 | |
| % of Var | | 28.874 | 20.146 | 10.05 | 8.841 | |
| Cumul % | | 28.874 | 49.02 | 59.07 | 67.911 | |

## APPENDIX C - FACTORS AND ITEMS OF CSSE

| Item | Factors | CSSE Item Description |
|---|---|---|
| Q12 | Performance Accomplishments and Technical Support | I believe I have the ability to send an encrypted e-mail message if someone who had done it before assisted me. |
| Q18 | | I believe I have the ability to send an encrypted e-mail message if the steps were clearly documented for me. |
| Q15 | | I believe I have the ability to send an encrypted e-mail message if someone is there to assist me. |
| Q16 | | I believe I have the ability to send an encrypted e-mail message if I could get help should I get stuck. |
| Q27 | | I believe I have the ability to send an encrypted e-mail message if I was knowledgeable in the use of encrypted e-mail. |
| Q9 | | I believe I have the ability to send an encrypted e-mail message if I had successfully sent encrypted e-mail before. |
| Q11 | | I believe I have the ability to send an encrypted e-mail message if it does not require too much effort. |
| Q19 | | I believe I have the ability to send an encrypted e-mail message if I had the user guide available. |
| Q4 | | I believe I have the ability to send an encrypted e-mail message if learning to use it was easy |
| Q10 | | I believe I have the ability to send an encrypted e-mail message if the task is not too difficult. |
| Q17 | | I believe I have the ability to send an encrypted e-mail message if I had just the built in help facility for assistance. |
| Q14 | | I believe I have the ability to send an encrypted e-mail message if someone else helped get me started. |
| Q25 | | I believe I have the ability to send an encrypted e-mail message if I had used encryption software in another task before. |
| Q26 | | I believe I have the ability to send an encrypted e-mail message if the software provided accurate feedback for each task completed. |
| Q7 | | I believe I have the ability to send an encrypted e-mail message if it is similar to applications I have used before. |
| Q8 | | I believe I have the ability to send an encrypted e-mail message if I had seen e-mail being encrypted before. |
| Q2 | | I believe I have the ability to send an encrypted e-mail message if I was adequately trained beforehand. |
| Q35 | Goal Commitment and Resource Availability | I believe I have the ability to send an encrypted e-mail message if I consider it beneficial to me. |
| Q33 | | I believe I have the ability to send an encrypted e-mail message if encryption software is used by others. |
| Q32 | | I believe I have the ability to send an encrypted e-mail message if I had no other choice. |
| Q31 | | I believe I have the ability to send an encrypted e-mail message if the software is not very expensive |
| Q30 | | I believe I have the ability to send an encrypted e-mail message because I am comfortable using a computer. |
| Q29 | | I believe I have the ability to send an encrypted e-mail message because information security is important to me. |
| Q34 | | I believe I have the ability to send an encrypted e-mail message if I had to use a mobile device to encrypt. |
| Q36 | | I believe I have the ability to send an encrypted e-mail message if I had access to the appropriate encryption software. |
| Q24 | | I believe I have the ability to send an encrypted e-mail message if I had a lot of time to complete the task. |
| Q13 | | I believe I have the ability to send an encrypted e-mail message if someone encourages me to use it. |
| Q20 | | I believe I have the ability to send an encrypted e-mail message if I tried very hard to do so. |
| Q5 | Experience Level | I believe I have the ability to send an encrypted e-mail message successfully given my current experiences. |
| Q1 | | I believe I have the ability to send an encrypted e-mail message because of my current training |
| Q3 | | I believe I have the ability to send an encrypted e-mail message if I had received no training on how to do so |
| Q28 | | I believe I have the ability to send an encrypted e-mail message with no knowledge in the use of encrypted e-mail. |
| Q23 | Individual Characteristics | I believe I have the ability to send an encrypted e-mail message because of my gender. |
| Q22 | | I believe I have the ability to send an encrypted e-mail message if I was younger. |
| Q21 | | I believe I have the ability to send an encrypted e-mail message if I was older. |