House of Security:
Locale, Roles and Resources for Ensuring Information Security

Wee Horng Ang
Yang W. Lee
Stuart E. Madnick
Dinsha Mistress
Michael Siegel
Diane M. Strong
Richard Y. Wang
Chrisy Yao

Working Paper CISL# 2006-08

August 2006

Composite Information Systems Laboratory (CISL)
Sloan School of Management, Room E53-320
Massachusetts Institute of Technology
Cambridge, MA 02142

House of Security: Locale, Roles and Resources for Ensuring Information Security

Research-in-Progress

Wee Horng Ang
Massachusetts Institute of Technology
weeang@mit.edu

Yang W. Lee
Northeastern University
y.lee@neu.edu, ylee@mit.edu

Stuart E. Madnick
Massachusetts Institute of Technology
smadnick@mit.edu

Dinsha Mistress
Massachusetts Institute of Technology
dmistree@mit.edu

Michael Siegel
Massachusetts Institute of Technology
msiegel@mit.edu

Diane M. Strong
Worcester Polytechnic Institute
dstrong@wpi.edu

Richard Y. Wang
Massachusetts Institute of Technology
rwang@mit.edu

Chrisy Yao
Suffolk University
yyao@suffolk.edu

ABSTRACT

In this paper we redefine information security by extending its definition in three salient avenues: locale (beyond the boundary of an enterprise to include partner organizations), role (beyond the information custodians' view to include information consumers' and managers' views), and resource (beyond technical dimensions to include managerial dimensions). Based on our definition, we develop a model of information security, which we call the House of Security. This model has eight constructs, Vulnerability, Accessibility, Confidentiality, IT Resources for Security, Financial Resources for Security, Business Strategy for Security, Security Policy and Procedures, and Security Culture. We have developed a questionnaire to measure the assessment and importance of information security along these eight aspects. The questionnaire covers multiple locales and questionnaire respondents cover multiple roles. Data collection is currently in process. Results from our analysis of the collected data will be ready for presentation at the conference.

Keywords

Information security, Security vulnerabilities, Information confidentiality, Security policy, Security procedures, Security culture

INTRODUCTION

In today's world, business is increasingly globalized and work is increasingly virtual and collaborative. For effective work and successful business, security of information and networks is a must. The locale for information security goes beyond a single enterprise or an organization. It encompasses an extended enterprise that includes partner organizations, e.g., supplier and customer organizations, beyond the boundary of a single enterprise. As such, the roles associated with information security include all stakeholders across the extended enterprise including partner organizations, the general public, and hackers since anyone can have access to various networks. Furthermore, the resources need to ensure information security go beyond technical solutions to include managerial and financial resources. Information security goes beyond the boundaries, roles and resources traditionally considered, to encompass other dimensions that are recognized by information consumers and managers.

Much of the current literature on information security, however, has taken a much narrower view, focusing on specific information security tools, such as firewalls (Oppliger 1977; Zwicky, Cooper et al. 2000; Cheswick, Bellovin et al. 2003), encryption (Needham and Schroeder 1978; Dolev and Yao 1983; Boneh and Franklin 2003), and antivirus technology (Kephart, Sorkin et al. 1997; Furnell 2004). There are few empirical studies on information security and little good advice for management (Kotulic and Clark 2004), with a few notable exceptions, e.g., (Straub and Welke 1998) which focuses on organization-level security planning models. Our research addresses this paucity of managerially relevant empirical research.

RESEARCH MODEL

Good information security, according to our definition, provides *Accessibility* to data and networks to appropriate users while simultaneously protecting *Confidentiality* of data and minimizing *Vulnerabilities* to attacks and threats. To ensure information security, good security practices also go beyond technical solutions. Good security practice is driven by a *Business Strategy* with associated *Security Policies and Procedures* implemented in a *Culture of Security*. These practices are supported by *IT Resources* and *Financial Resources* dedicated to ensuring information security. These eight constructs form what we call the "House of Security" (see Figure 1).

The first three constructs, providing Accessibility, protecting Confidentiality, and minimizing Vulnerabilities, capture the goals involved in information security, and thus are our dependent variables. All of these have been mentioned in some form the literature, e.g., (Klein 1993; McCumber 2005). They are defined below:

1. Vulnerability: Potential for data and networks to be tampered with, attacked, or destroyed
2. Accessibility: Availability of data and networks to appropriate users
3. Confidentiality: Protection of confidential corporate data and privacy of data about individuals

The next five constructs capture the security practices that contribute to highly security information, and thus are our independent variables. Although most of these have been mentioned in the literature, we found no study with all five. They are defined below:

4. Information Technology (IT) Resources for Security: IT Resources for supporting data and network security practices
5. Financial Resources for Security: Financial Resources for supporting data and network security practices
6. Business Strategy for Security: Business Strategy for setting the direction and agenda for data and network security practices
7. Security Policy and Procedures: Stated data and network security rules and procedures
8. Security Culture: Supporting environment for implementing data and network security practices

