Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2005 Proceedings

Americas Conference on Information Systems (AMCIS)

2005

The Interrelationship Between Objectives and Practices in Information Security Management

Qingxiong Ma
Central Missouri State University, qma@cmsul.cmsu.edu

J. Michael Pearson
Southern Illinois University Carbondale, jpearson@cba.siu.edu

The Inter-relationship between Objectives and Practices in Information Security Management

Qingxiong Ma
Department of Computer Information Systems,
Central Missouri State University
qma@cmsu1.cmsu.edu

J. Michael Pearson
Department of Management,
Southern Illinois University at Carbondale
jpearson@cba.siu.edu

ABSTRACT

To help practitioners effectively implement security programs, we explored the interrelationship between security objectives and practices by conducting a canonical analysis based on the data from 354 certified security professionals. We found that for moderately information-sensitive organizations, "Confidentiality" had the highest correlation with information security practices. In these organizations, the security practice contributing most to the security objectives was "Access Control". For highly information-sensitive organizations, the "Confidentiality", "Accountability," and "Integrity" together determine the security practices. In these organizations, the major security practices that impact on security objectives are: "Access Control", "Organizational Security", and "Security Policy". "Access Control" was the only practice contributing to information security objectives in both groups. The items in this dimension focused mainly on technical controls.

Keywords

Information security management, Objectives, Practices, Inter-relationships, Survey, Information security professionals, Canonical correlation analysis.

INTRODUCTION

Information security management (ISM) should be conceptualized as a process. The process starts with information security objectives. The security objectives should be set by top management, which should dictate the security infrastructure and be aligned with business strategy. Then, various kinds of security controls should be implemented to enforce the security objectives. Although ISM is a business case-based decision, and the "best practices" in one organization may not be the "best practices" for another organization, there are strong similarities between good security programs at a strategic level that can be analyzed and emulated to improve the security of most organizations (Bachman 2002). These strategies imply a number of tactics that are widely – but not universally – applicable. Recently, security professionals and organizations are making efforts to formulate these patterns.

Some researchers recognized that the relationships between security objectives and practices are complicated, but important for practitioners to understand (Dhillon and Torkzadeh 2001). Also some practices only contribute to a particular security objective (Byrnes and Procter 2002). Thus, it is important to explore the underlying relationships between management practices and information security objectives. Knowledge of how the practices interact and influence the information security objectives, which practice contributes to which information security objective(s), how much each of the management practices contributes to the total security goal, and how to maximize information security objectives, are important for managers to understand in resource allocation and diagnostics.

In this study, we investigate the relationship between information security objectives and practices by conducting a canonical analysis based on the data from 354 certified security professionals. We found that for moderately information-sensitive organizations, "Confidentiality" had the highest correlation with information security practices. In these organizations, the security practice contributing most to the security objectives was "Access Control". For highly information-sensitive organizations, the "Confidentiality", "Accountability," and "Integrity" determine the security practices. In this group of organizations, the major security practices that impact on information security objectives are: "Access Control", "Organizational Security", and "Security Policy". "Access Control" was the only practice which contributed to information security objectives in both groups. The items in this dimension focused mainly on technical controls.

LITERATURE REVIEW

Leiwo and Zheng (1997) categorized the duties of managerial information security personnel as upper boundary and lower boundary. Upper boundary duties are the formulation of information security requirements based on information security objectives, which are based on different national/international laws, agreements, standards, and organizational business objectives. They are set by top management and formulated in an unambiguous way. Lower boundary duties are the specification of technical security policies based on top management security requirements. They include the security enforcement mechanisms implemented by technical personnel. Based on this upper-lower boundary perspective, information security objectives should be strategic and at higher level.

