行政院國家科學委員會專題研究計畫 成果報告

評估資通安全有效管理之因素
研究成果報告(精簡版)

計畫類別	：個別型
計畫編號	：NSC 95-2416-H-004-058-
執行期間	：95年08月01日至96年01月31日
執行單位	：國立政治大學資訊管理學系

計畫主持人：許瑋元

計畫參與人員：碩士班研究生-兼任助理：陳韋均、羅國倫
大學生-兼任助理：鄭治中

報告附件：出席國際會議研究心得報告及發表論文

處理方式：本計畫可公開查詢

中華民國 96年07月11日

行政院國家科學委員會補助專題研究計畫期中進度報告

評估資通安全有效管理之因素

計畫類別：V **個別型計畫** □ 整合型計畫
計畫編號：NSC 95-2416-H-004-058-
執行期間： 95 年 8 月 1 日至 96 年 1 月 31 日

計畫主持人：許瑋元

執行單位：政治大學資訊管理系

成果報告類型(依經費核定清單規定繳交)：V 精簡報告 □完整報告

中 華 民 國 96 年 7 月 10 日

Abstract

Information systems security has gained renewed importance lately. We still, however, lack a comprehensive model of IS security effectiveness with a good theoretical underpinning. Previous research examined various effectiveness factors in isolation. Such an approach does not allow for the accurate assessment of the significance of these factors and their relative importance. In this research, we develop, operationalise and empirically test an integrative model of IS security effectiveness, drawing upon the theory of technology assimilation and the institutional theory. Our model provides a better understanding of the direct and indirect effects of various effectiveness factors and their interrelationships. It also enables a more accurate assessment of the significance and relative importance of specific technical and socio-organizational factors, providing senior executives and IS managers with guidelines for planning, prioritizing and implementing IS security programs. This report presents the research findings during a six-month study.

Keywords: information systems security management, security effectiveness

摘要

隨著網路運用之普及，資通管理安全的重要性也隨之受到公司以及政府的重視。近幾年 來，資通安全的趨勢演變已從技術面逐漸轉為對營運面以及風險管理的重視。然而，因安通安全仍屬於初步發展之階段，不同產業或公司對於如何達到及評估有效資通安全管理之標準往往認知上有相當大之差異，因此，即使公司花費在資安的預算逐年增加，每年因資安事件而導致的損失卻無下降的現象，反應資訊安全不能再單靠產品來滿足安全的需求。本研究計畫主要的目的在於探討政策面、產業面以及組織面影響資通安全有效管理之直接以及間接的因素。對於公司以及政府而言，如能了解各層面因素之影響力，並能充分考量內外環境等諸多因素，建立一套有效的資通安全的制度。此篇報告呈現為期六個月的研究成果[1]。

關鍵詞： 資通管理安全、資通安全政策、組織管理

[1] 計畫主持人因故需中止原爲一年期之研究計畫。

Introduction

Nicholas Carr (2003), in his recent highly controversial article, argues that the commoditisation of Information Technology (IT) requires the contemporary organisations placing increasing emphasis on "vulnerabilities, not opportunities" (p.11). In reality, computer security breaches and external risks such as terrorisms and natural disasters have increasingly posed a serious threat to the day-to-day running of an organisation. Furthermore, many industry reports have stated that organisational spending on information security have been on the rise for the past few years (Deloitte 2006; Gordon et al. 2006b). Even the regulatory agencies have introduced compliance requirements, e.g. the Sarbanes-Oxley Act, to ensure companies implementing appropriate corporate governance structure. Reflecting on these recent developments, we argue that the current focus on vulnerabilities protection implies that contemporary organisations are in the phase of searching for rationalised security management process in combating these vulnerabilities concerns and complying with the regulatory standards. Conceptually, we see this rationalised security management process, for instance ISO 17799, as form of an innovation.

