Available online at www.sciencedirect.com

SCIENCE DIRECT®

PERGAMON International Journal of Information Management 23 (2003) 139–154

International Journal of
Information
Management

www.elsevier.com/locate/ijinfomgt

An integrative study of information systems security effectiveness

Atreyi Kankanhalli*, Hock-Hai Teo, Bernard C.Y. Tan, Kwok-Kee Wei

Department of Information Systems, School of Computing, National University of Singapore, 10 Kent Ridge Crescent, 119260, Singapore

Abstract

As organizations become increasingly dependent on information systems (IS) for strategic advantage and operations, the issue of IS security also becomes increasingly important. In the interconnected electronic business environment of today, security concerns are paramount. Management must invest in IS security to prevent abuses that can lead to competitive disadvantage. Using the literature on security practices and organizational factors, this study develops an integrative model of IS security effectiveness and empirically tests the model. The data were collected through a survey of IS managers from various sectors of the economy. Small and medium-sized enterprises were found to engage in fewer deterrent efforts compared to larger organizations. Organizations with stronger top management support were found to engage in more preventive efforts than organizations with weaker support from higher management. Financial organizations were found to undertake more deterrent efforts and have stiffer deterrent severity than organizations in other sectors. Moreover, greater deterrent efforts and preventive measures were found to lead to enhanced IS security effectiveness. Implications of these findings for further research and practice are discussed.

Keywords: Information systems; Strategic advantage; Security; Organizations

1. Introduction

Organizations are increasingly relying on information systems (IS) to enhance business operations, facilitate management decision-making, and deploy business strategies. The dependence has increased in current business environments where a variety of transactions involving trading of goods and services are accomplished electronically. Increased organizational

*Corresponding author.
E-mail address: atreyi@comp.nus.edu.sg (A. Kankanhalli).

0268-4012/03/$ - see front matter
doi:10.1016/S0268-4012(02)00105-6

dependence on IS has led to a corresponding increase in the impact of IS security abuses. While such a trend would suggest IS security as a key management issue, this has not been the case in practice. Management attention for IS security has been low compared to other IS issues (Brancheau, Janz, & Wetherbe, 1996; Olnes, 1994). In a global information security survey of midsize and large firms, less than 50% of the 459 CIOs and IT directors polled said they had IT security awareness and training programs for employees (Verton, 2002).

The inadequate management concern for IS security is worrisome given evidence that significant IS security abuses do occur (Zviran & Haga, 1999). Several studies have documented actual and potential losses due to IS security abuses (e.g., Burger, 1993; Loch, Carr, & Warkentin, 1992; Panettieri, 1995). A 2002 Computer Security Institute survey stated that 90% of respondents detected security breaches in the last year and 44% reported their losses at $455 million, among the 503 surveyed security practitioners (Computer Security Institute, 2002). Besides actual and potential financial losses, other negative consequences of IS security abuses include negative publicity, competitive disadvantage, and even reduced organizational viability. The vulnerability of organizations is increasing with the advent of electronic commerce and open network architectures (Barsanti, 1999). Better computer literacy, increased computer user sophistication, and availability of advanced software tools may also contribute to increased IS security abuses in the future. Hence, management needs to pay more attention to IS security issues (Dhillon & Backhouse, 2000).

There are several plausible explanations for low management concern about IS security (Straub, 1990). First, managers may make a deliberate decision to invest little in IS security because they think the risk of IS security abuses is low. Second, managers may be sceptical about IS security effectiveness due to the difficulty in evaluating the benefits. Third, managers may lack knowledge about the range of controls available to reduce IS security abuses. To raise management involvement in IS security decisions, it is important to convince managers about the benefits of IS security efforts and let them know what kinds of IS security measures are effective under what organizational circumstances.

Previous studies on IS security have focused on software for detecting IS security abuses (Nance & Straub, 1988), measures for preventing IS security abuses (Straub, 1990), perceptions of IS security adequacy (Goodhue & Straub, 1991), and IS security planning models for management decision-making (Straub & Welke, 1998). With the exception of a few interpretive studies (Backhouse & Dhillon, 1996) (Baskerville, 1991), these studies tend to neglect organizational factors that may partially explain the extent of IS security abuses. The objective measures reported by these studies may also lack accuracy because people may be reluctant to report such incidents (Straub & Welke, 1998). Goodhue and Straub (1991) suggest using a perceptual measure of IS security effectiveness as an alternative to the inaccurate objective counts of IS security abuses. With the exception of the studies cited above, the body of literature on IS security has largely been purely empirical (e.g., Anthes, 1998; Burger, 1993; Loch et al., 1992; Panettieri, 1995) or purely theoretical (e.g., Madnick, 1978; Parker, 1983). Few studies have developed theoretical models and tested these models with empirical data.