Generally, information security professionals agree that the objective of information system security is to optimize the performance of an organization with respect to the risks to which it is exposed (Bosworth and Kabay, 2002). Information security is concerned with protecting the confidentiality, integrity, and availability of information and information systems (Fried, 1994; Blackwell, 1998). Therefore, the goal of ISM is to ensure business continuity, customer confidence, competitive advantage, protect business investments and opportunities, and reduce damage to the business by preventing and minimizing the impact of security incidents. Besides the three traditional information security objectives—confidentiality, integrity, and availability, more components of security objectives were suggested. A review of IS literature reveals that non-repudiation, authentication, accountability/auditability are three new objectives that are most often cited in current information security literature (Ma 2004).

The complex relationships between the means and ends in ISM not only indicate that both security practices and security objectives are multi-dimensional, but also interact with each other. The implementation of one security objective can impact the implementation of another objective. For example, risk-analysis is used by some organizations as a security objective. In another organization, it might be used as the means by which to identify controls for information security management. Similarly, the items listed in ISO 17799 were regarded as evaluation criteria by Dhillon and Backhouse (2001), but many security professionals consider these items to be the security practices necessary to achieve specific security objectives.

Researchers and practitioners indicated that some practices only contribute to a particular security objective. For example, the relationship between access control and confidentiality was described by Byrnes and Procter (2002) as:

> *"To accomplish the confidentiality objective requires that we know what data we are protecting and who should have access to it. It requires that we provide protection mechanisms for the data while it is stored in the computer and while it is being transferred over networks between computers. We will need to know the application programs that we use (or could use) to manipulate the data and control the use of those applications. Luckily, the Chief Security Officer (CSO) and the IT team will handle the mechanics of doing all this—just as soon as we tell them how to figure out who should have access to which data and applications and how far to go in providing confidentiality".*

Surprisingly, very few studies have concentrated on the relationship between information security objectives and practices. Dhillon and Torkzadeh (2001) did an exploratory study in which they used a value-focused thinking approach and interviewed 73 managers in a cross section of firms from various industries. They identified 9 fundamental objectives and 16 methods or practices that are essential to accomplishing those objectives in protecting a firm's information resources. In the framework they proposed, there was an interaction between these methods and fundamental objectives. Although their model provides insights into the understanding of interrelationships between the means (management practices) and the security objectives, its complexity makes it difficult for managers to follow, and therefore it needs to be improved. First, the terms used in the original model were confusing. Dhillon and Torkzadeh used "mean objectives" for the methods to be used, and "fundamental objectives" for objectives to be achieved. Second, they did not tell how the practices interact and influence the information security objectives, which practice contributes to which information security objective, how much each of the management practices contributes to the total security goal, and how to maximize information security objectives. Such knowledge is important for managers in resource allocation and diagnostics. Third, the model is too general to be effective. They did not specify the scenario in which the model can be applied. ISM is complex and many factors are involved. For example, organizational size is considered an important barometer of IT security's effectiveness (Briney and Prince 2002), and not all organizations are equally impacted by the problems of information security since the risk profile of companies differs across industries (Pelter 2003). Thus, we believe the study of the relationship based cluster analysis will provide deeper understanding, more meaningful interpretation, and more practical suggestions.

RESEARCH METHODOLOGY

To map the interrelationship between management practices and security objectives, a canonical correlation analysis method was used. Canonical correlation analysis is one of the most widely used methods to predict or explain a set of dependent variables with a set of independent variables. In this study, we proposed that organizations should set objectives first and based on the objectives selected, appropriate practices should be developed and enforced. Thus, the factors derived from information security objectives were treated as independent variables, while those generated from information security practices were considered as dependent variables (Table 1). This study is part of larger project, in which a factor analysis identified four dimensions for information security objectives: Information Integrity, Confidentiality, Accountability, and Availability; another factor analysis identified eight factors for security practices (Ma and Pearson 2005).

