An Exploratory Study of the Relationship among the High-level Management's Security Awareness, Organizational Information Security Activities, and the Execution Level of Organizational Information Security

Szu-Yuan Sun*, Ya-Chic Yeh*
*National kaohsiung First University of Science & Technology
Taiwan
sunnyy@ccms.nkfust.edu.tw

Pei-Chen Sun**, Ming-Yan Lan**
** National Kaohsiung Normal University
Taiwan

Abstract

As the issue of information security becomes increasingly important, high-level management security awareness on operation of organizational information security activities is a significant factor in success. Hence, the aim of this research is to explore how the organizational information security activities are being influenced by high-level management security awareness, and to use information security standard BS7799 to evaluate the execution phase of organizational information security. Combining literature research, case study and the main security codes of BS7799, this paper proposes a conceptual model of high-level management security awareness, organizational information security activities and organizational information security standard in relation to each other. In our conclusion, we discovered that the higher the high-level management security awareness cognizance about industry risks, the implementation of security measures and the threats to organizational security not only facilitate the four information security activities of deterrence, prevention, detection and recovery, they also enhance the standard of organizational information security. In practice, the conclusion of this paper hopes to remind high-level management to be aware of the threats of human factors and also to strengthen risk evaluation and deterrence activity.

Keywords：Information security, safety awareness, BS7799, case study.

(I) Introduction

The trend in the introduction of information security is reaching the mature stage overseas, but it is just at the starting stage within the country. In recent years, the rapid change in computer virus variety, the invasions by unavoidable hackers, the event of the 9/11 terrorist attack and the inferno at the Eastern Science-based Park altogether induced domestic security awareness. Nonetheless, Baskerville & Stage (1996) mentioned that information security management was an important but often ignored issue, and it was often restricted by the discussion of the information technology development viewpoint and was rarely discussed through the management viewpoint.

BS7799 stated that one of the significant success factors in information security introduction was the support by high-level management, but there are not many high-level managers in Taiwan corporations who really understand information security, and people within the industry are biased toward sales and not on resolving projects; these are the obstacles to the information security environment. High-level managers usually do not have sufficient cognizance about information security, although they do spend a lot of money and manpower to purchase related security products like fire-prevention walls, invasion detection, computer virus protection, but they do not effectively resolve a variety of security loopholes and threats of hacker invasion. Consequently, high-level management's security awareness can influence the implementation of information security activities within the whole organization.

The full name for 「BS7799」is 「BS7799 Code of Practice for Information Security」. It was proposed by a U.K. standard institution called BSI in 1995 and is currently the most well known security standard internationally. BS7799 is a set of fairly complex information security application and provides a complete set of policies, procedures, implementations and organizational structures as a reasonable safeguard to corporations in order to reach their corporation goals as well as to avoid, detect or correct the aftermath of unanticipated events. To combine all above mentioned points, the main aims of this research are as follows：

1. To understand what is the current security awareness of high-level management in high technology industry and how high-level management's security awareness influences the implementation of the four types of information security activities, deterrence, prevention, detection and recovery.

2. Through the use of BS7799-2：1999 to proceed with analysis of differences in the execution phase of information security and to understand the deficiencies in information security activities within the current high technology industry.

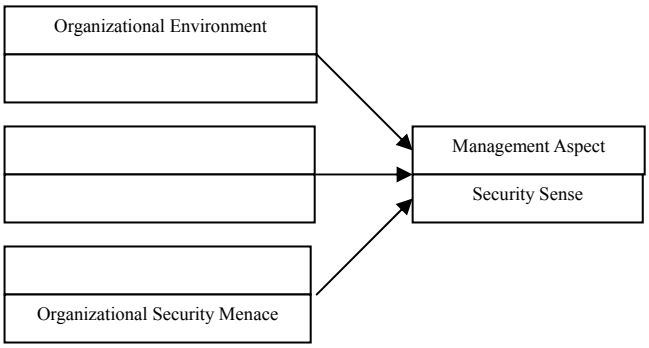
3. To propose a set of conceptual models to assist high technology industry in conducting information security activities.

