Communications of the Association for Information Systems

Volume 15 Article 32

April 2005

ISO 17799: "Best Practices" in Information Security Management?

Qingxiong Ma
Central Missouri State University, qma@cmsu1.cmsu.edu

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

Communications of the Association for Information Systems

ISO 17799: "BEST PRACTICES" IN INFORMATION SECURITY MANAGEMENT?

Qingxiong Ma
Department of Computer Information Systems,
Central Missouri State University

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

ABSTRACT

To protect the information assets of organizations, many different standards and guidelines have been proposed. Among them, International standard ISO 17799 is one of the most prominent international efforts on information security. This standard provides both an authoritative statement on information security and the procedures to be adopted by organizations to ensure information security. Security professionals claim ISO 17799 to be a suitable model for information security management and an appropriate vehicle for addressing information security management issues in the modern organization. However, to our knowledge, no empirical studies have been conducted to validate this standard. Based on a survey of information security professionals, we found that ISO 17799 is comprehensive, but not parsimonious.

Keyword: best practices, information security management, ISO 17799, factor analysis, certified security professionals

I. INTRODUCTION

With society's increasing dependency on information technology (IT), the consequences of computer crime can be grave [Rogers, 2001]. The Computer Security Institute (CSI) and the FBI report that approximately 74% of the businesses surveyed cited their Internet connection as a frequent point of attack. These respondents also reported financial losses of approximately $456 million during the previous fiscal year. Although 80% of these respondents acknowledged financial losses, only 40% were able to quantify the losses, suggesting that actual losses may be significantly higher than reported. The FBI estimated that the cost of electronic crimes is approximately $10 billion a year [CSIS, 2002].

Besides the monetary loss, breaches of information systems can have non-financial implications for a business. An example would be a security breach that causes a disruption of internal processes. This disruption would impact productivity negatively and create indirect costs such as

the loss of potential sales, loss of competitive advantage, and a negative impact on a company's reputation, goodwill, and trust [Bruce, 2002].

With the integration of the World Wide Web into organizations, information security problems drew considerable attention from researchers and practitioners. In November 2002, the United States Congress passed a series of bills that would allocate nearly one billion dollars for research on cyber security. These programs are intended to ensure that the United States is better prepared to prevent and combat terrorist attacks on private and government computer systems. Both private and public organizations realize that information security is a complex issue, involving both human and technical factors.

To protect the information assets of organizations, many different frameworks, guidelines, and standards were proposed by researchers, practitioners, consultants, and professional organizations. Among them, international standard ISO 17799 is one of the most prominent efforts on information security. This standard provides an authoritative statement on information security, and the procedures necessary to achieve information security in the modern organization. Information security professionals suggest that ISO 17799 provides "best practices" on information security management (ISM) and is an appropriate model for addressing ISM issues.

To our knowledge, no empirical studies have been conducted to validate ISO 17799 or other ISM standards. Without validating the appropriateness of these standards it is difficult to answer questions such as:

- Which standards should an organization implement to achieve their information security objectives?
- What management practices are perceived as critical by information technology professionals?

Answers to these questions are of practical importance for information security. Thus, to understand ISO 17799 better, we conducted an empirical investigation into the validity, reliability, and robustness of this international standard.

II. LITERATURE REVIEW

ISO 17799 provides information security professionals with a list of objectives and practices. The origin of ISO 17799 goes back to BS7799, published by the British Standards Institution in 1995. BS7799 was intended to provide a common basis for developing effective ISM practices [Peltier, 2003]. The ISO 17799 extended BS7799 and provides an authoritative statement on information security, and the procedures necessary to establish information security. The standard covers ten security dimensions consisting of 36 security practices (Appendix I). It provides the basis for self-assessment, reassessing the information security practices of business partners, and the independent evaluation of ISM within the business organization. Li, et al. [2000] claim that ISO 17799 is a comprehensive model for ISM. Dhillon and Backhouse [2001] describe this standard as a successful vehicle for addressing ISM issues in the modern organization.

III. RESEARCH METHOD

INSTRUMENT DESIGN

The development of survey items was relatively straight forward. The thirty six items which represent the ten dimensions in ISO 17799 were included in the survey instrument. Because several items in ISO 17799 are compound items representing multiple ideas and/or concepts, it was necessary to split them into multiple, single concept items within the survey instrument. For example, in ISO 17799 the initial statement for security policy includes two concepts: management direction and management support. These two concepts are closely related, but if

treated as one item in the survey instrument, respondents could possibly be confused as to the focus of the item. Thus, this item was broken down into two separate items. As a result, we ended up with fifty-six items in the survey instrument. Items were measured with 5-point Likert-type scales ranging from "Not Applicable" to "Fully Implemented".