Information Security Objectives (Independent)	Information Security Practices (Dependent)
Integrity	Security Policy
Accountability	Organizational Security
Confidentiality	Asset Classification
Availability	Continuity
	Access Control
	System Development
	Operations
	External Security

Table 1. Variables in the Canonical Analysis

Our sample for this study comes primarily from the website of the International Information Systems Security Certificate Consortium (ISC)[2], a not-for-profit consortium and certification organization. Utilizing the search capability of the directory provided on this website, we were able to obtain the contact information for certified information security professionals who reside within the United States of America. The data was collected via a web-based survey. The response rate was 11.8 percent, and 354 responses were used in this study. A majority of the respondents are male. 17.2 percent of respondents were under 30 years of age, while 46.4 percent were over the age of 40. It is also interesting to note that almost half of the respondents (47%) have received graduate level education. Compared to other information technology professionals, this is high. According to a study of 436 SQL server professionals (Pinnacle Publishing, 2003), only 14 percent of the respondents had graduate level education. Approximately 75 percent of certified information security professionals had six or more years of work experience, while only 53 percent of SQL server professionals had this level of experience. Over half of the respondents in this study are in management positions. Most work for small and medium size businesses. Approximately 23% work in financial institutions, healthcare or insurance companies, while many of the remaining respondents (over 60%) placed their organizations in the unclassified category.

Based on these four dimensions of information security objectives, organizations were clustered into two distinct groups (Ma 2004). Although we proposed that organizations could be classified into three groups (or clusters) in terms of information sensitivity—low, medium, and high, the cluster analysis resulted in two distinct types of organizations. This could be explained partly by the relatively low number of organizations which participated in this study that would be considered information insensitive. Apparently, respondents came mainly from medium information-sensitive and high information-sensitive organizations. The intuitive explanation for this would be that, since this study targeted information security professionals, organizations that don't perceive organization information as important or sensitive, probably would not feel a need to have these types of information technology professionals on their staff. We did additional t-tests on the demographic information for each cluster. Statistically, there was no significant difference on gender, education, position, and number of personal computers within the organizations. However, the clusters did differ significantly on age of the information security professional, business size, and years of work-experience involving information security professionals. The demographics indicated that organizations in cluster 1 were smaller in size. The results imply that the organizations which were moderately

information sensitive were smaller and had younger information security professionals with less work experience, while organizations dealing with higher levels of information-sensitivity were larger firms and had older, more experienced information security professionals.

Canonical Correlation Analysis for Cluster 1

In this study, a canonical correlation analysis was conducted for each of the clusters. In the canonical analysis, the factor variables rather than the item variables were used. This has several advantages. First, it avoids the risk of potentially misleading results by selecting specific items to represent a complex result. Second, it avoids the difficulty for calculating a summed scale when two or more item loadings are significant and fairly close to each other. Conceptually, a summated scale is a composite value. In this study, the calculation of composite score used a weighted-average of factor loading approach. The weights for each factor variable correspond to their factor loadings. Since the purpose of cluster analysis is to cluster the organization based on the similarity distance or distinctiveness of variables, the relationship among those item variables must be orthogonal. Therefore, the factor loadings from varimax, not from oblique rotated method were used in calculation of the composite scales. For example, if a factor has three items (I1, I2, and I3) and their factor loadings are .756, .701, and .674 respectively, the formula used to compute the composite scale for this factor is: (Item1*.756 + Item2*.701 + Item3*.674)/3.

Canonical analysis is sensitive to sample size and the number of cases in each cluster was not equally distributed, the ratio of cases to composite variables was examined for each cluster. Table 2 shows that the ratios of dependent and independent variables exceed the recommended guideline of 10 observations per variable (Hair et al. 1998).

Cluster	Number of Cases	Independent (4)	Dependent (8)
1	158	39.5	19.75
2	196	49	24.5

Table 2. Ratio of Cases to Variables

Canonical correlation analysis shares the same basic assumptions as other multivariate analysis techniques such as multiple regression, discriminant analysis, and factor analysis. Since there are two sets of variables in canonical analysis, it is necessary to test the assumptions related to linearity and normality for each set. For example, when linearity was tested for the independent variable set (information security objectives), one of the four composite variables was randomly chosen as a dependent variable, using the other three as independent variables. Then, the appropriate scatter plots were drawn. Visually inspection of these the graphs of scatter plots, we did not find nonlinear relationships between the selected dependent variable and the other independent variables. In the evaluation of normality, univariate normality was performed by visually checking the histogram of residuals of each variable in both independent and dependent variable sets. Based on this analysis, it was determined that the data distribution for the variables was normal. We also examined the statistical values for kurtosis and skewness. These values ranged from .18 to 1.38 and .135 to 1.58 respectively. Both are lower than the critical value of 1.96 (Hair et al. 1998).