By putting together the literature on security practices and organizational factors, this study proposes an integrative model of IS security effectiveness. In this model, IS security effectiveness refers to the ability of IS security measures to protect against unauthorized or deliberate misuse of IS assets by people (Straub, 1990). IS assets include hardware (e.g., personal computers,

peripherals, disks, network hardware, etc.), software (e.g., systems and applications programs), data, and computer services. Misuse of IS assets includes theft of or damage to hardware, theft or modification of software, embezzlement or modification of data, and unauthorized use or purposeful interruption of computer services. Proposed relationships among organizational factors, IS security measures, and IS security effectiveness are tested with empirical data. By offering a theoretical basis for empirical results, this study advances a theory on IS security effectiveness that informs IS managers about what kinds of IS security measures may be more effective and what types of organizations need to pay more attention on IS security.

2. Security practices

The security functions in an organization can be classified in various ways. White, Fisch, & Pooch (1996) distinguish between external (pertaining to physical, personnel, and administrative security) and internal security functions (which are implemented as part of hardware and software). When viewed as counter-measures for increasing IS security by reducing IS risk, security functions can also be classified as deterrent or preventive measures (Forcht, 1994; Parker, 1981). Straub and Nance (1990) also identified the purposeful detection of successful abuse incidents as a security measure that in turn acts as a deterrent to other potential abusers. The categorization of IS security measures as deterrents and preventives has been adopted by studies on IS security (e.g., Nance & Straub, 1988; Straub, 1990) and software piracy (e.g., Gopal & Sanders, 1997) and likewise by this study.

2.1. Deterrent measures

Deterrent measures are attempts to dissuade people from criminal behavior through fear of sanctions (Forcht, 1994). Research on criminology has demonstrated that people with an instrumental intent to commit crime or anti-social acts can be dissuaded from doing so by the administration of strong sanctions relevant to these acts (Blumstein, 1978; Cook, 1982; Pearson & Weiner, 1985). Sanctions are effective if people feel that they will definitely be punished for their crime or anti-social acts and the punishment will be harsh (Williams & Hawkins, 1986). Consequently, two characteristics of sanctions that can contribute to their effectiveness as deterrent measures are certainty of sanctions and severity of sanctions (Blumstein, 1978).

In the context of IS security, deterrent efforts correspond to certainty of sanctions because the amount of such efforts directly affects the probability that IS abusers will be caught. Typical examples of deterrent efforts are policy statements and guidelines on legitimate use of IS assets, security briefings on the consequences of illegitimate use of IS assets, and audits on the use of IS assets (Straub, 1990). Active and visible deterrent efforts can reduce IS abuses by convincing potential abusers that the probability of getting caught is high. Such efforts are particularly effective if the punishment for IS abuses is also severe (Straub, 1990). Hence, deterrent severity corresponds to severity of sanctions. Parker (1983) demonstrates the value of deterrent efforts in lowering crime rate of white-collar workers. Klete (1978) suggests that the absence of deterrent efforts may lead to people misunderstanding which constitutes acceptable IS use, thereby

contributing to IS abuses. In a survey of 1211 organizations, Straub (1990) found that deterrent efforts resulted in fewer IS abuses.

2.2. Preventive measures

Preventive measures are attempts to ward off criminal behavior through controls (Forcht, 1994). These measures constitute the next line of defense when potential abusers choose to ignore deterrent measures (Straub & Welke, 1998). Preventive measures can impede criminal activities by forcing the abusers to expend and deplete resources in their pursuit of crime and anti-social acts. The objective is to wear abusers down. Typical examples of preventive efforts in the context of IS security include implementing security software to impede unauthorized access to and use of IS assets, and designing physically secure IS facilities (Straub, 1990). Such efforts can help to enforce policy statements and guidelines by warding off illegitimate activities (Gopal & Sanders, 1997). Preventive efforts in the form of security software are likely to be crucial in the future because of better computer literacy, availability of advanced software tools, and increased electronic connection among organizations.

Security software can provide several levels of access control to IS assets (Nance & Straub, 1988; Weber, 1988). At a basic level, security software embedded in operating systems can enforce access control at the level of user accounts, specific databases, or specific files. Examples of such software functions are validation of user passwords, designation of read–write–execute capabilities for files, and maintenance of access violation logs for databases. At an intermediate level, security software embedded in database management systems can carry out access control at finer levels of granularity such as specific records and fields in databases. Examples of such software functions are restriction of access to predefined portions or views of databases, restriction of rights to update data or modify database structures, and control of simultaneous access to databases. Such software can also provide statistical summaries of accesses to databases and highlight unauthorized accesses to databases. At an advanced level, specialized security software can provide access control through advanced transaction-logging capabilities incorporating complete audit trails and in-depth security violation reports.

3. Organizational factors

The implementation of IS in organizations is strongly influenced by organizational factors (Ein-Dor & Segev, 1978) such as organizational size, top management support, and industry type. Raymond (1990) reported that smaller organizations suffer from a lack of human and financial resources. With insufficient managerial and technical skills, and the lack of funds to acquire such skills, smaller organizations often implement their IS in a less than optimal way, thereby attaining less benefits compared to larger organizations (Delone, 1988; Raymond, 1990; Thong, Yap, & Raman, 1996).

Top management support is a critical success factor for the implementation of IS (Thong et al., 1996; Yap, Soh, & Raman, 1992) and other organizational innovations (Damanpour, 1991). This support may take the form of guidance during planning, participation during design, or involvement during deployment. Besides the ability to secure adequate resources, top

management can also encourage positive user attitude towards the use of IS (Thong et al., 1996; Yap et al., 1992).