SAMPLE SUBJECTS

The subjects of this study are certified information security professionals. The contact information was obtained from the website of the International Information Systems Security Certificate Consortium (ISC)[2], a not-for-profit consortium and certification organization[1] This organization is charged with maintaining various Common Bodies of Knowledge (CBK) for information security professionals and for individuals seeking various certifications (including CISSP and SSCP). The directory on this website can be accessed through a search engine with search criteria options such as certification or location (country). Utilizing this search capability, we obtained contact information for certified information security professionals who reside in the United States.

The majority of subjects who participated in this study are males. 17.2 percent of respondents are under 30 years old, while 46.4 percent of the respondents are over the age of 40. Approximately 75 percent of the surveyed certified information security professionals have six or more years of work experience. Over half of the respondents in this study are in management positions.

PILOT STUDY AND INSTRUMENT REVISION

The survey instrument was pre-tested through a pilot study. Thirty certified information security professionals provided feedback. The respondents' feedback focused on several key points. For example, some respondents suggested that the item "Information should be complete" was not clear. Also, the two negatively phrased statements were confusing because the scales became inappropriate. Based on the feedback provided, modifications were made to the instrument. The items in the final version of the questionnaire are provided in Appendix II.

DATA COLLECTION

This study made use of a web-based survey for data collection. After the initial e-mail, two reminder e-mails were sent at approximately one week intervals. Each e-mail contained a request to participate and the researcher's contact information including phone number, e-mail address, and postal address; this allowed the respondent to contact us when they encountered technical problems or ran into questions about the survey. In an effort to increase the responses rate, we offered two incentives to the respondents. In our initial e-mail, we indicated that the results of this study would be available to respondents upon request; we also indicated that ten percent of the respondents would be randomly selected to receive $25 in cash for participation. Altogether, three thousand information security professionals were contacted, and 380 completed responses were received.

Considering the anonymity feature of the Internet, data validation was a concern. To solve this problem, two approaches were used. The initial data validation was implemented when the respondents submitted their answers. If the survey was not completed, a reminder message would appear when they tried to submit the form. The secondary data validation was used after the respondent submitted the survey. It was necessary to differentiate the surveys from different respondents in case the respondent submitted the survey multiple times. Thus, additional information about each respondent was collected, including their IP address, the name and version of their web browsers, and submission time for each form.

---

[1] https://www.isc2.org/cgi-bin/content.cgi?category=7

The responses were screened before doing analysis. If two responses shared the same IP address and were submitted with the same web browser, they were assumed to be from the same respondent. Only the first response was kept and others from that IP address were dropped. If the number of employees for an organization was five or fewer, the response was regarded as invalid since the unit of analysis of this study was the organization.

After data screening removed 26 "invalid" responses, 354 usable responses remained in the dataset, which represented a response rate of 11.8 percent (354/3000). This response rate was considered acceptable given the nature of the study. Non-response bias was tested based on a comparison between early and late respondents on age, education, and work experience. T-tests on these variables indicated that no systematic differences existed. Thus, we concluded that there was no non-response bias in the sample.

IV. DATA ANALYSIS

The objectives of this study were:

1. examining the validity of ISO 17799 and
2. improving this standard by generating a parsimonious model.

To achieve the first objective, a confirmatory factor analysis was conducted. The second objective was accomplished by conducting a principal component analysis to reduce the number of factors needed to account for the maximum portion of the variance represented in the original variables (items).

CONFIRMATORY FACTOR ANALYSIS

When doing the analysis, the number of factors was fixed at ten since ten security dimensions are identified in ISO 17799. A solution that accounts for 70 percent of the total variance is considered satisfactory in confirmatory factor analysis [Hair et al., 1998]. Inspecting the total variance in Table 1, we found that the total variance explained was 68.5 percent, which is close to the guideline of 70% set by Hair et al. [1998] for confirmatory factor analysis.

