8-15-1997

Determinants of Computer Security Practices

Amit Das
Nanyang Technological University, aadas@ntu.edu.sg

Determinants of Computer Security Practices

Amit Das
Nanyang Business School, Nanyang Technological University, Singapore 639798
aadas@ntu.edu.sg

Abstract

A survey of computer security practices at 67 medium and large organizations in Singapore shows that the level of computer security practices at these organizations is predicted better using their needs for confidentiality, integrity and availability rather than through a more traditional risk assessment methodology.

Introduction

As computers become more pervasive in every field of human activity, the security of information stored on them becomes a societal concern. Increasingly, computers are used to store data that may be considered sensitive (e.g. medical records, credit ratings, and trade secrets). Unauthorized access to such data renders the individuals and firms about whom data is stored vulnerable to embarrassment, discrimination, and even extortion. Secondly, computers are often embedded in the operation of mechanical and electrical equipment (e.g. electronic locks on doors, telephone switches, traffic control systems, and medical equipment), whose malfunction due to hardware / software failure poses serious threats to public safety. Finally, the potential for abuse has multiplied significantly in a networked environment wherein physical proximity to a computer is no longer a requirement for operating the computer - all that is needed is a connection to the machine over some combination of public and private networks.

Efforts devoted to securing the ever-increasing amounts of information stored on computers have not kept up with the higher levels of threats. According to a recent Datapro (1996) survey, organizations continue to spend less than 5% of their information technology (IT) budget on security measures. According to the same survey, the percentage of organizations that have explicit security policies aimed at protecting their information resources has dropped from 82% in 1992 to 54% in 1996. While some of this decline may be attributed to the falling costs of computers themselves (perhaps rendering them less worthy of protection), the same argument cannot be applied to the data stored on computer media.

This paper is based on a study of computer security practices among medium and large organizations in Singapore conducted in the second half of 1996. While the study covered a broad scope (encompassing the security practices of organizations, their perception of computer-related risks, and their use of specific technical solutions), this paper discusses a narrower issue - *the relation between the security needs of organizations and the security practices undertaken to meet these needs.* Using two distinct approaches to determining the security needs of an organization, we identify the approach that predicts more accurately the actual security practices undertaken by the organization.

Method

Based on a synthesis of practitioner-oriented literature such as the Computer Security Handbook (1995), the computer security practices of organizations were categorized into six factors : management policies on computer security, personnel policies related to computer security, restrictions on physical access, system access controls, backup and disaster recovery, and the location of computer security responsibility within the organization. Each factor was operationalized through 2 to 5 questionnaire items. Each question was implemented using a 5-point Likert scale (requiring the respondent to indicate his/her agreement with the statement presented). Subsequent analysis confirmed the reliability of the questionnaire items - Cronbach's alpha for all six factors ranged between 0.72 and 0.90. The level of computer security practices in an organization is computed as the sum of the scores on 22 separate items (representing all six factors). The possible range of computer security practices scores extends from 22 (22 x 1) to 110 (22 x 5).

Our first approach to assessing the security needs of an organization was based on the long tradition of risk assessment, wherein the risk from a particular threat is defined as the *product* of the *likelihood* of the threat and the *severity* of the threat. While some authors such as Carroll (1996) have compiled extensive data on the likelihood of various threats (using actuarial data), we did not wish to assume that these likelihood values would necessarily be valid in the Singapore environment. Instead, we asked survey respondents to rate their perception of the likelihood of a threat on a 5-point semantic differential scale ranging from "extremely unlikely" to "extremely likely". Five separate classes of threats to computer security were rated in terms of likelihood by our respondents : **natural disasters**, **accidental human errors**, **hardware / software failures**, **unauthorized access**, and **automated system penetration** (through viruses, worms, logic bombs, and Trojan horses).

For each of these threats, respondents were also required to assess the severity of potential damage, measured as a dollar level (below $100, between $100 and $1K, between $1K and $10K, between $10K and $100K, and above $100K). The logarithmic scale of severity was used to ease the task of severity assessment (the respondents felt more comfortable working with "ball park" numbers); it is also justifiable on the basis of studies of perception that find that responses to stimuli are often proportional to the logarithm of stimulus strength. The product of likelihood and severity ratings for a specific threat measures the risk ascribed to that threat. The sum of the risk measures for all five threats yields the total risk assessed by this approach. Since both likelihood and severity ratings are collected on 5-point scales, the range of possible total risk measures runs from 5 (5 x 1 x 1) to 125 (5 x 5 x 5). This total risk measure is one of the potential predictors of the level of computer security practices in organizations.

An alternative approach to assessing the security needs of an organization is based on a study conducted by the Systems Security Study Committee (SSSC) in 1991. In this approach, organizations rate their security needs in terms of three factors : **confidentiality** (ensuring the privacy of sensitive information), **integrity** (ensuring that information and programs are changed only in a specified and authorized manner), and **availability** (ensuring that authorized users get prompt access to information and system resources).

Confidentiality addresses the release of potentially sensitive information. For instance, some health records should be released to doctors but not to insurance firms or employers - release of the information to the latter would constitute a breach of confidentiality. Integrity requires that the information be tamper-proof. For example, faculty should be able to update the grades obtained by students, but the students themselves should not. Finally, availability refers to the ability of an information system to keep functioning amidst adverse conditions (e.g. an earthquake, a fire, or a flood).