(II) Literature Research

(i) High-management security awareness

Atreyi et al. [1] stated that although information security was becoming an important management issue, the industry did not attach importance to this in practice. Management's concern in information security was always lower than other issues (Brancheau, Janz & Wetherbe, 1996; Olnes, 1994). Verton (2002) did survey 459 CIO's and IT managers of medium and large corporations comprehensively about information security and discovered that less than 50% of their employees had IT security education and training within the company, indicating that high-level management in medium and large corporations attached low importance to information security. In addition, Zviran & Haga (1999) pointed out that high-level management did not give sufficient concern to information security, which could lead to serious invasion of information systems. The lack of concern by high-level management to information security might even influence the establishment of a corporation.

Goodhue & Straub [2] were the first researchers to apply the satisfaction level theory to cognizance of information security and proposed that the organizational environment, information system environment and individual characteristics could influence users to pay attention to the importance of security. Straub & Welke [3] improved Goodhue & Straub's Security Concern Model to become industry risk, risk reduction in security control measures and individual factors, which could influence high-level management's cognizance regarding information security.



Drawing 1：High-level management Security Concern Model

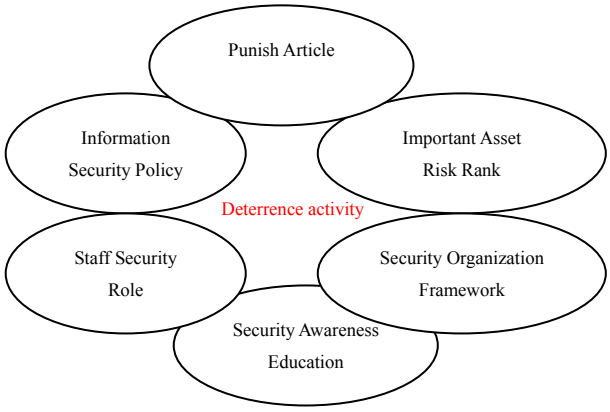
(ii) Organizational Information Security Activity

Based on the General Deterrence Theory, scholars (Forcht 1994; Martin 1973; Parker 1981) proposed four different types of sequential security activities, which could reduce information systemic risk. These four activities are：deterrence, prevention, detection and recovery.

Blumstein et al. (1978) wrote that the deterrence theory provided disincentives or restricted the occurrence of abnormal behaviors and also provided restrictions by deterring potential perpetrators. Furthermore, Straub and his research partners successfully applied deterrence theory to informational system environment. Sraub (1998) mentioned that information security activities could deter potential computer hackers who stealthily or overtly violate organizational policies.

Respective explanations of these four activities are as follows：

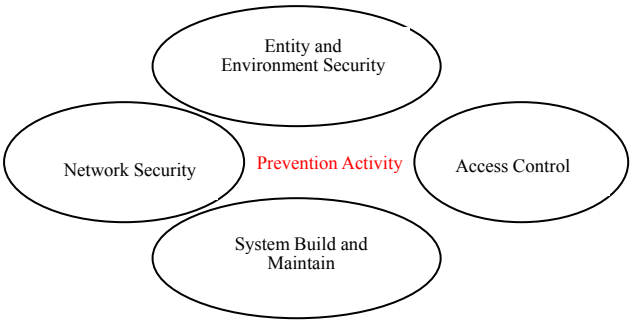
1. Deterrence activity：Blumstein et al. (1978) wrote that deterrence activity might cause potential hackers to understand the risk of penalty. Parker (1981、1983) pointed out that deterrence activity should include：security policy and clauses to reduce the invasion by white-collar people. Dunn (1982) also mentioned that deterrence activity should clearly explain how to use information system legally and to reduce potential hackers' perpetration motives. Straub (1990) stated that deterrence activity in practice should include：input of security man-power and time, reasonable system usage guidelines and clauses for system usage. Straub (1988) also wrote that security awareness education was a type of deterrence activity. The following drawing partially summarizes the above-mentioned details:



Drawing 2：Deterrence Activity (sorted by this research)

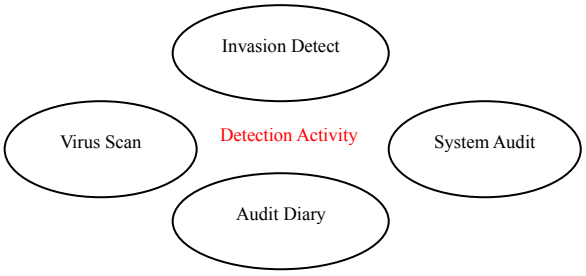
2. Prevention Activity：Gopal & Sander (1992、1997) wrote that prevention activity was mainly a proactive security control measure, including implementation of information security policy and prevention of invasion or intentional abusive usage by unauthorized people. Hsaio et al. (1979) stated that prevention activity should include：physical security and security software (e.g. password protection). Straub (1998) also mentioned that implementing door control system and password saving

and extraction control system for the computer room was also considered as prevention activity. Atreyi et al. [1] believed that operating system and database management including security functions and even the use of special security software could all prevent the risk information system from being invaded. The prevention activity can be categorized into the following parts：



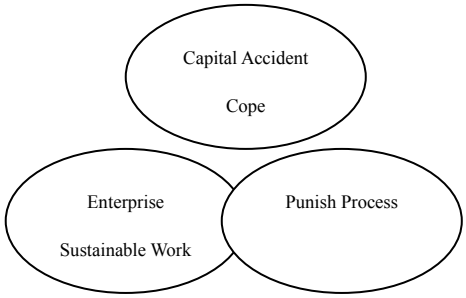
Drawing 3：Prevention Activity (sorted by this research)

3. Detection Activity：Detection activity is mainly for collection of invasion records and also to identify potential perpetrators. Straub & Nance (1987) wrote that only few invasion events were discovered by a pre-emptive type of detection activity because detection activity was more like fishing expeditions and could not successfully lock in on a target. However, Nance & Straub [10] also stated that relying only on two activities of deterrence and prevention could not totally avoid the occurrence of invasion events, organization also required detection activity to detect invasion before its occurrence. Straub (1998) indicated that detection activity could include two types：a pre-emptive type of security response and a reactive type of security response. The pre-emptive type of security response is to detect potential problems (risks) preemptively prior to their occurrences, examples of pre-emptive detection are invasion detection reports, system auditing, virus scan reports. Reactive type of security response is to proceed with detection through security invasion records after the event. The following is a brief summary of detection activity：



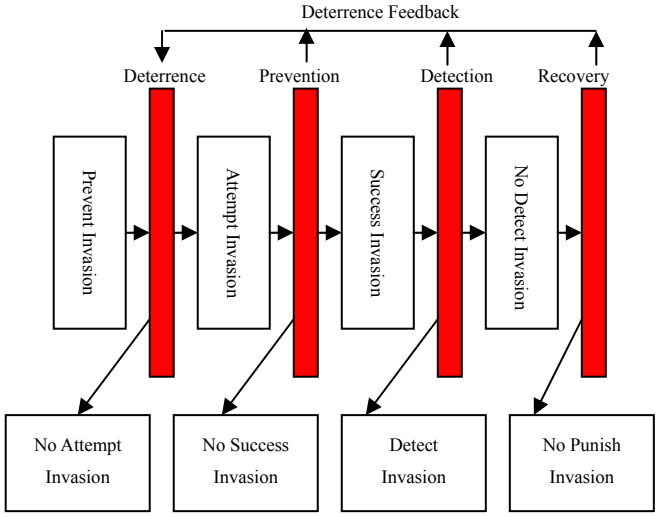
Drawing 4：Detection Activity (sorted by this research)