Organizations in different industries tend to differ in terms of their requirements for IS (King, 1994), use of IS (Reich & Benbasat, 1990), and role of IS (Jarvenpaa & Ives, 1990). Jarvenpaa and Ives (1990) found that IS play a more strategic and critical role in financial institutions as compared to other organizations. As a result, financial organizations tend to invest more resources in IS and reap more benefits from IS than other organizations. Given that these organizational factors can significantly impact the implementation of IS, it is likely that these factors will also affect IS security practices in organizations.

4. IS security effectiveness

Fig. 1 depicts the model of IS security effectiveness proposed in this study. In this model, the independent variables are three organizational factors (organizational size, top management support, and industry type) that affect implementation of IS. The mediating variables are IS security measures (deterrent and preventive). Two aspects of deterrent measures studied are deterrent efforts (reflecting certainty of sanctions) and deterrent severity (reflecting severity of sanctions). Preventive measures are assessed in terms of the sophistication of security software employed. The dependent variable is IS security effectiveness. Links among independent, moderating, and dependent variables constitute the hypotheses for this study.

4.1. Organizational factors and IS security practices

Straub (1986) reported that larger organizations spend more time and money on computer security and EDP audit activities than smaller organizations. Larger organizations also have proportionately larger security staff compared to smaller organizations (Hoffer & Straub, 1994). Nance and Straub (1988) found that larger organizations used a greater number of and more sophisticated security software than smaller organizations. By being more able to commit financial resources and more likely to have the necessary expertise, larger organizations are likely to undertake more deterrent and preventive efforts than smaller organizations.

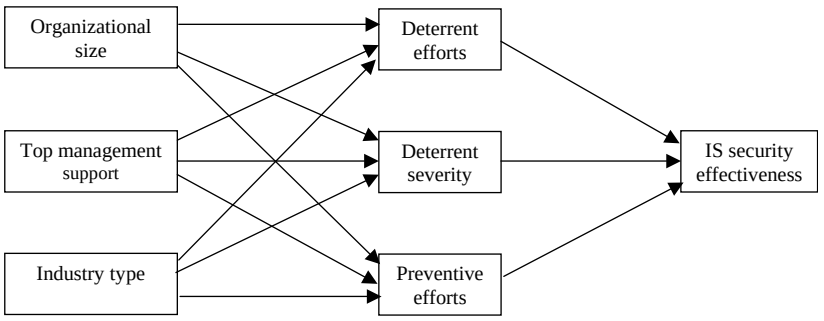

Fig. 1. Model of IS security effectiveness.

Furthermore, because they tend to rely heavily on IS and may incur heavier losses due to IS security abuses, larger organizations are likely to enforce more severe deterrents than smaller organizations.

H1a: Organizational size is positively related to deterrent efforts.
H1b: Organizational size is positively related to deterrent severity.
H1c: Organizational size is positively related to preventive efforts.

Eloff (1988) asserts that a critical success factor for implementing computer security is management commitment. Other scholars have reinforced this suggestion and discussed ways to raise management awareness about the importance of computer security (e.g., Weber, 1988; Wood, 1987). With top management support, more financial and technical resources are likely to be made available for IS security. Hence, more deterrent and preventive efforts can be carried out. Top management support may also be manifested in the form of active involvement during formulation of IS security policies and monitoring of IS security practices. If top management is aware of the importance of IS security, they are likely to propose more severe deterrents during IS policy formulation. Visible top management support may also signal their intention to severely punish abusers.

H2a: Top management support is positively related to deterrent efforts.
H2b: Top management support is positively related to deterrent severity.
H2c: Top management support is positively related to preventive efforts.

Industry type (financial industry or otherwise) may be an important factor affecting IS security practices for several reasons (Goodhue & Straub, 1991). First, financial organizations are likely to invest heavily on IS and rely extensively on IS for their business operations, compared to other organizations. Second, because the industry is information-intensive, potential losses for financial organizations due to IS abuses can be extremely large. Third, the public image of financial organizations, in terms of reliability and security of financial information, is critical to the success of their businesses but can be severely damaged by IS abuses. As a result, Hoffer and Straub (1994) reported that financial organizations have been adding security forces to their staff since the 1980s. Given the importance of IS to their businesses, financial organizations may undertake more deterrent and preventive efforts than other organizations. Furthermore, to strongly discourage IS abuses, financial organizations are also likely to enforce more severe deterrents than other organizations.

H3a: Industry type (financial organization) is positively related to deterrent efforts.
H3b: Industry type (financial organization) is positively related to deterrent severity.
H3c: Industry type (financial organization) is positively related to preventive efforts.

4.2. IS security practices and IS security effectiveness

Deterrent efforts (reflecting certainty of sanctions) and severity (reflecting severity of sanctions) can discourage people from committing crimes or anti-social acts (Blumstein, 1978; Williams & Hawkins, 1986). Deterrent efforts have been empirically found to lower crime rate (Klete, 1978; Parker, 1983). Active and visible deterrent efforts have also been reported to reduce IS security abuses (Straub, 1990). Deterrent efforts can discourage people from IS security abuses by raising

the probability that they will be caught. Deterrent severity can dissuade people from IS security abuses because they will be severely punished when they are caught.