Table 1. Total Variance Explained in Confirmatory Factor Analysis

	Initial Eigenvalues			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	24.139	43.106	43.106	5.605	10.008	10.008
2	2.563	4.577	47.683	4.618	8.246	18.254
3	2.198	3.925	51.609	4.370	7.803	26.057
4	1.868	3.336	54.944	4.192	7.485	33.542
5	1.555	2.778	57.722	4.082	7.288	40.831
6	1.409	2.517	60.239	3.799	6.783	47.614
7	1.279	2.284	62.523	3.450	6.160	53.774
8	1.154	2.060	64.583	3.324	5.935	59.709
9	1.128	2.014	66.596	3.206	5.724	65.434
10	1.081	1.930	68.527	1.732	3.093	68.527

Table 2 provides the results of this confirmatory factor analysis. From this table, we see that the loading of fifteen items do not exceed 0.5, suggesting that these items did not contribute significantly to any of the underlying dimensions. Expected item loads were obtained for only four dimensions (security policy, systems development and maintenance, asset classification and control, and business continuity planning). The other six dimensions contained items that did

Table 2. Initial Factor Loadings for Information Security Practices

	1	2	3	4	5	6	7	8	9	10
ISP1	**.686**	.178	.092	.256	.231	.162	.098	.159	.196	.002
ISP2	**.604**	.167	.158	.267	.167	.157	.187	.177	.184	.121
ISP3	**.703**	.077	.144	.160	.199	.242	.100	.069	.130	.190
ISP4	**.685**	.127	.266	.250	.209	.164	.031	.185	.136	.107
ISP5	**.755**	.174	.179	.191	.158	.106	.157	.103	.170	.097
ISP6	**.732**	.244	.127	.215	.160	.151	.180	.154	.165	.088
SDM1	.113	**.633**	.226	.183	.208	.198	.181	.156	.078	.077
SDM2	.200	**.632**	.212	.169	.143	.308	.207	.108	.186	.092
SDM3	.177	**.700**	.204	.112	.169	.067	.092	.138	.183	.014
SDM4	.163	**.771**	.170	.117	.185	.092	.154	.135	.106	.100
SDM5	.152	**.718**	.138	.032	.166	.110	.121	.050	.124	.213
ACC1	.238	.144	**.748**	.134	.057	.078	.235	.172	.067	.045
ACC2	.151	.154	**.800**	.164	.051	.095	.237	.055	.053	.014
ACC3	.038	.156	**.679**	.161	.194	.118	-.002	-.008	.146	.273
ACC4	.176	.207	**.689**	.167	.061	.068	.235	.069	.100	-.045
OS1	.281	.169	.061	**.798**	.068	.116	.100	.099	.091	-.061
OS2	.194	.091	.228	**.791**	.088	.091	.095	.030	.051	.065
OS3	.191	.153	.152	**.798**	.131	.180	.064	-.002	.172	-.007
OS4	.156	.027	.231	**.725**	.144	.137	.111	.128	.069	.158
0S5	.275	.143	.132	**.470**	-.036	.195	.146	.322	.254	.359
OS6	.272	.235	.067	**.440**	-.054	.130	.206	.401	.151	.362
COM1	.213	.359	.084	.177	.401	.263	.263	.342	-.063	.146
COM2	.287	.249	.138	.318	.396	.205	.432	.299	-.091	-.016
COM3	.194	.332	.120	.228	**.517**	.261	.286	.283	.023	.086
COM4	.202	.249	.093	.074	**.664**	.128	.167	.205	.257	-.067
COM5	.124	.161	.080	.033	**.739**	.176	.042	.204	.291	.059
COM6	.366	.135	.169	.104	**.594**	.118	.084	.153	.164	.025
COM7	.204	.172	.097	.106	**.565**	.101	.142	.094	.274	.168
COM8	.297	.182	.238	.195	.396	.162	.297	.087	.019	.266
COM9	.308	.341	.115	.131	.488	.293	.143	.155	.052	.247
COM10	.229	.273	.066	.081	.197	.211	.217	.291	.008	**.585**
COM11	.188	.330	.096	.158	.272	.196	.009	-.003	.069	**.503**

