

Synopsis: According to Fortinet's spokesperson Jim Liu, databases are the most important assets for enterprises and are currently the main targets for hackers with the increase in data theft. Liu went on to introduce FortiDB in his speech at the 2009 Information Security Trend Forum organized by Information Security Magazine on November 20 in Taipei, Taiwan.

活動伸展台
EVENTS

2009資安趨勢論壇 後續報導

在不景氣之時，更應當注意投資是否用對地方，讓企業達到永續經營的目標。

文 | 吳依恂、何依玟

最近有許多半導體產業的工廠，已經在進行歲修，甚至也鼓勵員工休假了。本刊總編輯侍家驊在資安趨勢論壇開場時便提到，資安工作是不是也應仿效這樣的作法？過去企業在衝刺業績的時候，系統要是出了問題業務就停頓了，所以可能只好睜一隻眼閉一隻眼，不得已只好讓可怕的系統繼續運作，但既然業務現在都已經停緩下來，豈不正是一個審視資安體質的好時機嗎？

而BSI台灣區副總經理蒲樹盛，也與大家分享了一則新聞，提到日本在這波不景氣當中，各項服務還是表現得很好，例如說儘管新幹線每年輸運上千萬人次，但一年裡卻僅誤點了36秒。對無可救藥的悲觀者來說，會覺得這波不景氣會讓大家都過不下去了，但對於無可救藥的樂觀者來說，卻會認為這卻是排除掉沒有競爭力部份的好時機，而這也是本次與大家分享的一企業的投資價值應該要專注在什麼地方？「ICT資通安全的投資價值」——他提到如今國際趨勢談的已不只是資安，而是資通安全(Information and Communication Security)。

他說，根據2008年ITGI(IT Governance Institute)的研究資料顯示，雖然90%的CIO認

同對IT投資能夠創造價值，但僅有78%的管理階層(CEO、CFO、COO)同意這樣的想法，並且只有62%的組織認為IT與營運策略是一致的。也就是說，對IT的投資，依然未能使得管理階層滿意，可能是認同付出成本太高或沒有得到期望的回報等。也因此，有高達98%的高階主管認為，針對IT治理的績效及進展進行量測是重要的活動。他也看到歐洲的企業開始有了「營運持續長」這樣的職位，資訊安全僅是企業的眾多風險之一，企業需要兼顧到全面性的風險，每項資安工作都是建立在風險管理之上，如果有好的風險管理能力，資安不可能做得差。他打趣的說，如果不能做好「風險管理」，就會被「風險」所「管理」；如果不能做好「危機處理」，就會被「危機」所「處理」。

他提出如果企業在客戶需求來時便馬上就做，未經確認，在後續反而要花費更多時間修改，如果能做到「Better」、「Faster」、「Cheaper」便能優於客戶需求，確保第1次就作對的事情，這樣才有價值可言。

根據CSI的報告，將近有半數的企業，都在事件發生後的1~3個月，才發現曾經遭到攻擊，也就是被攻擊的當下，企業並無所

資訊安全僅是企業的眾多風險之一，企業需要兼顧到全面性的風險，每項資安工作都是建立在風險管理之上。



圖為2009資訊安全趨勢論壇現場，與會者正專注聆聽演講。

圖為2009資訊安全趨勢論壇現場，與會者正專注聆聽演講。

知覺。Juniper香港暨台灣區技術總監游源濱認為，如果企業不能及時消除威脅，主動去隔離、去除掉惡意程式，之後再去補救，通常都已經來不及。他認為如今企業面臨到的4大挑戰分別是動態安全、擴充性與效能、透視度與控制性和協力合作。也因此他認為機動式威脅管理方案，才能防範不斷變化的網路威脅。

Novell台灣產品經理李逸凡談到的則是「資訊安全視覺化趨勢」，透過視覺化的資安報表來解讀威脅，例如說，當報表的時間單位區間為每8小時的時候，曲線或許看起來平淡無奇，安全無虞。但一旦將時間區間縮小至每2分鐘時，卻可清楚看見報表上的曲線開始變得時有起伏，而能解讀出細微卻不

