The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0968-5227.htm

Information security management objectives and practices: a parsimonious framework

Qingxiong Ma
Department of Computer Information Systems, University of Central Missouri, Warrensburg, Missouri, USA
Allen C. Johnston
Department of Accounting and Information Systems, University of Alabama Birmingham, Birmingham, Alabama, USA, and
J. Michael Pearson
Department of Management, Southern Illinois University, Carbondale, Illinois, USA

Received 14 October 2007
Revised 14 January 2008
Accepted 14 January 2008

Abstract

Purpose – As part of their continuing efforts to establish effective information security management (ISM) practices, information security researchers and practitioners have proposed and developed many different information security standards and guidelines. Building on these previous efforts, the purpose of this study is to put forth a framework for ISM.

Design/methodology/approach – This framework is derived from the development of an a priori set of objectives and practices as suggested by literature, standards, and reports found in academia and practice; the refinement of these objectives and practices based on survey data obtained from 354 certified information security professionals; and the examination of interrelationships between the objectives and practices.

Findings – The empirical analysis suggests: four factors (information integrity, confidentiality, accountability, and availability) serve as critical information security objectives; most of the security areas and items covered under ISO 17799 are valid with one new area – "external" or "inter-organizational information security"; and for moderately information-sensitive organizations, "confidentiality" has the highest correlation with ISM practices; for highly information-sensitive organizations, "confidentiality", "accountability", and "integrity" are the major ISM objectives. The most important contributor to information security objectives is "access control".

Research limitations/implications – This study contributes to the domain of information security research by developing a parsimonious set of security objectives and practices grounded in the findings of previous works in academia and practical literature.

Practical implications – These findings provide insights for business managers and information security professionals attempting to implement ISM programs within their respective organizational settings.

Originality/value – This paper fulfills a need in the information security community for a parsimonious set of objectives and practices based on the many guidelines and standards available in both academia and practice.

Keywords Data security, Communication technology

Paper type Research paper

Information Management & Computer Security
Vol. 16 No. 3, 2008
pp. 251-270

0968-5227
DOI 10.1108/09685220810893207

Introduction

With society's increasing dependency on information technology (IT), the consequences of security breaches can be extremely grave (Power, 2002). In addition to monetary losses, breaches of information systems can also cause damages to businesses such as disruption of internal processes and communications, the loss of potential sales, loss of competitive advantage, and negative impacts on a company's reputation, goodwill and trust (Hoffer and Straub, 1989; Bruce, 2003). As a result, information security management (ISM) has become a required function (Filipek, 2007). In many cases, it is impossible or nearly impossible to run a business without the smooth and secure operation of its information systems (Zviran and Haga, 1999).

To protect organizational information assets from both internal and external attacks, many different information security standards and guidelines have been proposed and developed. For example, the Generally Accepted System Security Principles (GASSP) is a joint international effort between ten countries to develop a set of rules, practices, and procedures to achieve information integrity, availability, and confidentiality. The Federal Information Processing Standards Publications (FIPs PUBs) provide guidelines that are mandatory for government agencies, but optional for the private sector. The International Organization for Standardization (ISO)17799 is described as a suitable model for ISM and an appropriate vehicle for addressing ISM issues in organizations (Dhillon and Blackhouse, 2001). Additionally, ISM literature has provided different checklists (Dhillon and Blackhouse, 2001) and hundreds of "best practices" (Stefanek, 2002) for practitioners to use.

Much of the existing literature in the field of ISM has been based largely on case studies, anecdotal evidence and the prescription of industry "leaders". Surprisingly, to our knowledge, there has been no scientific study conducted on synthesizing ISM practices and mapping the relationships between these practices with ISM objectives. As the result, ISM, in many cases, is less effective than it needs to be. Particularly, what is missing in the existing literature is:

- a research methodology to identify the objectives of ISM, management practices used to achieve these objectives, as well as the underlying relationships between information security objectives and practices; and
- empirical testing based on data collected from security professionals.

In essence, what is missing is a framework for ISM – developed from extant academic literature, practitioner reports, and standards, and refined via survey data from certified information security professionals. Such a framework would provide a preferred approach to ISM and future ISM research endeavors.

Information security objectives and practices

As an initial step toward the creation of this framework, we first developed a comprehensive list of ISM objectives and practices based on literature and reports from academia, industry, and other sources specialized in security management. Then, using survey data from 354 certified information security professionals in the USA, we empirically assessed the prescribed objectives and practices. From this analysis, the core underlying objectives and practices most prevalent in the field were exposed, thereby allowing the production a refined set of ISM objectives and practices. As a final step, the relationships between the objectives and practices were examined based on

characteristics of the organizations from which the surveyed data were obtained. The resulting relationships gave an indication as to which objectives correlate with which practices and contributed to the formulation of an ISM framework that is both parsimonious and applicable to most organizations.

The determination of common objectives is important for both establishing the starting point for effective information security programs and for establishing evaluation criteria for diagnostic purposes (Siponen *et al.*, 2006). A good security program is a customized program, and its characteristics depend upon the goals, resources, and environment of the organization (Straub and Welke, 1998; Siponen, 2000). However, there are strong similarities between good security programs that can be analyzed and emulated to improve the security of most organizations (Bachman, 2002).

