Available online at www.sciencedirect.com
ScienceDirect
Information & Management 44 (2007) 480–491
INFORMATION & MANAGEMENT
www.elsevier.com/locate/im

Threats and countermeasures for information system security: A cross-industry study

Quey-Jen Yeh [a,*], Arthur Jung-Ting Chang [b]

[a] Department of Business Administration, National Cheng Kung University, Tainan, Taiwan
[b] Department of Information Management, Chin Min Institute of Technology, Miaoli, Taiwan

Received 19 May 2005; received in revised form 20 March 2007; accepted 6 May 2007
Available online 27 June 2007

Abstract

IS security threats have increased significantly in recent years. We identified the gaps between manager perceptions of IS security threats and the security countermeasures adopted by firms by collecting empirical data from 109 Taiwanese enterprises. Industry type and organizational use of IT were seen as the two factors that affected the motivation of firms to adopt security countermeasures, but their implementation did not necessarily affect the threat perceptions of the managers. Analyses of responses suggested that the scope of the countermeasures adopted were not commensurate with the severity of the perceived threats. Among the threats, networks were rated as contributing the most severe threat and yet had the lowest level of protection, this was followed by threats due to personnel and administrative issues. We therefore addressed threat mitigation strategies, specifically in terms of the differences between industries.

Keywords: IS security; IS threats; Countermeasures; Security adoption; Threat mitigation

1. Introduction

According to a survey of 530 U.S. enterprises by the Computer Security Institute, 90% had suffered security breaches, and 75% had experienced business difficulties due to security breaches, resulting in losses of $201 million in 2002 [26]. Researchers investigating IS security have proposed various theories and approaches to manage the threats by analyzing IS risks (e.g., [30]), modeling IS security (e.g., [29]), developing security strategies and policies (e.g., [23]), and establishing international security standards (e.g., [6]). However, studies seldom consider how organizational characteristics influence security adoptions, nor do they pay attention to industrial applications [3].

The effect of IT value in industrial contexts is clear. High-tech businesses rely primarily on two opposing information values: the dissemination of information for innovation success and the protection of information to retain competitive advantage (e.g., [21]). In contrast, manufacturing firms coordinate activities with their supply chain partners, and service-based industries use information to service their customers directly [18]. In turn, IS threats differ according to the applications and arise from either technical system defects or human error and administrative flaws. The four main threats to IS assets (interruption, interception, modification, and fabrication) affect industries differently [14]; in retailing or service firms, interruption is most significant, whereas manufacturing firms consider interception and interruption critical, while banking and finance worry

* Corresponding author. Fax: +886 6 2376811.
E-mail addresses: yehqj@mail.ncku.edu.tw (Q.-J. Yeh), jungting@ms.chinmin.edu.tw (A.J.-T. Chang).

0378-7206/$ – see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.im.2007.05.003

about all four. As a component of the IS, security must keep pace with firm growth. Physical security and numerous backups no longer provide sufficient security, and managerial perceptions of threats without security activities do not help. Awareness of security principles based on specific business values at the firm and industry level thus is essential for IS security.

2. Background and research framework

2.1. Types of IS assets, threats, and security countermeasures

According to Straub and Nance [28], people frequently misuse hardware, programs, data, and computer services. Each has specific risks. *IS risk* involves the *vulnerability* of IS assets to attacks from *IS threats*, where a ''vulnerability'' can affect an IS asset negatively [25]. Risk occurs when assets are vulnerable to threats. Meanwhile, risk management attempts to avoid threats or reduce their impact under attack.

A *security countermeasure* refers to a way to detects, prevent, or minimize losses associated with a specific IS threat [24]. Threats frequently are categorized according to the type of assets involved. Icove et al. [13] used a criminology perspective to group security approaches into seven categories: software, hardware, data, network, physical, personnel, and administration (including security regulations and policies). Furthermore, Loch et al. [20] constructed a threat model that had four dimensions: sources, perpetrators, intent, and consequence, with threats occurring from the inside or outside with the perpetrators either be human or non-human and the actions accidental or intentional with the consequence a disclosure, modification, destruction, or denial of service. White et al. [33] in their study of responses to threats distinguished between internal and external IS security functions, where *internal functions* focused on technical issues, whereas *external functions* stressed managerial and operating security, or nontechnical issues, on the basis of the US security standard NIST SP800-30 [22].

Fitzgerald [7] listed 15 leading IS threats, including data processing errors, network breakdowns, software flaws, loss of key personnel, etc. Others proposed similar lists (e.g., [34]). Notably, the BS7799 Code [2], a security standard that proposes a minimum requirement for IS security, categorized a set of more than 100 security controls in 10 categories, 5 of which pertained to nontechnical issues involving personnel, compliance, security policies, security organization, and business continuity planning. Except for externally requested regulations, such as privacy laws or government regulations, firms mostly determine their security policies and procedures internally. Recent papers (e.g., [11]) have urged the inclusion of *insurance* and *risk transference*.

2.2. Adequacy of IS security

2.2.1. Summary of fundamental security countermeasures

As defined by CNSS [4], effective IS security should protect ''information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.'' According to Kankanhalli et al. [15], *preventive efforts* include deploying advanced security software or controls to protect IS assets, such as advanced access control, intrusion detection, firewall, surveillance mechanisms, and the generation of exception reports. *Deterrent efforts* include developing security policies and guidelines, educating users and training experienced auditors to audit IS use.

We split 50 fundamental security countermeasures commonly adopted to evaluate the adequacy of IS security, as shown in Table 1, into seven categories.