BCP1	.174	.195	.136	.141	.302	**.695**	.207	.156	.176	.039
BCP2	.198	.209	.094	.222	.171	**.752**	.170	.159	.092	.139
BCP3	.284	.175	.174	.176	.163	**.730**	.190	.182	.139	.082
BCP4	.231	.153	.229	.184	.153	**.734**	.205	.158	.191	.150
PES1	.204	.161	.054	.166	.242	.220	.083	**.656**	.136	.107
PES2	.167	.091	.088	.069	.338	.156	.109	**.693**	.231	.039
PES3	.144	.168	.167	.026	.145	.095	.064	**.644**	.311	.098
PES4	.282	.094	.400	.090	.166	.191	.313	.471	.158	-.006
SAC1	.164	.215	.198	.141	.209	.124	.356	.399	.306	-.205
SAC2	.145	.160	.108	.126	.146	.151	.149	.187	**.647**	-.132
SAC3	.120	.044	.113	.081	.218	.038	.116	.112	**.683**	.126
SAC4	.284	.163	.123	.141	.145	.138	.121	.237	**.585**	-.072
SAC5	.226	.148	.080	.154	.130	.195	.271	.155	**.515**	.239
SAC6	.106	.203	.156	.099	.216	.107	**.540**	.100	.468	.120
SAC7	.179	.187	.245	.127	.173	.233	**.656**	.068	.286	.024
SAC8	.122	.218	.233	.154	.099	.184	**.648**	.097	.241	.174
CPL1	.295	.180	.339	.167	.171	.284	**.507**	.219	.132	.000
CPL2	.350	.162	.335	.125	.159	.243	.478	.160	.148	-.019
CPL3	.157	.246	.395	-.019	.217	.111	.340	.171	.323	.102
PS1	.272	.232	.465	.262	.107	.308	-.032	.137	.123	-.110
PS2	.134	.263	.388	.212	.088	.269	-.139	.216	.278	-.049
PS3	.411	.372	.308	.230	.143	.199	.119	.199	.143	-.266
PS4	.381	.390	.278	.227	.144	.242	.180	.164	.049	-.261
PS5	.438	.207	.295	.103	.265	.094	.259	.262	.058	-.010

not load or items that loaded on different dimensions. Organizational security is an example of the first case where six items were specified, but only four items loaded significantly.

This situation also occurred for three other dimensions (physical and environmental security, compliance and personnel security). Two dimensions (systems access control, operations management) each broke into two sub-constructs. A review of the items that broke away from the intended construct did not show a clear definition or foundation for these sub-constructs.

PRINCIPAL COMPONENT ANALYSIS

In this step, we reran the analysis without restriction on the number of factors. We dropped all items with factor loadings less than 0.50. As a result, eight factors were identified. We also tested the reliability for each factor. The results are also displayed in Table 3. Nunnally [1978] suggests that the reliability of alphas below 0.6 is low.

Table 3. Final Factor Loadings for Information Security Practices

Constructs/Items	Loading	α
Information Security Policy		
clearly specifies the information security responsibility of employees.	.771	.927
clearly illustrates the importance of security to the organization.	.754	
has a clear owner who is responsible for its update and maintenance.	.750	
clearly indicates management's intention to support information security programs.	.722	
clearly defines information security objectives	.713	
Is regularly reviewed for effectiveness and completeness.	.638	
Organizational Security		
authorizes the ISM committee to make necessary decisions.	.812	.885
has information security advisors in each business unit to coordinate ISM.	.796	
has a dedicated security steering committee responsible for ISM.	.780	
has an information security forum to give management direction and support.	.743	
Asset Classification and Control		
are clearly labeled based on level of confidentiality.	.854	.851
are classified based on level of confidentiality.	.798	
are classified with a simple, effective system.	.743	
are recorded based on ownership.	.608	
Business Continuity Planning		
is tested regularly.	.784	.924
Includes a risk analysis of critical processes.	.755	
is assessed using effective techniques.	.754	
ensures speedy resumption of essential operations following system failure/interruption.	.731	
System Access Control		
monitors and logs access and use of computer systems.	.691	.845
has procedures for mobile computing control.	.678	
employs password management systems.	.625	
requires routinely reviewing audit logs.	.615	
Requires proper authentication for external connections.	.581	
audits all activities related to working remotely.	.575	
Requires users to follow security practices in selection and use of passwords.	.550	
Systems Development and Maintenance		
has formal procedures to maintain the security of application software (e.g., application testing, changing, and replacing).	.807	.886
uses cryptographic techniques to protect confidentiality, authenticity, and integrity of information.	.754	
protects system files by controlling program source libraries in the development process to restrict possible corruption or tampering.	.722	
has formal procedures to ensure security is built into operational systems.	.674	
follows risk assessment and risk management processes to determine acceptable controls.	.655	
Communications and Operations Management		
has a backup and recovery process to maintain the integrity and availability of essential information processing and communication services.	.786	.824
takes measures to protect the integrity and security of essential software and information against virus and intrusion.	.700	
has policies requiring compliance with software licenses and prohibiting the use of unauthorized software.	.614	
takes appropriate security measures for publicly available systems such as web servers.	.592	
Business Partner Security		
has formal agreements with partners for the exchange of information.	.609	.623
takes appropriate security measures for electronic commerce to ensure information exchange.	.605	