Peltier (2003) stated that the three traditional elements of ISM are confidentiality, integrity and availability of an organization's information. Confidentiality has received the most attention, probably because of its importance in military and government applications. Early work on security assurance was sponsored by the US Department of Defense. The most prominent model used in this environment was developed by Bell and La Padula (1976). This model dealt with mandatory and discretionary access controls with the primary objective of preventing illegal disclosure of information. Significant research efforts have been carried out to improve and supplement the information security evaluation criteria proposed in this model. As a result, integrity was added to the list of criteria (Dhillon and Blackhouse, 2001). Still, little attention has been paid to availability, with the exception of building fault tolerance into vendor products and including "hot and cold" sites for backup processing in disaster recovery planning. Most researchers and practitioners (Leiwo *et al.*, 1999; Rosenthal, 2002; Krauss and Tipton, 2002; Byrnes and Proctor, 2002) agree on these three essential or core objectives of ISM. They believe that these objectives can never be completely separated. Loss of one or more of theses objectives can threaten the continuity of even the largest corporate entity.

Byrnes and Proctor (2002) asserted that security is more than just trying to meet the confidentiality-integrity-availability objectives. They suggested a fourth information security objective: non-repudiation. Non-repudiation provides undisputable evidence that a specific action has occurred. The term "repudiate" is the synonym of "deny". In digital security, non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message (EarthWeb, 2003). The use of security-related technologies and the need for a secure and trusted method for creating digital signatures have led to non-repudiation becoming a new security objective. Krauss and Tipton (2002) include privacy in confidentiality. Other people suggest even more objectives such as accountability, utility, authorization, and identification (Host, 2001; Boykin, 2003).

Table I provides a summary of the 22 objectives of ISM proposed by information security researchers and professionals. The sources of these objectives and requirements come primarily from three groups: practitioners, academicians, and security organizations. Upon inspection, six objectives are most frequently cited. These objectives are confidentiality, integrity, availability, non-repudiation, authentication, and accountability. Going forward, these objectives will serve as the initial set of objectives for later refinement via a survey of certified information security professionals.

Table I.
Summary of ISM objectives

	Practitioners						Academicians						Organizations				
Objectives	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Confidentiality/privacy	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X
Integrity	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Availability	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X
Non-repudiation	X	X		X									X		X		
Identification	X																
Authentication	X	X			X			X					X				
Signature	X																
Authorization	X																
Access control	X					X		X									
Validation	X																
Certification	X																
Time-stamping	X																
Receipt	X																
Confirmation	X																
Ownership	X																
Anonymity	X																
Revocation	X																
Witnessing	X																
Utility					X			X									
Possession					X												
Auditability/accountability						X						X		X			X
Ethics									X								
References	1. Boykin (2003), 2. Host (2001), 3. Krauss and Tipton (2002), 4. Byrnes and Proctor (2002), 5. Parker (2002), 6. Hutt (2002)						7. Leiwo *et al.* (1999), 8. Rosenthal (2002), 9. Dhillon and Torkzadeh (2006), 10. Summers (2002), 11. Long (1999), 12. Rannenberg *et al.* (1999)						13. CIECA (2003), 14. ITsecurity.com, 15. SAWG (2002), 16. OIT (2002), 17. GASSP (2003)				

Note: Italicised areas represent most frequently cited information security objectives

Relating best practices and guidelines to objectives

Setting security objectives is just the first step towards implementing information security initiatives (Straub and Welke, 1998; Johnston and Hale, 2007). Without a series of actions or controls used to work towards these objectives, achieving them is merely a matter of chance. However, the complexity of security issues and the number of suggested practices make it increasingly difficult for managers to determine which practices should be implemented. Literature on ISM practices typically has provided checklists for practitioners to use. Many of the prevailing checklists were developed by analysts to check computer-based systems and make decisions on the necessary controls (Dhillon and Blackhouse, 2001). The most prominent checklists are IBM's 88-point security assessment questionnaire, SAFE checklist (Krauss, 1980), and AFIPS Checklist for computer center self-audits (Browne, 1979).

Although information security checklists are widely used, they have been criticized because they emphasize observable events and inevitably draw concern onto the detail of procedure without considering the social nature of the problems and without addressing the key task of understanding the underlying questions (Dhillon and Blackhouse, 2001). The ISO 17799 was released by the ISO in December 2000, was updated in 2005, and is one of many documents that provide information security professionals with a list of controls. It was intended to provide a common base for developing effective ISM practices and has become an internationally recognized ISM standard. This standard provides extensive guidance on the organizational aspects of ISM.

Table II presents 35 information security guidelines and "best practices" that have been provided by security individuals and organizations. The insights from these professionals suggest that some security practices are more important than others. For example, management policies, system access control, asset classification and control, employee training, physical security, and business continuity planning are often cited in literature as important guidelines and practices (see 11 italicised items in Table II). This table also indicates that all of these most frequently addressed "best practices" are included or implied by ISO 17799. For instance, the item "employee security education and training" is included under "personnel security", "security architecture design" is included in "system development and maintenance", and "authentication and authorization" is included in "access control." The broad coverage of these items by ISO 17799 suggests it is comprehensive and can be widely applied. As such, the complete set of ISO 17799 security practices will serve as the initial set of security practices to be refined via a survey of certified information security professionals.