Researchers in a variety of disciplines have been discovering the conditions that facilitate or hinder the adoption and diffusion process of organisational practices. Besides economics-driven motivation on innovation adoption (Bacon 1992; Reinganum 1981), institutional theorists offer another perspective emphasising the role of social actors such as regulatory authority and peer organisations in the innovation diffusion process (DiMaggio et al. 1991; Galaskiewicz et al. 1989). In Information Systems (IS) field, many researchers have examined the role of institutional isomorphism in influencing organisations' decision for the adoption or assimilation of technological innovations (Chatterjee et al. 2002; Iacono et al. 1995; Liang et al. 2007; Teo et al. 2003), but little has been found in studying the other form of innovation with the administrative core (Teece 1980; Westphal et al. 1997). Westphal *et al.* (1997) argue that academic researchers have the tendency of considering innovation "as a discrete phenomenon" (p368). In a critique of this assumption, they suggest that in contrast to technological innovations, administrative innovations have no concrete technical features and are subject to multiple interpretations during the diffusion process. Consequently, they contend that the uniqueness of administrative innovations lead to the difficulties to

> *" determine conformity from adoption alone; it may be necessary to examine conformity in the form of the innovation adopted or how it is implemented, treating the adoption of such innovations as continuous rather than discrete occurrence." (p368)*

Therefore, the research objective of this paper is threefold: first, this research is interested in identifying conditions that shape the spread of an administrative innovation in the context of IS management practices, ISO 17799, in the financial services sector. Second, our research interest is also to investigate the institutional effects at different stages of innovation by separating adoption from assimilation, as suggested by Westphal *et al.* (1997). Third, we aim to analyse different moderators of institutional conformity at each stage of ISO 17799 innovation diffusion in the financial sector.

Institutional Pressure for ISO 17799 Adoption and Assimilation in the Financial Sector

Neo-institutional theorists suggest that the practices travel from one organisation to another because of the operationalisation of different mechanisms of isomorphism in a social system (Scott 1995). DiMaggio and Powell (1983) argue that “the theory of isomorphism addresses ... the structural determinants of the range of choices that actors perceive as rational or prudent” (p149). Institutional researchers indicate that there exist three different mechanisms of institutional forces: *coercive, normative and mimetic* (DiMaggio et al. 1991; Meyer et al. 1991; Scott 1995). In the case of ISO 17799 diffusion in the financial sector, empirical research indicates that coercive and mimetic forces represent the source of power influencing the organisation decision on adoption and assimilation. Coercive isomorphism refers to the political influence stemming from the government agencies or powerful organisations such monopoly or multinational enterprises. For example, Haworth and Pietron (2006) demonstrate the relevance between ISO 17799 implementation and the Sarbanes-Oxley Act (SOX) of 2002. In the U.K, the requirement of Data Protection Act acts the regulatory mechanism for the British firms to implement IS security management practices (Backhouse et al. 2006). Although those requirements are not exclusively for financial institutions, the impact is equally profound. Besides, globally financial institutions are facing the pressure to comply with Basel II from the Basel Committee on Banking Supervision. A number of recent consultancy-firm driven surveys such as E&Y Global Information Security Survey or Deloitte Global Security Survey also highlighted the prevailing impact of regulations. When asking about the initiatives for security, firms in both studies rank “regulatory compliance” as the top one initiative. In particular, the respondents in Deloitte Global Survey were all global financial institutions including banking, insurance and securities brokerage houses.

Differing from coercive force, mimetic isomorphism represents the imitation of one organisation perceived by others as successful or legitimate in an organisational field. Institutional mimicry is more likely to occur for the competitive reasons or as a strategy to address uncertainty and ambiguity (DiMaggio et al. 1983; Guler et al. 2002; Tingling et al. 2002). In the context of the financial sector, Ang and Cumming (1997) point out that in the hypercompetitive environment, “peer banks exert considerable influence on each other because of tight professional networks formalised by memberships in regional and national bank association” (p.237). Peer influence on the adoption of ISO 17799 was seen in the example of the International Information Integrity Institute, where major financial institutions are members of, to include this international standard as part of materials for their members to use in risk management(Backhouse et al. 2006). In addition, to address the uncertainty and unpredictability associated with physical and cyber security threats, the financial sector in the U.S. has established the Financial Services Information Sharing and Analysis Centre in 1999. Having able to access the same information on the emerging security risks, financial organisations are experiencing “learning mimicry” (Guler et al. 2002) by adopting similar risk management strategies in the light of shared information on security threats.

From the institutional perspective, we have demonstrated that financial institutions are facing conformity pressures from regulatory bodies or from other peer organisations in the same sector. Nevertheless, due to other organisational or economic factors, firms can formulate different strategic decisions in response to external legitimacy pressures (Ang et al. 1997; Oliver 1991; Perrow 1985). Among research on administrative innovations, a number of researchers have identified various organisational contingencies that influence the adoption of ISO 9000 standard despite of institutional pressure (Beck et al. 2005; Shannon et al. 1999; Westphal et al. 1997).