The process of canonical analysis in this study follows three steps. The first step in canonical correlation analysis is to derive canonical functions. The second step is to interpret these functions. The last step is to test the stability of these functions.

In order to select the appropriate function(s) for interpretation, three criteria were used: 1) statistical significance, 2) magnitude of relationships, and 3) redundancy measure of shared variance. With these three steps, only one significant canonical function was identified for cluster 1. Its canonical correlation .975; its canonical R-square is .950; and its redundancy indices of the independent variate and dependent variate are approximately .335 and .140 respectively. No guidelines have been established for the minimum acceptable redundancy index. In a study exploring the relationship between flexible IT infrastructure and competitive advantage, Byrd and Turner (2001) indicated that explaining 20% of the variance was significant in an organization level study. That means, 33.5% of total variation in independent variate can be explained by dependent variables (security practices), and 14% of total variation in dependent variate can be explained by independent variable (security objectives). Since, we assume that the establishment of information security practices should be based on information security objectives, we focus mainly on the redundancy index of the independent variate. Similarly, examination of the redundancy indices of the second canonical function indicated that both dependent and independent variates were less than 5%, indicating that it should not be considered in the analysis.

Traditionally, canonical weights and canonical loadings have been used to interpret canonical functions. However, these two approaches have been criticized because the canonical weights can be unstable, particularly in instances where multicollinearity is a problem, and canonical loadings can experience significant variability from one sample to another, thus making interpretation difficult between samples. Alternatively, canonical cross-loadings have recently been suggested as a viable approach. Canonical cross-loadings involve correlating each of the original observed dependent variables directly with the independent canonical variate, and vice versa. It provides a more direct measure of the dependent-independent variable relationship (Hair et al. 1998).

Canonical cross loadings demonstrate the strength of the linear correlation between each security objective and the dependent variate (security practices) or between each security practice and the independent variate (security objectives). By looking at the canonical cross-loadings, the contribution of each independent variable (information security objective) to the dependent variate (information security practice) can be estimated. In this study, canonical cross-loadings were used to interpret the contributions of each variable in each variate in explaining the opposite variate. However, for comparison purposes, the canonical weights and canonical loadings are also presented in Table 3.

Variate/ Variables	Canonical Weights (Standardized)	Canonical Loadings	Canonical Cross-Loadings
Independent Variables – Information Security Objectives			
Integrity	.143	.473	.461
Accountability	-.014	.444	.433
Confidentiality	.952	.991	.966
Availability	-.009	.091	.089
Dependent Variables - Information Security Practices			
Security Policy	-.019	.171	.167
Organizational Security	.026	.219	.214
Asset Classification	-.005	.164	.160
Continuity	-.051	.079	.077
Access Control	1.001	.997	.972
System Development	-.028	.216	.211
Operations	-.073	.160	.156
External Security	.034	-.032	-.031

Table 3. Canonical Weights for the First Canonical Function in Cluster 1

From Table 3, the contribution of each dependent variable (information security practice) to the independent variate (information security objectives) can be estimated and vice versa. The influence of dependent variables on the independent variate comes mainly from "Access Control". The other dependent variables contribute very little to the independent variate. While, the influence of independent variables on the dependent variate comes mainly from "Confidentiality", "Integrity" and "Accountability" provide moderate impact, and "Availability" provides almost no impact. To determine the stability of the canonical results, sensitivity analysis was conducted. One method recommended by Hair et al. (1998) is to estimate multiple canonical correlations by removing a different independent or dependent variable from the analysis. In this study, four (Security Policy, Asset Classification, Continuity, System Development) of the eight dependent variables were deleted one at a time. The results indicated that the canonical loadings for Cluster 1 were very stable and consistent in each of the four cases where an independent variable was deleted. The overall canonical correlations also remained stable.