Survey methodology

To this point, we have generated a comprehensive set of ISM objectives and practices as suggested by extant literature, standards, and reports from academia and industry. These objectives and practices form the early foundation of our proposed ISM framework. The next step is to refine the framework by streamlining the list of objectives and practices based on survey responses of security professionals currently practicing in the field.

The instrument used to conduct the survey consisted of three parts. Part A solicited information about the respondent's demographics and background information such as position within the organization, industry, and business size. Part B solicited perceptions from respondents about information security objectives within their

Table II.
Summary of ISM practices

Practices	Practitioners						Organizations				
	1	2	3	4	5	6	7	8	9	10	11
Management policies	X	X		X	X	X		X	X	X	X
Personnel policies	X								X	X	X
System access controls	X	X				X			X	X	X
Location of responsibilities within the organization	X								X		
Asset classification and control			X		X	X	X		X		
Physical and environmental security	X	X	X			X		X	X	X	X
Communications and operations management									X		X
System development and maintenance		X				X			X		X
Assess the security needs for business environment					X		X				
Dedicated funding and staff for information security				X	X		X				
Effective policies and procedures	X				X		X				
Software protection (by using firewalls)						X	X				
Install virus protection software		X				X					
Continuous employee education/training		X	X		X	X	X		X	X	X
Implement strong passwords			X				X				
General management								X			
Risk management			X	X	X	X		X	X	X	X
Security architecture design		X		X				X	X		X
User issues											
System and network management										X	X
Authentication and authorization		X							X		X
Monitor and audit		X	X		X	X			X		
Business continuity planning	X	X	X			X	X	X	X	X	X
Compliance (legal and ethical)									X	X	
Information management										X	
System (data) integrity		X							X	X	X
Information systems and countermeasure life cycle										X	
Hardware and software selection		X									
Internet security		X									
Data encryption		X				X					
Configuration documentation			X								X

(*continued*)

Practices	Practitioners 1	2	3	4	5	6	Organizations 7	8	9	10	11
Incident response capability				X		X					X
Hold program or business managers accountable					X						
Establish a central security group				X	X						
Support policies through central security group				X	X						
References	1. Hutt *et al.* (1995), 2. Stefanek (2002), 3. Setty (2003), 4. Avolio (2000)				5. GAO, 6. CIAO, 7. CERIAS 2002, 8. ISAlliance 2002, 9. ISO17799 2000/2005, 10. GASS, 11. FASP						

Note: Italicised areas represent most frequently cited information security practices

Table II.

respective organizations, and Part C solicited perceptions from respondents about information security practices within their respective organizations. As described previously, six objectives were identified and used as the initial set of security objectives (Table I). These six objectives were confidentiality, integrity, availability, non-repudiation, authentication, and accountability. Each of the six ISM objectives was measured via multi-item scales, resulting in a total of 27 items in Part B of the survey instrument. In Part C, the 16 practices in ISO 17799, represented by 35 items, served as a starting point. These 16 practices, derived from the 11 control areas of ISO 17799, are highlighted in Table II with an X corresponding to a covered practice. As some of the practices in ISO 17799 were compound-practices representing multiple ideas and/or concepts, it was necessary to operationalize these as multiple single-concept items within the survey instrument. As the result, we ended up with 56 items for Part C in the initial survey instrument.

The targeted subjects of this study were certified information security professionals. Our sample for this study comes from the International Information Systems Security Certificate Consortium $(ISC)^2$, which is a non-profit consortium and certification organization – not a membership organization. It is charged with certifying professionals seeking various certifications (including CISSP and SSCP). On the $(ISC)^2$ web site, a directory is provided of individuals who have been certified by $(ISC)^2$. This directory can be accessed through a search engine with search criteria options such as certification or location (country). Utilizing this search capability, we were able to obtain the contact information for approximately 5,600 certified information security professionals who reside within the USA. A total of 2,494 certified information security professionals were contacted and asked to participate in our web-based survey, from which 354 usable responses were obtained (14.2 percent response rate).

Non-response bias was tested based on responses provided by early and late respondents on age, education and work experience. Specifically, the respondents to the initial request for participation were considered as early respondents and those who responded after the initial reminder were considered late respondents. *T*-tests on specific demographic variables indicated that no systematic differences existed. Thus, we concluded that non-response bias was not an issue in the sample.

Refinement of ISM objectives and practices

The analysis of the survey data were conducted in three steps. First, principal component analysis (PCA) was used to identify key constructs in information security objectives, thereby providing a reduced set of ISM objectives. Second, to verify the construct structure of 16 ISM practices specified in ISO 17799, confirmatory factor analysis was conducted. The result of this analysis was a reduced set of ISM practices. Together, the refined set of ISM objectives and practices form our proposed ISM framework. A cluster analysis was then used to classify organizations based on the similarity of these constructs and their use within the organizations, thereby allowing us to explore the relationships between information security objectives and practices for each classification via a canonical correlation analysis.

Analyses of information security objectives

A PCA was used to identify the underlying ISM objective constructs of 27 initial ISM objective items. The results of an initial factor analysis suggest that six items did not

load significantly on their appropriate construct. These items were subsequently removed and the analysis re-run. Final analysis reveals a four factor solution: confidentiality, integrity, accountability, and availability. Table III presents the factor names and their corresponding items.