2.2.2. IS security baseline

Effective IS security should span the entire IT environment, defining administrative regulations and educating individuals to understand the need for IS security and the consequences of IS abuse. As proposed by von Solms et al. [32], the security baseline should trace all countermeasures for all IS assets and threats. However, emphasizing security excessively may be costly and hamper a firm's productivity. They divided IS security into several levels of an *Operational Security Environment* (OSE). Among these levels, *ideal OSE* represented complete protection with no risk of services being disrupted; *prescribed OSE* represented a required set of countermeasures defined by interested external parties; and *survival OSE* defined the countermeasures that protected critical information whose disruption would be disastrous. The *baseline OSE* can lie anywhere between the prescribed and survival OSE. They also suggested that a warning should be triggered when the percentage of countermeasures installed was less than 60% of the baseline OSE.

2.3. Factors affecting organizational adoption of IS security

Many authors (e.g., [31]) have commented on the myth that security is simply a technical issue. Often, the

Table 1
A summary of fundamental security countermeasures

	P/D[a]
IT-related countermeasures	
Software	
User entrance log	P
System recovery	P
Multi-user system	P
Scanner	P
Automatic debug and test	P
Access control to program source	D
Verification of system modified	D
Covert channels and Trojan code	P
Hardware	
Remote mirroring	P
Surveillance system use	P
Entrance limitation	P
Emergency power source (UPS)	P
Periodical disk checking	P
Data	
Information backup	P
Data access controls, authentication	P
User access rights, authorization	P
Enforced path	P
Event logging	P
Information handling procedures	D
Management of removable media	D
Disposal of media	D
Network	
Anti-virus software	P
Encryption	P
User authentication	P
Instruction detection systems	P
Firewalls	P
Alternative circuit	P
Digital signatures	P
Limitation of connection time	P
Non-IT-related countermeasures	
Physical facilities and environment	
Lightning protector	P
Air conditioner	P
Fireproof installations	P
Waterproof installations	P
Quakeproof installations	P
Personnel	
Confidentiality agreement	D
Invalid account removing	D
Information security consultant	D
Security audit irregularly	D
Security education and training	D
Operational procedures training	D
Incident report procedures	D
Regulation and legality (including risk transference)	
Security policy	
Information security policy	D
Security in job responsibilities	D
Business continuity management	D
Compliance with legal requirements	
Privacy of personal information	D
Intellectual property rights	D
Risk transference	
Security service provider	D
Security outsourcing	D
First party insurance	D
Third party/public liability insurance	D

[a] P/D means preventive controls or deterrent controls.

benefits of security are not considered important until a security breach has occurred. Until recently, innovation adoption theory was ignored in security adoption studies. Based on theories in innovation adoption and planned behavior, some researchers have explored the influence of various factors on security adoption, such as firm size, industry type, top management support, moral compatibility, peer influence, and computing capacity [19].

Rogers's [27] innovation diffusion theory has served as the basis for many innovation and technology adoption studies. The theory suggests that adoption or implementation depends on five broad characteristics: relative advantage, compatibility, complexity, observability, and trialability. Iacovou et al. [12] proposed perceived benefits, organizational readiness, and external pressure, and Zmud [35] on the other hand suggested borrowing the "technology-push and need-pull" concepts from engineering literature to understand use of innovations.

Together, prior research has shown that studies of innovation adoption should cover three general categories: perceived innovation advantage, external pressure, and organizational need. Accordingly, we used three constructs – managerial perceptions of IS threats to business, industrial type, and level of organizational computerization – to explore organizational security preparations.

2.4. Current study

2.4.1. Managerial perceptions of IS security threats to business

In IS security, managers' perceptions of potential IS threats to business affect expectations of security risk management programs. Their awareness of existing IS threats are critical to security adoption. However, assessing threat severity using only existing perceptions may be inadequate for threat categories that are currently low but have significant potential to increase. A specific IS threat perceived to be growing should receive attention from security managers. Therefore, we

considered two types of threat: perceived present threat and threat increment from the past to the present.

2.4.2. Security needs in relation to industry

The rapid growth in supply chain management has altered the capabilities of manufacturing plants from individual transactions to mission-critical enablers of processes [1]. Mohr has argued that the information value of the high-tech industry should be retained through rigorous plans that institute only need-to-know sharing. Davamanirajan et al. [5] further noted that trade services in the financial market typically required capabilities designed with security considerations in mind.

Mohr also argued that IS security was particularly crucial for firms that were highly information-intensive or relied heavily on IS. Jung et al. observe that the threats associated with the Internet varied among industries according to the needs of the organization for information availability, confidentiality, and integrity. Goodhue and Straub [10] suggested three reasons for financial firms to invest more in IS security than other firms. First, they rely on IS for business operations; second, losses arising from IS abuse can be extremely large; and third, their public image is critical to their business. In contrast, manufacturing firms have internal operations and transaction processes and thus require fewer strategy-level IS applications [16]. In our study, we focused on these issues in four industries: general manufacturing (steel/metal, cement, paper, car spare parts, textile, petroleum, etc.), high-tech (electronics, computer and peripherals, communications, etc.), banking/finance, and retailing/service (wholesale/retailing, utilities, transportation, etc.).

