December 2007

DEVELOPMENT OF AN INFORMATION ASSURANCE AWARENESS ASSESSMENT INSTRUMENT FOR INFORMATION TECHNOLOGY STAFF

Kevin Streff
Dakota State University

Petter Lovaas
Dakota State University

DEVELOPMENT OF AN INFORMATION ASSURANCE AWARENESS ASSESSMENT INSTRUMENT FOR INFORMATION TECHNOLOGY STAFF

Kevin Streff
Dakota State University
kevin.streff@dsu.edu

Petter Lovaas
Dakota State University
lovaasp@pluto.dsu.edu

ABSTRACT

The government continually expresses concern that critical infrastructures are vulnerable to a host of electronic attacks and that people are the front line of defense. No previous academic research quantitatively measures security awareness in an organization. To accomplish this task an instrument must be developed. This study describes the development and administration of such an instrument that other studies can use to measure the level of security awareness in Information Systems staff to determine level of preparedness.

KEYWORDS

Information Assurance, Information Security, Awareness

INTRODUCTION

In the United States, over 85% of the critical infrastructure is owned by the private sector (Chabrow 2002a; 2002b; The Department of Homeland Security 2002; Garten 2002; Verton 2003a). Information assurance is a pivotal factor to secure critical infrastructures and assets, so much so that former President Clinton identified a National Goal to secure these national private-sector information assets and infrastructures in Presidential Decision Directive 63. Presidential Decision Directive 63 (1998) identifies eight key sectors that are extremely vulnerable to attack, including Telecommunications, Electrical Power Systems, Gas and Oil Storage and Transportation, Banking and Finance, Water Supply Systems, Transportation, Emergency Services, and Continuity of Government (Presidential Decision Directive 63 1998). Executive Order 13231 (2001) identifies several other critical sectors, including Manufacturing, Shipping, and Food.

Several researchers have purported socio-technical approaches to secure system development and information protection in general (Baskerville 1991; Siponen 2005). As such, employees have a role to playing in protecting these critical infrastructures by being aware of the importance of security and of the

techniques attackers use to exploit human, process, and technological vulnerabilities. People are said to be the front line of defense against attack (Marks 2002). "Your front line of defense needs to be properly trained for the safety of both the company and their personal well being" (Halbig 2004 p. 2). In 2002, the U.S. Department of Agriculture published a fact sheet entitled *Keep America's Food and Agriculture Safe* and stated "you [people] are the front line of defense in protecting America's food supply system" (*Keep America's Food and Agriculture Safe* 2002 p. 1). Homeland Security Secretary Tom Ridge has declared that people are the "front line of defense for protecting America's food and agriculture" (Stump 2003 p. 1). Homeland Security Presidential Directive (HSPD-9) acknowledged awareness as a key factor to carry out this directive as the directive explicitly stated developing awareness to recognize threats as one of the five key efforts the food sector should focus resources on. The information assurance awareness level of organizations and industries is not understood. A well-trained, security-conscious front line can help protect the organization against social engineering, accidental breaches, unnecessary exposures, and generally provide a layer of defense that attackers must compromise to penetrate the organization's critical assets and infrastructures (Homeland Security Presidential Directive/Hspd-9 2004). By developing, administering, and analyzing the results of an IS Information Assurance Awareness Survey, this research developed a reliable instrument that can be used in future studies to measure the level of security awareness in organizations and industries. In particular, this study focused on Information Systems (IS) staff who develop and support much of the technology-based infrastructure that organizations are so dependent upon.

RATIONAILE FOR THE STUDY

A security-conscious workforce goes a long way to protecting the food supply during production and distribution; however, do organizations and governments truly understand the state of security awareness in the food sector? Do differences exist in age, education level, length of time with company, length of time in the food industry, amount and timing of security training, or classification as management or nonmanagement affect the level of security awareness in one large food organization? This research study developed an information assurance awareness instrument to measure the level of security knowledge in IS staff.