Survey findings

Analyses of information security practices

With regard to information security practices, this study attempts to refine the complete set of ISO 17799 practices implemented by security professionals as part of their ISM strategies. To fulfill this objective, a principle component analysis similar to that performed for the ISM objectives was conducted. All 56 items representing the 16 practices provided within ISO 17799 were considered and the principle component analysis was then utilized to reduce the number of items and dimensions, thereby generating a more parsimonious set. The result of this analysis suggests an eight factor solution presented in Table IV.

It is interesting to note that the results from Table IV are different from that in the original instrument at two levels. First, at the factor level (construct), the number of factors has been reduced from 16 to eight. The two factors representing "personnel security" and "compliance" were eliminated. The factors "physical and environment security" and "communications and operations management" merged. Additionally, one new factor (external information security) was derived. Second, at the item level, the total number of

	Loading
Integrity (Cronbach's $\alpha = 0.865$)	
1. Information should be reliable	0.824
2. The privacy of employees and customers should be protected	0.802
3. All systems should be accessible by properly authorized persons	0.667
4. All parties to a transaction should be confident that the transaction is secure	0.645
5. We should provide reliable information to business partners when necessary	0.641
6. Integrity of the information on systems must be maintained	0.616
7. Information should be protected or secured from unauthorized use	0.568
Confidentiality (Cronbach's $\alpha = 0.899$)	
1. Biometric authentication should be used	0.813
2. Logging all access attempts of confidential files is mandatory	0.751
3. All new data copied on a server should be logged	0.664
4. Physical access control is always no. 1 priority	0.633
5. All connections through the secured access point(s) should be logged	0.623
6. The systems should log all user account events	0.618
7. Servers with classified information should reside on an isolated network	0.600
8. All confidential data transfers should use an authentication system to identify users	0.558
9. All systems should ensure that a party cannot subsequently repudiate (reject) a transaction	0.558
Accountability (Cronbach's $\alpha = 0.754$)	
1. All systems should be protected by software of anti-virus or firewall	0.861
2. Computer users should not share accounts	0.691
3. Computer users should take responsibility to protect their data	0.584
Availability (Cronbach's $\alpha = 0.668$)	
1. All servers should be continuously available to their clients	0.765
2. The company should have redundancy in hardware to tolerate hardware failure	0.647

Table III.
Final factor loadings for ISM objectives

	Loading
Information security policy (Cronbach's α = 0.927)	
1. Clearly specifies the information security responsibility of employees	0.771
2. Clearly illustrates the importance of security to the organization	0.754
3. Has a clear owner who is responsible for its update and maintenance	0.750
4. Clearly indicates management's intention to support information security programs	0.722
5. Clearly defines information security objectives	0.713
6. Is regularly reviewed for effectiveness and completeness	0.638
Organizational security (Cronbach's α = 0.885)	
1. Authorizes the ISM committee to make necessary decisions	0.812
2. Has information security advisors in each business unit to coordinate ISM	0.796
3. Has a dedicated security steering committee responsible for ISM	0.780
4. Has an information security forum to give management direction and support	0.743
Asset classification and control (Cronbach's α = 0.851)	
1. Are clearly labeled based on level of confidentiality	0.854
2. Are classified based on level of confidentiality	0.798
3. Are classified with a simple, effective system	0.743
4. Are recorded based on ownership	0.608
Business continuity planning (Cronbach's α = 0.924)	
1. Is tested regularly	0.784
2. Includes a risk analysis of critical processes	0.755
3. Is assessed using effective techniques	0.754
4. Ensures speedy resumption of essential operations following system failure/interruption	0.731
System access control (Cronbach's α = 0.845)	
1. Monitors and logs access and use of computer systems	0.691
2. Has procedures for mobile computing control	0.6783
3. Employs password management systems	0.625
4. Requires routinely reviewing audit logs	0.615
5. Requires proper authentication for external connections	0.581
6. Audits all activities related to working remotely	0.575
7. Requires users to follow security practices in selection and use of passwords	0.550
Systems development and maintenance	
1. Has formal procedures to maintain the security of application software (e.g. application testing, changing, and replacing)	0.807
2. Uses cryptographic techniques to protect confidentiality, authenticity, and integrity of information	0.754
3. Protects system files by controlling program source libraries in the development process to restrict possible corruption or tampering	0.722
4. Has formal procedures to ensure security is built into operational systems	0.674
5. Follows risk assessment and risk management processes to determine acceptable controls	0.655
Communications and operations management (Cronbach's α = 0.824)	
1. Has a backup and recovery process to maintain the integrity and availability of essential information processing and communication services	0.786
2. Takes measures to protect the integrity and security of essential software and information against virus and intrusion	0.700
3. Has policies requiring compliance with software licenses and prohibiting the use of unauthorized software	0.614
4. Takes appropriate security measures for publicly available systems such as web servers	0.592
External information security (Cronbach's α = 0.623)	
1. Has formal agreements with partners for the exchange of information	0.609
2. Takes appropriate security measures for electronic commerce to ensure information exchange	0.605

Table IV.
Final factor loadings for ISM practices

items was reduced from 56 to 36. Three factors (organizational security, access control, and communications and operations management) had the number of items reduced. The most complicated and problematic dimension was "communications and operations management". Originally, this construct consisted of 11 items. As a result of this analysis, two items broke off as a new dimension – "external information security" and five others were dropped because of low-factor loadings.

