Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

Information Security Compliances and Knowledge Management Capabilities in International Diversification

Kamphol Wipawayangkool
The University of Texas at Arlington, kamphol.wipawayangkool@mavs.uta.edu

Information Security Compliances and Knowledge Management Capabilities in International Diversification

Kamphol Wipawayangkool
The University of Texas at Arlington
kamphol.wipawayangkool@mavs.uta.edu

ABSTRACT

Information security compliance has become one of the top priorities for firms to remain competitive in this era. It is even more challenging to comply with foreign standards and laws, when a firm aims to internationalize its operations and remain competitive. This paper discusses the role of information security compliances in international diversification phenomena. Specifically, drawing from the organizational information processing theory, this paper proposes that the fit between knowledge management capabilities of a firm and the requirements of information security compliances influences the degree of international diversification of the firm. Unlike much of prior academic literature focusing on American firms, this paper discusses how certain American security compliances possess challenges for foreign firms to diversify their businesses in the US. Both implications and limitations are then discussed.

Keywords

Information security, compliances, knowledge management, international diversification, information processing.

INTRODUCTION

To remain competitive in this information-sensitive era, firms need to acknowledge the importance of information security issues and act accordingly. To have better information management and control systems, firms nowadays need to comply with certain regulations and laws (Luthy and Forcht, 2006). The 10th annual Ernst & Young Global Information Security Survey (EYGISS) (2007) with nearly 1300 firms from industries such as financial services, manufacturing, technology, and health services showed that compliance and regulations (64%) was the driver most significantly affecting security management of the firms. Similarly, the 2007 Deloitte Global Security Survey (DGSS) with respondents from 169 major global financial institutions reported that security regulation and compliance (49%) was one of the top three priorities. These two surveys unanimously show that practitioners worldwide realize the significance of information security compliances.

To become internationally competitive as it is a common goal for most modern firms, firms first must be able to enter foreign markets; as a result, certain security compliances of host countries are required (Gerber and von Solms, 2008; Luthy and Forcht, 2006). Firms face challenges in being accustomed to foreign security regulations and laws and learning how to manage them. Specifically, such diversifying firms need to know how to acquire and utilize necessary knowledge in order to tackle the requirements of those standards. Thus, depending on firms' knowledge management capabilities, information security compliance can be considered a barrier to the extent of international diversification of the firms.

This paper overall aims to discuss the role of information security compliances in international diversification phenomena. Specifically, drawing from the organizational information processing theory, this paper proposes that the fit between knowledge management capabilities particularly in technology and marketing of a firm and the requirements of the compliances influences the degree of international diversification of the firm. As Hitt et al. (2006) recommended in their intensive literature review that researchers should pay more attention to the role of institutional environments and as the inclusion of information security in international business literature is rather lacking, this paper contributes to literature by providing a theoretical foundation merging both information security and international business phenomena for future researchers to explore further this research stream. In addition, unlike much academic literature focusing on US-based firms, this paper discusses how American security compliances possess challenges for foreign firms to diversify their businesses in the US.

This paper is organized as follows. First, literature background on information security compliances, international diversification, and knowledge management capability are discussed. Second, the organizational information processing theory is discussed to provide a theoretical foundation to merge the two phenomena into one phenomenon: information security compliances in international diversification – particularly, the role of the fit between the information security compliances and knowledge management capabilities in international diversification. Then, research model and propositions are presented along with brief discussion of certain American regulations and laws. Finally, both theoretical and practical implications as well as limitations of this paper are discussed.

LITERATURE BACKGROUND AND RESEARCH MODEL DEVELOPMENT

Information Security Compliance

The principles of information security management are to ensure privacy of information (confidentiality), to ensure authorized operations on information (integrity), and to ensure availability of functional systems (availability) (Dhillon, 2007). Both technical and non-technical aspects exist in information security management. Technical aspects include computer software and hardware control concepts such as encryption and network security (Dhillon, 2007). Non-technical aspects cover topics such as management and regulatory compliance. Managerial aspects essentially include risk management, corporate governance, and culture management (Dhillon, 2007; Nosworthy, 2000; von Solms, 2000, 2001, 2006).