PURPOSE OF THE STUDY AND RESEARCH QUESTIONS

The purpose of the study was to establish an IS Information Assurance Awareness Survey instrument to measure security awareness in IS staff that can be used in additional studies by other researchers. The case study included one large company in the food industry; however, the instrument is universal and can be used in other industries. The instrument was flexible enough so that researchers could investigate the potential differences between management/nonmanagement, length of time with company, length of time in the food industry, education level, age, and the level of security awareness in IS staff. These research questions were important as they sought answers to how a company could improve security awareness in their organization. For example, if the study determined that those employees who have worked in the food industry for more than ten years significantly outperformed those who have worked in the food industry for less than ten years, then hiring practices for IS staff might include an industry tenure component. The purpose and research questions of this study were significant and an effective design for the research study was necessary. This topic is explored next.

RESEARCH DESIGN AND PROCEDURES

In developing the information assurance awareness survey, International Information Systems Security Certification Consortium, Inc. (ISC)² was leveraged because of its significant experience in the area of

security vulnerabilities and information assurance awareness and training programs. (ISC)² has authored the ten domains of the Common Body of Knowledge (Hansche, Berti, & Hare 2004). These ten domains served as the basis for the Information Assurance Awareness Instrument developed and administered in this study.

1	Information Security Management
2	Security Architecture and Models
3	Access Control Systems and Methodology
4	Applications and Systems Development
5	Operations Security
6	Cryptography
7	Physical Security
8	Telecommunications, Network, and Internet Security
9	Business Continuity Planning
10	Law, Investigations, and Ethics

Table 1. Ten Domains of the Common Body of Knowledge

From these ten domains, questions were asked via a focus group of information security experts regarding the importance of each domain. For example, are all the domains of equal importance? Table 2 highlights the results of weighting that one large food company determined after much deliberation and consultation:

1	Information Security Management	Maximum
2	Security Architecture and Models	Medium
3	Access Control Systems and Methodology	Maximum
4	Applications and Systems Development	Maximum
5	Operations Security	Maximum
6	Cryptography	Low
7	Physical Security	Maximum
8	Telecommunications, Network, and Internet Security	Maximum
9	Business Continuity Planning	Low
10	Law, Investigations, and Ethics	Maximum

Table 2. Weighted Domains of the Common Body of Knowledge

Therefore, more questions were provided on the survey in domain 1 (five questions) than domain 2 (three questions). The questionnaire was optimized to gather valid responses. Consequently, the questions were short and clear. Several security questionnaires exist that would take a respondent hours to complete (Krauss 1972), limiting the response rate necessary for this research study. The questionnaire developed by this research study required approximately 20 minutes to complete. In all, 8 demographic and 42 information assurance awareness questions were developed and included on the instrument.

Respondents were provided a brief introduction to the purpose of the research study at the beginning of the questionnaire to provide them context to answer questions and to ensure that they felt that they were not wasting their time in providing responses. The IS Information Assurance Awareness Survey was validated by a panel of experts in the security field.

A pilot test with five students enrolled in technology-related programs at Dakota State University ensured that the questions on the survey were understandable and written clearly. Because the researcher works at Dakota State University, he had access to a student base that represents IS employees who ultimately completed the survey. The Information Assurance Awareness Assessment Instrument was modified based on feedback from the pilot test.

INSTRUMENTATION RELIABILITY AND VALIDITY

Straub (1989) points out that a lack of validated measures in instrumentation raises the specter that no single finding in the study can be trusted. Hunter, Schmidt, and Jackson (1983) suggested that greater attention to instrument validation promotes cooperative research efforts. Straub (1989) expressed concern that MIS research lacked instrumentation validation (Straub 1989). While Boudreau and other key researchers (2001) extended Straub's research and identified an across the board improvement in all instrument validation processes (Boudreau, Gefen, & Straub 2001), they also conclude that instrument validation still has "ground to cover to make more rigorous and credible the instruments," including pre-testing instruments. Alreck and Settle (1995) defined *pre-test* as a preliminary trial of some or all aspects of the instrument to ensure that there are no unanticipated difficulties (Alreck & Settle 1995). Fowler (1984) suggested that every instrument should be pre-tested. The researcher used a pre-test with five students enrolled in technology-related programs at Dakota State University to ensure that the questions on the survey were understandable and written clearly. Because the researcher works at Dakota State University, he had access to a student base that represents the IS employees at Company XYZ who ultimately completed the survey. The Information Assurance Assessment Instrument was modified based on feedback from the pre-test.