H4a: Deterrent efforts are positively related to IS security effectiveness.
H4b: Deterrent severity is positively related to IS security effectiveness.

The use of security software (embedded in operating systems or database management systems, or specialized security software) have been reported to reduce IS abuses (Nance & Straub, 1988; Straub, 1990). In general, preventive efforts can ward off illegitimate activities (Gopal & Sanders, 1997). More advanced security software tends to provide more sophisticated access control, thereby making it more difficult for people to engage in IS abuses.

H4c: Preventive efforts are positively related to IS security effectiveness.

5. Research methodology

The survey research method was used for data collection in this study.

5.1. Operationalization of constructs

As far as possible, constructs were operationalized using measures validated by previous studies. This helped to enhance validity and facilitate comparison of results across studies (Stone, 1978). Organizational size was measured using number of employees (Delone, 1988; Ein-Dor & Segev, 1978; Raymond, 1990). Four questions were used to assess top management support: higher management attendance in IS security-related meetings, higher management involvement in IS security-related decisions, higher management involvement in monitoring IS security-related activities, and higher management support for IS security-related functions (Thong et al., 1996; Yap et al., 1992). These questions were all anchored on a seven-point scale from 'extremely low' (1) to 'extremely high' (7). Industry type was specified by classifying organizations as financial (1) or otherwise (0) (Goodhue & Straub, 1991).

Deterrent efforts were measured using total man-hours expended on IS security purposes per week (Straub, 1990). Deterrent severity was assessed based on the most severe form of punishment meted out by the organization for IS security abuse: no action taken (0), reprimand by management (1), suspension of duties (2), dismissal from appointment (3), and prosecution in court (4). Preventive efforts were gauged using level of sophistication of security software used in the organization: security software embedded in operating systems (1), security software embedded in database management systems (2), and specialized security software (3). Since quantitative measures are subject to respondent's ability to recall and their willingness to answer, IS security effectiveness was measured using perceptual responses to six questions: overall deterrent effect, overall preventive effect, effect in protecting hardware, effect in protecting software, effect in protecting data, and effect in protecting computer services. These items correspond to the two types of security measures and the four different types of IT assets (Straub, 1990). All these questions were anchored on a seven-point scale from 'strongly disagree' (1) to 'strongly agree' (7).

5.2. Survey administration

The survey was mailed to 164 IS managers with the aid of their professional association. These IS managers were chosen because, as the person in charge of IS activities in their respective organizations, they should be familiar with IS security practices and operations in their organizations. They could consult their subordinates or colleagues if they thought this was appropriate.

A parcel comprising a cover letter (which explained the purpose of this study), a copy of the survey, and a self-addressed return envelope was sent to each of these IS managers. To raise the response rate, follow-up phone calls were made to IS managers who had yet to respond, 4 and 6 weeks after the parcels were sent out. Additional parcels were sent to IS managers who had misplaced the original parcels. Missing data in several responses were obtained through telephone calls to the respondents. Among the 164 IS managers surveyed, 63 complete responses (38.4% response rate) were obtained and used for subsequent data analyses.

6. Data analyses

All statistical analyses were carried out at a 5% level of significance. Table 1 presents the descriptive statistics of the responding organizations. In this study, we distinguished between financial and non-financial organizations. Other industry categories such as education and transportation were also investigated but there were no significant differences in security effectiveness for these other industry groups.

6.1. Partial least squares

Partial least squares (PLS) analysis, using PLS-Graph (Chin, 1994), was carried out in this study because of its strength over traditional statistical techniques such as multiple regression and analysis of variance. Like other structural equation modeling techniques (Bagozzi, 1994), PLS allows the measurement model (relationships between constructs and measures) and structural model (theoretical relationships among constructs) to be tested simultaneously. Moreover, PLS does not impose multivariate homogeneity and normality requirements on the data. This makes PLS the appropriate choice for two reasons. First, small sample sizes of less than 100, such as the sample for this study, are unlikely to meet homogeneity and normality requirements (Hair, Anderson, Tatham, & Black, 1998). Second, this study involved nominal (e.g., industry type) and ordinal data (e.g., deterrent severity and preventive efforts) that could not satisfy homogeneity and normality requirements (Hair et al., 1998).

6.2. PLS measurement model

The PLS measurement model linked each construct to its measures. The strength of the PLS measurement model could be demonstrated through convergent and discriminant validity (Hair et al., 1998). Two constructs (top management support and IS security effectiveness) had to be assessed for convergent and discriminant validity because these were measured using perceptual questions.