Information security compliances refer to compliances with laws and regulations pertinent to information security issues. Certain laws and regulations may not directly address the implications of information security, but given the pervasiveness of information technology in business today, they are certainly involved with information security (Luthy and Forcht, 2006). For example, although developed for financial sector, the Sarbanes-Oxley Act (SOX) has implications for information security issues since virtually all financial activities are typically handled by computer systems (Luthy and Forcht, 2006; Schultz, 2004). International security standards such as ISO/IEC 27001 and 27002 (previously ISO/IEC 17799) become more relevant to many organizations as they operate abroad. The ISO/IEC 27001 and 27002 explicitly include controls in security policy, organizing information security, asset management, human resources security, physical and environmental security, communication and operations management, access control, information systems acquisition, development, and maintenance, incident management, business continuity management, and compliance (Humphreys, 2008). Other well-known compliances include the Computer Fraud and Abuse Act, Computer Security Act, USA Patriot Act, and Federal Information Security Management Act; this latter set of compliances affects federal-related agencies including the government units (Dhillon, 2007). Since this paper intends to emphasize the role of information security compliances in foreign firms' international diversification, only certain compliances applicable to foreign firms planning to diversify their operations in the US are discussed in the research model development section. In addition, in order to point out the omnipresence of information security issues, this paper presents the discussion of those compliances in not single but several industries, namely financial, healthcare, and marketing sectors.

International Diversification

International diversification is defined as a strategy through which a firm expands its business into different geographic locations or markets (Hitt et al., 2006). Similar terms such as internationalization and multinationality also refer to the concept of international diversification. Firms diversify internationally because of such reasons as to gain competitive advantage (Hitt et al., 2006), to increase returns of investment (Hymer, 1976), and to compensate the inefficiencies of doing business in the current market (Hennart, 1982). It can be simply stated that firms internationalize through different strategies in order to improve firms' ultimate performance. Hitt et al. (2006) provided an intensive review on the antecedents, outcomes, and moderators in international diversification phenomena. A brief discussion is provided as follows. The antecedents include top management team characteristics (Herrmann and Datta, 2005), firm structure (Sanders and Carpenter, 1998), and processes and resources (Tseng et al., 2007). The international diversification may be measured in terms of scale and scope. The ultimate performance outcome may be measured in terms of accounting, market share, and growth. Relevant to this paper is the discussion of the moderators that include environmental factors such as host country resources, institutional environment, and industry competitive environment. For example, Calof and Beamish (1995) found that regulation influences the mode of international diversification. Nonetheless, finding that the current evidence of the relationship between host country regulations and international diversification is mixed, Hitt et al. (2006, p. 859) suggested that future researchers should explore further on the role of institutional environments.

Firms face a number of difficulties when diversifying their operations internationally. Drawing from the resource-based theory, Cuervo-Cazurra et al. (2007) categorized three sets of the difficulties as: resources losing their advantages when they are transferred abroad, resources creating disadvantages when they are transferred abroad, and complementary resources required to operate in the new country are lacking. Although all those difficulties might be applicable, but given that the objective of this paper is to emphasize the role of host-country compliances, the lack of complementary resources seems to be the most relevant to the challenges imposed by foreignness of those regulations and laws. Indeed, Cuervo-Cazurra et al.

(2007) categorized further that the lack of complementary resources includes liability of foreignness which is caused by institutional environment factors of the new country. Firms need to develop or gain complementary resources to ease such difficulty. Prior literature shows that knowledge-based resources particularly technological and marketing knowledge are significantly associated with the degree of international diversification of a firm (Tseng et al., 2007). Thus, it is reasonable to infer that aiming to internationalize, a firm needs to know how to possess necessary knowledge especially in technology and marketing in order to use it to solve the issue of the lack of complementary resources to become complied with certain regulations and laws. Indeed, Chari et al. (2007) found that greater investment in technology promotes capability in coordinating and processing information, and that such promotion increases the scope of internal diversification and ultimately improves firm performance. Consequently, it can be deduced further that diversifying firms need not only complementary knowledge but also effective knowledge management practices such as coordination and processing in both technology and marketing areas.