2.4.3. Security needs in relation to organizational computerization

The requirement for IS security also varies within an industry. Organizations with different IS/IT architectures differ in their microcomputer, mainframe, network, and client–server settings. Computer stage theory (e.g., [8,9]) indicates that organizations must upgrade their computer technology and applications as they pass through identifiable stages determined by four infrastructures: IT architecture, IS strategy, application portfolio, and organizational structure. Although these models differ, they all agree that stages can be used as a framework to plan the IS needs of organizations across different development phases. Recently, Iacovou et al. included level of technological resources, which refers to IT usage sophistication and management as a factor that determines organizational readiness for IT innovation. As a part of the IS development plan, security planning should therefore be determined within the computer stage concept.

2.4.4. Research framework

Fig. 1 illustrates the framework of our study. It is explorative and therefore focuses on the gaps between the threats perceived by managers and the scope of countermeasures actually adopted; industry and computerization level serve as the two reference frames. We attempted to

1. Identify the influences of the four factors on firm security adoptions and explore differences in the scopes of countermeasures adopted across industries.

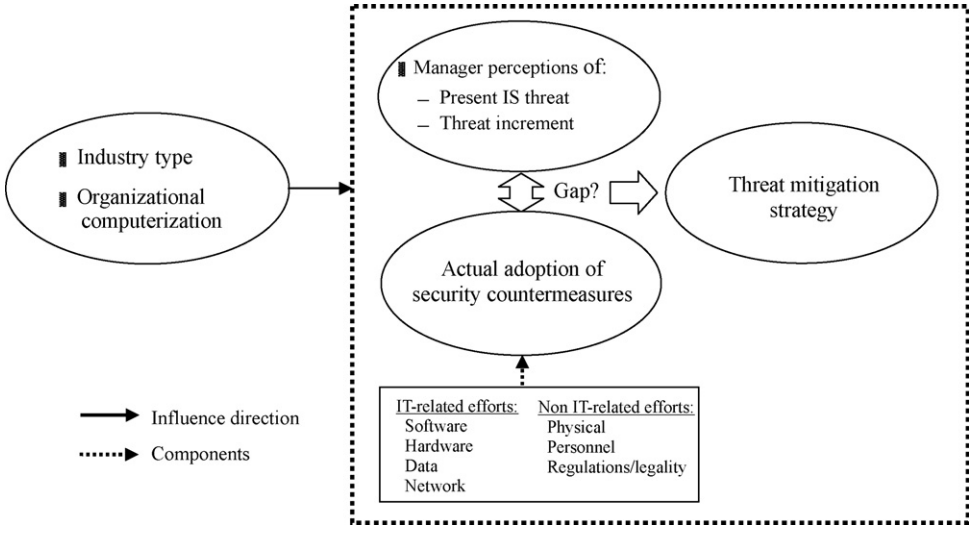

Fig. 1. The research framework.

2. Theoretically determine if managerial perceptions of threat severity was useful in motivating the adoption of relevant security countermeasures. The irrelevance or insignificance of such relationships would imply incommensurate security gaps.
3. According to the findings, identify a threat mitigation strategy for each industry that indicates which countermeasures are especially useful.

3. Research procedure

3.1. Measurement instrument

3.1.1. Scope of countermeasure adoption

This factor assesses the scope of security countermeasures that firms have adopted to protect themselves against the seven types of IS threats tested in our study. Each category contained five to eight countermeasures, for a total of 50 measures. Respondents to our questionnaire selected the countermeasures they had adopted to protect each type of IS asset. The measurement we used was the percentage of the total number of countermeasures listed in each category that has been adopted by the respondent's company at the time of survey.

3.1.2. Managerial perceptions of the present IS threat and threat increments

Two measurements were used to identify IS managers' perceptions of severity of various IS threats; they consisted of seven statements about the severities of potential threats rooted in software, hardware, data, network, personnel, regulation/legality, and environmental facilities. The responses were collected on a Likert scale ranging from (1) ''almost no threat'' to (7) ''a very high threat'' for both past and present severities. Consequently, an average rating that exceeded 4 indicated a threat. In addition, the threat increment implied a positive difference between the present and past threats (present minus past); this represented the extent to which current IS threats to business exceeded those in the past. A difference close to 0 or a negative difference indicates that the perceived threat was, respectively, either stable or declining.

3.1.3. Level of computerization

Firm IT capability primarily consists of resources based on IT infrastructure, employees, and intangibles. In addition to the four stage variables—IS/IT architecture, IS strategy, application scope, and organization structure, we included the number of full-time IS staff and age (experience) of IT department to assess this construct. The detailed characteristics of the four stage variables for the six stages are shown in Table A.1 of Appendix A. The questionnaire listed statements about each characteristic according to the stage order. Respondents selected the single statement that best described the status of their firms for each.

Principal component with Varimax rotation served to integrate the six variables in this construct; this approach formed fewer variables or indices than the number of variables given, and the variables then explained the maximum variance in the data. After variable integration, we applied a two-step clustering approach to locate the computerization level for each firm; the number of levels was not determined in advance. With this two-step approach, we thus determined the level number during the first hierarchical scheme and then the level location of each response in the second K-means procedure.

3.2. Classification of threat security levels and security baselines

We developed a list of security baselines to assess the adequacy of the firms' countermeasures to protect

Table 2
Classification of threat severities and security baselines in proportion to manager perceptions of the present threats and threat increments

Threat severities	Threat measurement		Security baseline (%)
	Range of managers' perceived present threat[a]	Significance of managers' perceived threat increment[b]	
Insignificant	<3.5	Negative increment	60
Slight	3.6–4.0	Insignificant positive increment	65
Minor	4.1–4.5	0.1 significant increment level	70
Major	4.6–5.0	0.05 significant increment level	75
Crucial	5.1–5.5	0.01 significant increment level	80
Very crucial	>5.6	0.001 significant increment level	85

[a] A 7-point scale, 1 almost no threat, 7 a very high threat; therefore, <3.5 is classified as an insignificant threat that requires the minimum security of 60%.