4. Recovery Activity：Straub (1998) stated that the majority of top-managers were rarely concerned about how to recover after security was invaded and the system was damaged leading to unsalvageable corporation loss. In fact, other than deterrence, prevention and detection, effective security procedures needs to include recovery activity to reduce damages caused by invasion activity so that corporations can recover their operations at the shortest time period and also to punish perpetrators. Recovery activity is summarized below：



Drawing 5：Recovery activity (sorted by this research)

According to deterrence theory, Straub (1998) stated that the combination of these four security activities could have continuous future deterrence effects. The integration of these four activities is as follows：



Drawing 6：The process of four security activities (sorted by this research)

(iii) Evaluation of Information Security Execution

NIST in the U.S. announced the self-evaluation guide on the information security management system in 2001 and requested using the Risk Based Decision Mode as a basis for secrecy, wholeness, undeniability, regularity and usability of the information industry for self-evaluation. In our country, “the Electronic Information Management

Center within the Directorate General of Budget Accounting and Statistic Executive Yuan, R.O.C." also announced "self-evaluation form for external auditing on information security" to assist corporations in understanding the facts in executing information security management system and can be used as a reference for improvement.

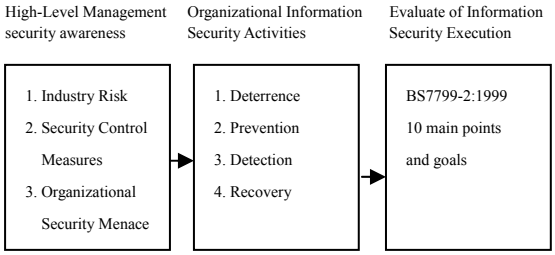
BS7799 includes two parts, Part 1：Practical criteria for information security management and Part 2：Standard for information security management system. Because BS7799 Part 2 explained in detail the requirement for establishment, implementation and maintenance of information security system, pointed out that organizations need to follow one type of risk evaluation for the most appropriate control items, and also used the appropriate control items for their own needs, we will use BS 7799-2 to analyze the differences in the execution phase of information security in order to understand an individual company's current information security execution level.

Drawing 7：10 main points and goals of BS7799 (sorted by this research)

(III) Conceptual Model and Research Method

(i) Conceptual model

Similar to the literature research discussed previously, Straub (1998) stated that if organizations implemented those four security activities, they could effectively deter potential hackers and reduce invasion risks for organizations. In addition, Straub (1998) also mentioned that if high-level management executed these four security activities, this would effectively reduce systemic risk. Hence, the level of high-level management cognizance and security awareness about industry risk, security control measures and threats to an organizational can influence the execution of information security activities and can even influence organizational information security standard. R.Von Solms et al. [6] also wrote that through BS7799, high-level management could evaluate the information security execution phase to adjust the deficiencies in organizational information security activities in order to meet legal standards, industry standards, customer requirements, supplier requirements and the requirements of anyone who is related to corporation profits. Through literature research, we proposed a conceptual model to evaluate high-level management security awareness, organizational information security activities and organizational information security execution.



Drawing 8：This research paper's conceptual model

As indicated in drawing 8, Straub (1998) mentioned that high-level management's security awareness and cognizance about industry risk, implementation of security measures and threats to organizational security could lead to differences in organizational activities of deterrence, prevention, detection and recovery. Consequently, we believe that high-level management security awareness affects organizational information security activities. Solms & Haar (1994) wrote that organizational information security control measures could use international security evaluation standards to understand the execution level of organizational information security. Because BS7799 is an internationally well known security standard, we believe that BS7799-2：1999 can be used on organizations' deterrence, prevention, detection and recovery activities to proceed with the differential analysis on information security execution phase and to understand the differences between an organizations' four information security activities and the basic standard.

(ii) Creation of Assumptions

Through the modification of variables in the conceptual model, various assumptions were made in this research. Assumptions are categorized into two main parts：The first part is assumption between the relation of high-level management's security awareness and organizational information security activities. The second part is assumption between the relation of organizational information security activities and evaluation of information security execution phase.