Building on this line of reasoning, we argue that while acknowledging the institutional effects, financial institutions might exhibit different rate of ISO 17799 adoption and assimilation resulting from the influences of other economic or organisational contingencies. In other words, given the hypercompetitive environment of the financial services sector, economics driven factors play an important role in influencing firms' adoption decision while internal organisational capability have stronger relevance during the assimilation stage.

Moderators of Institutional Conformity on ISO 17799 Adoption and Assimilation

As mentioned above, our main theoretical assumption starts with how institutional isomorphism places conformity pressure on financial institutions during the diffusion process. In our view, the diffusion of ISO 17799 comprises two stages: adoption and assimilation. This separation of innovation stages is not a new concept in organisational or IS literature. For instance, Zmud (1982) and Damanpour (1991) have applied this approach to examine the organisational adoption on innovations. Zaltman *et al.* (1972) suggest that the process of innovations and organisational changes involves:

> *"at the outset, it is useful to subdivide the innovation process. From the point of view of the individual adoption unit, the two resulting stages can be termed "initiation" and "implementation." (p.58)*

They explained that the determinant distinguishing the initiation and implementation stage rests on the point when the power holders in an organisation legitimate the introduction of new products or practices. Zmud (1982) shared similar assumptions and considered that adoption as "represented by an organisational mandate for change," while implementations refers to such an innovation "becomes ingrained within organisation behaviours" (p.1422). For purpose of this research, although we align our assumptions on the distinction of stages in innovation phases, we consider that the terms of adoption and assimilation are more appropriate. In particular, we replace the phrase implementation with assimilation, which is defined as "the extent to which an innovation diffuses across the organisational work activities and processes, and becomes routinised and embedded in these activities" (Cooper et al. 1990). Given the nature of administrative innovations described earlier, we argue that assimilation is a better conceptual construct for examining and understanding the process of and conditions for this particular type of innovation.

Furthermore, in this research, we propose that the relationship between the institutional forces and receptiveness of an organisation to ISO 17799 is moderated by economics-based considerations for adoption decision and by organisational characteristics during the assimilation of IS security management practices in the organisation, as shown in Figure 1. A number of researchers have demonstrated importance of other decision-making criteria interacting with the institutional conformity force (Ang et al. 1997; Shannon et al. 1999; Westphal et al. 1997). Nevertheless, there is no integrative framework available so far to depict how organisations make adoption and assimilation decision in the light of institutional pressure. The next sections elaborate upon our research model and present the rationale for the development of each moderating consideration that influences ISO 17799 adoption and assimilation.

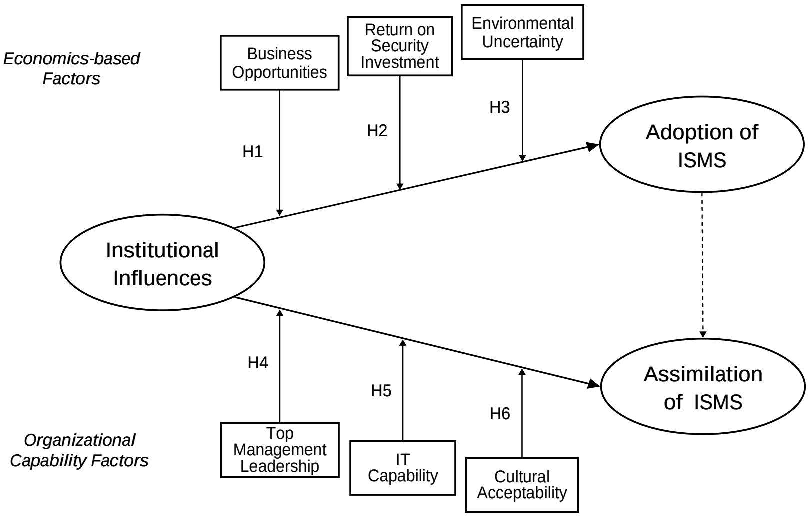

Figure 1: Research Model

Economics-Based Considerations for ISO 17799 Adoption

As defined, adoption decision is made when the power holders in the organisation mandate for change. In the context of ISO 17799 adoption, we propose that financial institutions' perception on gaining new business opportunities, achieving good return on security investment, and high environmental uncertainty will strengthen the relationship between the institutional pressures and ISO 17799 adoption.