Relationships between objectives and practices

As a first step in examining the relationships between ISM objectives and ISM practices, we first clustered the organizations of the participating information security professionals based on their use of information. The high-end of this continuum were organizations that are information-sensitive and the low-end of this continuum were organizations who work primarily with non-sensitive information. For example, the information utilized and retained in manufacturing is typically less sensitive than that in education, government and insurance companies, which, in turn, is less sensitive than that in financial institutions and healthcare.

Although we expected that organizations could be classified into three groups (or clusters) in terms of information sensitivity (high, medium, and low), 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, the responding information security professionals 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 do not perceive organization information as important or sensitive, probably would not feel a need to have these types of IT professionals on their staff.

As a result of the cluster analysis, 158 cases were assigned to Cluster one and 196 were assigned to Cluster two. Additional *t*-tests on the demographic information for each cluster were performed. 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 results imply that the organizations which were moderately information sensitive (Cluster one) were smaller and had younger information security professionals with less work experience, while organizations dealing with higher levels of information-sensitivity (Cluster two) were larger firms and had older, more experienced information security professionals.

Cluster one analysis

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. Organizations should set objectives first and then develop and enforce appropriate practices based on those objectives. As such, the eight composite variables for ISM practices were treated as the dependent variable set and the four composite variables for ISM objectives were treated as the independent variable set. The results of the canonical correlation analysis (shown in Table V) reveal that the influence of dependent variables (security practices) on the independent variate (security objectives) comes mainly from "access control".

Variate/variables	Canonical weights (standardized)	Canonical loadings	Canonical cross-loadings
Independent variables – ISM objectives			
Integrity	0.143	0.473	0.461
Accountability	− 0.014	0.444	0.433
Confidentiality	0.952	0.991	0.966
Availability	− 0.009	0.091	0.089
Dependent variables – ISM practices			
Security policy	− 0.019	0.171	0.167
Organizational security	0.026	0.219	0.214
Asset classification	− 0.005	0.164	0.160
Continuity	− 0.051	0.079	0.077
Access control	1.001	0.997	0.972
System development	− 0.028	0.216	0.211
Operations	− 0.073	0.160	0.156
External security	0.034	− 0.032	− 0.031

Table V.
Canonical weights for the first canonical function in Cluster one

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[1].

Cluster two analysis

Following the same procedures as described previously, canonical correlation analysis was conducted for Cluster two. The results of the canonical correlation analysis (shown in Table VI) reveal that the influence of dependent variables (security practices) on the independent variate (security objectives) comes mainly from "access control", with a small portion coming 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",

Variate/variables	Canonical weights (standardized)	Canonical loadings	Canonical cross-loadings
Independent variables – ISM objectives			
Integrity	0.067	0.510	0.470
Accountability	0.343	0.604	0.556
Confidentiality	0.714	0.940	0.865
Availability	0.037	0.244	0.224
Dependent variables – ISM practices			
Security policy	0.149	0.350	0.322
Organizational security	− 0.004	0.431	0.397
Asset classification	− 0.023	0.293	0.270
Continuity	− 0.030	0.202	0.186
Access control	0.970	0.991	0.912
System development	0.030	0.273	0.251
Operations	− 0.032	0.288	0.265
External security	0.013	0.160	0.148

Table VI.
Canonical weights for the first canonical function in Cluster two

"accountability" and "integrity". The importance order of their contribution is "confidentiality", "accountability", "integrity", and "availability".

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

Summary of statistical analyses and framework presentation

In this study, we propose a parsimonious framework for ISM based on a refined set of ISM objectives and practices as determined by a survey of 354 certified information security professionals. Through a review of literature, industry reports and standards, 22 distinct ISM objectives were identified. Following an analysis of the survey data, this initial set of objectives was reduced to four. Similarly, the initial set of 16 ISM practices – based on the ISO 17799 international standard – was reduced to seven. One new dimension – "external" or "inter-organizational information security" was derived, thereby bringing the total number of ISM practices to eight.

In an effort to advance the framework even further, we explored the relationships between ISM objectives and ISM practices. The relationships between the objectives and practices were examined using cluster analysis and canonical correlation analysis. Based on the four objectives, organizations were separated into two distinct groups. The first cluster was composed of 158 respondents (44.6 percent) and the second cluster had 196 members (55.4 percent). 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 most important information security objectives were "confidentiality", "accountability", and "integrity". Different from Cluster one, besides the major contributor "access control", "organizational security" and "security policy" also contributed to the achievement of information security objectives. The results of this study suggest, "access control" is the most important information security practice in both groups.

Cluster one	Canonical cross-loadings	Cluster two	Canonical cross-loadings
Independent variables			
Confidentiality	0.966	Confidentiality	0.865
Integrity	0.461	Accountability	0.556
Accountability	0.433	Integrity	0.470
Availability	0.089	Availability	0.224
Dependent variables			
Access control	0.972	Access control	0.912
Organizational security	0.214	Organizational security	0.397
System development	0.211	Security policy	0.322
Security policy	0.167	Asset classification	0.270
Asset classification	0.160	Operations	0.265
Operations	0.156	System development	0.251
Continuity	0.077	Continuity	0.186
External security	−0.031	External security	0.148

Table VII. Contribution order of variables

Based on both the refinement of ISM objectives and practices as well as the analysis of relationships between objectives and practices, a parsimonious framework for ISM is proposed and illustrated in Table VIII. A discussion of the results of this study, the proposed framework and its implications and contribution is provided in the following section.