Table 1
Descriptive statistics of responding organizations

Construct	No. of organizations	% of respondents
Organizational size		
Less than 100 employees	3	4.8
100–499 employees	16	25.4
500–999 employees	14	22.2
1000–2499 employees	14	22.2
2500–9999 employees	12	19.0
More than 9999 employees	4	6.3
Industry type		
Financial organizations	13	20.6
Other organizations	50	79.4
Deterrent efforts		
Less than 5 h per week	14	22.2
6–15 h per week	17	27.0
16–45 h per week	16	25.4
More than 45 h per week	16	25.4
Deterrent severity		
No action taken	2	3.2
Reprimand by management	25	39.7
Suspension of duties	4	6.3
Dismissal from appointment	14	22.2
Prosecution in court	18	28.6
Preventive efforts		
Operating systems	5	7.9
Database management systems	12	19.1
Specialized security software	46	73.0

Three tests were used to assess convergent validity: reliability of questions, composite reliability of constructs, and variance extracted by constructs (Fornell, 1982). Reliability of questions was determined by examining the loadings of questions on their intended constructs, provided by PLS. Hair et al. (1998) proposed 0.5 as indication of adequate reliability. When computing composite reliability of constructs, PLS took into account relationships among constructs. Evidence of composite reliability could also be obtained based on Cronbach's alpha. Nunnally (1978) suggested that the reliability of a construct should be at least 0.7. PLS computed variance extracted by constructs based on the extent to which all questions measuring a construct actually tapped into the same underlying construct. Fornell (1982) suggested 0.5 as indication of adequate variance extracted. Based on the above criteria, both constructs (top management support and IS security effectiveness) had adequate convergent validity (see Table 2).

Two tests were used to assess discriminant validity. First, all questions were subjected to factor analysis to ensure that questions measuring each construct loaded more highly on their intended constructs than on other constructs (Cook & Campbell, 1979). Comrey (1973) indicated that

Table 2
Results of convergent validity tests

Construct and questions	Reliability of question	Composite reliability of construct	Cronbach's Alpha	Variance extracted by construct
Top management support		0.91	0.88	0.72
Attend meetings	0.84			
Involve in decisions	0.87			
Involve in activities	0.93			
Support for functions	0.79			
IS security effectiveness		0.95	0.90	0.76
Overall deterrent effect	0.77			
Overall preventive effect	0.75			
Protect hardware	0.88			
Protect software	0.80			
Protect data	0.85			
Protect computer services	0.83			

factor loadings of 0.45–0.54 were fair, 0.55–0.62 were good, 0.63–0.70 were very good, and above 0.71 were excellent. Table 3 shows that each question had excellent loading on its intended construct and was a good measure of that construct. Second, variance extracted by each construct should exceed the shared variance between that construct and other constructs (Fornell, 1982). Table 4 indicates that this criterion had been satisfied.

6.3. PLS structural model

With an adequate PLS measurement model, the hypotheses could be tested by examining the PLS structural model. Explanatory power of the PLS structural model was assessed based on the amount of variance in the endogenous constructs for which the model could account. The proposed PLS structural model could explain 51.3% of the variance for deterrent efforts, 11.3% of the variance for deterrent severity, 9.1% of the variance for preventive efforts, and 18.7% of the variance for IS security effectiveness (see Fig. 2). All these figures (except the figure for preventive efforts) exceeded 10%, which Falk and Miller (1992) suggested as indication of substantive explanatory power.

Jack-knifing was used to compute the T-statistic for each path in the structural model (Fornell, 1982). Since each hypothesis corresponded to one such path, support for each hypothesis could be determined based on the sign (positive or negative) and statistical significance for its corresponding path (see Table 5). Organizational size was positively related to deterrent efforts ($T = 4.79,\ p < 0.01$). H1a was supported but H1b and H1c were not supported. Top management support was positively related to preventive efforts ($T = 2.07,\ p < 0.03$). H2a and H2b were not supported but H2c was supported. Industry type (financial organizations) was positively related to deterrent efforts ($T = 6.24,\ p < 0.01$) and deterrent severity ($T = 1.67,\ p < 0.05$). H3a and H3b were supported but H3c was not supported. Deterrent efforts ($T = 2.83,\ p < 0.03$) and preventive

Table 3
Results of factor analysis

Question	Factor 1 (IS security effectiveness)	Factor 2 (Top management support)
Attend meetings	0.11	0.79
Involve in decisions	0.11	0.89
Involve in activities	0.18	0.88
Support for functions	0.09	0.84
Overall deterrent effect	0.78	0.07
Overall preventive effect	0.76	0.09
Protect hardware	0.87	0.15
Protect software	0.83	0.20
Protect data	0.85	0.18
Protect computer services	0.73	0.37
Eigenvalue	3.94	3.13
Variance explained	39.4%	31.3%
Cumulative variance	39.4%	70.7%

Table 4
Shared variances (variance extracted) among constructs

Construct	Top management support	IS security effectiveness
Top management support	(0.72)	
IS security effectiveness	0.33	(0.76)

efforts ($T = 1.68$, $p < 0.05$) were positively related to IS security effectiveness. H4a and H4c were supported but H4b was not supported.

7. Discussion and implications

In this study, a model of IS security effectiveness was formulated and empirically tested (see Fig. 2). Key findings are discussed along with the implications for further research and practice.