Perceived Gain in Achieving Business Opportunities: In a hypercompetitive and globalised business environment, organisations and market participants increasingly find the need to deploy signaling strategies to potential customers and business partners in attempt to differentiate their products and services from those of lower quality. In this economics literature, this has been understood as the "Lemons problem" where the market is experiencing the problems of information asymmetry. Among the counteracting mechanisms ameliorating information gap and quality uncertainty in the market, there is a growing practice of developing certification schemes in conjunction with a set of recognised standards such as ISO 9000 and ISO 4000. Anderson *et al.* (1999) and Terlaak *et al.* (2006) conclude that complying with ISO 19000 can generate greater product volume or yield a higher price premium. In the IS literature, researchers have also argued for the importance of a third-party certification in establishing and maintain transaction trust in the Internet shopping context (Lee et al. 2001; Tan et al. 2000). The increase in transaction trust can lead to new business opportunities. Therefore, we hypothesise that when the organisation perceive an increase in business opportunities, we expect financial institutions to confirm more keenly to institutional influences on IS security management adoption.

H1: The greater the business opportunities perceived by the organisation, the stronger the relationship between institutional influence and ISMS adoption

Perceived Value in Justifying Return on Information Security Investment (ROSI): In an organisation's decision-making process for innovation adoption, the evaluation of return on investment plays a significant role in justifying the cost and predicting the benefits (Bacon 1992; Chatterjee et al. 2002). In contrast to the common view on the return on investment, ROSI is understood through the view of preventing the potential loss from information security breaches (Gordon et al. 2006a; Gordon et al. 2002). However, determining effective measurements for ROSI have been difficult and sometimes can be misleading. Gordon and Loeb (2002a) advocate the economic notion of the internal rate of return (IRR) instead of standard ROI because the former measures asset value based on “future (ex ante) risk-adjusted discounted cash flows” while the latter considers “historical (ex post) accrual and non-discounted concepts” (p.28). The annual CSI/FBI computer crime and security survey also show that management’s doubts in using ROI or IRR to quantify the cost and benefit aspects of computer security investment (Gordon et al. 2006b). However, contrasting to quantitative approach, Straub and Welke (1998) argue that the increasing awareness of security standards and controls can help managers to achieve effective decision-making in risk planning and security management. Therefore, we hypothesise that the higher perceived value of ISMS adoption in justifying return on information security investment, we expect firms to conform to external pressures to adopt IS security management.

H2: The greater the perceived value in justifying return on security investment, the stronger the relationship between institutional influence and ISMS adoption

Perceived Environmental Uncertainty: Other than pursuing production efficiency, organisations also face the challenge of legitimating its actions in its immediate institutional environment (DiMaggio et al. 1991; Scott 1995). When decision-makers fail to acknowledge or misinterpret the sources and potential consequences of environmental uncertainties, the impact can be a serious decline in organisation performance or damage in organisational legitimacy in the institutional environment (Elenkov 1995). One strategic response to the environmental volatility is through the practice of interorganisational imitation (Haunschild et al. 1997). In the context of information security management, environmental uncertainty refers to the unpredictability of major trends or risks in the business environment, or the difficulties in determining the likelihood and impact of different security risks threatening the survival of the organisation. The globalisation and increasing complexities of technology-enabled services means that the financial institutions are confronting with challenges of maintaining legitimacy and economic performance (Ang et al. 1997). With such a high degree of environment uncertainty, information security managers are turning their attention in searching for appropriate risk management methodology to assist their decision-making process (Baskervile 1991; Rainer et al 1991). Therefore, we hypothesise that when organisations perceive greater environmental uncertainty, we expect firms to conform to external pressures to adopt IS security management.

H3: The greater the environmental uncertainty perceived by the organisation, the stronger the relationship between institutional influence and ISMS adoption

Organisational Considerations for ISO 17799 Assimilation

When the power holders in the organisation make a decision to initiate or adopt a certain organisational practice, the next important question in the innovation diffusion phase is that to what extent the adopting organisational practices are accepted by internal organisational members and become institutionalised. In this study, we define this as the stage of assimilation, and the following section describes organisational characteristics interacting with the institutional forces during the assimilation stage of ISO 17799.