Knowledge Management Capability

The discussion above results in a conclusion that both complementary knowledge resources and knowledge management processes are crucial in meeting the requirements of certain compliances and subsequently in determining the extent of internal diversification of a firm. First, based on the theory of complementarities, complementary knowledge refers to a set of knowledge that produces greater returns than the sum of their individual return (super-additive) (Tanriverdi, 2005). In this case in order to internationalize, firms need to develop or acquire complementary knowledge relevant to help comply with certain foreign regulations and laws. According to such a definition, a set of complementary knowledge is likely to enable the firms not only to establish compliances but also benefits other aspects of the firms' performance. However, possessing complementary knowledge does not warrant the success of being complied and internationalized.

Second, effective knowledge management capabilities pertinent to different sets of complementary knowledge are required. Knowledge management capability is a firm's capability to create, transfer, integrate, and utilize related and necessary knowledge in a domain to benefit the firm's desired performance (adapted from Tanriverdi, 2005). Indeed, Tanriverdi (2005) essentially found that knowledge management capability mediates the relationship between the use of common technology and management across business units and firm performance. As mentioned previously that technological and marketing knowledge are significant predictors of the extent of internal diversification, it is deducible that firms need to know how to effectively create, transfer, integrate, and utilize complementary knowledge in both areas. Nevertheless, since Tseng et al. (2007) found that the relationship between marketing knowledge-based resources and the extent of internationalization is an inverted U-shaped, indicating that excessive use of marketing resources may trigger adverse responses from the host country and that an optimal level exists in the relationship. An explanation is that marketing concepts tend to be more sensitive to people's preferences than the effects of technology especially when the host country is greatly different. Thus, technological knowledge management capability may directly increase the extent of international diversification of a firm more than marketing knowledge management capability. Figure 1 depicts the concept of knowledge management capability in technological and marketing areas.

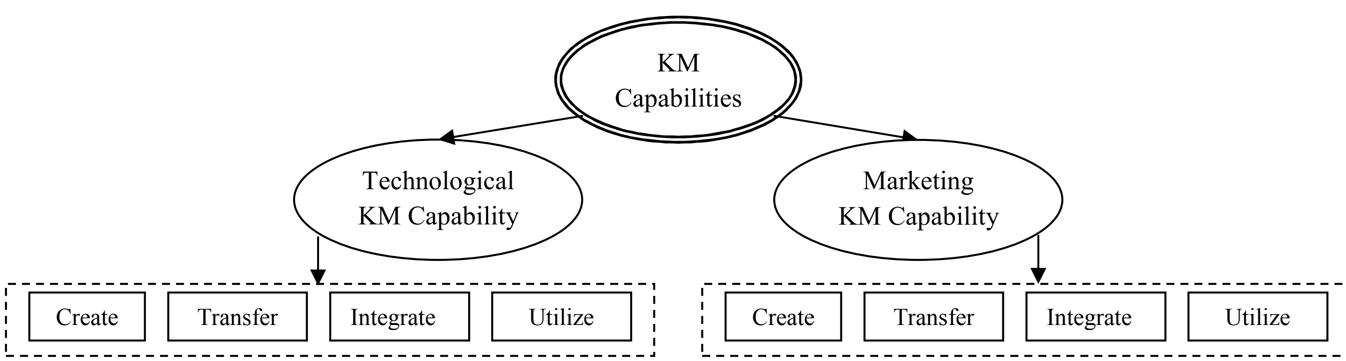

Figure 1. Knowledge Management Capabilities

Organizational Information Processing Theory

The principle of the organizational information processing theory is that firms can obtain their optimal performance in a domain through strategies that either reduce the need for information processing or increase the capacity to process information or both (Galbraith, 1974). Central to the theory are information processing needs, information processing capability, and the fit between information processing needs and capability. In short, through such a fit, a firm can achieve its optimal performance. Figure 2 illustrates the essences of the theory.