Assumption 1：When high-level management's understanding is higher with respect to the cognizance on industry risk, implementation of security measures and threats to organizational security, organizations can do better on the four information security activities of deterrence, prevention, detection and recovery.

Assumption 2：When high-level management is being influenced by other external factors, they cannot do as well for those four information security activities.

Assumption 3：Organizations pay more attention to prevention activities than other activities of deterrence, detection and recovery.

Assumption 4：As organizations' information security activities of deterrence, prevention, detection and recovery are being actually executed, they can better conform to the information security standard of BS7799-2：1999.

(iii) Research Method

This research paper uses various case studies to solve research problems, mainly directed to：factors that influence high-level management security awareness(Why), how high-level management security awareness affect the c of organizational information security activities(How) and investigation about what is used to evaluate organizational information security execution phase(What). Further analysis through interviews and other literature are conducted to investigate the execution phase of information security in the current high technology industry.

Case study is a form of empirical inquiry for investigation, Yin (1994) wrote that when research objects and actual situations were not very distinctive, using case study to solve "How" and "Why" types of research problems and through multi-varied evidence sources could emphasize the object events for research purposes. Because case study conforms to our research aim, we will use case study to solve research problems.

(IV) Analysis Individual Cases

I Individual case findings

Our method to choose cases is as follows：1.Choose higher information density within high technology industries; 2. Industry members who agree to accommodate us by having interview visits. Data collected conforms to points raised by Yin(1994)：(1) Using multi-varied evidence sources with two or more sources to obtain evidence; (2) Establish a database for individual cases to formally assemble together all the collected data from interview visits; (3) Connect all relevant evidences and connect research problems, data from interview visits and verified conclusions together.

Table 1： Basic data for individual cases

Individual Case Name	Industry	capitaliz_ ation	Overseas Subsidiary Location	Staffs population	Exection IS Initial Time	co-opera_ tive enterprise
X Company	Informat_ ion	700 million	USA	1500	1979/8	Trend Symantec Sysware
Y Company	Photoele_ ctric Tec_ hnology	680 million	China	1100	1999	Trend An Yi Accounting Services Company

This research paper analyzed the interview results of system development engineers from Company X and the MIS departmental head of c Y as well as these two companies' information, together with other information security management literature were analyzed. The conclusions of analysis are discussed below.

(i) The Security Awareness of High-level Management

Comparison was conducted based on "cognizance of industry risk", "security measured implemented" and "threats to organizational security" (shown in Table 2), it was discovered that high-level management's security awareness performance from Company X is not only affected by security events within the same industry, this company also pays attention to the importance of human factor threats; although the organization does not conduct risk evaluation, this company has an IT background, so it believes that it is more likely to be influenced by mainframe computer loopholes and copyright issues, hence the security measures are biased toward the technological side. The security awareness of high-level management within Company Y is not influenced by events within the same industry, it would strengthen security phase only through client requests. Because high-level managers do not have IT backgrounds, they need to be informed by employees from lower levels to know basically that the organization is affected by copyright issues, hacker invasions and other human and non-human factors. When faced with security problems, they should authorize lower level employees to solve problems, hence this company is also biased toward the technological side. In comparison, the security awareness of high-level management from Company X is higher than those from Company Y; furthermore, security awareness is higher if high-level management have IT backgrounds.

Table 2：Comparison of security awareness between high-level management in individual cases

		X Company	Y Company
High-level Management security awareness	Industry Risk	affected within the same industry, enhance deterrence activity	affected without the same industry, within the customer
	Security Control Measures	biased toward the technological side	biased toward the technological side
	Organizational Security Menace	mainframe computer loopholes and copyright issues, and no rsik estimte	copyright issues and hacker invasion, and no rsik estimte

