Cloud Computing

了解社交工程的威脅對於資訊安全治理與管理的影響

The Underestimated Social Engineering Threat in IT Security Governance and Management

作者: Roberto Puricelli, CISM,

is a senior information and communications technology (ICT) security consultant at CEFRIEL, an innovation company of Politecnico di Milano. He has experience in various domains of information security, including vulnerability assessment, penetration testing, web application and mobile security, and risk analysis. He is involved in research on new generation threats, with a particular focus on social engineering attacks. As such, he contributed in developing a specific methodology aimed at measuring the related risk.

譯者: **黃劭彥**, 國立中正大學會計與資訊科技學系教授, 電腦稽核協會編譯出版委員會委員

網路犯罪生態系統正快速的變化，科技的進步和更容易取得的強大惡意軟體使網路犯罪者有 business-oriented mind-set。近幾年來，有許多進階持續性的攻擊(APTs) 和資料外洩發生在最大型、高收益的企業，而引起媒體的注意。這樣的案例只代表那些已知的網絡犯罪問題，同時，還有許多尚未發現或未向公眾揭露的攻擊。2014 年是關鍵的一年，Sony, JP Morgan Chase, Target 等都遭受造成公司及其客戶嚴重後果的網絡攻擊。分析新的攻擊策略發現，網絡攻擊變得越來越明顯且頻繁，網絡攻擊透過攻擊漏洞，橫向移動延長周邊範圍，並取得目標公司內其他系統的控制權，進一步獲得關鍵信息，使其在企業網絡有立足之地。此外，攻擊的第一階段包含透過社交工程操縱員工行為。

人是資訊安全中必要部分

歷史上，員工一直是在組織中安全議題的來源。第一部分是關於內部威脅，也就是任何心懷不滿，惡作劇或離經叛道的員工(和之前員工，顧問或貿易夥伴)會利用資訊或系統的內部知識來傷害公司。本文會著重於討論粗心的員工，因為這樣人，可能會受到社交工程的威脅，而沒有意識地從事惡意，使企業的資訊處於風險中。

網絡犯罪分子明白社交工程技術可用於操縱受害者而獲取重要信息，並說服他們執行某些操作，而增加攻擊的成功率。事實上，最近許多資料外洩都是這樣的案例。ICANN 資料外洩是起源於網路釣魚，就是允許攻擊者獲得對集中數據系統用戶的資訊 [1]。根據 Carabank 攻擊事件的調查包含幾個跨國的銀行，員工被當成社交工程攻擊的目標，允許惡意軟體攻擊。研究證實，人是資訊安全鏈中的薄弱點。人為錯誤或不當行為往往涉及到非理性與因素，如個人的經驗和心理的態度，特別是在缺少風險意識時 [2]。例如，研究證明，只要提供美金 1 元的獎勵就足以說服大量的用戶下載並運行潛在的惡意軟體，忽略了典型的安全警告 [3]。這行為確認來自網絡釣魚，這仍然是最有效的社交工程武器之一，網絡攻擊不斷進步變得越來越複雜 [4]。綜合上述原因，不能再將企業的資訊安全治理與管理僅限於科技面而已。在過去，獲得新的設備和配置系統足以維持的安全水平已經不夠，資訊外洩和其他威脅也是企業必須考量的已。