Discussion

Interpretation of findings for ISM objectives

The findings of this research and the resultant ISM framework have two important implications. First, when practitioners establish information security objectives, they should use the four objectives identified in this study as a starting point. Based on their specific business environment and organizational goals, they can establish information security objectives that are appropriate for their organizations. Although previous studies have focused on the internal aspect of ISM, we argue that organizational objectives for information security should not be based solely on internal analysis. The development of ISM objectives should also consider external forces. For example, it is crucial for top management to comply with security laws such the Privacy Act, the Sarbanes-Oxley Act (SOX) of 2002, the Gramm-Leach-Bliley Act (GLB Act), and the Health Insurance Portability & Accountability Act of 1996 (HIPAA). Failure to comply with these laws can result in severe consequences. For example, according to SOX, a corporate officer who knowingly authorizes a false financial report can be fined up to $1 million and sentenced to as many as ten years in prison. In this case, the information security initiatives come from external pressure rather than internal forces.

Interpretation of findings for ISM practices

In ISM, standards play an important role by enforcing security baselines. However, they should not be relied upon blindly. Instead, they should reflect the constantly changing environments in which they are being deployed (Mercuri, 2003). ISO 17799 was originally developed based on the experiences of information security professionals worldwide. It has been widely accepted and recognized as a "best guide" by information

Medium information sensitivity organizations	High information sensitivity organizations
Rank of ISM objectives	
1. Confidentiality[a]	1. Confidentiality[a]
2. Integrity	2. Accountability[a]
3. Accountability	3. Integrity[a]
4. Availability	4. Availability
Rank of ISM practices	
1. Access control[a]	1. Access control[a]
2. Organizational security	2. Organizational security[a]
3. System development	3. Security policy[a]
4. Security policy	4. Asset classification
5. Asset classification	5. Operations
6. Operations	6. System development
7. Continuity	7. Continuity
8. External security	8. External security

Note: [a]Most significant contribution to ISM

Table VIII.
Proposed framework for ISM

security professionals. Since information security is a dynamic process and costs money to achieve, focusing on the right objectives and aligning and implementing the right practices are important. Therefore, this and other standards should be periodically refined to reflect the changing environment.

The difference between the original dimensions in ISO 17799 and those obtained in this study can be partially explained by redundancy. The eliminated dimensions included items that were closely related to the items underlying "security policy", "operations management" or "system access control". Practically, in order to enhance the effectiveness of information security, it may be necessary to allow all critical information systems and thus, security practices to be redundant across the organizations. For example, the requirement on "personnel security" in terms of recruiting and training can be included in "security policy." However, theoretically, this is not necessary. Compared with ISO 17799, the refined model has fewer dimensions, no single-item constructs or compound items (items with multiple meanings), but is still representative of the original model. Thus, the refined framework is more parsimonious and precise, but with higher operationality. The importance of parsimony lies in that practitioners can focus their limited resources on the essential practices and eliminate redundant practices. With precise measures (items) of those security practices, ambiguity and misunderstanding will be removed or reduced. As a result, the security practices are better focused and understood, and thus, their applicability and the effectiveness of the security practices should be improved.

The finding that the implementation of "organizational security" has the items with lowest means and highest standard deviation implies that the implementation level of this component is very low and it deserves more attention. This factor defines the organizational information security infrastructure. Feedback provided by information security professionals suggested that the reasons for low implementation include the lack of authority, lack of executive support, and lack of understanding the importance of information security. This finding has special significance to management in organizations. First, information security professionals must increase communication with management, trying to raise the information security awareness within the organization, and propose applicable solutions. Second, management in the organizations needs to realize the value of information security, assign appropriate priority to information security, and give necessary authority to information security professionals. Third, organizations should have trained and experienced personnel in charge of information security. Any improvement of this factor will improve the effectiveness of information security initiatives.

The finding of the new dimension "inter-organizational security" suggested that practitioners should pay more attention to external information security in forming information partnerships or adopting electronic business. Within the globalized business environment, organizations depend on IS/IT to exchange information, goods, and services. Many organizations are increasingly adopting inter-organizational IS/IT (IOS) infrastructures to establish and maintain closer cooperative relationships with their partners in the supply chain. A secure information system not only can ensure business continuity, minimize business damage, facilitate business partnerships by providing confidence in the information sharing process, but can also meet customers and trading partners' security expectations of an organization's information systems.

Interpretation of findings for relationships between objectives and practices

For the first cluster of organizations (medium information sensitivity), "confidentiality" had the highest correlation with information security practices. Information security professionals in these organizations believed that the security practice contributing most to their security objectives was "access control". For the second cluster of organizations (high-information sensitivity), "confidentiality", "accountability," and "integrity" together determined the security practices. The major security practices that impacted information security objectives for this group were: "access control", "organizational security", and "security policy". "Access control" was the only practice which contributed heavily to information security objectives in both groups. The items in this dimension focused mainly on technical controls. This finding is consistent with that of previous studies.

Briney and Prince (2002) indicated that most of the security decisions in small- and medium-sized organizations are guided by management-approved policies. The majority of these organizations spend the most security dollars per user and per machine. However, in large organizations, security has generally become institutionalized into the corporate culture via policies (Baskerville and Siponen, 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.