The percentage of variance extracted from these eight factors was 71 percent (Table 4), which was considered satisfactory for an exploratory study.

Table 4. Total Variance Explained in Principal Component Analysis

Component	Initial Eigenvalues			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	16.891	43.311	43.311	4.450	11.411	11.411
2	2.363	6.059	49.370	3.832	9.825	21.235
3	1.924	4.932	54.302	3.422	8.775	30.010
4	1.614	4.137	58.439	3.347	8.581	38.591
5	1.397	3.581	62.021	3.294	8.447	47.038
6	1.304	3.343	65.364	3.233	8.290	55.328
7	1.078	2.765	68.129	3.204	8.216	63.543
8	1.045	2.680	70.809	2.834	7.266	70.809

The results in Table 3 differ from those in the instrument at two levels. Table 5 presents these changes. First, at the factor level (construct), the number of factors is reduced from 10 to 8. The two factors representing "Personnel Security" and "Compliance" were eliminated. The factors "Physical & Environment Security" and "Communications & Operations Management" merged. In addition, one new factor (Business Partner Security) which consisted of two items was derived.

Furthermore, at the item level, the total number of items was reduced from 56 to 36. The number of items in three constructs (Organizational Security, System Access Control, and Communications & Operations Management) went down. The most complicated and problematic dimension was "Communications & Operations Management". Originally, this construct consisted of 11 items. As a result of the analysis, two items broke off as a new dimension—"Business Partner Security" and five others were dropped because of low factor loadings.

Table 5. Item and Construct Changes for Information Security Practices

Construct	Original Items	New items	Original Alpha	New Alpha
Original Constructs				
Information Security Policy	6	6	.9269	.9269
Organizational Security	6	4	.8845	.8851
Asset Classification & Control	4	4	.8511	.8511
Business Continuity Planning	4	4	.9241	.9241
System Access Control	8	7	.8597	.8452
System Development & Maintenance	5	5	.8859	.8859
Communications & Operations Management	11	4	.9072	.8241
Physical & Environmental Security	4	None	.8094	
Personnel Security	5	None	.8290	
Compliance	3	None	.8330	
New Construct				
Business Partner Security	None	2		.6229

V. DISCUSSION AND CONCLUSION

Although security checklists are widely used, they were criticized by Dhillon and Backhouse [2001] as carrying less conviction than work based on theoretical foundations. They contended that checklists emphasize observable events and focus attention on procedure without considering the social nature of the problems and without addressing the key task of understanding what the significant questions are. Thus, practices should be considered as part of the whole process. Information security is not a "stand alone" phenomenon.

ISO 17799 is widely accepted and recognized as "best practices" by information security professionals. The analysis in this study indicates that most of the security dimensions and items covered under ISO 17799 are highly valid. Seven of the ten original dimensions in the ISO 17799 were confirmed. Three dimensions in the ISO 17799 were not identified ("personnel security", "physical & environmental security", and "compliance"), and one new dimension "Business

Partner Security" was derived. As a result, eight dimensions of information security practices were generated. The new dimension ("external" or "business partner security") was derived from the original dimension of "communications and operations management". The model from the exploratory factor analysis is more parsimonious than the original ISO 17799.

The difference between the original dimensions in ISO 17799 and the ones from factor analysis is explained partly because of redundancy. All three eliminated dimensions are related to policies, operations or maintenance. Practically, to enhance the effectiveness of information security, it maybe necessary to allow all critical information systems and thus, security practices to be redundant across organizations.