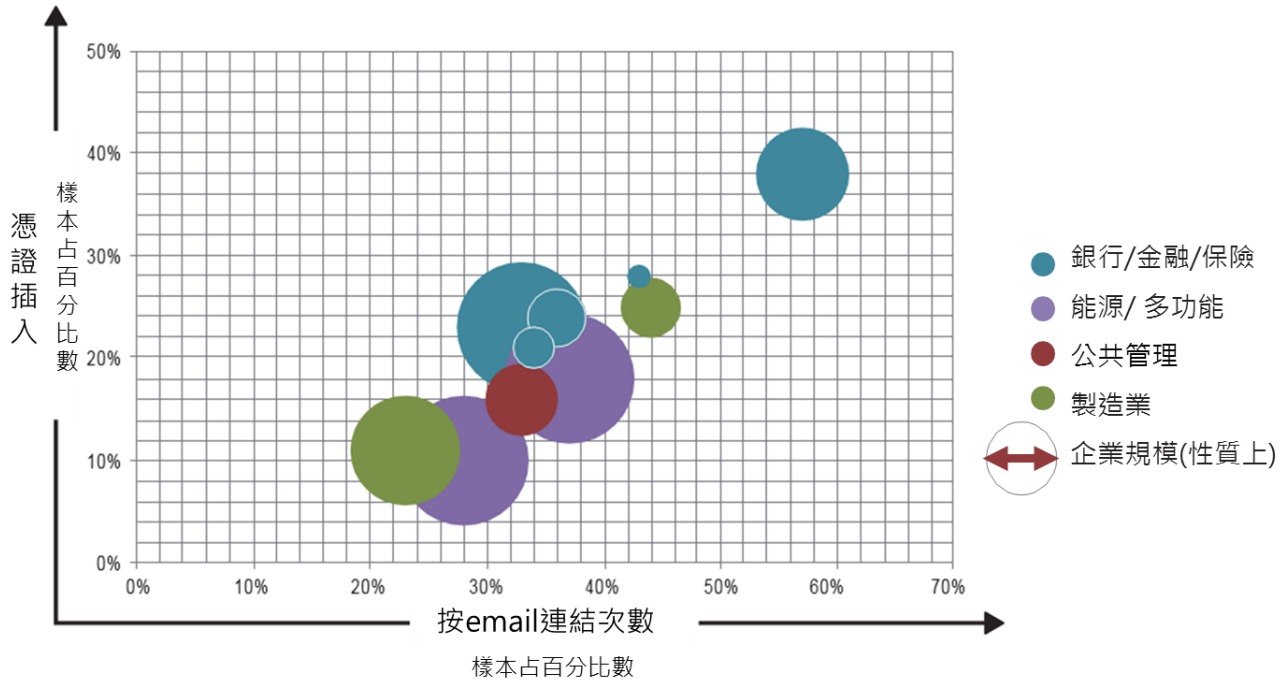
不幸的是，目前的威脅還不止這些。關鍵不是目標企業的資訊安全專業人員是否部署了最佳的科技，流程和解決方案（與行業慣例和標準完全相容），而是這些安全措施是遠遠不夠的，安全攻擊越來越依賴於人類的弱點；因此，延伸資訊安全治理，將人的因素納入企業風險分析和評估，是很基本的。要有效做到這一點，必須了解和衡量實際風險，以提出有效的對策來減輕風險。

如何衡量人的因素

目前在評估資訊安全和風險管理模型、工具、流程和法律結構時，往往會低估甚至忽視人的因素。由於將員工納入評估是一個比較創新，且被認為較有風險的做法，所以合適的評估方式扮演重要的角色。首先，資訊和安全部門不是唯一決定評估方法的人員，因為攻擊的目標是員工。因此，需要所有的利益相關者參與，如人力資源（HR），法律和通信部門的參與以了解面對的威脅，評估的標準和共同的目標。此外，有幾個在執行評估人的因素時需要考慮的倫理問題[5]。

社交工程攻擊意味著員工被欺騙而做出違反政策的行為。儘管不法犯罪分子努力使員工做出這些行為，企業必須更嚴格要求員工遵守道德和法律的限制，特別是保證雇主和員工彼此之間的相互尊重和避免侵犯到個人的私領域。此外，有必要考慮到勞動法規的不同。在保護員工不受雇主任何的干涉這方面，美國和歐洲是不同的。例如，在意大利，法律禁止雇主監控員工的行為;因此，在一個評估中，不能洩漏可能被利用參與攻擊員工的個人詳細資料。儘管這樣的局限性和一些法律和道德風險的存在，歐洲對這樣

圖 1—比較以社交為主漏洞評估結果



Source: CEFRIEL. Reprinted with permission.