Top Management Leadership: It is believed to be a critical characteristic for every successful innovation implementation (Gallivan et al., 1994; Zmud, 1982). The revolutionary pace or the enterprise-wide scope adds to the importance of the positive top management commitment because organisation-wide resource allocation is demanded and inhibitors such as employee resistance should be removed (Damanpour, 1991). Bantel (1989) shows the significance of top management team in relation to innovation decision in the banking sector. The role of top management has been found to be much more important in the implementation stage than the adoption process (Liang et al., 2007). That is, continuous top management support would be required for the innovation implementation, resulting in the revolutionary and enterprise-wide organisational change. Thus, the strong participation of top management results in efficient innovation processes and activities intended to assimilate them (Ba et al., 2001). Studies in the area of IS security also demonstrates that top management support has a positive impact on increasing security effectiveness (e.g., Kankanhallie et al., 2003). Therefore, stronger top management leadership leads to a higher degree of innovation assimilation of IS security management within the organisation.

H4: The greater the top management leadership, the stronger the relationship between institutional influence and ISMS assimilation

IT Capability: An organisation manages its innovations through an IT infrastructure, which is a framework connecting different members of the organisation with different internal and external knowledge and processes (Tippings et al. 2003). It is a support system, consisting of knowledge and guidelines (technical as well as non-technical) about how innovation knowledge is developed and transferred in order to meet the organisation objective in an efficient manner. The usefulness and roles of IT in diffusion of innovations have been widely discussed (Borghoff et al. 1998; Teece et al. 1997). For example, Gill (1995) emphasizes using IT to support organisational learning because modern IT can best support the amount and richness of bi-directional information flow, multi-channel communication, and performing tasks that cannot be performed manually. Accordingly, it is widely accepted that IT capability, which is defined as "an ability to mobilize and deploy IT-based resources in combination or co-present with other resources" (Bharadwaj 2000), can help an organisation to connect not only people to people, but also people to innovation activities such as IS security management (Junarkar 1997). This can eliminate communication barriers between different parts of an organisation in the process of technological innovation (Teece 1986). Therefore, we hypothesise that when IT capability is high, we expect firms to conform to external pressures to assimilate IS security management.

H5: The greater the IT capability, the stronger the relationship between institutional influence and ISMS assimilation

Cultural Acceptability: Since an innovation in organisation is as much a social activity as a managerial and/or technical activity, cultural change is a prerequisite for its successful implementation (Ettlie 1983; Klein 1998; Miller et al. 1980). The organisational culture involves the shared meanings, norms and values that have been collectively constructed over the years. The creation and change of an organisational culture usually take a long time and are context- or climate-dependent (Schein 1985). Leonard-Barton (1988) argues that the successful use of an innovation depends on the degree of the mutual adaptation of the innovation and the organisational context into which the innovation is being introduced. Furthermore, since innovations result in the adaptation of the existing organisational and industrial arrangements and the transformation of the existing structure and practice in the given environment, innovation activities should be managed by a holistic vision, which allow idea to be transformed into actual and concrete reality (Leonard-Barton 1988; Van De Ven 1986). According to the learning organisation literature, typical characteristics of the organisational culture include leadership, learning orientation, commitment, trust-based communication and collaboration, openness, and voluntary participation (Davenport et al. 1998; O'Dell et al. 1998). Accordingly, if a supportive organisational culture for IS security management does not exist, there will be no motivation for organisation members to engage in unfamiliar social activities. Specifically, we expect the relationship between institutional influence and the assimilation of IS security management to be higher when cultural acceptability of innovation is high.

H6: The higher the cultural acceptability of innovation, the stronger the relationship between institutional influence and ISMS assimilation

Research Method

In order to test the proposed model and its hypotheses, a field survey method was adopted. The unit of analysis was the organisation implementing or having already implemented enterprise-wide IS security initiatives in the financial services sector. Survey instruments were designed to measure one independent (i.e., institutional influence), two dependent (i.e., adoption and assimilation of ISMS), and six moderating variables. Based on the previous literature on institutional theories and adoption and assimilation of innovation especially from economics and organisational capability viewpoints, we developed a questionnaire to empirically test the proposed hypotheses.