Therefore, to have more effective security practices, practitioners should pay attention to "organizational security" and "security policies". Since 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. Recently, many researchers have noticed the importance of human factors within the ISM environment.

Finally, the results from canonical analysis also indicated that "inter-organizational" 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. Kauffman and Mohtadi (2003) as well as Kinsey and Ashman (2000) found that information sharing is not equally bi-directional in the supply chain. Usually, it was initiated by suppliers because of business strategy, and buyers have limited benefits from this initiative. Also information sharing must be based on trust and insufficient trust generally deters buyers from sharing critical information with their suppliers. Currently, 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 will increase.

Contributions

The findings of this study can provide a foundation that can facilitate further study in the area of ISM. In this study, we proposed a framework for ISM derived from:

- the development of an a priori set of objectives and practices as suggested by literature, reports, and standards in academia and practice;

- the refinement of objectives and practices based on survey data obtained from 354 certified security professionals; and
- the examination of interrelationships between information security objectives and practices.

Thus, our research provided a comprehensive and holistic perspective on ISM.

Pragmatically, this study provides some implications for practitioners to follow. By following this framework, information security practitioners can develop a better understanding of how to initiate ISM plans in order to provide secure information for their organizations. Another contribution of this study is that it refined ISO 17799. Typically, practitioners have been overwhelmed by the number of guidelines and "best practices" suggested by various agencies/academicians. Since practitioners believe ISO 17799 provides an authoritative statement on information security, it is important to improve this standard so that more organizations can benefit from it. The findings from this study can be used as a guideline by organizations such as ISO, internet engineering task force, and the US National Institute of Standards and Technology. For example, for organizations that do not have specific information security requirements, the refined ISO 17799 can be used as a basis and metric for plotting progress towards the achievement of information security practices. Based on their organizational information security objectives, organizations can determine appropriate security practices using this framework.

Limitations and future research

As with all studies, this study has limitations. First, the study is subjective because the data were self-reported. This suggests that different respondents may have different understanding about the same questions. This also implies that a respondent's answer might be biased or influenced by external factors when they evaluated the questions. For example, when respondents were asked to evaluate the information security objectives, their answers might be influenced by cost.

Next, the survey for security practices was based on ISO 17799. Since ISM is an emerging area, this and other guidelines may be unstable and rapidly changing. Other guidelines are available and there are no statistics to show which standards are most popular or widely accepted. Thus, factors may have been missed in our research.

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

The primary extension of this study is to validate the proposed framework for ISM. To set up more feasible and effective information security systems, the information security program should be based on theory and rigorously tested within specific industries. Potential classification criteria include information intensity, information sensitivity, or information confidentiality. The next logical extension would be additional study related to information security objectives and practices. The four constructs for information security objectives and eight constructs for information security practices need to be validated. These constructs need further improvement in terms of construct reliability and face validity.

The findings also point to a limited perception regarding the importance of availability. The rationale for this finding has many possible roots, including the role in which the survey respondents have within their respective firms, or a potential bias among the respondents toward technical security as opposed to business value. Future research endeavors within this stream should consider such potential bias based on roles and industry, as well as the business implications of implementing a framework such as the one proposed in this study.

Finally, the implementation of information security initiatives needs more study. Since both information security objectives and practices can be defined at different levels and have different implementation priorities, it is important to identify the inter-relationships among practices. In this way, it is easy for practitioners to associate an information security practices with security objectives and implement the practices more effectively. Identification of critical factors such as executive support, organizational policy, organizational culture, organizational self-efficacy, and financial benefit can have practical significance to ISM.

Conclusion

Through an empirical study, we examined the dimensions of information security objectives and practices. Specifically, we explored the inter-relationships between information security objectives and practices and developed a parsimonious framework for ISM. Practitioners should use the proposed framework as a starting point to develop particular information security objectives, which reflects their business environment and business goals. Based on the information security objectives selected, organizations should implement the most effective practices. They can use the eight information security practices as a guideline or checklist to enhance this implementation.

As opposed to most of the studies in the literature, our data comes from security professional groups, which entails our findings have better external validity. To our knowledge, this is the first time that ISM has been discussed under a process-oriented framework; it is the first time the underlying relationships between security objectives and practices have been analyzed; and it is the first time that security standard ISO 17799 has been empirically examined. Therefore, we hope this study has special contribution to the ISM community.

Note

1. Sensitivity was estimated by removing a different independent or dependent variable from the analysis. The results indicated that the canonical loadings for Clusters one and two were very stable and consistent in each of the cases where an independent variable was deleted. The overall canonical correlations also remained stable.

References

Avolio, F. (2000), "Best practices in network security", available at: www.networkcomputing.com/1105/1105f2.html?ls = NCJS_1105bt (accessed February 2007).

Bachman, D. (2002), "Information systems security: principles and perspectives", Sprint E|Solutions White Paper, Overland Park, KS.

Baskerville, R. and Siponen, M. (2002), "An information security meta-policy for emergent organizations", *Journal of Logistics Information Management*, Vol. 15 Nos 5/6, pp. 337-46.

Bell, D. and La Padula, A. (1976), *Secure Computer Systems: Unified Exposition and Multics Interpretation*, MITRE Corp., Bedford, MA.