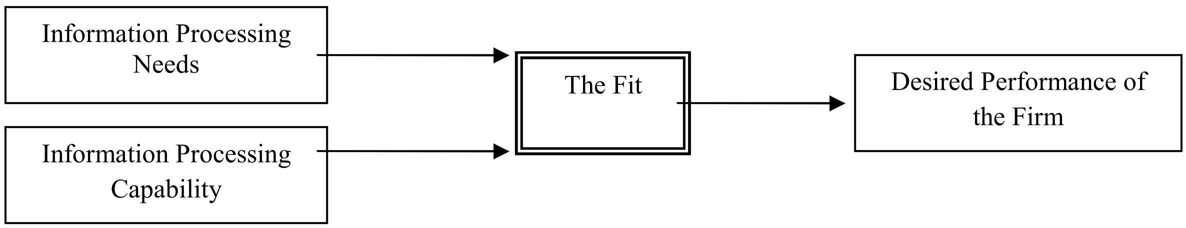

Figure 2. The Framework of the Organizational Information Processing Theory

Based on such a framework, this paper conceptualizes the degree of international diversification as the desired performance, information security compliances as information processing needs, and knowledge management capabilities as information processing capabilities. In other words, the firm needs to know how to create and apply necessary knowledge in order to comply with certain regulations and laws – and particularly through the fit, the firm will be able to achieve the optimal extent of its international diversification.

The Fit between Information Security Compliances and Knowledge Management Capabilities

Based on the organizational information processing theory and all the discussion above, this paper posits that the fit between knowledge management capabilities of a firm and the requirements of foreign compliances influences the extent to which the firm can diversify its business abroad. Discussed in this section are specific American regulations and laws foreign firms face when internationalizing their businesses in the US. To be consistent with prior literature emphasizing the role of technological and marketing knowledge, the following regulations and laws are combined based on their implications into either technology-related or marketing-related compliances.

Technology-related Compliances

First, triggered by scandalous and outrageous cases such as Enron, the Sarbanes-Oxley Act (SOX) requires publicly traded companies to establish an accurate and reliable internal control structure for financial reporting activities that are typically handled by computer systems (Luthy and Forcht, 2006; Schultz, 2004). In short, this law is designed to strengthen the integrity of corporate financial practices. The SOX applies to not only US domestic publicly traded firms, non-public firms whose debt instruments are publicly traded, but importantly foreign companies that are registered to operate business in the US regardless of their physical locations (Dhillon, 2007; Luthy and Forcht, 2006). For example, Pacific Internet, which is a Singapore-based Internet service provider yet is Nasdaq-listed, also had to comply with SOX (Yeo, 2006).

Although SOX is not designed to tackle information security directly, information technology is under great pressure to complete its requirements (e.g. data authentication, encryption, and storage recoverability). It is known that complying with SOX is costly especially for small and medium size firms. Indeed, Piotroski and Srinivasan (2008) found that SOX does not influence the decision of large foreign firms to register their business in the US, but influences small foreign firms by decreasing the likelihood of their registrations. Incidentally, Haworth and Pietron, (2006) suggested that firms that implemented ISO 17799 are more ready to comply with SOX.

Second, as the first American regulation on medical privacy and the most intensive federal legislation involving health information management and systems affecting the store, use, release, and transmission of private medical data, the Health Insurance Portability and Accountability Act (HIPAA), requires firms, regardless of its size and practices (e.g. healthcare providers, insurance companies, physician practice, and consulting firms), to implement security strategies (e.g. reviewing information systems activities and risk management) for personal history information (Dhillon, 2007). Firms that fail to comply with the HIPAA could be subjected to heavy fines and potential lawsuits.

Marketing-related Compliances

Many of the most significant privacy rules focus on marketing practices through defining appropriate restrictions and explaining the degree to which those practices can be (Nahra, 2006). The Do-Not-Call and CAN-SPAM are two of renowned and aggressive marketing rules issued by the Federal Trade Commission (FTC) and Federal Communication Commission (FCC) (Nahra, 2006). As many firms nowadays outsource telemarketing and Internet-marketing activities, the firm must be cautious in selecting marketing partners and be sure that they strictly adhere to the requirements of the rules. For example, the FTC charged DirecTV in December 2005 for its affiliates' violations of the Do-Not-Call restriction with the $5.3 million penalty fees, the largest violation yet (Hughes, 2007). In other words, the firm needs to know how to acquire the complementary knowledge, for example through marketing partners, and ensure that it can be appropriately and effectively utilized.

Based on all the literature background and discussion above, the propositions and research model are developed as follows.

Proposition 1a: The fit between technology-related information security compliances (e.g. SOX and HIPAA) and technological knowledge management capability of a firm significantly influences the extent of international diversification of the firm.

Proposition 1b: The fit between marketing-related information security compliances (e.g. CAN-SPAM and Do-Not-Call) and marketing knowledge management capability of a firm significantly influences the extent of international diversification of the firm.