Most of the measures were based on previously validated instruments, while others were developed based on conceptual definitions and theoretical statements made in the existing literature. For example, institutional influences were measured in terms of three major pressures including mimetic (Teo et al. 2003), coercive (Liang et al. 2007; Tingling et al. 2002), and normative pressures (Ang et al. 1997; Teo et al. 2003). Regarding two dependent variables, measures of ISMS adoption was developed by applying Azjen and Fishein (1980)’s definition to the context of IS security while its assimilation was measured by the best-know six-stage model of the assimilation of technology innovation in organisations developed by Cooper and Zmud (1990). In addition, for all variables, perceptual measures were employed. Each variable was measured based on a seven-point Likert scale from ‘strongly disagree’ to ‘strongly agree’. Also, multiple-item measures were used for all variables to improve the reliability and validity of the measures (Churchill 1979).

To account for extraneous sources of variation in the adoption and assimilation of ISMS, we incorporated *organisation size* and *time length after ISMS was introduced* as control variables in our models. We controlled for organisation size that was measured by total sales volume. Also, since the experiences of ISMS may have some influences on the degree of its adoption and assimilation, we decided to control the time length after ISMS was introduced to an organisation to eliminate the potential spurious effect of time. Using the process of conceptual construct validation (Moore et al. 1991), an initial version of the survey instrument was subsequently refined through an extensive pre-test with several academics who have significant expertise in the study of IS security. The instrument was further tested with a sample of companies in the UK.

This study is currently in the stage of data gathering. We contacted financial association in the UK and selected 100 financial organisations under the supervision of the UK Financial Service Authority as convenient samples, which already have enterprise-wide ISMS. Questionnaires were mailed to CIOs in the selected organisations with personalized cover letters accompanying an explanation of the study and assurance of confidentiality of collected data. To increase the response rate, we adopted the Total Design Method proposed by Dillman (1991).

To test our hypotheses, we plan to use *hierarchical moderated logistic regression models*. This approach allows us to form multiplicative terms as moderating variables and to use a series of logistics regression analysis in order to test the relative contribution of the moderator terms to the explanation of the variance in dependent variables (Ang et al. 1997), which is appropriate for the purpose of this study in testing the effects of moderating variables on the base relationship between institutional influence and the adoption and assimilation of ISMS. Before testing hypotheses, the basic procedures to test validity and reliability of measures such as factor analysis, inter-item reliability analysis should be done.

Expected Contributions and Concluding Remarks

As a response to the recent emphasis on the technology vulnerabilities in the organisational field, we identify the ISO 17799 as an administrative innovation that the decision-makers in the financial sector can adopt to ameliorate the information security risks. Furthermore, drawing from the institutional perspective, we demonstrate that institutional rules and norms place conformity pressure on financial institutions for ISO 17799 adoption and assimilation, and how economics-based factors and internal organisational capabilities impact on the relationship between institutional influences and the adoption/assimilation of IS security management. We argue that this research contributes to not only the literature of institutional theories but also the area of IS security management. Our integrative framework provides a better understanding for practitioners about the diffusion process of administrative innovations, and it also can be used as an analytic tool in investigating organisational strategic behaviours at different stage of innovation diffusion in the light of institutional conformity influences. In addition, our framework contributes the “still at a theory-building stage” of social-organisational perspective in IS security research (Dhillon et al. 2001).

Publication

1. Hsu, C. “Making Sense of Institutionalising Information Systems Security Management in Organisations” submitted to 2007 *The International Conference on Information Systems*
2. Hsu, C., J.Y. Lee. “Conformity Only? Expediting the Institutional Process on the Adoption and Assimilation of An Administrative Innovation” submitted to 2007 *The International Conference on Information Systems*

References

Ang, S., and Cummings, L. "Strategic Response to Institutional Influences on Information Systems Outsourcing," *Organisation Science* (8:3) 1997, pp 235-256.

Backhouse, J., Hsu, C., and Silva, L. "Circuits of Power in Creating De Jure Standards: Shaping an International Information Systems Security Standard," *MIS Quarterly* (30:Special issue) 2006, pp 413-438.

Bacon, C.J. "The Use of Decision Criteria in Selecting Information Systems/Technology Investments," *MIS Quarterly* (16:3) 1992, pp 335-353.