The most problematic dimension is "communications and operations management". Originally, 11 items were proposed to measure this construct. As a result of the analysis, this dimension split into two separate dimensions, and five items resulted in low loadings. Examining the specific items, we found that three of these five items were ambiguous. For example, the first item is "uses formal procedures for processing information, scheduling, error handling, support, and recovery." This consequence resulted from the complex nature of operations management. The statements for operations management can never be too specific and detailed to be understood. This finding implies that when practitioners define information security practices, the definition cannot be too general or too detailed. The guideline is it should be specific, but applicable.

The finding of the new dimension "Business Partner Security" suggests that practitioners should pay more attention to external information security in forming information partnerships or adopting electronic business.

VI. CONTRIBUTIONS OF THE STUDY

This research is the first empirical attempt, to our knowledge, to validate information security guidelines and practices suggested by practitioners and organizations. It is usually difficult for academicians to suggest information security guidelines or practices to the practitioners as information security management tends to be organization-specific. However, academicians can provide insights and tools that enable practitioners either to develop or benchmark practices that ensure information security within their organizations. In this study, the international security management standard ISO 17799 was verified.

This study is one attempt to construct scales to measure information security practices. The development of high validity and reliability scales is an important step in the development of future research studies. The eight practice constructs are much shorter than the original 10 dimensions in the ISO 17799. Thus, the measures for these constructs are parsimonious and applicable.

The scales for information security practices generated in this study can be used as the basis for self-assessment, reassessing the security management of business partners, and independent evaluation of the effectiveness of ISM. The security practices framework can be used as a guideline or checklist to implement practices. For example, in the instrument, if two Likert-type scales were used (one measures the current practice, the other measures practices for the near future), the organizations can identify the strengths and weaknesses of their security practices. The instrument can also be used for benchmarking. If the instrument is used regularly, the comparison of results can identify which areas were improved and which areas need management to allocate the necessary resources to ensure the effectiveness of the security initiatives.

The findings from this study can also be used as a guideline for revising existing standards by established organizations such as International Standards Organization (ISO), Internet Engineering Task force (IETF), US National institute of Standards and Technology (NIST) as well as sector-specific and industry standards.

LIMITATIONS

We recognize three limitations to this study.

1. Since end-users access the system daily, their appropriate operations are vital to the systems' security. As the result, excluding the end-users opinion in the survey of security practices not only reduces the applicability and effectiveness of the security practices, this omission also limits the generalizability of our research results. Therefore, future research should use focus-group subjects and grounded-theory methods.

2. The survey of security practices was based on ISO 17799. Since information security management is an emerging area, guidelines may be unstable and change quickly. Many guidelines are available. Unfortunately, no statistics show which standards are most popular and widely accepted. Therefore, some factors may have been missed in our research.

3. The scope of organizations involved in this study was broad in terms of sector such as education, government, military, and business. Studies that focused on a specific sector or industry would identify practices that are more closely related to organizations within that specific sector or industry.

DIRECTIONS FOR THE FUTURE RESEARCH

For future research, the first extension of this study is to validate the eight-dimension security practice framework derived from this study. As such, confirmatory studies focused on specific industries are needed. Classification by the four digit industry code does not help in studying information security because the classification is too complex. Potential classification criteria include information intensity, information sensitivity, and/or information confidentiality.

The relationships between security objectives and practices are complicated, but important for practitioners to understand [Dhillon and Torkzadeh 2001]. Some practices only contribute to a particular security objective [Byrnes and Procter 2002]. Thus, it is necessary to explore the interrelationships between management practices and security objectives to answer questions such as how the practices interact and influence information security objectives, which practice contributes to which information security objective, and how much each of the management practices contributes to the total security goal. Such knowledge is important for managers in resource allocation and diagnostics.

The implementation of information security initiatives needs more study. On one hand, since information security practices can be defined at different level and have different implementation priority, it is important to identify the inter-relationships among security practices and provide sight to the underlying structure. In this way, it is easier for practitioners to associate the information security practices with security objectives and implement the practices more effectively. On the other hand, many factors influencing the success of security practices implementation. Identifying these factors (such as executive support, organizational policy, organizational culture, organizational self-efficacy, and financial benefit) are of practical significance to information security management.

Editor's Note: This article was received on March 16, 2005 and was published on April __, 2005.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the paper on the Web, can gain direct access to these linked references. Readers are warned, however, that
1. these links existed as of the date of publication but are not guaranteed to be working thereafter.

2. the contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. the author(s) of the Web pages, not AIS, are responsible for the accuracy of their content.
4. the authors of this article, not AIS, are responsible for the accuracy of the URL and version information.