[b] The increment is determined by present threat minus past threat; therefore, a negative value indicates no threat increment and thus requires the minimum security of 60%.

each class of IS assets. We set the minimum security baseline at 60% for each class of fundamental countermeasures. This baseline increased in proportion to the list of threat severity levels related in the two threat measurements from managers. Table 2 displays this list of threat severity levels and the corresponding security baselines. Consequently, if subtracting the required baseline from the scope of the countermeasures produced a negative figure, the countermeasures installed were inadequate and we identified it as a gap. The baseline does not imply an adequate level of security; rather, its explanation requires a connection to the perceived threat level, as Table 2 shows.

3.3. Sample

For our empirical study, we distributed 1000 questionnaires to the head offices of the 1000 major enterprises in Taiwan. This population not only covers a wide range of businesses but also consists of large firms, which normally expend more effort on applied IS/IT and have well-developed IS security strategies. Each questionnaire included a statement congratulating the enterprise on its success and explaining the purpose of the research and the voluntary nature of participation; it also assured participants of the confidentiality of their response and stressed that the stage development part should be completed by a high-level manager and the computerization part by a senior IS personnel. A prepaid reply envelope was provided to encourage direct return of the questionnaires to the authors. Demographics (company age, number of employees, sales amounts, and industry type) was also requested. A total of 109 usable questionnaires were returned. Because security investigation research is a most intrusive type of research [17], it was not surprising that the response rate was only 10.9%. Table 3 lists the individual demographics and organizational features.

As Table 3 shows, more than 85% of the respondents had professional tenure exceeding 11 years while 99% held jobs involving IS security, including IS security strategic planning (61%), IS security implementation (23%), risk analysis and auditing (4%), and general systems engineering (11%). In terms of firm size, more than 85% had more than 201 employees and 96% had annual sales exceeded 1.1 billion NT dollars. The returned questionnaires were almost equally distributed across different industries. Overall, these data match approximately with those of the top 1000 enterprises in Taiwan.

Table 3
The sample profile ($N = 109$)

Respondents' individual demographics	Freq.	Percentage
Professional tenure (years)		
Less than 10	24	22
Between 11 and 20	54	50
Between 21 and 30	30	28
More than 31	1	1
Gender		
Male	95	87
Female	14	13
Education		
Senior high school	2	2
Junior college	19	17
Bachelor	68	62
Master and above	20	18
Age (years)		
Between 26 and 30	5	5
Between 31 and 40	48	44
Between 41 and 50	48	44
More than 51	8	7
Involvement in IS security		
Strategic planning of IS security	67	61
Implementation of IS security	25	23
Risk analysis and auditing	4	4
General system engineering	12	11
Others	1	1
Organizational features	**Freq.**	**Percentage**
Organizational age (years)		
Less than 10	16	15
Between 11 and 20	26	24
More than 21	67	61
Industry type		
General manufacturing	30	28
High-tech industry	26	24
Banking/financial	24	22
Retailing/service	29	27
Firm size (# employees)		
Between 101 and 200	17	16
Between 201 and 500	21	19
Between 501 and 1000	25	23
Between 1001 and 2000	21	19
Between 2001 and 5000	17	16
More than 5001	8	7
Annual sales (NT$)[a]		
Less than 1 billion	6	6
Between 1.1 and 5 billions	48	44
Between 5.1 and 10 billions	23	21
More than 10.1 billions	32	29

[a] 32 NT$ = 1US$.

3.4. Data analysis

We started by making a principal component analysis of the six computerization variables and

calculations of the component scores for each sampled enterprise. Next, a two-step clustering served to place enterprises into their level of computerization according to the calculated component scores.

Subsequently, ANCOVAs were used to examine the influence of the four factors – industry type, computerization level, and the two manager threat perceptions – on security countermeasure adoption. The response variables represented the scopes of the seven classes of countermeasures adopted. The ANCOVA process removed extraneous variation in the dependent variables due to one or more uncontrolled covariates. Because larger firms were more likely to adopt computer technology, we included firm size as a covariate in the models. It was operationalized by both the annual sales and number of employees in the organization. In total, we tested eight ANCOVAs, seven individual and one integrated model. Each model tested the effects of individual types of threat on the adoption of the corresponding countermeasure; the integrated model, which used the averages of the seven scopes and threat severities as integration indices, examined the overall effect. Because both industrial type and level of computerization are categorical variables, we required further analysis of the interaction of these two variables to determine whether their interaction effect was significant. We determined the security gaps and threat mitigation strategies by industry after the ANCOVA tests.

