社交工程對公部門資訊安全管理影響之研究 = A study of social engineering on the impact of information security management

余建輝、楊豐兆

E-mail: 354848@mail.dyu.edu.tw

摘 要

電子化政府對提升行政效率即便民服務，帶來極大的助益，然而隨著資訊科技的快速發展，亦同樣帶來了資訊安全的問題，由於政府機關所擁有的資訊，是涉及了民眾個人的隱私資料、企業重要的商業資料、乃至於國家機密等，因此如何確保公部門之資訊安全，是現在公部門電子化所必須因應的課題之一。本研究針對基層公務人員為抽樣對象，以組織內部人員對社交工程的威脅認知、社會心理弱點及建立資訊安全管理系統等相關構面及其因素、相關性之相互關係做統計分析。由於社交工程對於資訊安全的危害是一直層出不窮不斷的在演進，所使用的社交工程手法也跟著進化，不變的是無論科技、資訊如何演進，人們的心理弱點、七情六欲等等…卻無法變的鐵石心腸，因此針對社交工程如何利用人們的社會心理弱點作攻擊，應如何做防範與宣導，不是讓人非得無感情、感覺，而是能具體了解那些訊息應注意。

關鍵詞 : 社交工程、電子郵件社交工程演練、社會心理弱點、資訊安全管理系統政策

目錄

內容目錄
中文摘要 iii

英文摘要 iv

致謝辭 v

內容目錄 vi

表目錄 viii
圖目錄 x
第一章　緒論. 1
　第一節　研究背景與動機. 1
第二節　研究問題. 3
　第三節　研究目的. 4
　第四節　研究範圍. 4
　第五節　研究流程. 5
第二章　文獻探討. 6
　第一節　資訊安全. 6
　第二節　社交工程. 14
　第三節　社會心理弱點. 25
第三章　研究方法. 27
第一節　研究架構. 27
第二節　研究假設. 28
第三節　研究對象. 31
　第四節　衡量工具. 32
第五節 資料分析方法. 32
第三章　研究結果. 36
第一節　基本資料分析. 36
第二節　信度與效度分析. 39
第三節　基層公務人員對社交工程認知評價. 46
　第四節　個人屬性變異數分析. 55

第五節 各變項相關分析. 84
第五章　結論與建議. 89
第一節　結論. 89
第二節　建議. 93
參考文獻 95
附錄A 問卷調查 104

?表目錄

表 2-1 資訊安全的威脅分類. 8
表 2-2 整體遭遇資通安全事件概況. 10
表 2-3 社交工程手法. 15
表 2-4 網?釣魚手法與技術. 19
表 4-1 基本資料統計表. 36
表 4-2 基本資料統計表. 37
表 4-3 基本資料統計表. 38
表 4-4 社交工程威脅認知因素分析表. 40
表 4-5 社會心理弱點因素分析表. 41
表 4-6 資訊安全管理系統政策因素分析表. 43
表 4-7 社交工程威脅認知描述性統計分析. 47
表 4-8 社會心理弱點描述性統計分析. 49
表 4-9 資訊安全管理系統政策描述性統計分析. 51
表 4-10 性別與受訪者社交工程變異數分析表. 55
表 4-11 婚姻與受訪者社交工程變異數分析. 58
表 4-12 職務與受訪者社交工程變異數分析表. 60
表 4-13 年齡與社交工程威脅認知變異數分析表. 62
表 4-14 年齡與社會心理弱點變異數分析表. 63
表 4-15 年齡與資訊安全管理系統政策變異數分析表. . . 66
表 4-16 教育程度與社交工程威脅認知變異數分析表. . . 68
表 4-17 教育程度與社會心理弱點變異數分析表. 69
表 4-18 教育程度與資訊安全管理系統政策變異數分析. . 71
表 4-19 服務年資與社交工程威脅認知變異數分析表. . . 72
表 4-20 服務年資與社會心理弱點變異數分析表. 73
表 4-21 服務年資與資訊安全管理系統政策變異數分析. . 77
表 4-22 電腦處理公務時間與社交工程威脅認知變異數分. 79
表 4-23 電腦處理公務時間與社會心理弱點變異數分析. . 80
表 4-24 電腦處理公務時間與資訊安全管理政策變異數分. 84
表 4-25 各變項之pearson相關分析. 88
表 5-1 研究假設彙整表. 91
表 5-2 研究假設彙整表. 91

