An Empirical Study of constructing a Corporate Information Security Governance System Using Balanced Scorecard---Evidenc

曹子珊、曹偉駿

E-mail: 9315871@mail.dyu.edu.tw

ABSTRACT

Based on the theory of corporate governance, the thesis develops the information security balanced scorecard for the benefit of fulfilling the information security management system (ISMS). On the purpose of achieving the mission and the maximum value of the stakeholders, we make ISMS more effective by the character of balanced scorecard which turns the strategy into motive program that tightly combines information security policy, the recognition of whole employees, and the culture and process of business management by core strategy to reach the corporate information security governance system. In order to evaluate whether the compliance of employees follows the information security practices, we solve the problem which the information security management system cannot completely do it well in a corporate using the information security balanced scorecard and strategy map. According to interviews with several domain experts, the thesis further shows that this strategic management framework is useful to raise the level of information security to protect the privacy of the clients and the demand of teaching and research, and also concerned about management performance. In summary, the thesis helps some medical center to construct the information security balanced scorecard and strategy map based on the theory of case study. Through detailed interviews with domain experts, the thesis also shows that the proposed strategic management framework can efficiently strengthen the information security management for the medical center to accomplish the purpose of sustained management.

Keywords : Information Security ; Information Security Management System ; Balanced Scorecard ; Strategy Map ; Corporate Governance

Table of Contents

REFERENCES

參考文獻 中文文獻 1 Clyde, R. A.（2002），「資安著重管理架構」，資訊傳真周刊，Nov.4, 2002, 頁46- 47。 2 于泳泓（2002），「從台灣企業成功導入平衡計分卡實例談－平衡計分卡導入與企業變革管理」，會計研究月刊，第200期，頁126－136。 3 于泳泓譯，「平