The confidentiality-integrity-availability model of security needs is sometimes referred to as the CIA model based on the initials of the three factors. The ratings (on a 5-point scale ranging from "not important" to "absolutely critical") attached to the three factors measure the security needs of an organization. In this paper, we investigate whether these CIA ratings predict the observed level of computer security practices in organizations.

Findings

Characteristics of Respondents

The survey questionnaire was sent to a convenience sample of 90 organizations in Singapore. In all, 67 usable responses were obtained. Respondents included legal and accounting firms (8), banks and financial institutions (9), manufacturing businesses (12), service businesses (10), IT providers (13), government agencies (7), and other firms (8). 56% of the respondents identified themselves as middle managers in the IS function, while another 36% were middle / senior managers with responsibilities extending beyond IS. The median level of experience of respondents in their current line of work was 6 years. Most (65%) of the business firms in the sample reported a turnover ranging between $10 million and $1 billion. In terms of number of employees, 29% of the organizations had less than 100 employees and 39% between 100 and 999 employees (17% had more than 999 employees, while 15% did not provide this information).

Security Practices

On aggregating the responses to all 22 questions about computer security practices (corresponding to the six factors), a mean score of 78.4 (maximum 34, minimum 104) was obtained. The scores were slightly different for the different industry groups (with government agencies turning out to have the highest level of security practices, and manufacturing the lowest), but due to the small sample sizes in individual industry groups, no cross-industry comparisons were performed.

Risk Perception

A total of 58 respondents provided complete responses to the risk assessment section of the questionnaire. Based on these responses, the total risk score varied between 25 and 82 with a mean of 50. Again there were differences across the industry groups, with IT providers assessing risk at the lowest level and banks / financial institutions at the highest, but the small sample size precludes inter-industry comparisons.

Confidentiality, Integrity and Availability

All 67 respondents indicated their level of need for confidentiality, integrity and availability. On all three factors, government agencies indicated the strictest security requirements and legal / accounting firms some of the lowest.

Determinants of Security Practices

A main objective of this paper is to explore the relation between perceived risks, the need for confidentiality, integrity and availability, and the actual computer security practices in an organization. For this purpose, the level of computer security practices is modeled as the dependent variable in a regression equation whose independent variables are the perceived risk and the need for confidentiality, integrity and availability

Due to the inter-relationships among confidentiality, integrity and availability (evidenced by their high correlations with one another) that can potentially lead to multicollinearity in the regression model, we computed a single index which is the sum of the confidentiality, integrity and availability ratings for an organization. This index, hereby referred to as the CIA index, is another candidate for explaining the observed level of security practices in the organization.

Both the independent variables, total risk and the CIA index, as well as the dependent variable, level of security practices are approximately normally distributed.

The results of the regression analysis are as follows. The overall regression is significant ($R^2 = 0.34$, adjusted $R^2 = 0.32$, $F_{2,55} = 14.2$, $p = 0.000$). Of the independent variables, only the CIA index is a statistically significant predictor ($t = 5.21$, $p = 0.000$) of the level of security practices. The total risk measure does not add significantly to the variance explained and has an insignificant $t = 1.22$ ($p = 0.226$).

Conclusions

Based on the above findings, we conclude that an organization's security practices are predicted far better by its need for confidentiality, integrity and availability than by its assessment of total risk (sum of the *likelihood* x *severity* products for all threats). The implications of our findings are two-fold. In a descriptive sense, the CIA approach seems to capture much better how organizations make computer security decisions. In a normative sense, IS managers seeking to justify security-related spending in their organizations are encouraged to cast their arguments in terms of confidentiality, integrity and availability rather than as a form of "insurance" against anticipated losses.

Further Research

The reasons for the superior performance of the CIA model of computer security needs in predicting security practices are not investigated in this study. One possibility is that the domain-specific and concrete nature of the CIA factors is easier for the respondents to grasp than the highly abstract structure of the total risk model. Another possibility is that computer security levels are set based on an organization's willingness to "invest" in sound business processes rather than as an "insurance" to contain losses. The actual processes by which computer security decisions are made in organizations promise to be an interesting area of study for the future.

An early study of computer security concerns among computer users (Goodhue & Straub, 1991) examined how industry risk (i.e. the susceptibility of the industry to computer crime), company actions (measures taken by the company to improve security), and users' individual characteristics influenced their concerns about computer security at their workplace. Only the effect of company actions in allaying security concerns proved significant in that study. Our data enables the hypotheses tested by Goodhue & Straub (1991) to be re-examined. We have data from a number of industries (to operationalize the *industry risk* variable), and for each firm in our sample, we have detailed information on the measures adopted by the firm to improve security (to operationalize the *company actions* variable). We also have information on the respondents themselves (*individual characteristics*). We are therefore in a position to re-examine how industry risk, company actions, and users' characteristics influence decision making about computer security in firms.

Acknowledgments

I thank Kenneth Kwok, Tio Guat Kuan and Yap Kuan Sze for their contributions to this research.

References

Carroll, J. M. (1996). **Computer security (3rd edition)**. Butterworth-Heinemann.

Datapro (1996). **Computer security issues : 1996 survey**. Datapro Information Services Group.

Goodhue, D.L. & Straub, D.W. (1991). Security concerns of system users: A study of perceptions of the adequacy of security measures, **Information & Management**, 20(1), 13-27.

Hutt, A. E., Bosworth, S., & Hoyt, D. B. (ed.) (1995**). Computer Security Handbook**. Wiley.

Systems Security Study Committee (1991). **Computers at Risk : Safe Computing in the Information Age**. National Research Council.