In addition, other factors of organizational information security goals, security behavior, serious information security events, security event reports and high-level management's managing methods can be used to understand high-level management's level of security awareness (shown in table 3). For example, high-level management in Company X believes that security is mainly for maintenance of normal organizational operation system, when security events occur managers not only are management involved in managing the event, they also proactively teach employees about the importance of security so they adjust information security

activities based on their experience of previous serious security events. In contrast, although high-level managers in Company Y also believe that the goal of the company's information security is to maintain normal operation of the system and procedures, they normally authorize lower level employees to manage serious security events when they occur, so their support for information security is more passive and their security activities will also be influenced by previous serious security events that occurred. Hence, the other factors listed in the table below can further strengthen the support that high-level management's security awareness in Company X to be higher than that of Company Y.

Table 3：Comparison of other security awareness factors in individual cases.

		X Company	Y Company
other factors	security goals	maintenance of normal operation system	maintain operation of the system and procedures
	security behavior	positive attitude	passive attitude
	serious IS events	hacker invasion	virus invasion
	after events action	prevention and detection	enhance prevention
	security event reports and managing methods	management involve	management authorize

(ii) Organizational Information Security Activities

X and Y Companies' information security activities are shown in table 4. Although Company X's deterrence activity does not have a uniform information security policy, its policy does include some provisions about information security and employees understand their own responsibilities in security. Even though there are no information security experts to assist the drive of information security activities, high-level management actively participate in the policy formulation on information security and also regularly educate and train employees on information security. This induces the organization to conduct deterrence activity, indicating that this company pays attention to the importance of information security and can deter intentional or unintentional hackers. In contrast, although there is a uniform information security policy in Company Y, high-level managers only orally support this issue and do not personally drive the matter; the information security education is conducted irregularly depending on the volume of sales. In addition, there is no clear strict penalties in penalty clauses, so their overall performance in deterrence activity is passable.

With respect to prevention activity, although Company X does not have suitable documentation, because high-level managers have IT experience and there are more information technology personnel in the organization, this company tends to apply self-management of information security protection, maintenance or correct versioned security software purchase in the areas of physical security, internet security, saving and extraction control, virus protection and system development, so its prevention level is very good. In contrast, Company Y has suitable documentation, but because high-level managers do not have IT experience and there are few information technology personnel in the organization, the physical security, Internet security, saving and extraction control and system development tend to be outsourced. The IT personnel only need to conduct simple information security maintenance and management. Hence, the overall performance of Company Y is passable.

Table 4：Comparison of information security activities between individual cases.

		X Company	Y Company
security activities	Deterrence Activity	achieve expect security experts, risk analysis ,policy formulation management actively participate	achieve expect security expects, risk analysis, irregularly depending management passively participate
	Prevention Activity	have quite level except suitable documentation	although have suitable documentation, but not have quite level
	Detection Activity	no detection unit each team member to detect, have inner and outer auditors full use daily	no detection unit have inner and outer auditors few use daily
	Recovery Activity	security limit is lower strict penalties continuous procedures	no security limit no strict penalties procedures irregularly

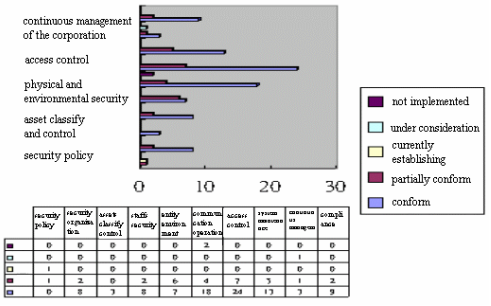
Regarding the detection activity, although Company X does not have a security detection unit, each team member within the organization does his/her best to detect the existence of any undiscovered security invasion and even uses abnormalities reported in auditing diary to find relevant security events. Company auditors will regularly audit to find out whether the company complies with security environment and security measures; and clients will come unannounced to audit the use of working capital by the company. Hence, the overall performance of detection activity in Company X is clearly better. There is no security detection unit in Company Y as well, but invasions are often discovered only after the event. Although there is a security diary to report abnormal security events, it is rarely inspected and reviewed to determine whether any abnormal events are occurring. Because the internal and external auditors in this company are not very familiar with IT, complete and effective audits cannot be achieved. Consequently, the overall performance of detection activity is very poor for Company Y.