4. Results

4.1. Organizational computerization level across industries

Principal component analysis extracted two components. As the loadings indicated, component 1 was mainly made up of and explained by the first three characteristics, and component 2 consisted of the last three characteristics. In terms of the contents, we termed them, respectively, the applied and capability levels. The results also suggested that, with almost equal explained variances of 34.1 and 28.5%, respondents were equally aware of the two components:

$$\begin{bmatrix} \text{Applied level} \\ \text{Capability level} \end{bmatrix} = \begin{bmatrix} 0.8571 & 0.7800 & 0.7660 & 0.1409 & -0.0048 & 0.3136 \\ 0.1271 & 0.1192 & 0.1327 & 0.8278 & 0.8181 & 0.5511 \end{bmatrix} \times \begin{bmatrix} \text{IS strategy} \\ \text{Org. structure} \\ \text{Appicaiton scope} \\ \text{No. of IS staffs} \\ \text{Age of IS dept.} \\ \text{IS/IT architecture} \end{bmatrix}$$

The subsequent hierarchical clustering applying these two scores suggested that a three-level cluster was most appropriate. Therefore, we located each firm on one of the three levels according to its scores. Table 4 displays the distribution of the level of organizational computerization across the four industries. Our analysis also showed that the average stage scores of the four stage variables (Table A.1 in Appendix A) among the three levels were 3.0, 3.8, and 4.8, equivalent to stages 3–5 in the theoretical six-stage model. This narrow range of computerization level appeared to be related to the medium to large size of most firms in the sample. Therefore, the three levels were relative rather than absolute. This consistency between the two approaches verifies the construct validity of the current computerization measurement.

Although we found no statistically significant differences among the four industries (p-value of Pearson chi-square test was 0.230), the banking/finance and retailing/service industries appeared heavily reliant on IT, with 38 and 54% of the firms falling into the high-level computerization category. The high-tech industry was the next most reliant on IT, with 41% of its firms into medium-level computerization category. Manufacturing had a lower level of computerization; 41% being at the low-level.

4.2. Influences of industry, computerization, and threat perception on security adoption

Table 5 lists the results of the ANCOVAs on the influence of the manager threat perceptions, industry type, organizational computerization level, and the two covariates of firm size on the scopes of the countermeasures adopted to secure the seven types of assets. Both individual and integrated effects suggested that industry type, computerization level, and the firm size covariate (number of employees) had significant influence across the seven asset classes. Except for software and physical assets, the scope of countermeasure adoption for the IS asset clusters differed significantly with industry and computerization level; the significant effect of number of employees on

Table 4
Distribution of level of computerization across the four industries[a]

Level of computerization			Industry type							
Level [b]	Factor scores		General Manuf. (N=32)		High-tech (N=27)		Bank/finance (N=24)		Retailing/service (N=26)	
	Applied level	Capability level								
Low (N=34)	-0.9764	-0.5311	13	(41%)	8	(30%)	6	(25%)	7	(27%)
Medium (N=37)	-0.1481	0.1692	12	(38%)	11	(41%)	9	(38%)	5	(19%)
High (N=38)	1.0692	0.3385	7	(22%)	8	(30%)	9	(38%)	14	(54%)

[a]Dark color: the highest percentage in each sector. [b] Equivalent to stages 3–5 in Galliers and Sutherland's six-stage model.

network and physical assets suggested that IS security improved with organization size. However, the effects of the two manager threat perceptions and the interaction effect of industry and computerization were insignificant in both the individual or integrated results.

4.3. Identification of security gaps across industries

The insignificant effects of the two threat perceptions in Table 5 implied a lack of any relationship between the severity of the perceived threats and the scope of the countermeasures adopted. That is, preparations to protect IS assets do not increase with greater managerial perceptions of the severity of IS threats. Also, the actual adoption of countermeasures is strongly influenced by industry type and organizational computerization. We therefore performed a *post hoc* analysis to clarify the security gaps according to industry.

4.3.1. Current countermeasure adoptions

Table 6 shows the countermeasure adoption scopes for the seven categories of IS assets across the four industries. Values in a darker color indicate that the scope of countermeasure adoption exceeded the average of each industry listed on the left side; this implied relatively robust security for the IS assets. Regardless of industry, higher security applied to software, hardware, data, and physical assets, whereas lower security was apparently required of the network, personnel, and regulation/legality assets. Regarding overall security, the banking/finance industry was most secure.

Table 5
Influences of managers' threat perceptions, industry type, and organizational computerization on the seven scopes of countermeasure adoption—results of ANCOVAs

Independent variables	Responses							
	Individual effect[a]							Integrated effect[b]
	Software	Hardware	Data	Network	Physical	Personnel	Regulation	
Manager perceptions of								
Present IS threat[a]	1.71	0.25	0.54	0.36	0.04	0.07	0.00	0.00
Threat increment[a]	1.20	0.68	1.20	0.28	0.59	0.14	0.34	1.26
Industry type	0.88	3.23*	2.01†	5.25**	2.12†	4.19**	5.76***	6.39***
Level of computerization	4.71*	4.45*	4.46*	4.24*	0.95	3.04*	4.33*	7.77***
Industry × level of comp.	0.25	1.30	0.54	1.32	0.67	0.68	0.54	0.43
Covariates								
Number of employees	0.27	0.76	0.70	6.35*	8.31**	2.32	0.07	2.95†
Annual sales	0.24	0.06	1.61	0.00	0.58	0.67	2.03	0.57
R^2	0.22	0.31	0.26	0.44	0.32	0.35	0.33	0.48
Adjusted R^2	0.08	0.19	0.12	0.34	0.2	0.24	0.21	0.39

[a] Each individual effect was tested according to the respective threat measurements and countermeasure adoption scope.
[b] Using the averages of the seven threat measurements and the seven adoption scopes as the integrated indices.
* $p \leq 0.05$.
** $p \leq 0.01$.
*** $p \leq 0.001$.
† $p \leq 0.1$.

