5-2008

Research in Progress: Evaluating the Role of Risk Models in Information Assurance

Kerry W. Ward
University of Nebraska at Omaha, Kward@mail.uomaha.edu

Jackie Rees
Purdue University, jrees@purdue.edu

Prince G. Adu
University of Nebraska at Omaha, padu@mail.unomaha.edu

Research in Progress: Evaluating the Role of Risk Models in Information Assurance

Kerry W. Ward
University of Nebraska at Omaha
Kwward@mail.uomaha.edu

Jackie Rees
Purdue University
jrees@purdue.edu

Prince G. Adu
University of Nebraska at Omaha
padu@mail.unomaha.edu

ABSTRACT

Traditionally, organizations have approached the protection of valuable assets from a risk management perspective and applied a variety of models to protect the organization from losses. The intangible nature of information and the unknown threats to such information assets have given rise to questions concerning whether traditional approaches to risk management are sufficient for the domain of information assurance. This paper discusses the issues of applying traditional risk models to the domain of information assurance and proposes a focus group approach to determine what approaches to risk management are actually being used in practice and whether traditional risk management models are appropriate for information assurance.

KEYWORDS

Risk Management, Information Assurance, Security

INTRODUCTION

With the global expansion of markets and the evolution of the information age, organizations are increasingly information dependent and vulnerable to the loss of their information assets. Traditionally, the approach to managing threats to valuable assets has been referred to as risk management while the process of protecting information assets is referred to as information assurance (IA). There has, however, been discussion as to whether traditional approaches to risk management adequately address risk in an information assurance domain (See for example, Blackley, McDermott, and Geer 2002; Covert and Nielsen 2005; Layton and Wagner 2007; Sun, Srivastava and Mock 2006).

This paper provides an overview of the issues in applying traditional risk approaches to assess the risks associated with information assets. The formal research question addressed in this paper is: Are traditional risk assessment approaches applicable to information assurance? We propose using focus groups to determine what approaches are actually being used in practice and how effective these models are perceived to be.

RISK MANAGEMENT IN THE INFORMATION ASSURANCE DOMAIN

Risk is managed via the application of risk models following a basic formula that identifies assets and threats to those assets, assigns a probability to a threats' occurrence and then multiplies this probability by the value of the asset. The applicability of the traditional risk models to information assurance is being challenged in all three of the risk management processes: identifying assets and threats, determining the likelihood of occurrence, and in determining the value of loss.

First, the application of traditional risk models to IA is being challenged due to the perceived difficulties in assessing threats to information. The interaction of people, hardware, and software designed to openly create and move information, creates a complex interaction that allows for a multitude of unknown

exploits to exist in any given system. Malicious attackers, both internal and external to the organization, are an adaptive threat that learns from past mistakes and failures and continue to seek out new modes of attack and new vulnerabilities. With information technology, increasingly complex and valuable information can be collected, stored, and analyzed by organizations, and the value and threats to this information is often poorly understood or simply not assessed.

Second, the probabilities of many information security incidents are virtually unknown and the likelihood of a potential security breach or damage is very difficult to quantify. If the likelihood of occurrence is based on past experience, managers cannot account for new types of attacks or vulnerabilities that have not yet been discovered; this is referred to as the zero-frequency problem (Hope, Lavenhar, and Peterson 2005). Thus a traditional risk model is unlikely to accurately reflect the probability of a threat in the information assurance domain (Black 2003; Blackley et al. 2002; Covert and Nielsen 2005).

Third, even if we can identify the threats and provide some likelihood of it occurring, there is still an issue of assigning value to the information asset. Historically, the most valued assets in organizations were something physical, like gold, diamonds, or money. Such physical assets are relatively easy to assign a value to as well as secure. Today, however, the most valuable assets are frequently intangible, such as intellectual property or information (Parker 2001). This type of intangible asset is difficult to value and if lost or compromised, difficult to recover.

In view of the above analysis there are reasons to be concerned with applying traditional risk management models to the information assurance domain. Many sophisticated risk management models have been applied over the years to address the essential elements of information assurance but there is an argument that they still fall short of providing an accurate picture of risk to managers. There is therefore the need for further research to be done on risk management in information assurance in order to determine whether traditional models of risk management apply to the information assurance domain. .