Proposition 2: Due to different levels of the salience of sensitivity affecting people in the host country of knowledge, the fit between technology-related information security compliances and technological knowledge management capability of a firm directly increases the extent of international diversification of the firm more significantly than the fit between marketing-related information security compliances and marketing knowledge management capability of the firm does.

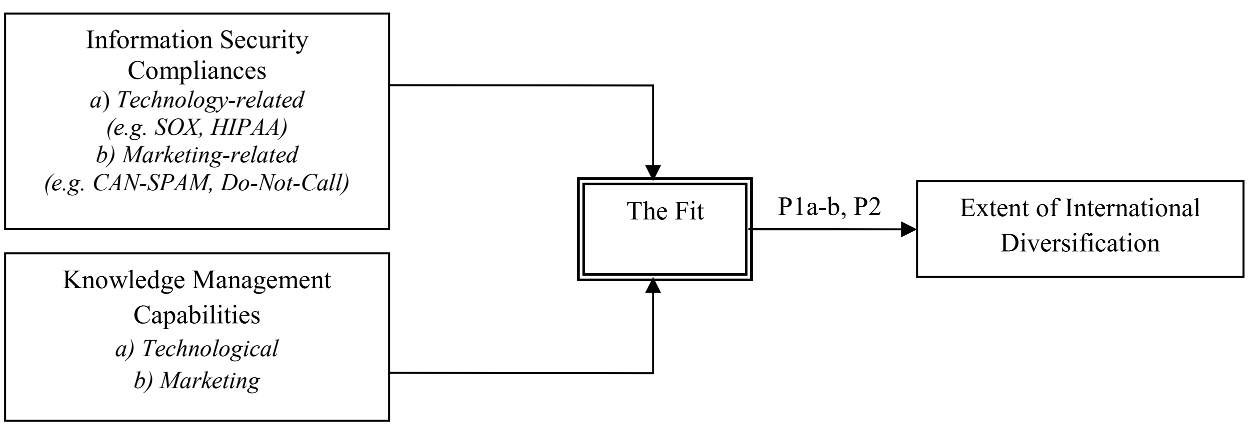

Figure 3. Research Model

IMPLICATIONS AND LIMITATIONS

To research, this paper provides a theoretical framework based on the organizational information processing theory for future researchers to investigate the role of information security compliances and knowledge management capabilities in international diversification phenomena. To the best of the author's knowledge, the interdisciplinary nature of the framework among the three constructs has not been much explored in prior literature; thus, this paper contributes to the body of knowledge of all the three areas. To information security literature, regulatory and compliance aspects, compared to other aspects especially technical, are still relatively immature and need more attention. As recent interests in knowledge management are in security issues, this paper clearly provides another direction for future studies in this area. To international business, as pointed out, this paper fills in the recommendation for considering regulatory factors in international diversification. To practitioners, managers should first examine the availability of knowledge and the effectiveness of knowledge management of the firms before making a decision to diversify business internationally. If a company possesses the fit between its knowledge management capabilities and the requirements of foreign information security compliances, as required in a new country, then the extent of international diversification can be optimal.

Regarding limitations, although this paper may succeed in pointing out the important role of information security compliances, the number of regulations and laws discussed here is rather limited. Second, this paper primarily draws from the organizational information processing theory as its key notion of the fit between the information processing needs and capabilities evidently corresponds to the fundamental theme of this paper; nonetheless, other theories such as Barney (1991)'s resource-based view of the firm could also be integrated in future works to provide stronger justification as it includes more types of resources such as physical capital resources (e.g. technology infrastructure), human capital resources (e.g. intelligence, experience, and relationships), and organizational capital resources (e.g. firm structure and management systems). Firms' sustainable competitive advantage may in fact be conceptualized as produced by a combination of those. Furthermore, empirical work is needed to examine the propositions and may appear to be practically difficult to gather data related to corporate security compliances. Nonetheless, assessing the fit in qualitative study (e.g. interviews provided confidentiality) arguably may be relatively less difficult than measuring the fit in quantitative study as corporate responses in this area is virtually impossible to collect.