7.1. IS security effectiveness

Greater deterrent efforts (in the form of man-hours expended on IS security purposes) and greater preventive efforts (in the form of more advanced IS security software) appear to contribute to better IS security effectiveness. Straub and Welke (1998) reported that many managers are not comfortable with the notion of using deterrent and preventive efforts to reduce IS risks. This is because they are not familiar with the value of systematic and purposeful detection measures and the effects of preventive counter-measures. Results of this study can help

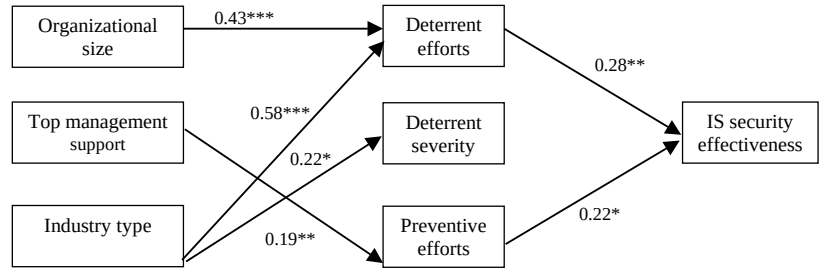

Fig. 2. Empirically tested model of IS security effectiveness.

Table 5
Results of hypotheses tests

Hypothesis	Estimate	*T*-statistic	*p*-value
H1a: larger organizational size → greater deterrent efforts	0.43	4.79	0.01
H1b: larger organizational size → greater deterrent severity	0.04	0.19	n.s.
H1c: larger organizational size → greater preventive efforts	0.15	1.34	n.s.
H2a: greater top management support → greater deterrent efforts	0.05	0.62	n.s.
H2b: greater top management support → greater deterrent severity	0.21	1.41	n.s.
H2c: greater top management support → greater preventive efforts	0.19	2.07	0.03
H3a: industry type (financial industry) → greater deterrent efforts	0.58	6.24	0.01
H3b: industry type (financial industry) → greater deterrent severity	0.22	1.67	0.05
H3c: industry type (financial industry) → greater preventive efforts	0.10	0.74	n.s.
H4a: greater deterrent efforts → higher IS security effectiveness	0.28	2.83	0.03
H4b: greater deterrent severity → higher IS security effectiveness	0.11	0.80	n.s.
H4c: greater preventive efforts → higher IS security effectiveness	0.22	1.68	0.05

to allay their fears and to assure them that deterrent and preventive efforts can be worthwhile in the context of IS security.

Deterrent severity (in the form of punishments meted out to IS abusers) does not seem to affect IS security effectiveness. Enforcing more severe penalty for IS abusers, who are caught in their act, does not seem to deter IS abuses. A plausible reason may be because the maximum penalty for IS abuses tends to be less severe than those for crimes involving human victims (e.g., murder or physical assault). Indeed, Silberman (1976) found that deterrent severity does help to discourage crimes involving human victims but not crimes involving property or other non-human artifacts (which should include IS abuses). Hence, in the context of IS security, organizations should focus their attention on deterrent and preventive efforts rather than deterrent severity.

The lack of management awareness about the impact of deterrent and preventive efforts suggests that some form of management and user education (Straub & Welke, 1998) may be useful in the context of IS security. In this study, key elements of deterrent efforts are policy statements and guidelines on legitimate use of IS assets, security briefings on the consequences of illegitimate

use of IS assets, and audits on the use of IS assets. These elements offer some directions for management and user education. First, the importance of policy statements and guidelines, as the basis for all aspects of preventive efforts, can be emphasized to management. Visible and active management participation during the formulation of policy statements and guidelines are crucial. Second, users need to be educated on what constitutes legitimate use of IS assets and what are the consequences of illegitimate use of IS assets. This can help to reduce instances where users misunderstand the rights and privileges accorded to them and carry out unauthorized IS activities (Dhillon & Backhouse, 2000). Third, trained and experienced IS auditors (Champlain, 1998) should be employed to carry out audits on the use of IS assets periodically. Besides studying exception reports generated by the security software, IS auditors can be given authority to randomly check how users are currently using IS assets.

As for preventive efforts, management needs to be educated on the value of deploying advanced security software to protect IS assets. Besides offering better access protection and intrusion detection through more sophisticated firewalls, advanced security software can detect unauthorized IS activities through surveillance mechanisms and generation of exception reports.

7.2. Organizational size

Larger organizations appear to invest more in terms of deterrent efforts than smaller organizations. This finding agrees with prior studies, which found larger organizations to have proportionately more IS security staff and IS security resources (Hoffer & Straub, 1994; Straub, 1986). Smaller organizations often invest less in deterrent efforts because they have fewer employees so they think they know their employees well enough to trust them (Hoffer & Straub, 1994). However, given the significant positive relationship between deterrent efforts and IS security effectiveness and the fact that they may have greater difficulty recovering from IS security abuses, smaller organizations are advised to reassess their deterrent efforts so as to ensure sufficient protection for their IS assets.

7.3. Top management support

Top management support appears to be positively related to preventive efforts. This finding suggests that top management support often result in the allocation of resources to deploy advanced security software. Given the significant positive impact of preventive efforts on IS security effectiveness, organizations with weaker top management support can benefit from attempts to raise top management interest in IS security. One way of doing this is to carry out penetration testing (Champlain, 1998) and report IS vulnerabilities, as well as the business impact, to top management. Another way is explaining to top management how IS security can bring about tangible business benefits by raising the confidence of customers with their organization (Anthes, 1998).