Beck, N., and Walgenbach, P. "Technical Efficiency or Adaptation to Institutionalised Expectations? The Adoption of ISO 9000 Standards in the German Mechanical Engineering Industry," *Organisation Studies* (26:6) 2005, pp 841-866.

Bharadwaj, A. "A Resource-based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation," *MIS Quarterly* (24:1) 2000, pp 169-196.

Borghoff, U.M., and Parenschi, R. *Information Technology for Knowledge Management* Springer, New York, 1998.

Chatterjee, D., Grewal, R., and Sambamurthy, V. "Shaping Up For E-Commerce:Institutional Enables of The Organisational Assimilation Web Technologies," *MIS Quarterly* (26:2) 2002, pp 65-89.

Churchill, G. "A Paradigm for Developing Better Measures of Marketing Constructs," *Journal of Marketing* (16:1) 1979, pp 64-73.

Cooper, R.B., and Zmud, R. "Information Technology Implementation Research: A Technological Diffusion Approach," *Management Science* (36:2) 1990, pp 123-139.

Davenport, T.H., and Prusak, L. *Working Knowledge* Harvard Business School Press, Boston, 1998.

Deloitte, T.T. "The Global Security Survey," p. 42.

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

DiMaggio, P.J., and Powell, W.W. "The Iron Cage Resivited: Institutional Isomorphism and Collective Rationality in Organisational Fields," *American Sociological Review* (48:2) 1983, pp 147-160.

DiMaggio, P.J., and Powell, W.W. "The Iron Cage Resivited: Institutional Isomorphism and Collective Rationality in Organisational Fields," in: *The New Institutionalism in Organiational Analysis*, P.J. DiMaggio and W.W. Powell (eds.), The University of Chicago Press, London, 1991, pp. 63-82.

Elenkov, D. "Strategic Uncertainty and Environmental Scanning: The Case for Institutional Influences on Scanning Behaviour," *Strategic Management Journal* (18:4) 1995, pp 287-302.

Ettlie, J.E. "Performance Gap Theories of Innovation " *IEEE Transactions on Engineering Management* (30:2) 1983, pp 39-52.

Galaskiewicz, J., and Burt, R.S. "Mimetic Processes within an Interorganisational Fiedl: An Empirical Test," *Administrative Science Quarterly* (34) 1989, pp 454-479.

Gordon, L., and Leob, M. "Budgeting Process for Information Security Expenditures," *Communications of the ACM* (49:1) 2006a, pp 121-125.

Gordon, L., and Loeb, M. "The Economics of Information Security Investment," *ACM*

Transactions on Information System Security (5:4) 2002, pp 438-457.

Gordon, L., Loeb, M., Lucyshyn, W., and Richardson, R. *2006 CSI/FBI Computer Crime and Security Survey* Computer Security Instiute, 2006b, p. 29.

Guler, I., Guillen, M., and Macpherson, J. "Global Competition Institutions, and the Diffusion of Organsational Practices: The International Spread of ISO 9000 Quality Certificates," *Administrative Science Quarterly* (47:2) 2002, pp 207-223.

Haunschild, P., and Minner, A. "Modes of Interorganisational Imitation: The Effects of Outcome Salience and Uncertainty," *Administrative Science Quarterly* (42:3) 1997, pp 472-500.

Iacono, C., Benbasat, I., and Dexter, A. "Electronic Data Interchange and Small Organisations: Adoption and Impact of Technology," *MIS Quarterly* (19:4) 1995, pp 465-485.

Junarkar, B. "Leveraging Collective Intellect by Building Organisational Capabilities," *Expert Systems With Applications* (13:1) 1997, pp 29-40.

Klein, D.A. "The Strategic Management of Intellectual Capital: An Introduction," in: *The Strategic Management of Intellectual Capital,* D.A. Klein (ed.), Butterworth Heinenmann, Boston, 1998, pp. 1-9.

Lee, M., and Turban, E. "A Trust Model for Consummer Internet Shopping," *International Journal of Electronic Commerce* (6:1) 2001, pp 75-91.

Leonard-Barton, D. "Implementation as Mutual Adaptation of Technology and Organisation," *Research Policy* (17) 1988, pp 251-267.

Liang, H., Saraf, N., Hu, Q., and Xue, Y. "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management," *MIS Quarterly* (31:1) 2007, pp 59-87.