衡計分卡最佳實務」，商周出版社。 4 中華民國電腦稽核協會（2001），「資通安全管理制度導入手冊」，行政院國家資通安全會報技術服務中心。 5 王河清、童超塵（2001），「運用平衡計分卡建構新策略管理制度－以醫療產業為例」，醫院管理。 6 司徒達賢（2000），「非營利組織的經營管理」，天下遠見出版股份有限公司。 7 伍忠賢（2003），「公司治理的第一本書」，商周出版社。 8 江向才、何里仁（2003），「公司治理之資訊透明度與經營績效關聯性之實證研究」，管理會計第六十三期春季號，頁1-19。 9 江明修（2002），「非營利管理」，智勝文化事業有限公司。 10 余佩珊譯（1994），「非營利機構的經營之道」，遠流出版社。 11 吳安妮（2001），「非營利重顧客構面能連結享整合綜效—策略為焦點的組織—平衡計分卡式的公司—如何在新企業環境中取勝（三）」會計研究月刊，186期，頁126。 12 吳安妮（2002），「淺談平衡計分卡成功實施之精髓概念」，會計研究月刊，第198期，頁26-32。 13 吳琮璠（1996），「國外政府機構資訊系統安全稽核制度」，存款保險資訊季刊，第10 卷，第2 期，頁21-40。 14 吳琮璠（1997），「資訊管理個案研究方法」，資訊管理學報，第4 卷，第1期，頁7-17。 15 吳琮璠（2002），「會計財務資訊系統」，智勝文化事業有限公司。 16 宋振華、楊子劍（2000），「組織資訊安全體系與資訊安全整體架構」，資訊系統可信賴作業體制研討會論文集，頁114-125。 17 李東峰（2001），「企業資訊安全控制制度之研究」，第三屆全國資訊管理博士生聯合研討會論文集，頁1-22。 18 李東峰、林子銘（1999），「資訊安全的風險管理」，第五屆國際資訊管理研究暨實務研討會論文集，頁165-172。 19 李東峰、林子銘（2001），「風險評估觀點的資訊安全規劃架構」，台灣大學資訊管理學系第十二屆國際資訊管理學術研討會。 20 李東峰、林子銘（2002），「資訊主管企業資訊安全之風險控管決策」，資訊管理研究，第四卷，第二期，2002，頁1-42。 21 李書行（1995），「過程結果並重，個人群體兼顧-務實創新的策略性績效評估」，會計研究月刊，第113期，頁19。 22 周齊武（2002），「平衡計分卡於服務部門之應用-以資訊部門為例（三）」，會計研究月刊，第194期，頁85-90。 23 林宜賢、蔡慧菁譯（2001），「公司治理」，天下遠見出版股份有限公司。 24 林勤經、樊國楨、方仁威（2001），「資訊安全管理系統建置初始工作的研究，建立我國通資訊基礎建設安全機制標準規範實作芻議研究報告書」，經濟部標準檢驗局委託計畫，頁49-79。 25 林勤經、樊國楨、方仁威（2001），「資訊安全認證與電子化網路社會，建立我國通資訊基礎建設安全機制標準規範實作芻議研究報告書」，經濟部標準檢驗局委託計畫，頁80-104。 26 林鈴玉（2001），「國內網路銀行現況發展及交易安全之研究」，國立交通大學管理學院（資訊管理學程）碩士論文。 27 邱碧珠（2000），「資訊揭露程度與權益資金成本間之關係:我國資訊電子業之關係」，國立台灣大學會計學研究所碩士論文。 28 洪國興（2003），「資訊安全『影響因素與評估模式』之研究」，國立政治大學資訊管理研究所博士論文。 29 徐廣寅（2003）「資訊安全管理導論」，金禾資訊股份有限公司。 30 馬嘉應譯（2002），「財務報表革命—公司治理的徹底解決方案」，商周出版。 31 曹子珊、曹偉駿（2003），「基於平衡計分卡架構之資訊安全管理研究—以金融控股產業為例」，第九屆資訊管理暨實務研討會，論文集。 32 梁定澎（1997），「資訊管理研究方法總論」，資訊管理學報，第4 卷，第1 期，頁1-6。 33 陳至哲（2002），「我國資通安全應用之省思」，產業焦點評析，資策會。 34 陳依蘋（2002），「透明度與企業價值」，會計研究月刊第200期，頁48-54。 35 陳依蘋（2004），「不能描述就無法衡量，不能衡量就無法管理—策略地圖與平衡計分卡」，會計研究月刊第221期，頁53-58。 36 陳依蘋（2004），「描述溝通執行策略，聚焦即能成功導入—專訪平衡計分卡創始人」，會計研究月刊第221期，頁48-52。 37 黃承聖（2000），「企業資訊安全的起點－資訊安全政策」，網路通訊2000年8月號。 38 黃芳川（2002），「資訊安全手冊」，第三版，行政院主計處電子資料處理中心。 39 黃慶堂（1999），「我國行政機關資訊安全管理之研究」，國立政治大學公共行政學系碩士論文。 40 楊金炎（2001），「企業內部控制有關資訊系統與安全的個案研究」，中原大學資訊管理學系碩士論文。 41 葉銀華、李存修、柯承恩（2002），「公司治理與評等系統」，商智文化。 42 遠擎策略績效事業部譯（2001），「策略核心組織—以平衡計分卡有效執行企業策略」，臉譜文化事業股份有限公司出版。 43 劉常勇（1999），「科技管理的發展方向與省思-專訪中山大學企業管理學系劉常勇教授」，中山管理評論，第7卷第2期，頁269－277。 44 樊國楨（2002），「資訊安全風險管理」，行政院國家科學委員會科學技術資料中心。 