Table 6
Countermeasure adoptions for the seven IS categories across the four industries[a]

		IS category						
	Overall	IT-related				Non IT-related		
Industry	average	Software	Hardware	Data	Network	Physical	Personnel	Regulation
General manuf. (N=32)	***54%***	66%	63%	62%	40%	63%	52%	29%
High-tech (N=27)	***61%***	73%	67%	75%	51%	63%	58%	42%
Bank/finance (N=24)	***71%***	75%	81%	80%	65%	77%	69%	51%
Retailing/service (N=26)	***54%***	66%	66%	70%	41%	59%	46%	31%

[a]Dark color: the scope is larger than the industry average listed on the left of the same row.

Table 7
Perceived threat severities for the seven IS categories across the four industries[a,b]

	IS category						
	IT-related				Non IT-related		
Industry	Software	Hardware	Data	Network	Physical	Personnel	Regulation
General manuf. (N=32)				(*)			
High-tech (N=27)	4.1 (*)	(†)	4.2 (**)	4.7 (***)		4.3 (*)	(†)
Bank/finance (N=24)	4.5 (*)	4.2	4.8 (†)	5.0 (***)	4.0 (†)	4.7 (*)	(**)
Retailing/service (N=26)	(†)		4.3	4.6 (**)		4.3 (†)	(*)

[a]Dark colors: present threat is perceived larger than 4. [b]Parenthesis: the threat increment is perceived. †Minor; *major; **crucial; ***very crucial.

4.3.2. Perceived threat severities

Table 7 shows the threat severity levels according to managerial perceptions of existing threats and threat increments across the four industries. Symbols indicate the threat increments shift from slight (<0.3 or insignificant) to minor (0.3–0.5 or significant at 0.1 level), major (0.5–0.7 or significant at 0.05 level), crucial (0.7–0.9 or significant at 0.01 level), and very crucial (>0.9 or significant at 0.001 level). Values in darker colors indicated that the perceived present threats to the assets were greater than 4.0; their respective severity levels, from minor to very crucial. Overall, the banking/finance sector suffered the most, followed by high-tech, retailing/service, and general manufacturing. Threats to network, personnel, and data appeared as the first three severe present threats across the four industries. In terms of threat increment, network also indicated the greatest threat severity, followed by regulation, personnel, and software. Managers had started paying attention to the threat of regulation even though their perceptions of the threat remained less than 4.0 in all four industries. On the basis of this table, we chose between present threat and threat increment depending on which was more severe and used that as the final severity level to decide the security baseline of each threat. For example, regulation in banking/finance had an insignificant present threat value of 3.50 and a crucial threat increment, so we classified the threat severity as crucial.

4.3.3. The security gaps

Table 8 depicts the security gaps in the seven categories of IS threats across the four industries, calculated by subtracting the required security baseline from each countermeasure scope. The security baseline was determined by both the threat severity level and the baseline list. A value of 0 indicated that the scope of

Table 8
Security gaps in the seven IS categories across the four industries[a,b]

	IS category						
	IT-related				Non IT-related		
Industry	Software	Hardware	Data	Network	Physical	Personnel	Regulation
Manufacturing (N=32)	0%	0%	0%	-35%	0%	-13%	-36%
High-tech (N=27)	-2%	-3%	-5%	-29%	-2%	-17%	-28%
Bank/finance (N=24)	0%	0%	0%	-15%	0%	-6%	-29%
Retailing/service (N=26)	-4%	0%	0%	-39%	-6%	-24%	-44%

[a]0 means that the scope is fit or over the required. [b]Dark color: the inadequacy gap is over 10% with the darkest approximately and over 30%.

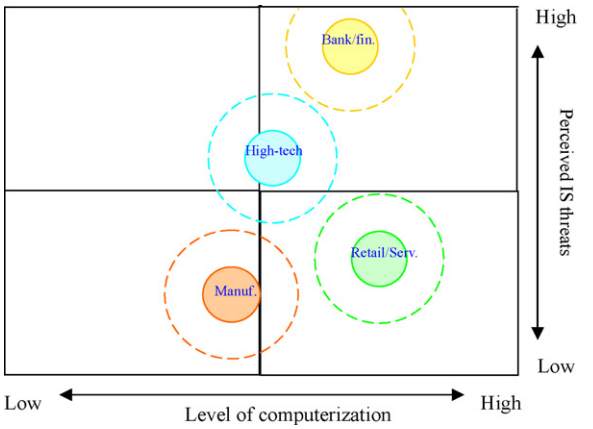

Fig. 2. Perceived IS threat and computerization level among the four industries.

current countermeasure adoption fit or exceeded the required security; a negative value indicated that an IS asset class was inadequately protected. The dark values denote security inadequacy exceeding 10%, and the darkest ones refer to inadequacy that was close to or exceeded 30%. Regardless of industry, three classes – network, regulation/legality, and personnel – were obviously insufficient.

5. Discussion

5.1. Perceived IS threats and computerization level among industries

The severity of perceived threats for individual IS assets differ across the four industries and the three levels of computerization. Fig. 2 contains a 2 × 2 plane to illustrate the relationship among industry, organizational computerization, and managerial perceptions of IS threat severity. The three computerization levels in the four subject industries are equivalent to medium to low-high computer stages. Therefore, the projections of the four industries on the horizontal computerization axis congregate in the range between the center and the low-high computerization level, which suggests that the comparisons here were relative, rather than absolute.