Avolio, F. M. (2000). Best Practices in Network Security (digital version). www.networkcomputing.com/1105/1105f2.html?ls=NCJS_1105bt (current March 10, 2005).

Bruce, L. S. (2003). Information Security – Key Issues and Developments at www.pwcglobal.com/jm/images/pdf/Information%20Security%20Risk.pdf (current March10, 2005).

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.

Center for Strategic and International Studies (CSIS), (2002). *Cybercrime Cyberterrorism Cyberwarfare* at www.csis.org/pubs/cyberfor.html (current March 10, 2005).

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

Dhillon, G., and Torkzadeh, G., (2001). Value-Focused Assessment of Information System Security in Organizations, *Proceedings of ICIS* 2001, Atlanta, GA: Association for Information Systems

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

Hutt, A. E., Bosworth, S., and Hoyt, D. B. (1995). *Computer Security Handbook,* New York: Wiley.

Li, H., King G., Ross M., and Staples,G. (2000). BS7799: A Suitable Model for Information Security Management, *America's Conference on Information Systems*, Electronic Commerce track, August 10–13, Long Beach, CA, Atlanta, GA: Association for Information Systems

Nunnally, J.C. (1978). *Psychometric Theory* (2nd ed.). New York: McGraw-Hill.

Peltier, T. R. (2003). Preparing for ISO 17799, *Security Management Practices*, January/February, p21-28.

Rogers, M. (2001). A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: an Exploration Study, Unpublished dissertation. http://www.mts.net/~mkr/cybercrime-thesis.pdf (current January 5, 2005).

Setty, H. (2001). System Administrator – Security Best Practices. http://www.sans.org/rr/practice/sysadmin.php (current March 10, 2005).

Stefanek, G. L. (2002). Information Security Best Practices 205 Rules, Boston: Butterworth-Heinemann.

APPENDIX I. ISO 17799 FRAMEWORK

ISO 17799 Framework covers a total of 10 control areas consisting of 36 control objectives

Categories/Items

1. Security policy –Management direction and support for information

2. Organizational security – To help you manage information security within the organization
   -Information Security Infrastructure
   -Third-party access control
   -Outsourcing

3. Asset classification and control – To help identify assets and appropriately protect them
   -Asset accountability
   -Information classification

4. Personnel security – To reduce the risks of human error, theft, fraud, or misuse of facilities
   -Security in job definition & resourcing
   -User training
   -Responding to security incidents and malfunctions

5. Physical and environmental security – To prevent unauthorized access, damage and interference to business premises and information
   -Secure areas
   -Equipment security
   -General control

6. Communications and operations management – To ensure the correct and secure operation of information processing facilities
   -Operational procedures & responsibilities
   -System planning & acceptance
   -Protection against malicious software
   -Housekeeping
   -Network management
   -Media handling & security
   -Exchanges of information and software

7. Access control – To control access to information
   Business requirement for access control
   User access management
   User responsibilities
   Network access control
   Operating system access control
   Monitoring system access and use
   Mobile computing and teleworking

8. Systems development and maintenance – To ensure that security is built into information systems
   -System and application security requirements

-Cryptographic controls
-Security of system file
-Security in development and support processes

9. Business continuity management – To counteract interruptions to business activities and to protect critical business processes from effects of major failures or disasters

10. Compliance – To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations, and any security requirement. An organization using IS17799 as the basis for its ISMS, can become registered by BSI, thus demonstrating to stakeholders that the ISMS meets the requirements of the standard.
-Compliance with legal requirements
-Security policy & technical compliance review
-System audit considerations

APPENDIX II. ITEMS USED IN QUESTIONNAIRE[2]

The information security policy in your organization...
clearly defines information security objectives.
is regularly reviewed for effectiveness and completeness.
has a clear owner who is responsible for its update and maintenance.
clearly indicates management's intention to support information security programs.
clearly specifies the information security responsibility of employees.
clearly illustrates the importance of security to the organization.

Your organization...
has a dedicated security steering committee responsible for ISM.
has information security advisors in each business unit to coordinate ISM.
authorizes the ISM committee to make necessary decisions.
has an information security forum to give management direction and support.
controls third-party access by documenting the organization's security policy in the third-party contract.
controls outsourcing by communicating legal requirements with the service provider(s).