的資訊安全威脅也越來越重視。

從 2010 年以來，一些對歐洲大型企業嘗試克服這種困難的評估促成了社交導向弱點評估的發展 [6]。這種評估的目的是測試員工對模擬魚叉式網路釣魚攻擊時的行為，就是其中一個攻擊者試圖欺騙用戶（即公司員工）進行把公司資產放在風險中的行為，例如：1.讓員工點擊電子郵件內的鏈接，訪問一個可能的惡意網站，這網站讓公司暴露於一個感染攻擊 2.讓員工以網頁表單的方式插入特定要求的信息，從而提供了重要的信息，如企業憑證藉由使用受控的網站，並跟踪用戶的行為，並且也可以從模擬釣魚技術估計企業的暴露水平做後續的攻擊（例如，找出未修補的安全漏洞）。

什麼是真正的風險？

很多的大型企業（超過 12,000 名員工）使用社交導向弱點評估方法來評估企業的風險水平。在大多數這些評估中，魚叉式網路釣魚利用一般的方法例如對員工的特別優惠來進行攻擊。大多數攻擊是利用公司具體的情境（通過顏色，標誌，模板和適當的方式溝通）來進行。在一些情況下，公司公開的資訊被引用來攻擊。但這並沒有顯著影響結果。

圖 1 顯示出了評價結果的比較，繪製每個先前為參與測試的樣品中描述的兩個步驟的成功率：員工點擊網絡釣魚電子郵件內的鏈結的百分比在 x 軸和員工插入公司憑證的百分比在 y 軸。每個圓圈代表一個公司進行的評估，其半徑表示該公司本身的大小和顏色表示產業部門。平均結果是相當令人印象深刻，並確認魚叉式網路釣魚攻擊實際上很有效。在這些評估中，三個員工中有一個（34%），點擊網絡釣魚電子郵件內的鏈結，五個員工中有一個（21%）在網頁的表格上插入公司憑證。當關聯到現在的因素時，這些結果更令人印象深刻。根據這些結果，網路釣魚行動的特點是一個員工一時的衝動行為會使釣魚行動的成功率快速增長，在 20 分鐘內達到 50%的有效率。這意味著，信息和通信技術（ICT）的安全部門能反應的時間很短。

特別是在大企業，似乎缺乏根據使用者報告產生對策的正式流程和員工對如何報告安全漏洞的知識不足。另一個有趣的一點是，所有的員工都受到這種威脅。似乎沒有因為年齡，位置，部門或角色而有任何的差異。即使是管理階層和執行主管也是不能倖免。在一般情況下，在公司職位越高的越不容易遇到安全問題但是被詐騙的管理階層還是不少，這指出從風險管理的角度來看，有些問題需要被解決。最後，透過指紋識別技術，信息被收集了用來瀏覽網站（用戶的工作站）的設備的安全狀況，並發現高風險容易被攻擊的安全漏洞。這意味著使用漏洞，惡意代碼和定制的（但簡單的）技術的結合，就有可能繞過公司內部的技術對策，並獲得進入內部網絡的權利，進入內部網絡的權利正是現代網絡攻擊的主要目的。

如何減輕風險

從一個資訊安全管理的角度來看包括人的因素納入弱點評估來降低風險是最終目標。最有效的對策是警覺性的培養和訓練，這有助於提高員工的安全意識。不幸的是，傳統的警覺性提升方案並不總是有效的 [7]，在警覺性提升方案實施過後的測試顯示警覺性並沒有多大的改變。對一般不懂科技的人來說由社交工程造成的網路犯罪還是很容易被了解的而且有風險的定量指標可以補救和預防這樣的犯罪。一個客觀的衡量指標還可以用來安排訓練項目的優先次序。此外，透過在訓練計劃之前和之後的評估可以了解警覺性提升方案的有效性。真正的問題是如何建立長效的培訓計劃，可以有效地提高了公司的安全水平，以及如何保持這種安全水平，傳統警覺性提升方案有時會失敗，因為

用戶可能缺乏動機去關注他們日常生活習慣中可能被用來詐騙的溝通管道[8,9]。所以警覺性的提高是一個關鍵因素。最有用的方法都涉及到使用視覺元素，諸如視頻，信息圖形或信息懶人包來刺激人。此外，遊戲化是最有前途的趨勢之一。獎勵，日常工作生活中的社會參與和直接的反饋也有所幫助，正確的策略取決於仔細探索不同的因素。