圖目錄

圖 1- 1 研究流程圖. 5
圖 2- 1 社交工程之威脅圖像 15
圖 2- 2 社交工程電子郵件附件檔案. 17
圖 2- 3 電子郵件夾藏陷阱. 17
圖 2- 4 偽裝安全程式. 20
圖 2- 5 下載軟體為掩護. 21
圖 2- 6 網頁掛馬攻擊模式. 22
圖 2- 7 社交工程攻擊步驟. 24
圖 3- 1 研究架構圖. 28

參考文獻

參考文獻 一、中文部份 卡巴斯基社交工程類型解析[線上資料]，來源: http://www.kaspersky.com.tw/。 行政院(2009)，國家資通訊安全發

展方案，98年至101年。 行政院研考會(1999)，行政院及所屬各機關資訊安全管理要點，來源: http://www.dgbas.gov.tw/eyimc/switch6/law/af08.htm。 行政院科技顧問組(2010)新型社交工程攻擊手法通知。 行政院國家科學委員會(2011)，行政院國家科學委員會科學發展期刊，461期，23。 何全德(1999)，資訊安全控管與偵防-從電子化政府談資訊安全控管與偵防，資訊安全通訊，6(1)。 吳明隆，涂金堂(2008)，SPSS與統計應用分析，台北:五南。 吳啟文(2009)，2009年防駭年會，行政院研究發展考核委員會ppt。 李德治，童惠玲(2007)，統計學，台北:博碩文化。 林順傑(2010)，漫談網路釣魚問題常見手法與分析，淡江大學資訊。 張博俊(2004)，資訊安全管理實物，台北:松崗出版社。 陳永裕(1993)，銀行業資訊安全管理之研究，東海大學企業管理研究所碩士論文。 陳銘言(2008)，社交電子郵件攻擊之使用之使用者行為模式分。 黃亮宇(1993)，資訊安全規劃與管理，台北，松崗。 經濟部標準檢驗局(2006)，資訊技術-安全技術--資訊安全管理系統-要求事項，國家標準CNS 27001。 萬幼筠(2001)，資訊安全管理vs.企業風險管理，網路通訊(91)，頁24-30。 資策會(2001)，資訊安全發展趨勢與科專研發方向建議；資策會(MIC)資訊軟體產業報告；1-133，2001年12月31日，來源: http://www.itis.org.tw/pubinfo-detail.screen?pubid=246。 劉國昌，劉國興(1998)，資訊安全，儒林圖書公司。 樊國楨，楊晉寧(1996)，互連網(Internet)電子信息交換安全－以電子公文交換作業安全為本，電腦稽核，14-25。 蔡星樺(2001)，從ISO/TR 13569談金融機構之資訊安全，財金資訊雙月刊，來源: http://www.fisc.org.tw/information/maz/19/p2_2.asp。 蔡興樺(1999)，企業如何做好資訊風險管理，網路通訊(91)，31-34。 謝清佳、吳琮璠(1997)，資訊管理，台北:智勝文化事業，23-32。 行政院主計處電子處理資料中心中(2011)，電腦應用概況報告。 二、英文部份 Ansoff, H. I., & McDonnell, E. J. (1990). Implanting strategic management. New York: Prentice-hall, 403-429. Bass, B. M. (1990). From transactional to transformational leadership: Learning to share the vision. Organizational Dynamics, 18(3),19-31. Bass, B. M., & Avolio, B. J. (1990). Full range leadership development. California: Mind Gradern. Inc. Bass, B. M., & Avolio, B. J. (1994). Improving organizational effectiveness through transformational leadership. London: Sage Press. Bennis, W., & Nanus, B. (1985). Leaders: The strategies for taking change. New York: Haper & Row. Berry, L. L., & Parasuraman, A. (1991). Marketing services: Com-peting through quality. New York: The Free Press. Brooks, R. F., Lings, I. N., & Botschen, M. A. (1999). Internal marketing and customer driven wavefronts. The Service Industries Journal, 19(4), 49-68. BSI (1999). "Information security management- Part 1: Code of practiice for information security management", BS 7799-1:1999, BSI(British Standards Institution). Buell, V. P. (1984). Marketing management: A strategic planning approach. New York: McGraw-Hillbook Co. Crawford, J. C., & Getty, J. M. (1991). The marketing of services: A quality perspective. Journal of Professional Service Marketing, 8(1), 5-15. Crosby, P. B. (1979). Quality is free: The art of making quality certain. New York: McGraw-Hill Book Company. CSI/FBI(Computer SecurityInstitute / Federal Bureau of Investigation) Edvardsson, B., Larsson, G., & Setterlind, S. (1997). Internal service quality and the psychosocial work environment: An empirical analysis of conceptual interrelatedness. The Service Industries Journal, 17(2), 252-263. Garfield, G. (1994). Service imperative. Executive Excellence, 11, 1-19. Garnett, J., & Kouzmin, A. (2000). Strateic change in organizational communication: Emerging trends for wealth formation in the new millennium. Strategic Change, 9(1), 55-65. Garvin, D. A. (1984). What does product quality reaiiy mean. Sloan Management Review, 25(Fall), 25-43. Garvin, D. A. (1987). Competing on the einght dimensions of quality. Harvard Business Review, 65(Nov-Dec), 101-109. Gronroos, C. (1990). Service