In your organization, information technology assets...
are classified based on level of confidentiality.
are clearly labeled based on level of confidentiality.
are recorded based on ownership.
are classified with a simple, effective system.

In your organization, the business continuity plan...
ensures speedy resumption of essential operations following system failure or interruption.
is tested regularly.
includes a risk analysis of critical processes.
is assessed using effective techniques.

[2] Note: Single underline indicates the item was kept in the same construct in the factor analysis; double underline indicates the item was loaded to other construct in the factor analysis. Note that each section corresponds to the equivalent section in Appendix I.

When it comes to personnel security...
job descriptions define relevant security responsibility.
job applications are screened if the job involves access to information processing facilities.
employees receive formal training on information security and organizational policies.
employees are instructed on how to handle information security incidents.
the company has disciplinary procedures for dealing with employees violating information security policy.

When it comes to physical and environmental security...
critical IT facilities are secured by logging and supervising physical entry of visitors.
IT equipment is properly located and protected to reduce risks from environmental threats and hazards.
IT equipment cannot be removed without authorization.
the organization has policies for confidential information handling.

When it comes to system access control, your organization...
has procedures for registration/de-registration for access to all multi-user information systems.
employs password management systems.
requires proper authentication for external connections.
requires users to follow security practices in selection and use of passwords.
has procedures for mobile computing control.
monitors and logs access and use of computer systems.
requires routinely reviewing audit logs.
audits all activities related to working remotely.

When it comes to compliance...
information systems are regularly reviewed to ensure that they are in compliance with company security policies and standards.
all policies and procedures are implemented to ensure compliance with legal requirements such as data protection and privacy of personal information.
access to system audit tools is restricted to prevent misuse or compromise.

When it comes to systems development and maintenance, your organization...
has formal procedures to ensure security is built into operational systems
follows risk assessment and risk management processes to determine acceptable controls.
uses cryptographic techniques to protect confidentiality, authenticity, and integrity of information.
has formal procedures to maintain the security of application software [e.g., application testing, changing, and replacing).
protects system files by controlling program source libraries in the development process to restrict possible corruption or tampering.

When it comes to computer and operations management, your organization...
uses formal procedures for processing information, scheduling, error handling, support, and recovery.
has a documented process for an incident management.
has documented management responsibilities in place to ensure control of all changes to equipment, software, and procedure.
takes measures to protect the integrity and security of essential software and information against virus and intrusion.
has a backup and recovery process to maintain the integrity and availability of essential information processing and communication services.
has policies requiring compliance with software licenses and prohibiting the use of unauthorized software.
has documented procedures for managing removable computer media such as CDs, disks, and printed reports.

has formal agreements with partners for the exchange of information.
has formal procedures to minimize the risk of essential systems failure.
takes appropriate security measures for electronic commerce to ensure information exchange.
takes appropriate security measures for publicly available systems such as web servers.

ABOUT THE AUTHORS

Qingxiong Ma is assistant professor of Computer Information Systems at Central Missouri State University. He received his Ph.D. in Management Information Systems in Southern Illinois University at Carbondale, and an MBA from Eastern Illinois University, Charleston, IL. His research interests include information technology adoption/diffusion, electronic commerce, and information security management. His articles appear in *International Journal of Healthcare Technology and Management, Journal of Organizational and End User Computing,* and *The DATA BASE for Advances in Information Systems.* He presented numerous papers at the America's Conference on Information Systems and Decision Sciences Institute Annual Meetings. His teaching interests include Systems Analysis and Design, Data Communication and Networks, Management of Information Systems, Database Management Systems, and Client/server Application Development.

J. Michael Pearson is Associate Professor of Information Systems at Southern Illinois University at Carbondale. Dr. Pearson is currently editor of the *Journal of Internet Commerce* and director of the Pontikes Center of Information Management at SIUC. Before coming to SIUC, Dr. Pearson was department chair (Business Computer Information Systems) at St. Cloud State University. Dr. Pearson presented several papers at regional, national and international conferences. He published articles in *Communications of the ACM*, *Information & Management*, *Journal of Strategic Information Systems*, *Journal of Information Systems*, *Journal of Computer Information Systems*, *Decision Support Systems*, *Review of Business*, *Journal of Internet Commerce*, *Information Resources Management Journal* and *Public Administration Quarterly*. His research interests are in technology adoption, e-commerce, management of quality, and IT project management.

Communications of the Association for Information Systems

ISSN: 1529-3181