社交工程風險管理策略

社交工程風險管理中的人為因素，是企業系統的主要漏洞。這種特殊風險領域往往被低估，並難以管理。員工可能是社交工程攻擊的受害者，因為他們沒有關於這些威脅的訓練也沒有能力辨別哪些種類的網站或文件附件是安全的。關鍵是要去建構一個能把人的因素也納入風險考量的資訊工程管理流程。 COBIT®5 也將人的因素和行為列入設計 GEIT.10 的考量[10]。對人的因素評估增加了一個對資訊安全目標達成率的評估指標。藉由改正,鼓勵,和維持整個企業文化對安全認知的實行是很重要的。特別是通信和安全意識和訓練必須以適當的方式去提高他們的有效性。在這方面的整體方法應用可能是困難的。解決方案應該包括增加參與的各部門的內部合作。這樣的合作可以透過客觀的結果和可測量的數據這種簡單的方法達成。這種合作對重新定義投資計畫以發現風險進一步在人力因素，安全相關活動上帶入共用預算（不只是從 IT）因為該行動已經從技術開始著手轉移到人力資源領域。部門間的合作可以支持企業，幫助他們實施能夠使他們提升資訊安全管理的方案。

結論

現今，只有資訊科技方面的對策，是無法讓資訊與通信科技達到安全的水平，因為，因為現代網絡攻擊可以繞過所有防守層，通過社交工程進行攻擊。本文中討論的結果證實員工可能被欺騙去執行可能使公司資訊安全面臨風險的行為。因此，為了降低這種風險，企業必須制定一項策略去了解問題的嚴重和進行有效的行動解決問題。要找出風險的威脅程度，企業需要評估他們的員工。無論從道德和規範的角度來看，企業必須使用為自己公司量身訂做的方法去測量社交工程攻擊的潛在性。具體有效地應用這種方法，可以讓資深的管理人員願意主動的進行減少社交工程攻擊的潛在性的方案也就是針對資訊安全而實施的員工教育。為了提高對資訊安全的意識以減輕資訊安全的風險，不應只重視資安傳統教育也要用創新的方法提高員工的資安意識。這可能可以有效地改變公司文化，並促進其整體資訊安全水平的提升。

ENDNOTES

1.ICANN, “ICANN Targeted in Spear Phishing Attack. Enhanced Security Measures Implemented,”16 December 2014, https://www.icann.org/news/announcement-2-2014-12-16-en

2 Kaspersky Lab, “The Great Bank Robbery: The Carbanak,” Securelist, 16 February 2015, APT, http://securelist.com/blog/research/68732/the-great-bankrobbery-the-carbanak-apt/

3 Guanotronic, “It’s All About The Benjamins: An Empirical Study on Incentivizing Users to Ignore Security Advice,” http://guanotronic.com/~serge/papers/fc11.pdf

4 Dhamija, R.; et al.; “Why Phishing Works,” Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, April 2006, www.cs.berkeley.edu/~tygar/papers/Phishing/why_phishing_works.pdf

5 Mouton, F.; et al.; “Social Engineering From a Normative Ethics Perspective,” Information Security for South Africa (ISSA), Johannesburg, South Africa, 2013, http://icsa.cs.up.ac.za/issa/2013/Proceedings/Full/77/77_Paper.pdf

6 Brenna, R.; et al.; CEFRIEL, “Social Driven Vulnerability,” Technology, February 2014, www.slideshare.net/ CEFRIEL/social-driven-vulnerability-english-version

7 Kumaraguru, P; et al.; “Teaching Johnny Not to Fall for Phish,” Journal ACM Transactions on Internet Technology, 2010

8 Kumaraguru, P.: et al.; “Lessons From a Real World Evaluation of Anti-phishing Training,” APWG eCrime Researcher’s Summit, January 2008

9 Caputo, D.; et al.; “Going Spear Phishing: Exploring Embedded Training and Awareness,” Security and Privacy, IEEE, vol. 12, iss. 1, 23 August 2013

10 ISACA, COBIT® 5, USA, 2012, www.isaca.org/cobit

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 3, 2015 of the ISACA Journal articles by the Taiwan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the ISACA. The Taiwan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

品質聲明：

ISACA臺灣分會在ISACA總會的授權之下，摘錄ISACA Journal 2015,Volume 3中的文章進行翻譯。譯文的準確度及與原文的差異性則由臺灣分會獨立負責。

Disclaimer:

The ISACA Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the ISACA Journal.

Opinions expressed in the ISACA Journal represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. ISACA Journal does not attest to the originality of authors' content.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

免責聲明：

ISACA Journal係由ISACA出版。ISACA 為一服務資訊科技專業人士的自願性組織，其會員則有權獲得每年出版的ISACA Journal。

Cloud Computing