PROPOSED METHODOLOGY

Due to the exploratory nature of the research question, this research proposes a series of focus groups. A focus group is an exploratory method that is appropriate to use when a researcher wants to gain general background information about an issue or when the researcher wants to generate research questions and hypotheses that can be used to design and conduct quantitative research (Calder 1977; Cooper and Schindler, 2006; Kerlinger and Lee, 2000). Both of these situations are the case here. First, while several references have indicated issue with applying the traditional risk models to the information assurance domain, there is a dearth of research on the topic. Therefore one of the goals of this research is to explore the issue and to gain general background information. A second goal of this research is thus to generate more specific research questions and hypotheses and to develop potential measures (survey questions, etc.) that can be used to conducted more detailed quantitative research.

The purpose of a focus group is to examine the participants' attitudes and behaviors and to find out what people think about the topic being discussed (Kerlinger and Lee, 2000) For our purposes, we will be investigating what risk management approaches, if any, they are using for information assurance and whether they are applying any alternative approaches for the three main processes (asset and threat identification, likelihood of occurrence, and valuation of potential loss) to the information assurance domain. Additionally we will ascertain participants' opinions about whether the traditional risk management models are adequate for information assurance, including asking why and how they may or may not be adequate.

Currently three focus groups are being considered: one to be conducted in Omaha, Nebraska, one in Chicago, Illinois, and a third in Indianapolis, Indiana. A focus group needs to be large enough to get a diversity of thoughts, but small enough to allow each person to participate (Kerlinger and Lee, 2000) and therefore our focus groups will include seven to ten participants in each group (Krueger, 1994). The targeted participants are high ranking officers responsible with either risk management or information assurance oversight responsibilities. A semi-structured script will be used to ensure consistency of issues

addressed across the three groups. The groups will be recorded and transcribed for data analysis purposes.

CONCLUSION

This research is exploratory in nature designed to better understand whether traditional risk models apply to the domain of information assurance. This research will provide insight into current industry practice by conducting focus groups with individuals responsible for managing risk associated with information. Specifically we hope to gain insight into whether current management practice is to apply existing risk management models to information assurance and if so, what models they are applying. If not, we hope to ascertain why not and whether alternative approaches are being applied. A final contribution of this research is the use of focus groups in the MIS domain. Few studies have been conducted in IS that apply this methodology. The goal of this research is to gain background information and to develop hypotheses and measures for future research.

REFERENCES

Blakley, B., McDermott, E. and Geer, D. "Information Security is Information Risk Management," Proceedings of the 2001 Workshop on New Security Paradigms, Cloudcroft New Mexico, 2001 pp. 97-104.

Black, R. "Quality Risk Analysis," Rex Black Consulting (RBC), 2003. Retrieved at http://www.rexblackconsulting.com/publications/Quality%20Risk%20Analysis1.pdf

Calder, B,J. (1997) "Focus Groups and The Nature of Qualitative Research," Journal of Marketing Research, 14, 353-364.

Cooper, C. and Schindler, P.S. Business Research Methods, (9th Edition) McGraw-Hill, New York, NY 2006.

Covert, E., and Nielsen, F. "Measuring Risk Using Existing Frameworks," *EDPACS* (32:10), April 2005, pp. 1-7.

Hope, P., Lavenhar, S., and Peterson, G. "Architectural Risk Analysis," U.S Department of Homeland Security, Build Security in Setting a Higher Standard for Software Assurance, 2005. Retrieved at https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/architecture/10.html

Kerlinger, Fred N. and Lee, Howard B. Foundations of Behavioral Research, (4th Edition) Wadsworth/Thomson Learning, U.S., 2000.

Krueger, R. A. Focus Groups: A Practical Guide for Applied Research, Sage Publications, (2nd. Ed.), Thousand Oaks, CA, 1994.

Layton, M., and Wagner, S. "Traditional Risk Management Inadequate To Deal with Today's Threats," *International Risk Management Institute*, March 2007. Retrieved at http://www.irmi.com/Expert/Articles/2007/Deloitte03.aspx

Parker, X. L, "Understanding Risk," *The Internal Auditor* (58:1), February 2001, pp. 61-65.

Sun, L., Srivastava, R. P., and Mock, T. J. "An Information Systems Security Risk Assessment Model Under the Dempster–Shafer Theory of Belief Functions," *Journal of Management Information Systems* (22:4), 2006, pp. 109–142.