CANONICAL CORRELATION ANALYSIS for CLUSTER 2

Following the same procedures as described previously, canonical correlation analysis was conducted for Cluster 2. Similar to the results obtained in Cluster 1, two canonical functions were statistically significant with p-value of less than 0.05. The test statistics (Pillais, Hotellings, Wilks) for the overall model fit indicated that the canonical functions, taken collectively, are statistically significant at the 0.001 level..Only one canonical function has significant canonical correlation and significant reduuncy indices. Its Canonical Correlation is .920; its canonical R-square is .847 and redundancy indices for the dependent variate is .332, which is adequate according to the .20 level suggested by (Byrd and Turner 2001). For the second function, the dependent and independent variable sets have low shared variance (.027). Thus, based on the results of the redundancy analysis and the statistical significance tests, only the first function was considered in further analysis.

Based on the size of the three values, the importance of dependent variables and independent variables can be identified. First, the contribution of dependent variables (security practices) to the independent variate is mainly from "Access Control", and a small portion comes from "Organizational Security" and "Security Policy". The other variables only have marginal correlation with the independent variate. The impact of the independent variables on the dependent variate comes mainly from "Confidentiality" and "Accountability". The importance order of their contribution is "Confidentiality", "Accountability", "Integrity", and "Availability".

The result of the sensitivity analysis in Cluster 2 indicated that the canonical cross-loadings for Cluster 2 are stable and consistent in each of the four cases when a dependent variable (Security Policy, Organizational Security, Continuity, or Access Control) was deleted. The overall canonical correlations also remained stable.

Summary of Statistical Analyses

To have a better understanding of the contribution of each factor to their respective variate, the standardized canonical weights were sorted and presented in Table 4.

Cluster 1		Cluster 2	
	Canonical cross-loadings		Canonical cross-loadings
Independent Variables		Independent Variables	
Confidentiality	.966	Confidentiality	0.865
Integrity	.461	Accountability	0.556
Accountability	.433	Integrity	0.470
Availability	.089	Availability	0.224
Dependent Variables		Dependent Variables	
Access Control	.972	Access Control	0.912
Organizational Security	.214	Organizational Security	0.397
System Development	.211	Security Policy	0.322
Security Policy	.167	Asset Classification	0.270
Asset Classification	.160	Operations	0.265
Operations	.156	System Development	0.251
Continuity	.077	Continuity	0.186
Business Partner Security	-.031	Business Partner Security	0.148

Table 4. Contribution Order of Variables

The results from the canonical correlation analysis revealed that for the first group (Cluster One), "Confidentiality" had the highest correlation with information security practices. The most important contributor to information security objectives was "Access Control". For the second group of organizations (Cluster Two), the major information security objectives were "Confidentiality", "Accountability", and "Integrity". Different from Cluster 1, besides the major contributor "Access

Control", "Organizational Security" and "Security Policy" also contributed to the information security objectives. Based on the results of this study, "Access Control" is the most important information security practice in both groups.

Based on Table 4, the importance of each security practice in their correspondent function was displayed in Figure 1. In the diagram, MSO stands for moderately information-sensitive organizations and HSO is for high information-sensitive organizations.