Boykin, P. (2003), "Practical cryptography and internet applications", available at: www.ee.ucla.edu/ ~ boykin/crypto_course/crypto_alg.ppt (accessed February 2007).

Briney, A. and Prince, F. (2002), "Does size matter?", available at: www.infosecuritymag.com/2002/sep/2002survey.pdf (accessed February 2007).

Browne, P. (1979), *Security: Checklist for Computer Center Self Audits*, AFIPS Press, Arlington, VA.

Bruce, L. (2003), "Information security – key issues and developments", available at: www.pwcglobal.com/jm/images/pdf/Information%20Security%20Risk.pdf (accessed February 2007).

Byrnes, F. and Proctor, P. (2002), "Information security must balance business objectives", available at: http://informit.com (accessed February 2007).

Dhillon, G. and Blackhouse, J. (2001), "Current directions in IS security research: towards socio-organizational perspectives", *Information Systems Journal*, Vol. 11 No. 2, pp. 127-53.

Dhillon, G. and Torkzadeh, G. (2006), "Value-focused assessment of information system security in organizations", *Information Systems Journal*, Vol. 16 No. 3, pp. 293-314.

EarthWeb (2003), "IT management", available at: http://itmanagement.webopedia.com/TERM/N/nonrepudiation.html (accessed February 2007).

Filipek, R. (2007), "Information security becomes a business priority", *Internal Auditor*, Vol. 64 No. 1, p. 18.

Hoffer, J. and Straub, D. (1989), "The 9 to 5 underground: are you policing computer crimes?", *Sloan Management Review*, Vol. 30 No. 4, pp. 35-43.

Host, R. (2001), "New information security requirements for federal agencies", available at: www.sans.org/rr/policy/fed.php (accessed February 2007).

Hutt, A., Bosworth, S. and Hoyt, D. (1995), *Computer Security Handbook*, 3rd ed., Wiley, New York, NY.

Johnston, A. and Hale, R. (2007), "Improved security through information security governance", *Communications of the ACM*, Fall (in press).

Kauffman, R. and Mohtadi, H. (2003), "Analyzing interorganizational information sharing strategies in B2B e-commerce supply chains", *Proceedings of INFORMS Conference on Information Systems and Technology, Atlanta, GA*.

Kinsey, J. and Ashman, S. (2000), "Information technology in the retail food industry", *Technology in Society*, Vol. 22 No. 1, pp. 83-96.

Krauss, L. (1980), *SAFE: Security Audit and Field Evaluation for Computer Facilities and Information Systems*, Amacon, New York, NY.

Krauss, M. and Tipton, H. (2002), *Handbook of Information Security Management*, CRC Press, Boca Raton, FL.

Leiwo, J., Gamage, C. and Zheng, Y. (1999), "Organizational modeling for efficient specification of information security requirements", *Advances in Databases and Information Systems: 3rd East European Conference, ADBIS'99, Maribor*, pp. 247-60.

Long, C. (1999), "A socio-technical perspective on information security knowledge and attitudes", unpublished dissertation, The University of Texas at Austin, Austin, TX.

Mercuri, R. (2003), "Standards insecurity", *Communications of the ACM*, Vol. 46 No. 12, pp. 21-5.

Parker, D. (2002), "Toward a new framework for information security", in Bosworth, S. and Kabay, M.E. (Eds), *Computer Security Handbook*, Wiley, New York, NY.

Peltier, T. (2003), "Establishing business controls for electronic mail communications", *Information Systems Security*, Vol. 12, pp. 34-43.

Power, R. (2002), "2002 CSI/FBI computer crime and security survey", *Computer Security Issues &Trends*, Vol. 8 No. 1, pp. 1-22.

Rannenberg, K., Pfitzmann, A. and Muller, G. (1999), "IT security and multilateral security", in Muller, G. and Rannenberg, K. (Eds), *Multilateral Security in Communications – Technology, Infrastructure, Economy*, Addison-Wesley-Longman, Reading, MA.

Rosenthal, D. (2002), "Intrusion detection technology: leveraging the organization's security posture", *Information Systems Management*, Vol. 19 No. 1, pp. 35-44.

Setty, H. (2003), "System administrator – security best practices", available at: www.sans.org/rr/practice/sysadmin.php (accessed February 2007).

Siponen, M. (2000), "A conceptual foundation for organizational information security awareness", *Information Management & Computer Security*, Vol. 8 No. 1, pp. 31-41.

Siponen, M., Baskerville, R. and Heikka, J. (2006), "A design theory for secure information systems design methods", *Journal of the Association for Information Systems*, Vol. 7 No. 11, pp. 725-70.

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

Straub, D. and Welke, R. (1998), "Coping with systems risk: security planning models for management decision making", *MIS Quarterly*, Vol. 22 No. 4, pp. 441-69.

Summers, R. (2002), *Secure Computing: Threats and Safeguards*, McGraw-Hill, New York, NY.

Zviran, M. and Haga, W. (1999), "Password security: an empirical study", *Journal of Management Information Systems*, Vol. 15 No. 4, pp. 161-85.

Further reading

Everitt, B., Landau, S. and Leese, M. (2001), *Cluster Analysis*, 4th ed., Edward Arnold Publishers Ltd, London.

Corresponding author
Allen C. Johnston can be contacted at: ajohnston@uab.edu