Regarding the last activity of recovery, the specified information security limit is lower for Company X; damage recovery is to proceed when that reached is lower than the specified limit . There are rules for strict penalties, but no record of cases about actual penalties being applied. There are regular meetings to review the continuous operation procedures in the organization as well as regular important data about assistance from other sources in case of a serious events occurring, so the overall performance of recovery activity for Company X is fairly good. In Company Y, there is no clear

information security limit, no active execution of strict penalties and only modifications of continuous operation procedures irregularly, so the recovery activity for Company Y is passable.

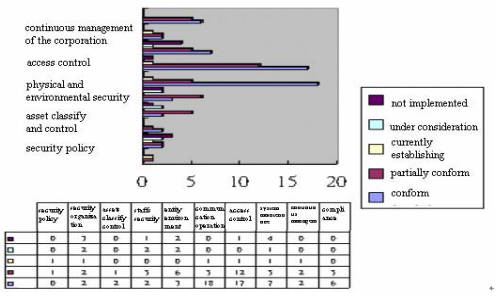
(iii) Evaluation of Execution phase on Information Security

This research paper used the ten main control points in BS7799-2：1999 to evaluate whether company X and Y's execution phase of information security conforms to the standard. We used conform, partially conform, currently establishing, under consideration and not implemented to evaluate information security execution phase for both company X and Y, and categorized them into three results：good performance, passable performance and poor performance. These three results are relative concepts and are not absolute.



Drawing 9：Evaluation of information security execution phase for company X.

It can be seen from drawing 9 that based on the ten controls in BS7799-2：1999, company X nearly conforms to all controls, except the security policy and few parts are either currently establishing, under consideration or not implemented. This result supports the performance of those four information security activities mentioned previously. Hence, the information security execution phase for company X is judged to be of good performance.



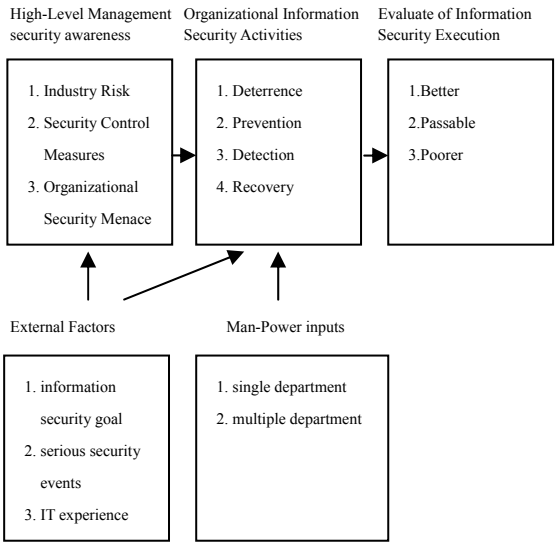
Drawing 10：Evaluation of information security execution phase for company Y.

It can be seen from drawing 10 that based on the ten controls in BS7799-2：1999, company Y conforms to the standard for the following controls：communication and operation management, saving and extraction control, system development and maintenance and compliance.

The rest, for example：security organization, personnel security, physical security, physical and environmental security, saving and extraction control, system development and maintenance and continuous operation management of the corporation, are mainly categorized into the partially conform type.

It appears that the majority of security organizations, physical and environmental security and system maintenance and development are in the not implemented category. Therefore, the overall result of company Y supports the performance of those four information security activities mentioned previously. Hence, the information security execution phase for company Y is judged to be of passable performance.

Based on the above analysis, the former conceptual model is modified (as shown in drawing 11) to understand that the security awareness of high-level management not only influences organizational information security activities, external factors also influence organization information security activities of deterrence, prevention, detection and recovery. Furthermore, adding the man-power input through high-level management information security activities also influence the execution phase of organizational information security.