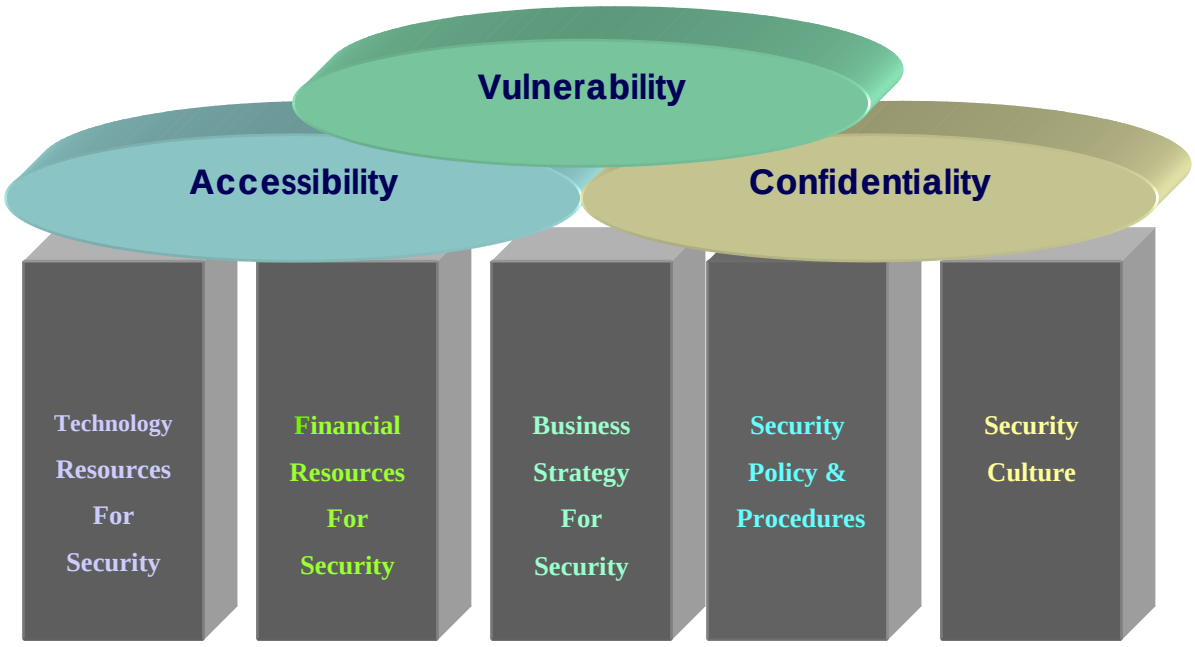


Figure 1: Eight Constructs Organized as the House of Security

Locale

The locale for information security captures the concept that information security cannot be limited to the boundaries of a single enterprise. In this research, we conceptualize locale as encompassing three environments, *within the enterprise*, the

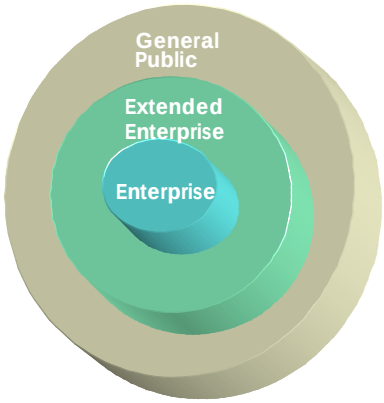
extended enterprise encompassing partner organizations involved in the organization's daily functioning, and the *general public* which includes customers of the company as well as government policy makers and regulators (see Figure 2a). These locales provide the context for understanding the stakeholders or roles involved in information security.

Role

Every organization, especially large organizations, has many different stakeholders – often with differing needs and perceptions. It is important to identify the various stakeholders related to information security. A broad view can be seen in Figure 2a, where information security stakeholders can be classified into three different locales: Within the Enterprise, the Extended Enterprise and the General Public.

The first subset of stakeholders, within the enterprise, can be further stratified based on the role and rank of the individual within the organization, as illustrated in Figure 2b. The stratification is classified into two dimensions. The first dimension is the domain or role: General Employee, IT-related Personnel, and General Security (i.e., non-IT related), such as security guards. The second dimension is the level or rank: ranging from top executives, to line or middle managers, to professionals or other general workers in the organization.

(a) Locales of Extended Enterprise Security



(b) Stakeholders & Roles

	Domain/Role			
Level/Rank	General business	IT Organization	General security/ physical security	Partners (Extended Enterprise)
Top exec	CEO, CFO, …	Top IT Mgt/CIO	Top Security Mgt / CSO	
Line/middle manager	Business unit manager	IT non-security managers --- IT security manager	Security managers	
Workers	Business personnel	IT non-security personnel --- IT security personnel	Security personnel (e.g., guard)	

Figure 2: Information Security Locales and Stakeholders

The extended enterprise encompasses partner organizations involved in the organization's daily functioning. These organizations can be directly supporting daily business operations, such as materials or services suppliers, or can have indirect organizational links, such as banks or financial companies. Most organizations have vested interests in the security status of their partners for many reasons, such as to ensure that their organization's information security is not compromised. The general public category includes customers of the company as well as government policy makers and regulators.