Meyer, J., and Rowan, B. "Institutioanlised Organisations: Formal Structure as Myth and Ceremony," in: *The New Institutionalism in Organisational Analysis,* P.J. DiMaggio and W.W. Powell (eds.), The University Press of Chicago, London, 1991, pp. 41-62.

Miller, G., and Friesen, P. "Momentum and Revolution in Organisation Adaptation," *Academy of Management Journal* (23) 1980, pp 591-614.

Moore, G., and Benbast, I. "Development of an Instrument to Measure the Perceptions of Adopting an Information Innvoation," *Information Systems Research* (2:3) 1991, pp 192-222.

O'Dell, C., and Grayson, C.J. *If Only We Know What WE Know* The Free Press, New York, 1998.

Oliver, C. "Strategic Response to Institutional Processes," *Academy of Management Review* (16:1) 1991, pp 145-179.

Perrow, C. "Review Essay: Overboard with Myth and Symbols," *American Journal of Sociology* (91:1) 1985, pp 51-55.

Reinganum, J. "On the Diffusion of New Technology: A Game Theoertic Approach," *The Review of Economic Studies* (48:3) 1981, pp 395-405.

Schein, E.H. *Organisational Culture and Leadership: A Dynamic View* Jossey-Bass Publishers, San Francisco, 1985.

Scott, W.R. *Institutions and Organisations* Sage Publications, London, 1995.

Shannon, W., Andersson, J., Daly, D., and Johnson, M. "Why firms seek ISO 9000 certification regulatory compliance or comeptitve advantage?," *Production and Operation Management* (8:1) 1999, pp 28-43.

Tan, Y., and Thoen, W. "Toward a Generic Model of Trust for Electronic Commerce," *International Journal of Electronic Commerce* (5:2) 2000, pp 61-74.

Teece, D.J. "The Diffusion of An Administrative Innovation," *Management Science* (26:5) 1980, pp 464-470.

Teece, D.J. "Profiting From Technological Innovation," *Research Policy* (15) 1986.

Teece, D.J., Pisano, G., and Shuen, A. "Dynamic Capabilities and Strategic Managment," *Strategic Management Journal* (18:7) 1997, pp 509-533.

Teo, H.H., Wei, K.K., and Benbasat, I. "Predicting Intention to Adopt Interorganisational Linkage: An Institutional Perspective," *MIS Quarterly* (27:1) 2003, pp 19-49.

Tingling, P., and Parent, M. "Mimetic Isomorphism & Technology Evaluation: Does Limitation Transcend Judgement?," *Journal of Associsation for Information Systems* (3:5) 2002, pp 113-143.

Tippings, M.J., and Sohi, R.S. "IT Competency and Firm Performance: Is Organisational Learning a Missing Link?," *Strategic Management Journal* (24) 2003, pp 745-761.

Van De Ven, A.H. "Central Problems in the Management of Innovation " *Management Science* (32:5) 1986, pp 590-607.

Westphal, J., Gulati, R., and Shortell, S. "Customisation or Conformity? An Institutional and Network Perspective on the Content and Consequences of TQM Adoption," *Administrative Science Quarterly* (42) 1997, pp 366-394.

出席國際學術會議心得報告

計畫編號	NSC 95-2416-H-004-058
計畫名稱	Assessment of Factors Influencing the Information Security Management Effectiveness
出國人員姓名 服務機關及職稱	許瑋元國立政治大學 資訊管理學系
會議時間地點	民國 95 年 12 月 10 日至 13 日
會議名稱	國際資訊系統會議(International Conference on Information Systems 2006)
發表論文題目	

一、參加會議經過

The purpose of attending the conference was to interact with international researchers in the field of information systems. During the conference, other than participating and networking in the conference, there was an opportunity to present working-in-progress research to other scholars working in the area of information systems security management.

二、與會心得

The opportunity of interacting and exchanging ideas with other researchers was greatly valuable in moving this research project forward. As a result, two papers were submitted to International Conference on Information Systems 2007.

1.Hsu, C. “Making Sense of Institutionalising Information Systems Security Management in Organisations” submitted to 2007 *The International Conference on Information Systems*

2.Hsu, C., J.Y. Lee. “Conformity Only? Expediting the Institutional Process on the Adoption and Assimilation of An Administrative Innovation” submitted to 2007 *The International Conference on Information Systems*