5.2. Threat mitigation strategy by industry

This study also considered that the scope of countermeasure adoption; it did not appear to be commensurate with the severity of the perceived IS threats. In particular, industry type and level of organizational computerization significantly affected the scopes but not the two types of managerial threat perceptions. Businesses should use their industry as a starting point for understanding their security requirements and adopt appropriate countermeasures to mitigate IS threats. Table 9 summarized the IS threats and threat mitigation strategies proposed for organizations in the subject industries.

For high-tech businesses, information confidentiality and efficiency are major requirements due to the use of IS for technological innovations and quick response to partners. Such business should ensure that they avoid disclosure of business secrets in their systems. Network and data are crucial threats, and software and personnel also are perceived as major threats.

Banking/financial businesses frequently depend on IS for their strategic value and invest in IS planning. Such businesses are information intense; therefore, they must make sure that information is not modified and that confidential data is not leaked. In addition, they should give greater consideration to the privacy of customer information.

Table 9
Threat mitigation strategy by industry

	Industry type			
	High-tech	Bank/finance	Retailing/service	General manufacturing
IS/IT characteristics	Medium computerized; connection to business partners	High computerized; information-intensive	High computerized; market-oriented	Low computerized; transaction process
Threat severity level[a]				
Major	Personnel^{S} software	Data personnel software	Regulation^{V}	Network^{V}
Crucial	Data^{S} network^{V}	Regulation^{V} network^{S}	Network^{V}	–
Threat mitigation strategy	Major: user authentication, network security, security responsibility; minor: security training, incident report procedures	Major: risk transference, privacy of personal information; minor: user authentication, digital signatures	Major: network security enhancement, setting security policy; minor: system & security training, incident report procedures	Minor: network security enhancement, setting security policy

[a] S: security protection is somewhat inadequate; V: very inadequate.

Table A.1
The six-stage measurement for the four IS/IT characteristics[a]

Stage	Characteristics			
	Organization structure	System architecture	IS strategy	Applied scope
Stage I	No computer related development	Ad hoc unconnected, operations	Acquiring required hardware and software, etc.	Accounting and financial data transaction
Stage II	Attached to accounting or other department	Operational and overlapping	Developing software within a functional department	Operational activities
Stage III	A data processing department	Integrated and centralized DBS	Top-down IS planning	Covering most major managerial activities
Stage IV	An information center	Decentralized but lack of co-ordination	Integration, coordination and control of IT resources	Decision supporting and strategic planning
Stage V	SBU coalitions	Decentralized with central control and coordination	Environmental scanning & opportunity seeking	Market-oriented, value added system
Stage VI	Centrally coordinated coalitions	External and internal data integration	Maintaining comparative strategic advantage	New IS-based products or services are included

[a] The measurement is modified from the six-stage model of Galliers and Sutherland.

Finally, retailing/service businesses invest more in IS, particularly market-oriented applications, for which availability is a key security requirement. However the IS threat is perceived as low. This may exist because information is less sensitive and used to maintain normal system functions.

6. Conclusions

Security adoption tends to be a need-pull innovation rather than technology-push. As a result, organizations probably only adopt new countermeasures when their security methods appear insecure. Our findings suggest that IS security is not simply an ''off-the-shelf,'' technical issue but rather a context-dependent business problem.

For practitioners, this study suggests two implications of IS security management: first, the IS assets – network, personnel, and regulation/legality – clearly provide inadequate protection for Taiwan's enterprises, regardless of industry. Second, organizations with lower IS threats, such as general manufacturing and retailing/service, should emphasize their security policy development and allocate security accountability; organizations facing higher IS threats should also consider risk-transference approaches to control their financial losses and enhance regulation/legality security.

In conclusion, we empirically investigated the differences and adequacy of IS security countermeasure adoption among firms in different industries. We also examine the impacts of several variables, namely, industry, level of computerization, and managerial perceptions of IS threats, on IS security adoption. Strong evidence supports the objectives of the study, though the research model was parsimonious.

Acknowledgments

The authors express their gratitude to the editor, screening reviewer and three anonymous reviewers whose comments have helped improve this paper considerably. We also acknowledge support from the National Science Council of Taiwan (NSC93-2416-H-006-036).

Appendix A

The measurement of organizational computerization involved the number of full-time IS staff members, age (experience) of IT department, and four characteristics related to firm IS/IT environment. These four IS/IT characteristics were modified from the six-stage model of Galliers and Sutherland. Detailed stage differences with regard to the four characteristics across the six stages appear in Table A.1.

References

[1] R.D. Banker, I.R. Bardhan, H. Chang, S. Lin, Plant information systems, manufacturing capabilities, and plant performance, MIS Quarterly 30 (2), 2006, pp. 315–337.
[2] BS7799-2, Information Security Management. Part 2. Information Security Management Systems Specification with Guidance for Use, British Standards Institution, London, 2002.
[3] M.W. Chiasson, E. Davidson, Taking industry seriously in information systems research, MIS Quarterly 29 (4), 2005, pp. 591–605.
[4] CNSS, National Information Assurance (IA) Glossary (CNSS Instruction No. 4009), Committee on National Security Systems, revised in June 2006, http://www.cnss.gov/instructions.html (cited July 5, 2006).
[5] P. Davamanirajan, R.J. Kauffman, C.H. Kriebel, T. Mukhopadhyay, Systems design, process performance, and economic out-