Drawing 11：Modified conceptual model.

The following table lists the variables in individual cases：

Table 5：A list of variables in individual cases

	X Company	Y Company
Industry Risk	Yes	No
Security Control Measures	Widely Understand	Narrowly Understand
Security Menace	Understand	Not Understand
information security goal	fit organization goals	fit organization goals
serious security events	Yes	Yes
IT experience	Yes	No
Security Activities	Deterrence passable others better	Detection passable other poorer
Man-Power inputs	Multiple department	Single department
Evaluate Security Execution	better	passable

II Verification of Assumptions

Our verification result for this research is contained in table 6.

Table 6：This research's verification result for both company X and Y.

hypothesis	X Company	Y Company
Assumption 1	fit	partial fit
Assumption 2	fit	high-level managers do not have IT backgrounds
Assumption 3	fit	fit
Assumption 4	partial fit	partial fit

(V) Conclusions and Recommendations

This research is mainly to investigate how high-level management security awareness affect the drive for organizational security activities, and ten control points from BS7799-2：1999 are used to evaluate the performance in the execution of other information security. Our conclusions are as follows：

1. Through analysis of individual cases for the understanding of organizational information security goal, serious information security events previous occurred and IT experience can influence the bias of organizations for particular information security activities.

2. High-level management with higher security awareness can do better on the four information security activities of deterrence, prevention, detection and recovery with better performance in the execution of information security.

3. Through individual cases to understand slight deficiencies in the performance of deterrence activity in organizations, which appears in corporations with weak information security management.

4. Through individual cases to understand that corporations have a tendency to ignore threats from human factors. This can be a hidden worry worthy of consideration.

5. Through individual cases to understand that corporations need to strengthen risk evaluation to effectively distinguish sources of threat and severity level in order to assist in the choice of effective security control measures.

Our research follow-up recommendations are listed below：

1. Outsourcing of information security can be investigated to determine how it influences information security management between corporations.

2. We recommend that follow-up research can be directed to discover how organizational information security activities can be improved through humans, technology, policies and procedures and to propose effective improvement methods.

(VI) Reference

[1]. Atreyi Kankanhalli*, Hock-Hai Teo, Bernard C.Y. Tan, Kwok-Kee Wei, "An integrative study of information systems security effectiveness," *International Journal of Information Management*, 2003(23), pp:139-154

[2]. Dale L. Goodhue and Detmar W. Straub, "Security concerns of system users – A study of perceptions of the adequacy of security," *Information & Management,* 1991(20), pp:13-27

[3]. Detmar W. Straub and Richard J. Welke, "Coping With Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly*, DECEMBER 1998, pp:441-469

[4].Karen D. Loch ,Houston H. Carr and Merrill E. Warkentin, "Threats to Information Systems: Today's Reality,Yesterday's Understanding," *MIS Quarterly*, June 1992, pp:173-182

[5].Melvin Schwartz, "Computer Security: Planning to Protect Corporate Assets," *The Journal of Business Strategy*, JANUARY /FEBRUARY 1990, pp:38-41

[6]. R.Von Solms ,H.van de Haar, S.H. von Solms, W.J.Caselli, "A framework for information security evaluation," *Information & Management,* 1994(26),pp:143-153

[7]. Steven Schlarman , "The People, Policy, Technology (PPT) Model: Core Elements of the Security Process," *Information System Security* , Nov/Dec2001, Vol. 10 Issue 5, pp:36-41

[8].Stuart E. Madnick, "Management Policies and Procedures Needed for Effective Computer Security," *Sloan Management Review,* 1978, pp:61-73

[9].Thomas R. Peltier, "Preparing for ISO 17799," *Security Management Practices*, JANUARY/FEBRUARY 2003,pp:21-28.

[10]. William D. Nance and Detmar W. Straub, "An investigation into the use and usefulness of security software in detecting computer abuse," *Proceedings of the ninth annual international conference on information systems*, 1988, pp: 283- 294