基於ISO 27001之校園成績管理系統的資訊安全治理-以某國中為例

徐敏凱、曹偉駿

E-mail: 386732@mail.dyu.edu.tw

摘 要

21世紀開始，隨著資訊科技和網路連結快速發展，政府機關和企業為了保持競爭力和提高效能紛紛開始導入資訊系統，隨著這股潮流和資訊網路科技不斷的創新，各種功能強大且處理速度快速的系統如雨後春筍般湧出。而這些系統除了為組織帶來相當的益處外，也使得團體組織對於資訊系統的依賴不斷提高。從民國八十八年起政府為了振興社會經濟，在教育方面推行全面網路化，讓校園內的網路資源運用能夠更加的順暢。但隨著網路的全面化所伴隨而來的是資訊和通訊所面臨到資訊安全及保密問題，包含病毒入侵、駭客入侵、內部人員控管疏失等各類相關問題。這當中以教師同仁的隱私資料及學生的成績更是需要被安全保護的對象。部分校園網頁因程式設計老舊，駭客可輕易植入木馬程式，竊取或竄改學校電腦中的試題或成績等檔案，更有甚至是竊取密碼資料，其中以中小學校園網站最嚴重，目前雖有所改善，但學校的資安仍處在危險邊緣。政府雖然推行學校網路資訊化，但卻也常忽略資訊安全相關問題。以資訊安全治理來說，資訊技術與資訊安全一直在企業中扮演重要的角色，而較少針對校園成績系統進行資訊安全治理的探討與分析。因此，本研究透過資安管理的流程及相關措施來改善，藉由ISO 27001的導入來檢驗校園成績管理系統的資訊安全，進而提出相關建議。

關鍵詞 : 資訊安全治理、資訊安全威脅、成績管理系統

目錄

參考文獻

一、中文部分 蔡憶懷(2000)，開放原始碼-Linux與自由軟體運動對抗軟體巨人的 故事，台北:商周出版。 陳萬淇(1995)，個案研究法，台北:萬泰。 李順仁(2003)，資訊安全，台北:文魁圖書出版社。 潘天佑(2011)，資訊安全概論與實務(二版)，台北:基豐資訊。 古永嘉，楊雪蘭(譯)(2011)，企業研究方法，台北:華泰。 樊國楨、林樹國、鄭東昇(2005)，資訊安全保證框架標準初探:根基於ISO/IEC 17799，台北:行政院國家科學委員會科學技術資料中心。 樊國禎(2002)，資訊安全能力評鑑，台北:行政院國家科學委員會科學技術資料中心。 行政院(1999)，行政院及所屬各機關資訊安全管理要點，台北。 行政院教育部(2007)，教育體系資通安全規範，台北。 行政院勞工委員會職業訓練局(2002)，資訊安全管理作業守則，台北。 行政院研考會(2001)，台北電子化政府推動方案執行情形，台北。 葉俊榮(2005)，電子化政府資通安全發展策略與展望，研考雙月刊， 29(1)，20-34。 劉文鈞(2006)，論資訊安全，品質月刊，42(10)，66-70。 吳琮璠(1997)，資訊管理個案研究方法，資訊管理學報，4(1)，7-17。 梁定澎(1997)，資訊管理研究方法總論，資訊管理學報，4(1)，1-6。 楊峻榮(2004)，以風險評估方式規畫校園資安機制，台灣區域網路中心93年度研討會。 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。 陳耀民(2008)，應用自由軟體建構集中式學務管理系統-以嘉義縣國民小學為例，南華大學資訊管理學系碩士論文。 鄭植尹(2010)，基於ITIL與ISO 27001建構大學校園資訊安全治理-以中部某大學為例，大葉大學資訊管理學系碩士班碩士論文。 胡雯婷(2011)，建置銀行業私有雲之資訊安全治理-以某銀行為例，大葉大學資訊管理學系碩士論文。 黃文谷(2011)，校園資訊系統安全關鍵評估機制之調查研究-以雲林縣國民小學SFS3學務系統為例，雲林科技大學資訊管理系碩士論文。 行政院研究發展考核委員會(2009)，網路安全的挑戰與策略[線上資料]，來源: http://www.seminar2009.twnic.tw/download/d2s2c.pdf [May 23, 2013]。 二、英文部分 A. E. Brown and G. G. Grant (2005). Framing the Framework:A Review of IT Governance Research. Communications of the Association for Information Systems, 15(2), 696-712. A. Calder (2006). Implementing Information Security Based on ISO 27001/ISO 17799: A Management