7.4. Industry type

Financial organizations seem to invest more in deterrent efforts and have stiffer deterrent severity compared to other organizations. This result agrees with Goodhue and Straub (1991) that

financial organizations tend to have a greater concern for IS security due to large potential losses (financially and in reputation) that may occur from IS security abuses. Given that IS security effectiveness is significantly affected by deterrent efforts but not by deterrent severity, financial organizations should concentrate on enhancing key elements of deterrent efforts rather than trying to enforce severe penalties for IS abuses.

Non-financial organizations should be aware of their relatively lower deterrent efforts and concomitantly lower IS security effectiveness. This may become a concern in the future as organizations rely increasingly on IS for competitive advantage. Such organizations include those that have established electronic networks with their suppliers and customers as well as those that have embarked on electronic commerce initiatives, among others. For such organizations, the enormity of potential losses arising from IS security abuses should motivate them to raise their deterrent efforts so as to enhance their IS security effectiveness.

8. Conclusion

Given that the results of this study were based on one sample of organizations, attempts to generalize these results must be done with caution. Future studies can validate these results by replicating this study with more samples of organizations and a wider range of deterrent and preventive measures. Future research can also extend these results by incorporating other organizational factors such as organizational maturity, organizational culture, and organizational reliance on IS for competitive advantage (Ward & Griffiths, 1996).

In summary, this study theoretically developed and empirically tested a model of IS security effectiveness that incorporates organizational factors. By simultaneously testing relationships between organizational factors and security measures, and relationships between security measures and IS security effectiveness, this study assesses the adequacy and usefulness of security measures undertaken by different types of organizations and offers suggestions on how organizations may improve their IS security effectiveness. More studies on IS security are warranted in the future as organizations rely increasingly on IS for strategic advantage and operations, and as organizations become increasingly networked in the context of electronic commerce.

References

Anthes, G. H. (1998). Lotsa talk, little walk. *Computerworld*, *32*(38), 70–71.

Backhouse, J., & Dhillon, G. (1996). Structures of responsibility and security of information systems. *European Journal of Information Systems*, *5*(1), 2–9.

Bagozzi, R. P. (1994). *Advanced methods of marketing research*. Cambridge, MA: Blackwell.

Barsanti, C. (1999). Modern network complexity needs comprehensive security. *Security*, *36*(7), 65–68.

Baskerville, R. (1991). Risk analysis: An interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems*, *1*, 121–130.

Blumstein, A. (1978). Introduction. In A. Blumstein, J. Cohen, & D. Nagin (Eds.), *Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates*. Washington, DC: National Academy of Sciences.

Brancheau, J. C., Janz, B. D., & Wetherbe, J. C. (1996). Key issues in information systems management: 1994–95 SIM Delphi results. *MIS Quarterly*, *20*(2), 225–242.

Burger, K. (1993). The new age of anxiety. *Insurance and Technology*, *18*(10), 48–54.
Champlain, J. J. (1998). *Auditing information systems: A comprehensive reference guide*. New York: Wiley.
Chin, W. (1994). *PLS-Graph: Version 2.7*. Calgary, AB: University of Calgary.
Comrey, A. L. (1973). *A first course in factor analysis*. New York, NY: Academic Press.
Computer Security Institute, (2002). *CSI/FBI computer crime and security survey*, http://www.gocsi.com/press/20020407.html.
Cook, P. J. (1982). Research in criminal deterrence: Laying the groundwork for the second decade. In N. Morris & M. Tonry (Eds.), *Crime and justice: An annual review of research* (pp. 211–268). Chicago, IL: University of Chicago Press.
Cook, T. D., & Campbell, D. T. (1979). *Quasi-experimentation: Design and analysis issues for field setting*. Boston, MA: Houghton Mifflin.
Damanpour, F. (1991). Organizational innovation: A meta-analysis of effects of determinants and moderators. *Academy of Management Journal*, *34*(3), 555–590.
Delone, W. H. (1988). Determinants of success for computer usage in small business. *MIS Quarterly*, *12*(1), 51–61.
Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125–128.
Ein-Dor, P., & Segev, E. (1978). Organizational context and the success of management information systems. *Management Science*, *24*(10), 1064–1077.
Eloff, J. H. P. (1988). Computer security policy: Important issues. *Computers and Security*, *7*(6), 559–562.
Falk, R. F., & Miller, N. B. (1992). *A primer for soft modeling*. Akron, OH: University of Akron Press.
Forcht, K. A. (1994). *Computer security management*. Danvers, MA: Boyd and Fraser.
Fornell, C. (1982). *A second generation of multivariate analysis*: *Methods*, *Vol. 1*. New York, NY: Praeger.
Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users: A study of perceptions of the adequacy of security. *Information and Management*, *20*(1), 13–27.
Gopal, R. D., & Sanders, G. L. (1997). Preventive and deterrent controls for software piracy. *Journal of Management Information Systems*, *13*(4), 29–47.
Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate data analysis with readings*. Englewood Cliffs, NJ: Prentice-Hall.
Hoffer, J. A., & Straub, D. W. (1994). The 9 to 5 underground: Are you policing computer crimes? In P. Gray, W. R. King, E. R. Mclean, & H. Watson (Eds.), *Management of information systems* (pp. 388–401). Fort Worth, TX: Harcourt Brace.
Jarvenpaa, S. L., & Ives, B. (1990). Information technology and corporate strategy: A view from the top. *Information Systems Research*, *1*(4), 351–375.
King, W. R. (1994). Organizational characteristics and information systems planning: An empirical study. *Information Systems Research*, *5*(2), 75–109.
Klete, H. (1978). Some minimum requirements for legal sanctioning systems special emphasis on detection. In A. Blumstein, J. Cohen, & D. Nagin (Eds.), *Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates*. Washington, DC: National Academy of Sciences.
Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly*, *17*(2), 173–186.
Madnick, S. (1978). Management policies and procedures needed for effective computer security. *Sloan Management Review*, *20*(1), 61–74.
Nance, W. D., & Straub, D. W. (1988). An investigation into the use and usefulness of security software in detecting computer abuse. *Proceedings of the ninth annual international conference on information systems* (pp. 283–294). Minneapolis, MN.
Nunnally, J. C. (1978). *Psychometric theory*. New York, NY: McGraw-Hill.
Olnes, J. (1994). Development of security policies. *Computers and Security*, *13*(8), 628–636.
Panettieri, J. C. (1995). Informationweek/Ernst and Young security survey. *Informationweek*, *555*, 32–37.
Parker, D. B. (1981). *Computer security management*. Reston, VA: Reston Publishing.
Parker, D. B. (1983). *Fighting computer crime*. New York, NY: Scribner.