comes in international banking, Journal of Management Information Systems 23 (2), 2006, pp. 65–90.
[6] M.M. Eloff, S.H. von Solms, Information security management: a hierarchical framework for various approaches, Computers and Security 19 (3), 2000, pp. 243–256.
[7] K.J. Fitzgerald, Information security baselines, Information Management & Computer Security 3 (2), 1995, pp. 8–12.
[8] R.D. Galliers, A.R. Sutherland, Information systems management and strategy formulation: the ''stages of growth'' model revisited, Journal of Information Systems 1, 1991, pp. 89–114.
[9] D. Gibson, R.L. Nolan, Managing the four stages of EDP growth, Harvard Business Review 52 (1), 1974.
[10] D.L. Goodhue, D.W. Straub, Security concerns of system users: a study of perceptions of the adequacy of security, Information and Management 20 (1), 1991, pp. 13–22.
[11] L.A. Gordon, M.P. Loeb, T. Sohail, A framework for using insurance for cyber risk management, Communications of the ACM 2003, pp. 81–85.
[12] C.L. Iacovou, I. Benbasat, A.S. Dexter, Electronic data interchange and small organizations: adoption and impact of technology, MIS Quarterly 19 (4), 1995, pp. 465–485.
[13] D. Icove, K. Seger, W. Vonstorch, Computer Crime—A Crimefighter's Handbook, O'Reilly & Associates, Inc., 1999.
[14] B. Jung, I. Han, S. Lee, Security threats to Internet: a Korean multi-industry investigation, Information and Management 38 (8), 2001, pp. 487–498.
[15] A. Kankanhalli, H.H. Teo, B.C.Y. Tan, K.K. Wei, An integrative study of information systems security effectiveness, International Journal of Information Management 23, 2003, pp. 139–154.
[16] W.R. King, Organizational characteristics and information systems planning: an empirical study, Information Systems Research 5 (2), 1994, pp. 75–109.
[17] A.G. Kotulic, J.G. Clark, Why there aren't more information security research studies, Information and Management 41 (5), 2004, pp. 597–607.
[18] K.L. Kraemer, J. Gibbs, J. Dedrick, Impacts of globalization on e-commerce use and firm performance: a cross-country investigation, Information Society 21 (5), 2005, pp. 323–340.
[19] Y. Lee, K.A. Kozar, Investigating factors affecting the adoption of anti-spyware systems, Communications of the ACM 48 (8), 2005, pp. 72–78.
[20] K.D. Loch, H.H. Carr, M.E. Warkentin, Threats to information systems: today's reality, yesterday's understanding, MIS Quarterly 16 (2), 1992, pp. 173–186.
[21] J.J. Mohr, The management and control of information in high-technology firms, The Journal of High Technology Management Research 7 (2), 1996, pp. 245–268.
[22] NIST SP 800-30, Risk Management Guide for Information Technology Systems (Special Publication 800-30), National Institute of Standards and Technology Computer Security Resource Center, 2002.
[23] J. Olnes, Development of security policies, Computers and Security 13 (8), 1994, pp. 628–636.
[24] T.R. Peltier, Information Security Risk Analysis, Auerbach, New York, 2001.
[25] R.K. Rainer Jr., C.A. Snyderr, H.H. Carr, Risk analysis for information technology, Journal of Management Information Systems 1991, pp. 192–197.
[26] R. Richardson, 2003 CSI/FBI Computer Crime and Security Survey, Computer Security Institute, 2003http://www.gocsi.com/ (cited September 20, 2003).
[27] E.M. Rogers, Diffusion of Innovations, 3rd ed., The Free Press, New York, NY, 1983.
[28] D.W. Straub, W.D. Nance, Discovering and disciplining computer abuse in organization: a field study, MIS Quarterly 1990, pp. 45–55.
[29] D.W. Straub, R.J. Welke, Coping with systems risk: security planning models for management decision making, MIS Quarterly 1998, pp. 441–469.
[30] B. Suh, I. Han, The IS risk analysis based on a business model, Information and Management 41 (2), 2003, pp. 149–158.
[31] B. von Solms, R. von Solms, The 10 deadly sins of information security management, Computers and Security 23 (5), 2004, pp. 371–376.
[32] R. von Solms, H. van de Haar, S.H. von Solms, W.J. Caelli, A framework for information security evaluation, Information and Management 26 (3), 1994, pp. 143–153.
[33] G.B. White, E.A. Fisch, U.W. Pooch, Computer System and Network Security, CRC Press, Boca Raton, FL, 1996.
[34] M.E. Whitman, Enemy at the gates: threats to information security, Communication of the ACM 46 (8), 2003, pp. 91–95.
[35] R.W. Zmud, An examination of push–pull theory applied to process innovation in knowledge work, Management Science 30 (6), 1984, pp. 727–738.

Quey-Jen Yeh is a professor of business administration at the National Cheng Kung University, Taiwan. She received her Ph.D. in industrial engineering and operational research from Columbia University, NY, and M.S. from Pennsylvania State University and B.A. from National Taiwan University. Her research interests include managing engineers and scientific professionals in technological organizations, organizational acceptance of information technologies, and management of small business in newly developed countries. Her perspective tends to stem from Taiwan's experiences in its developments of economy, technology and human knowledge. She has publications in R&D Management, Information & Management, Journal of Business Ethics, Journal of the Operational Research Society, IEEE Transactions on Engineering Management, and others.

Arthur Jung-Ting Chang is an assistant professor of the Department of Information Management at Chin Min Institute of Technology, Miaoli, Taiwan. He received his Ph.D. in business administration from the National Cheng Kung University, Tainan, Taiwan. His research interests focus on IT adoption, information system security policy, and information risk analysis and management.