尋常的威脅活動正在產生。然而對大多數的企業來說，尤其是多數委外的企業，往往會得到一大堆的報表，卻不能正確的解讀，則該些資安管理設備便將形同虛設。

趨勢科技技術顧問黃源慶則提到，如今的主流威脅型態來自網頁，而一般資安廠商的作法可能是頻繁更新或採用更大的病毒碼檔案，但其實可運用雲端運算技術，將龐大病毒碼放在雲端，在信譽評等的技術支援下，再搭配威脅關聯性分析、使用者回報機制等，達到多層次防禦。而針對防制資料外洩DLP議題，他提到根據2006年Ponemon Institute的研究報告，78%資料外洩來自於經過授權的內部使用者，而他也認為可透過類似資料指紋的技術進行內

容辨識，不需要加解密因此也不會降低效能。

輪番上陣 剖析最新威脅

下午場的內容同樣精彩可期。Web要防範的安全議題廣泛，駭客不斷衍生的新手法包括SQL Injection、點閱綁架(clickjacking)，再透過電子郵件、部落格等方式作為攻擊媒介，使廣大使用者受騙上當；為此，美商8e6科技資深顧問呂守箴帶來的「網路陷阱無所不在，Web內容安全防护面面觀」，便於會中介紹web入侵的腳本攻擊工具Webshell，並在現場示範如何將木馬程式放置在跳板網址主機上，使網頁入侵的過程；面對倍增的網頁威脅，其推出產品R 3000與Enterprise Reporter(ER)，可記錄上網行為並提供詳細的線上網路分析及企業網路系統潛在的風險報表，做到網路安全及資源的有效運用。

接著，達友科技的技術顧問陳逸倫發表「IP大混戰！敵我分不清？認證型IPAM/DHCP建構具有身分識別能力的網路環境」，探討在網路存取控制(NAC, Network Access Control)議題漸流行之際，如何讓合法授權的使用者取得網路資源的存取權力。陳逸倫對此指出，Infoblox網路服務設備提供認證式的DHCP服務，將DNS、IPAM、RADIUS、TFTP等功能整合，集中管理，並具有強大的分散式資料庫技術，可達到企業網路的連接控管，協助企業網路進行認證式網路管理，再透過網路身分識別服務，更加強化企業網路存取安控能力。」Fortinet資深技術顧問劉乙帶來的「你的資料庫安全嗎？Fortinet打造固若金湯資料庫」，由於企業資料庫內含有身分證字號、人事薪資等大量敏感資訊，常成為駭客鎖定的目標，根據調查，美國每10家公司就有1家歷經過資料庫破壞，過去3年，資料偷竊成長更超過60%，資料庫安全影響甚大，因此需要偵測工具，避免資

料受到傷害。Fortinet的資料庫弱點評估安全設備FortiDB-1000B，便有其偵測功能，除了能遵循相關法規，並能支援不同的資料庫，每一設備更可同時支援達30個資料庫，藉由找出資料庫易受攻擊的弱點，警告系統管理員潛在的威脅，並給予修正的建議，以防止個人專屬資料遭竊取。

據統計，「垃圾郵件、員工非法授權行為及沒有遵循法規」為2008亞太區重大資安威脅的前3名，電子郵件安全性逐漸被重視，因此，Openfind產品經理張世鋒探討「訊息即戰力！郵件安全稽核歸檔的應用趨勢」，面對電子郵件及風險日增之趨勢，提出一系列的郵件安全稽核解決方案，灌輸與會者電子郵件需長期保存，並有一標準作業流程，便日後進行適當的調查動作。優碩資訊產品經理陳品翰提出「面對資料外洩新威脅，別用全面防堵舊思維」，以往防止資料外洩的產品是將資料流通的管道鎖住，針對設備做全面性控管，但卻造成使用者不便，其DRM產品係針對檔案做權限控管，做到文件到哪，保護到哪的機制，讓方便與安全兼顧。

最後，由中華民國電腦稽核協會秘書長徐敏玲，分享「資訊治理的重要性」；IT治理在企業營運中扮演著重要角色，如何運用完善的IT管理策略為公司創造最高價值，是管理階層的重大課題；徐敏玲在會中從IT治理的影響力及如何管理等各個層面，告訴與會者IT治理的重要性。

結論

2009年資安趨勢論壇雖告一段落，然而資安人員所被授與的艱鉅任務才正要揭開序幕。未來一年，除要對抗有增無減的資安威脅，還要面對因全球不景氣所造成資安預算縮減等種種挑戰，這些難題，再再都考驗著專業資安人員的智慧與應變力。