CONCLUSION

Information security compliances have become one of the top priorities for firms to remain competitive in this information-sensitive era. To internationalize and remain competitive, firms first face challenges in complying with foreign regulations and laws. By drawing from the organizational information processing theory, this paper discusses the role of information security compliances in international diversification. Specifically, this paper posits that the fit between knowledge management capabilities of a firm and the requirements of foreign information security compliances influences the extent of international diversification of the firm. This paper contributes to information security, knowledge management, and international business literature by providing a theoretical framework and propositions for researchers to investigate further this interdisciplinary research stream.

REFERENCES

1. Barney, J. (1991) Firm resources and sustained competitive advantage, *Journal of Management*, 17, 1, 99-120.
2. Calof, J.L. and Beamish, P. (1995) Adapting to foreign markets: Explaining internationalization, *International Business Review*, 4, 115-131.
3. Chari, M.D.R., Devaraj, S., and David, P. (2007) International diversification and firm performance: Role of information technology investments, *Journal of World Business*, 42, 184-197.
4. Cuervo-Cazurra, A., Maloney, M.M., and Manrakhan, S. (2007) Causes of the difficulties in internationalization, *Journal of International Business Studies*, 38, 709-725.
5. Dhillon, G. (2007) Principles of information systems security: Text and cases. John Wiley & Sons, Inc.
6. Galbraith, J. (1974) Organization design: An information processing view, *Interfaces*, 4, 3, 28-36.
7. Gerber, M. and von Solms, R. (2008) Information security requirements – Interpreting the legal aspects, *Computers & Security*, 27, 124-135.
8. Haworth, D.A. and Pietron, L.R. (2006) Sarbanes-Oxley: Achieving compliance by starting with ISO 17799, *Information Systems Management*, winter, 73-87.
9. Hennart, J.F. (1982) The theory of multinational enterprise. Ann Arbor: University of Michigan Press.
10. Herrmann, P. and Datta, D.K. (2005) Relationships between top management team characteristics and international diversification: An empirical investigation, *British Journal of Management*, 16, 69-78.
11. Hitt, M.A., Tihanyi, L., Miller, T., and Connelly, B. (2006) International Diversification: Antecedents, Outcomes, and Moderators, *Journal of Management*, 32, 6, 831-867.
12. Hughes, T. (2007) How well do you know your Internet marketing partners? *Journal of Internet Law*, May, 3-6.
13. Humphreys, E. (2008) Information security management standards: Compliance, governance, and risk management, *Information Security Technical Report*, doi: 10.1016/j.istr.2008.10.010
14. Hymer, S.H. (1976) The international operations of national firms: A study of foreign direct investment. Cambridge, MA: MIT Press.
15. Luthy, D. and Forcht, K. (2006) Laws and regulations affecting information management and frameworks for assessing compliance, *Information Management & Computer Security*, 14, 2, 155-166.
16. Nahra, K.J. (2006) A privacy and security compliance checklist for the Internet era, *Journal of Internet Law*, 9, 12, 11-21.

17. Nosworthy, J.D. (2000) Implementing information security in the 21st century – Do you have the balancing factors? *Computers & Security*, 19, 337-347.
18. Piotroski, J.D. and Srinivasan, S. (2008) Regulation and bonding: The Sarbanes-Oxley Act and the flow of international listing, *Journal of Accounting Research*, 46, 2, 383-425.
19. Sanders, WM.G. and Carpenter, M.A. (1998) Internationalization and firm governance: The roles of CEO compensation, top team composition, and board structure, *Academy of Management Journal*, 41, 2, 158-178.
20. Schultz, E. (2004) Sarbanes-Oxley-a huge boon to information security in the US, *Computers & Security*, 23, 353-354.
21. Tanriverdi, H. (2005) Information technology relatedness, knowledge management capability, and performance of multibusiness firms, *MIS Quarterly*, 29, 2, 311-334.
22. Tseng, C.H., Tansuhaj, P., Hallagan, W., and McCullough, J. (2007) Effects of firm resources on growth in multinationality, *Journal of International Business Studies*, 38, 961-974.
23. Von Solms, B. (2000) Information Security – The third wave? *Computers & Security*, 19, 615-620.
24. Von Solms, B. (2001) Information Security – A multidimensional discipline, *Computers & Security*, 20, 504-508.
25. Von Solms, B. (2006) Information Security – The fourth wave, *Computers & Security*, 25, 165-168.
26. Yeo, V. (2006) SOX clock ticking for overseas business. http://www.news.com/2102-7350_3-6098931.html