Resource

The resources needed to ensure information security include all five of our independent variables. That is, resources are not only IT and financial resources, but also business strategies for security, security policies and procedures, and the security culture. According to our House of Security model, all these resources work together to ensure information security.

METHOD

Our method is a questionnaire designed to gather information about the eight constructs in our House of Security model, across the roles and locales involved in extended enterprise information security.

Developing the House of Security Model

The House of Security research model was developed from simultaneously gathering exploratory data from security stakeholders and examining the literature. We used empirical data to develop the eight constructs in the research model because the available literature did not adequately address security from a managerial and stakeholder perspective and did not adequately consider the stakeholders in the extended enterprise. The exploratory data collection to form the model involved three questionnaires. The first was completely open, asking what holistic security meant to the security stakeholder completing the questionnaire. This questionnaire was administered to twenty security professionals. The second questionnaire builds on the first, by asking the same question, but prompting the respondent with some of the security aspects obtained from the first questionnaire. This was administered to another twenty-five security professionals. The third questionnaire was administered to these same twenty-five professionals. It was a semi-structured questionnaire with thirteen questions covering issues related to improving security and costs and benefits of security practices. Data from these questionnaires, supported by a review of the literature, provided the basis for the House of Security model and the questionnaire items for measuring these constructs.

Developing the House of Security Questionnaire

Questionnaire development for the House of Security questionnaire followed standard procedures. A number of items were generated by the researchers for each construct. These items were based on the definitions of the constructs and were informed by the responses to the first three questionnaires. These items were reviewed by three other security researchers for construct coverage and answerability. Items were revised and eliminated until there were five good items per construct. These were used in the pilot questionnaire. The pilot questionnaire was administered to a small group of twenty security professionals, resulting in minor revisions to the wording of questions. It was then administered to approximately seventy five professionals to provide data for testing the reliability and validity of the constructs. This construct testing is in process now.

Analyzing Performance, Inter-Enterprise, and Role Gaps

The questionnaire is designed to collect the data needed to perform gap analysis. First, the questions are asked for the locale of within the enterprise in two forms, an assessment of the level of security along that security aspect and an assessment of the importance of that security aspect for information security within the enterprise. From these data, we will perform an analysis of the gaps between assessment and importance, which we call performance gaps. Second, these two forms are also asked about a partner organization. From these data, we will perform an analysis of the differences in security between the enterprise and its extended enterprise, which we call inter-enterprise gaps. Third, the questionnaire respondents will cover the variety of stakeholders in Figure 2b. By comparing responses from different stakeholder groups, we will be able to examine the differing views of information security across stakeholders, which we call role gaps. Gap analysis provides information management for determining where to focus information security improvement efforts.

Testing the House of Security Model

In addition to gap analysis, we will also test the House of Security model. Starting with correlation analysis, we will examine relationships among the eight constructs to further understand how each construct and group of constructs impacts other constructs.

CONCLUSION

Our House of Security model addresses limitations of the current literature on information security, which focuses primarily on technologies and tools for ensuring information security. Our research will provide the evidence and understanding managers need to promote a better and more comprehensive information security strategy, policy, procedures, and culture.

By the time we present this paper in August, we will have collected more data with a refined data collection instrument and will have analyzed these data. We will present the empirical evidence for the House of Security model and explain analytical results for each of the security construct. We will also present gap analysis results, i.e., security assessment and importance gaps across roles and enterprises, and the performance gap indicated by differences in assessment and importance ratings. These gap analysis results will be the basis for providing descriptive data findings about the comparative effects of role, locale, and resource.

REFERENCES

1. Boneh, D. and M. Franklin, M. (2003) Identity Based Encryption From the Weil Pairing, *Siam Journal of Computing*, 32, 3, 586-615.
2. Cheswick, W. R., Bellovin, S. M. et al. (2003) *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley.
3. Dolev, D. and Yao, A. (1983) On the Security of Public Key Protocols, *IEEE Transactions on Information Theory*, 29, 2, 198-208.
4. Furnell, S. (2004) Cyber Threats: What Are the Issues and Who Sets the Agenda? SGIR Conference.
5. Kephart, J., Sorkin, G., et al. (1997) Fighting Computer Viruses, *Scientific American*, November.
6. Klein, S. A. (1993) Information Security Considerations in Open Systems Architectures, *IEEE Transactions on Power System*, 8, 1.
7. Kotulic, A. G. and Clark, J. G. (2004) Why there aren't more information security research studies, *Information & Management*, 41, 597-607.
8. McCumber, J. (2005) *Assessing and Managing Security Risk in IT Systems*, Auerbach Publications.
9. Needham, R. M. and Schroeder, M. D. (1978) Using Encryption for Authentication in Large Networks for Computers, *Communications*, 21, 12, 993-999.
10. Oppliger, R. (1977) Internet Security: Firewalls and Beyond, *Association for Computing Machinery*, 40, 5, 92-103.
11. Straub, D. W. and Welke, R. J. (1998) Coping with Systems Risk: Security Planning Models for Management Decision Making, *MIS Quarterly*, 22, 4, 441-464.
12. Zwicky, E., Cooper, S., et al. (2000) *Building Internet Firewalls*, O'Reilly & Associates.