45 樊國楨、方仁威、林勤經、徐士坦（2001），「資訊安全管理系統驗證作業初探，建立我國通資訊基礎建設安全機制標準規範實作芻議研究報告書」，經濟部標準檢驗局委辦計畫，頁105-125。 46 樊國楨、方仁威、林勤經（2001），「資訊安全管理稽核概要-以電子銀行為例」，資訊系統可信賴作業體制研討會論文集，頁169-185。 47 樊國楨、徐鈺宗（2003），「數位社會資訊安全管理系統驗證規範初探」，資訊安全論壇第10期，頁39-50。 48 蔡其諭（2002），「揭露程度與負債代理成本之關係」，國立政治大學會計學系碩士論文。 49 蔡坤哲（2003），「資訊揭露程度與盈餘管理關係之探討—以上市電子類股為例」，國立東華大學企業管理研究所碩士論文。 50 蕭新煌主編 （2000），「非營利部門:組織與運作」，巨流圖書。 英文文獻 51 BSI,“ Information security management—Part 1: Code of practice for information security management ”, BS 7799-1:2000, BSI （British Standards Institution）, 2000. 52 BSI,“ Information security management systems-- Part 2: Specification with guidance for use ”, BS 7799-2:2002, BSI （British Standards Institution）, 2002. 53 Carter, D. L. and Katz, A. J., “ Computer Crime and Security: the Perceptions and Experiences of Corporate Security Directors ”, Security Journal, Vol.7, pp.101-108, 1996. 54 Carver, John,“ Boards That Make a Difference : A New Design for Leadership in Nonprofit and Public Organizations ”, Jossey-Bass, 2nd edition, 1997. 55 COBIT （2000）,“ Governance Control and Audit for Information and Related Technology, 3rd Edition Control Objectives ”, 2000. 56 CSI/FBI （Computer Security Institute / Federal Bureau of Investigation）,“ 2003Computer Crime and Security Survey ” May 28, 2003. 57 Elliot, R. K. and Jacobson, P. D.,“ Costs and benefits of business information disclosure ”, Accounting Horizon, December, pp.80-96, 1994. 58 Eloff, M. M. and Von Sloms, S. H.,“ Information Security Management: An Approach to Combine Process Certification and Product Evaluation ”, Computers and Security, Vol.19, No.8, pp.698-709, 2000. 59 Eloff, M. M. and Von Solms, S. H.,“ Information Security management: A Hierarchical Framework for Various Approaches ”, Computers and Security, Vol.19, No.3, pp.243-256, 2000. 60 Goodwin, J., and Seow, J. L.“ The influence of corporate governance mechanisms on the quality of financial reporting and auditing: Perceptions of auditors and directors in Singapore ”, Accounting and Finance, Vol.4 No.23, pp.195-224, 2002. 61 Healy, P. M., and Palepu, K. G.,“ The effect of firm ’s financial disclosure strategies on stock prices ”, Accounting Horizon, Vol.7, No.1, pp.1-12, 1993. 62 Hinde, S.,“ If You Can Meet with