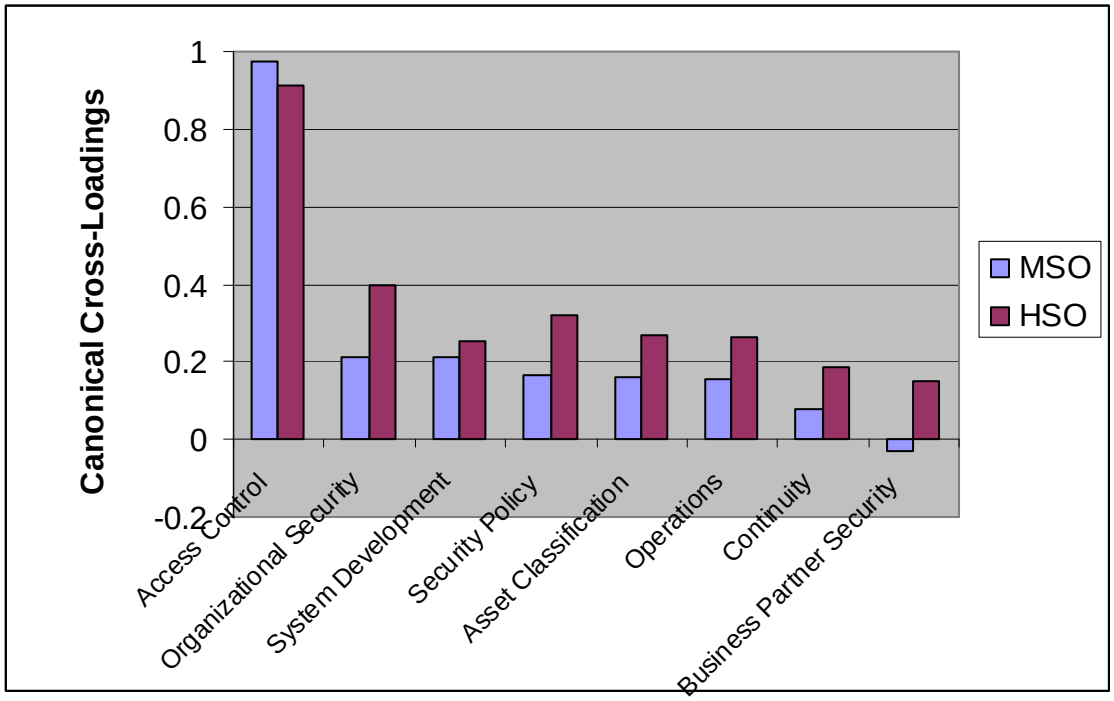

Figure 1. The Importance of Each Security Practice for Different Clusters

IV. Discussion

The canonical correlation analysis "Access Control" was the only practice which contributed to information security objectives in both groups. The items in this factor focused mainly on technical controls. These controls are easy to implement. In the information non-sensitive organizations (e. g. manufacturing) where information security expertise is typically lacking, implementation of technical oriented "access control" is economical and thus, the first option that should be selected. However, in information sensitive organizations, security has generally become institutionalized into the corporate culture via policies (Briney and Prince 2002). It is recognized that information security is more of a "human" problem rather than pure technical problem. The human related problems are on all levels of the organization —from uninformed end users to ambivalent upper management. Although technical controls (such as firewalls, anti-virus, and auditing measures) are easy to be implemented, they are not sufficient to ensure the achievement of multiple information security objectives. This was confirmed by the following quote provided by an "experienced" information security professional:

Technical control measures only go so far. The key to information systems security is user buy-in to the measures to be taken. This can only be accomplished through senior management support and proper education of the users of the information system(s) in question.

The analysis also found that to have more effective security practices, practitioners should pay attention to "Organizational Security" and "Security Policies". This finding has special practical significance because information or computer security is typically an afterthought, it can be hard to change the culture of an organization to accept information security practices. It takes time, effort, and compromise and painful experiences for an organization to learn to establish the policies, and to enforce these policies.

This finding is consistent with that of previous studies. Straub and Welke (1998) proposed a security planning model for management, which includes countermeasure analysis and education/training in security awareness. For example, they proposed that security policies not only provide guidelines for proper system use such as password management, but also convince potential abuser that it is too risky to violate the rules. However this approach is passive because it depends wholly on the willingness of system users to follow the policies. Instead, preventive measures such as access control are active countermeasures.

Last, the canonical analysis indicated that "Business Partner Security" is the least important among the eight security practices. This may be because currently, information sharing across organizations is still at a relatively low level. Researchers (Kauffman and Mohtadi 2003; Kinsey and Ashman 2000) found that information sharing is not fair to different parties in the supply chain. Usually it was initiated by suppliers because of business strategy, and buyers had less benefited from this initiative. Also information sharing must be based on trust and insufficient trust generally deters buyers from sharing critical information with their suppliers. At present, the majority of electronic information exchange typically occurs within an organization. With the development of electronic commerce and more frequent business coordination, the importance of this practice may increase.