Pearson, F. S., & Weiner, N. A. (1985). Toward an integration of criminological theories. *Journal of Crime and Criminology*, *76*(1), 116–150.
Raymond, L. (1990). Organizational context and information systems success: A contingency approach. *Journal of Management Information Systems*, *6*(4), 5–20.
Reich, B. H., & Benbasat, I. (1990). An empirical investigation of factors influencing the success of customer oriented strategic systems. *Information Systems Research*, *1*(3), 325–347.
Silberman, M. (1976). Toward a theory of criminal deterrence. *American Sociological Review*, *41*, 442–461.
Stone, E. (1978). *Research methods in organizational behavior*. Santa Monica, CA: Goodyear.
Straub, D. W. (1986). Computer abuse and computer security: Update on an empirical study. *Security, Audit, and Control Review*, *4*(2), 21–31.
Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255–276.
Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, *14*(1), 45–60.
Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22*(4), 441–469.
Thong, J. Y. L., Yap, C. S., & Raman, K. S. (1996). Top management support, external expertise and information systems implementation in small businesses. *Information Systems Research*, *7*(2), 248–267.
Verton, D. (2002). Disaster recovery planning still lags. *Computerworld*, *36*(14), 10.
Ward, J., & Griffiths, P. (1996). *Strategic planning for information systems*. Chichester: Wiley.
Weber, R. (1988). *EDP auditing: Conceptual foundations and practice*. New York, NY: McGraw-Hill.
White, G. B., Fisch, E. A., & Pooch, U. W. (1996). *Computer system and network security*. Boca Raton, FL: CRC Press.
Williams, K. R., & Hawkins, R. (1986). Perceptual research on general deterrence: A critical review. *Law and Society*, *20*(4), 545–572.
Wood, C. C. (1987). Information systems security: Management success factors. *Computers and Security*, *4*(6), 314–320.
Yap, C. S., Soh, C. P. P., & Raman, K. S. (1992). Information system success factors in small business. *Omega*, *20*(5), 597–609.
Zviran, M., & Haga, W. (1999). Password security: An empirical study. *Journal of Management Information Systems*, *15*(4), 161–185.

Atreyi Kankanhalli holds a B.Tech. from the Indian Institute of Technology, an M.S. in Electrical Engineering from Rensselaer and is a Doctoral Candidate in the Department of Information Systems at the School of Computing, National University of Singapore. Her research interests are in knowledge management, computer-mediated communication, virtual teams, cross-cultural studies and information systems security.

Hock-Hai Teo holds a B.Sc.(Hons.), M.Sc., and Ph.D. from the National University of Singapore and is an Assistant Professor in the School of Computing there. He served on the EDIMAN (Electronic Data Interchange for Manufacturing) Standards Working Committee (1995–96), for electronic and petrochemical industries in Singapore. His research interests include electronic commerce, distributed work, knowledge management, and user–database interactions.

Bernard C.Y. Tan, Ph.D. (National University of Singapore) is an Associate Professor and Head of the Department of Information Systems in the School of Computing. He has published widely in a variety of Management and IS journals. His research focuses on cross-cultural issues, computer-mediated communication, knowledge management, and electronic commerce.

Kwok-Kee Wei is a Professor in the Department of Information Systems at the National University of Singapore. He has published widely in the Information Systems and Electronic Commerce literature. His research focuses on electronic commerce (Internet and electronic data interchange), human–computer interaction, and knowledge management.