Triumph and Disaster and Treat Those Two Impostors Just the Same ”, Computers and Security, Vol.20, Issue: 8, pp.657-666, 2001. 63 Hinde, S., “ Security Survey Spring Corp ”, Computer and Security, Vol.21, Issue: 4, pp.310-321, 2002. 64 Hoffecker and Goldenberg, “ Using the Balanced Scorecard to Develop Companywide Performance Measures ”, 1994. 65 International Federation of Accountants, Managing Security of Information, 1998 66 ISACA （2002）, IS Standards, Guidelines and Procedures for Auditing and Control Professionals, 2002. 67 ISO/IEC 17799（2000）, “ Information technology-code of practice for information security management ”, 2000. 68 Kabay, M. E., “ The NCSA Guide to Enterprise Security ”, McGraw- Hill., 1996. 69 Kaplan, Robert S. and Norton, David P., “ Having Trouble with Your Strategy? Then Map It. ”, Harvard Business Review, Vol. 78 Issue: 5, pp.167-177, 2000. 70 Kaplan, Robert S. and Norton, David P., “ Linking the balanced scorecard to strategy ”, California Management Review, Vol. 39 Issue: 1, pp.53,-80, 1996. 71 Kaplan, Robert S. and Norton, David P., “ Strategy maps: converting intangible assets into tangible outcomes ”, Boston: Harvard Business School Press, 2004. 72 Kaplan, Robert S. and Norton, David P., “ The Balanced Scorecard--Measures That Drive Performance. ”, Harvard Business Review, Vol.70 Issue 1, pp.71-80, 1992. 73 Kaplan, Robert S. and Norton, David P., “ Transforming the Balanced Scorecard from Performance Measurement to Strategic Management: Part II ” Accounting Horizons, Vol. 15 Issue 2, pp.147-161, Jun. 2001. 74 Kaplan, Robert S. and Norton, David P., “ Putting the balanced scorecard to work ”, Harvard Business Review, Vol. 71 Issue 5, pp.134-141, 1993. 75 Lang, M. H. and Lundholm, R. J., “ Corporate disclosure policy and analyst behavior ”, The Accounting Review, Vol.17 No.4, pp.467-492, 1996. 76 Lee, S. M. and Luthans, F. and Olson, D. L, A Management Science Approach to Contingency Models of Organizational Structure, Academy of Management Journal, Vol. 25, No.3, pp.553-566, 1982. 77 Lindup, Ken, “ The Role of Information Security in Corporate Governance ” Computers and Security Vol. 15, Issue 6, pp. 477-485, 1996. 78 Luthans, F., “ Introduction to Management: A Contingency Approach ”, McGraw-Hill, 1976. 79 NIST, “ An Introduction to Computer Security: The NIST Handbook ” Special Publication 800-12, 1995. 80 OECD, “ Guidelines for Security of Information Systems ”, OECD, 1992. 81 OECD, “ Guidelines of the Security of Information Systems and Networks—Towards a Culture of Security ”, OECD, 2002. 82 OECD, “ Principles of Corporate Governance ”, OECD, 1999. 83 OECD, “ White Paper on Corporate Governance, Asian Roundtable on Corporate Governance ”, 2003. 84 Ozier, W., “ Generally Accepted System Security Principles （GASSP） ”, Computer Security Journal, Vol.13, No.2, pp.69-75, 1997 85 Reid, R. C. and Floyd, S. A, “ Extending the Risk Analysis Model to Include Market-Insurance ”, Computers and Security, Vol.20, Issue: 4, pp.331-339, 2001. 86 Rosemann M. and Wiwse, J. “ Measuring the performance of ERP software—a balanced scorecard approach ” Australasian Conference on Information Systems. Vol.10, pp.773-784. 87 Roussey, Robert S. and Cangemi, Michael, “ Board Briefing on IT Governance ”, IT Governance Institute, 2001. 88 Schultz, E. E., Proctor, R. W., Lien, M. C. and Salvendy, G., “ Usability and Security An Appraisal of Usability Issues in Information Security Methods ”, Computer and Security, Vol.20, Issue: 7, pp.620-634, 2001. 89 Sengupta, P., “ Corporate disclosure quality and the cost of debt ”, The Accounting Review Vol.73, pp.459-474, 1998. 90 Sherwood, J. “ SALSA: A Method for Developing the Enterprise Security Architecture and Strategy ”, Computer and Security, Vol.2, No.3, pp.8- 17, 1996. 91 Steward, M.E., “ Balanced Scorecard for projects. ” Project Management Journal, Vol.32, Issue 1, pp.38-53, 2001. 92 Tr?ek, D., “ An Integral Framework for Information Systems Security Management ”, Computers and Security, Vol.22, Issue: 4, pp.337-360, 2003. 93 Tryfonas, T. and Kiountouzis, E. and Poulymanakou, A., “ Embedding Security Practices in Contemporary Information Systems Development Approaches ”, Information Management and Computer Security, pp.183-197, 2001. 94 Von Solms Basie, “ Corporate Governance and Information Security ” Computers and Security Vol. 20, Issue: 3, pp. 215-218, 2001. 95 Von Solms, R., Van Haar, H., Von Solms, S. H. and Caelli, W. J., A “ Framework for Information Security Evaluation ”, Information and Management, Vol.26, pp.143-153, 1994. 96 Whitman, Michael E., “ Enemy at the Gate: Threats to Information Security ” Communications of the ACM Volume 46, Number 8, pp. 91-95, 2003. 97 Williams, Paul; Anderson, “ Information Security Governance ” Information Security Technical Report Vol. 6, Issue: 3, pp. 60-70, 2001. 98 World Bank, “ Corporate Governance:A Framework for Implementation—Overview ”, The World Bank, 1999. 99 Wright, M., “ Third Generation Risk Management Practices ”, Computer Fraud and Security, Feb., pp.9-12, 1999.