Case studies lag behind other studies with respect to most validation criteria (Boudreau, Gefen, & Straub 2001). Because the survey encouraged self-selection, potential threats to internal validity resulted (Ryan, et al. 1998). Cronbach's α, which addresses instrument reliability, (Cronbach 1971) is the most popular technique to assess instrument reliability (Boudreau, Gefen, & Straub 2001) and the researcher used this technique to assess the IS Information Assurance Awareness Instrument.

Content validity is the degree in which items of an instrument reflect the content universe to which the instrument will be generalized (Cronbach 1971). Content validity is primarily stabled through literature reviews and expert judges or panels (Rogers 1995). The researcher conducted a thorough literature review (Streff 2004) and used a group of experts to review and revise each question on the instrument. The expert group was also leveraged to identify weightings of the ten domains to ensure the content of the instrument reflected reality. Content validity also concerns itself with representative questions (Kerlinger 1964) and the expert group was put in place to enhance content validity.

Construct validity is the extent in which the instrument measures the concepts that it purports to measure (Zaltman et al. 1973) and the researcher employed statistical techniques to address these concerns. Internal validity which looks at rival hypotheses for observed effects (Jarvenpaa et al. 1984) and the researcher did not take this into consideration.

Ives, Olson, and Baroudi (1983) stressed that the length of the instrument can tax respondents' concentration or motivation if not carefully planned. The researcher addressed these concerns two ways: First, the questionnaire developed by this research study required approximately 20 minutes to complete. Respondents were provided a brief introduction to the purpose of the research study at the beginning of the questionnaire to provide them context to answer questions and to ensure that they felt that they were not wasting their time in providing responses. Second, to encourage participation in the study and

completion of the survey, respondents were entered into a drawing where they had an opportunity to win a $50 gift certificate via a random drawing.

CONCLUSION

When measuring security awareness an organization may discover a need to formalize a security awareness and training program. This study developed an instrument that organizations can use to measure information assurance awareness in IS staff. Organizations today have no way of benchmarking their level of information assurance awareness and this instrument arms organizations to do just that for their IS staff.

RECOMMENDATIONS

There is little doubt that the real value of this research study is the IS Information Assurance Awareness Survey that was created through the process. Of value would be utilizing this new instrument at a variety of companies, including those involved in the critical infrastructure protection highlighted in PDD-63. For example, if many food companies could take the survey, a food company could compare itself to other food companies and determine where they stand with regard to security awareness. Food companies could possibly compare its results to that of the medical industry to really begin to understand how ready an industry is to defend against attack. Repeating the study with non-information-systems employees at Company XYZ would also be valuable; however, the instrument must be refined for a non-technical audience. A future research study could refine the instrument used in this research study for the non-technical audience and publish the results. Repeating the study in other critical sectors, including banking and finance, oil and gas, and transportation would also be valuable, as security awareness in these sectors has not been quantified.

REFERENCES

Alreck, P. A. and Settle, R. B. *The Survey Research Handbook*, Second Edition, Irwin, Chicago, 1995.

Baskerville, R. "Information Systems Security Design Methods: Implications for Information Systems Development," *ACM Computing Surveys (CSUR)* (25:4), 1993, pp. 375–414.

Boudreau, M., Gefen, D., and Straub, D. W. "Validation in Information Systems Research: A State-of-the-art Assessment," *MIS Quarterly* (25:1), March 2001, pp. 1–16.

Chabrow, E. "Businesses Urged to Share," *Insurance & Technology (27:8),* 2002a, p. 14.

Chabrow, E. "Businesses Urged to Share Data About Security Holes," *InformationWeek* (888), 2002b, p. 36.

Cronbach, L. J. "Test Validation in Educational Measurement. American Council on Education," in R.L. Thorndike (ed.), Washington, DC, 1971, pp. 443–507.

Detmar W. S. "Validating Instruments in MIS Research," *MIS Quarterly* (13:2), June 1989, pp. 147–169.

"Executive Order 13231," *Federal Register* (86), October 18, 2001, pp. 53063–53071.