V. CONCLUSION

Although the relationship between information security objectives and practices is complex and very few studies have focused on it in the ISM literature, it is very important for information security practitioners to understand because such knowledge allows them to take the appropriate management intervention to improve the effectiveness of ISM. The importance of such studies also lies in that they investigate the security issues from a dynamic and holistic perspective, following a basic cause-effect logic. Dhillon and Torkzadeh (2001) conducted their study using qualitative method based on interviews. Different from their study, this study examined the relationship using quantitative approach based on survey. More important, this study explored the relationship for different cluster of organizations. Since organizations facing different threats and have different security profiles, in order to provide specific and applicable suggestions, such cluster analysis is necessary and helpful.

Future study should be cluster-based as organizations in the same cluster often share similar security profiles. The possible factors can be used for cluster analysis include security objectives, organizational size, industry, or information sensitivity.

REFERENCES

1. Bachman, D. (2002) "Information Systems Security: Principles and Perspectives", Sprint E|Solutions white paper.

2. Blackwell, E. (1998). Building a solid foundation for intranet security**,** *Information Systems Management*, Spring 1998, 15(2), p26, 8p.

3. Bosworth, S. and Kabay, M. E. (2002). Computer Security Handbook (4th edition, Bosworth and Kabay eds.), 2002.

4. Briney, A. and Prince, F. (2002). Does Size Matter? The 2002 *Information Security* Magazine (ISM) survey, http://www.infosecuritymag.com/2002/sep/2002survey.pdf

5. Byrd, T. A. and Turner, D. E., (2001). An Exploratory Examination of the Relationship Between Flexible IT Infrastructure and Competitive Advantage, *Information & Management*, 39, 41-52.

6. Byrnes, F. C. and Proctor, P. (2002). Information Security Must Balance Business Objectives (Article is provided courtesy of Prentice Hall PTR), *InformIT.com*, MAY 24, 2002.

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

8. Dhillon, G., and Torkzadeh, G., (2001). Value-Focused Assessment of Information System Security in Organizations, *ICIS.*

9. Fried, L., (1994). Information security and new technology, *Information Systems Management,* Summer 1994, 11(3), p57, 7p.

10. Hair, Jr., J. F., Anderson, R. E., Tatham, R. L., and Black, W. C. *(1998).* Multivariate Data Analysis with Readings *(5th edition).* Prentice-Hall, Englewood Cliffs, NJ.

11. Kauffman R. and H. Mohtadi. (2003) "Analyzing interorganizational information sharing strategies in B2b E-commerce supply chains." University Carlson School of Management. Working paper. http://www.uwm.edu/~mohtadi/km_mgmt_science_040404_working_paper.pdf

12. Kinsey, J. and Ashman, S. (2000). "IT in the Retail Food Industry," *Technology in Society*, 22(1), 83-96.

13. Leiwo, J. and Zheng, Y, (1997). A Framework for the Management of Information Security. Proceedings of the 1997 Information Security Workshop (ISW'97). Ishikawa, Japan, September. Springer-Verlag, LNCS 1396.

14. Ma, Q. (2004). Information Security Management Objectives and Practices, unpublished dissertation. Southern Illinois University.

15. Ma, Q. and Pearson, J. M. (2005). ISO 17799: "Best Practices" in Information Security Management? *Communications of the Association for Information Systems*, Volume 15, 577-591.

16. Peltier, T. R. "Preparing for ISO 17799," *Security Management Practices*, Janurary/February 2003, pp. 21-28.

17. Pinnacle Publishing, 2003. The SQL Server Professional Salary Survey Report:

18. http://www.hardcoreaspdotnet.com/admin.nsf/(lookupsurvey)/SQ?open

19. Straub, D. W. and Welke, R. J. (1998). Coping with systems risks: security planning models for management decision making. *MIS Quarterly*, 22, 441-469.