management and marketing: Managing the moments of truth in service competition. Massachusetts: Lexington Books. Hartline, M. D., & Ferrell, O. C. (1996). The management of customer-contact service employees: An empirical investigation. Journal of Marketing , 60(October), 52-70. Heskett, J. L., Jones, T. O., Loveman, G. W., Sasser Jr, W. E., & Schlesinger, L. A. (1994). Putting the service profit chain to work. Harvard Business Review, 72(2), 164-174. House, R. J. (1971). A path-goal theory of leader effectiveness. Administrative Science Quaterly, 16, 321-338. Jones, C. R. (1996). Customer satisfaction assessment for internal supplier. Management Services, 40(2), 16-18. Keith Osborne(1988). Auditing The IT Security Function, Computer & Secrutity, 17(1), 34-41. Kilmann, R. H., Saxton, M. J., & Serpa, R. (1985). Five key issues in understanding and change culture. In Ralph Kilmann et al. (Eds.), Gaining Control of Corporate Culture. San Francisco: Jossey-Bass. Kirkpatrick, S. A., & Locke, E. A. (1991). Leadership: Do traits really matter? Academy of Management Executive, 5(2), 48-60. Lindup, K. P.,(1995). "A New Model for Information Security Policies", Computer & Security, 14,691-695. McDermott, L. C., & Emerson, M. (1991). Quality and service for internal customer. Training & Development Journal, 45(1), 61-64. Milakovich, Michael E. (1993). Leadership for public service quality improvement. Public Manager, 22(3), 49-53. Olnes, J.,(1994). Development of Security Policies, Computer & Security, 13, 628-636 Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (1985). A conceptual model of service quality and its implications for future research. Journal of Marketing, 49(Fall), 41-50. Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (1988). SERVQUAL: A multiple-item scale for measuring consumer perceptions of service quality. Journal of Retailing, 46(1), 12-40. Rausch, E. (1999). More effective leadership can bring higher service quality. Managing Service Quality, 9(3), 154. Reynoso, J., & Moores, B. (1995). Towards the measurement internal service quality. International Journal of Service Industry Management, 6(3), 64-83. Robbins, S. P. (1993). Organizational behavior. New Jersey: Prentice-Hall Inc, 670- 673. Robbins, S. P. (2001). Organizational Behavior. New York: Prentice Hall. Rusell, D. & Gangemi, G. T. (1992). “ Computer Security Basics ”, California, U.S.A., O ’Reilly & Associates Inc. Schneider, E. C. & Gregory, W. T. (1990). “ How Secure Are Your System Avenues to Automation, Nov. Sherwood, J.,(1996). SALSA: A method for developing the enterprise security architecture and strategy, Computer & Security, Amsterdam,15(6), 501-506. Tunstall, W. B. (1985). Breakup of the bell system: A case study in cultural transformation. In Ralph H. Kilmannetal (Ed.), Gaining of the Corporate Culture. 44-65. San Francisco: Jossey-Bass. Vandermerwe, S., & Gilbert, D. J. (1991). Internal services: Gaps in needs/performance and prescriptions for effectiveness. International Journal of Service Industry Management, 2(1), 50-60. Wallach, E. J. (1983). Individuals and organizations: The cultural match. Training and Development Journal, 37(2), 29-36. Yukl, G. (1994). Leadership in organizations (3rd ed.). Prentice Hall International, Inc. Zeithaml, V. A. (1988). Consumer perceptions of price, quality, and value: A means-end model and synthesis of

evidence. Journal of Marketing, 52(Jual), 2-21.