Fact Sheet on FDA's New Food Bioterrorism Regulation, (2003).,www.cfsan.fda.gov/%7Edms/fsbtac12.html, February 16, 2004.

Fowler Jr., F.J. *Survey Research Methods*, Sage Publications, Beverly Hills, CA, 1984.

Gall, M. D., Borg, W. R., and Gall, J. P. *Educational Research: An Introduction*, Sixth Edition, Addison-Wesley, Reading, MA,.1996

Garten, J. E. "Homeland Security Could Really Shake Up Business," *Business Week* (3797:24), 2002.

Halbig, W. W.. *What is Your First Line of Defense?* (2004), www.nisws.com/article013.html, February 4, 2004.

Hansche, S., Berti, J., and Hare, C. *Official (ISC)2 Guide to the CISSP Exam*, Auerbach, Boca Raton, FL, 2004

HHS Creates Food Security Research Program, Increases Import Exams More than Five Times to Protect Nation's Food Supply, (2003), http://www.hhs.gov/news/press/2003pres/20030723.html, February 17, 2004.

Homeland Security Presidential Directive/Hspd-9, *Defense of United States Agriculture and Food*, http://www.whitehouse.gov/news/releases/2004/02/text/20040203-2.html, January 30, 2004.

Hunter, J.E., Schmidt, F.L., and Jackson, G.B. *Meta-Analysis: Cumulating Research Findings Across Studies*, Sage Publications, Beverly Hills, CA, 1983

Ives, B., Olson, M. H., and Baroudi, J. J. "The Measurement of User Information Satisfaction," *Communications of the ACM*, (26:10), 1983, pp. 785–793.

Jarvenpaa S.L., Dickson, G.W. and DeSanctis G.L. "Methodological Issues in Experimental IS Research: Experiences and Recommendations," *Proceedings of the Fifth International Information Systems Conference*, Tucson, AZ, November 1984, pp. 1–30.

Kerlinger, F.N. *Foundations of Behavioral Research*, Holt, Rinehart, and Winston, New York. 1964.

Krauss, L. *SAFE: Security Audit and Field Evaluation for Computer Facilities and Information Systems,* Firebrand, New Jersey,. 1972.

Marks, P. "Airport Security to Grow," *The Hartford Courant*, February 3, 2002.

Presidential Decision Directive 63, "Critical Infrastructure Protection: Sector Coordinators, Presidential Decision Directive 63," *Federal Register* (63:150), August 5, 1998, p. 41804.

Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (3448), 2002.

Rogers, T.B. *The Psychological Testing Enterprise,* Brooks/Cole Publishing Company, Pacific Grove, CA, 1995.

Ryan A. M., Ployhart R. E., Gregaras G. J., and Schmit M. J. Test Preparation Programs in Selection Contexts: Self-selection and Program Effectiveness, *Personnel Psychology* (SI:51), 1998, pp. 599–621.

Siponen, M. "An Analysis of the Recent IS Security Development Approaches: Descriptive and Prescriptive Implications," in *Information Security Management: Global Challenges in the New Millennium*, G. Dhillon (ed.), Idea Group, Hershey, PA,. 2001.

Strohm, C.. *Homeland Security Critical Infrastructure Effort Proceeds Unevenly*, (2004), www.govexec.com/dailyfed/0204/020904c1.htm, February 8, 2004

Stump, J..*Food Security—Protect and Prevent*. , from (2003) www.vdacs.state.va.us/foodsafety/advisory.html, February 1, 2004.

"The Department of Homeland Security," *The Department of Homeland Security*, Washington, DC, 2002.

Verton, D. "Protection of Critical Systems Still Haphazard," *Computerworld* (37:36), 2003a, p. 4.

Verton, D. "Regulatory Requirements Place New Burdens on IT: Calif. Privacy Law to Debut; Panic Emerging," *Computerworld,* (37:26), 2003b, p. 1.

Yin, R. K. *Case Study Research, Design and Methods*, Second Edition, Sage, Newbury Park,.1994.

Zaltman, G, Duncan, R and Holbek, J *Innovations and Organizations*, John Wiley, New York, 1973.