Guide. J. Van Bon (Ed.). Van Haren Publishing. A. Calder (2009). Implementing Information Security Based on ISO 27001/ISO 27002: A Management Guide. Van Haren Publishing. A. Cobit (2008). 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit. IT Governance Institute (ITGI) and Office of Government Commerce (OGC). CSA. (2010). Top Threats to Cloud Computing. Retrieved from Cloud Security Alliance, Institute for Learning Technologies Web site: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf [December 20, 2012]. D. B. Parker (1997). Information Security in a Nutshell. Information System Security, 6(1), 14-19. E. Maiwald (2004). Network Security: A Beginner`s Guide (2nd ed.). New York: McGraw-Hill. H. C. Relyea (2008). Federal Government Information Policy and Public Policy Analysis: A Brief Overview. Library & Information Science Research, 30(1), 2-21. H. Susanto, F. Muhaya, M. N. Almunawar and Y. C. Tuan (2012). Refinement of Strategy and Technology Domains STOPE View on ISO 27001. arXiv preprint arXiv, 1204-1385. I. M. Haw, S. S. M. Ho, B. Hu and D. Wu (2010). Concentrated Control, Institutions, and Banking Sector: An International Study. Banking & Finance , 3(3), 485-497. J. Esteves and R. C. Joseph (2008). A Comprehensive Framework for the Assessment of Government Projects. Government Information Quarterly, 25(1), 118-132. J. N. Rosenau (1995). Governance in the Twenty-First Century. Global Governance, 1, 13-43. J. S. Broderick (2006). ISMS, Security Standards and Security Regulations. Information Security Technical Report, 11(1), 26-31. M. Raydel and F. Stefan (2011). Automation Possibilities in Information Security Management. European Intelligence and Security Informatics Conference (EISIC), 259-262. M. Reiter and P. Rohatgi (2004). Homeland Security. IEEE Internet Computing, 8(6), 16-17. M. S. Saleh, A. Alrabiah and S. H. Bakry (2007). Using ISO 17799: 2005 Information Security Management: A STOPE View with Six Sigma Approach. International Journal of Network Management, 7(1), 85-97. M. E. M. Spruit and M. Looijen (1996). IT Security in Dutch Practice, Computers & Security, 15-2, 157. N. Pham, L. Baud, P. Bellot and M. Riguidel (2008). A Near Real-time System for Security Assurance Assessment. The Third International Conference on Internet Monitoring and Protection. 152-160. P. Nastase. F. Nastase and C. Ionescu (2009). Challenges Generated by the Implementation of the IT Standards COBIT 4.1, ITIL V3 and ISO/IEC 27002 in Enterprises. Economic Computation & Economic Cybernetics Studies & Research, (3), 1-16. P. W. Andersen (2001). Information Security Governance. Information Security Technical Report, 6(3), 60-70. R. Richardson (2008). CSI Computer Crime and Security Survey. Computer Security Institute, 1, 1-30. R. Ahmad and L. Janczewski (2011). Governance Life Cycle Framework for Managing Security in Public Cloud: From User Perspective, IEEE International Conference on Cloud Computing (CLOUD), 372-379. R. K. Yin (2003). Case study research: Design and methods (Rev. ed.). Newbury Park, California: Sage Publications. S. H. Bakry (2004). Development of e-Government: A STOPE View. International Journal of Network Management, 14(5), 339-350. S. H. Solms and R. V. Solms (2006). Information Security Governance: A Model based on the Direct-Control Cycle. Computers & Security, 25(6), 408-412. S. Hosseinbeig, D. Karimzadgan-Moghadam, D. Vahdat and R. A. Moghadam (2011). IT Strategic Alignment Maturity and IT Governance. International Conference on Interaction Sciences (ICIS), 67-72. S. J. Mousavian, Sh. Gilaninia, O. Taheri, H. Nikzad, H. Mousavi and F. Z. Seighalani (2012). Information Security Management on Performance of Information Systems Management, Journal of Basic and Applied Scientific Research, 2(3), 2582-2588. S. Sahibudin, M. Sharifi and M. Ayat (2008). Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. International Conference on Modeling & Simulation, 749-753. T. Finne (2000). Information Systems Risk Management: Key Concepts and Business Processes. Computer & Security, 19(3), 39-50. T. V. Bonoma (1985). Case Research in Marketing: Opportunities, Problems and a Process. Journal of Marketing Research, 22(2), 199-208. W. D. Bruijn, M. R. Spruit and M. Heuvel (2010). Identifying the Cost of Security. Journal of Information Assurance and Security, 5, 74-83.