掌握雲端時代，企業資安新關鍵

國泰世華銀行營運長章光祖：

個資法與APT將是金融業的兩大挑戰

「新版個資法與日益猖獗的APT攻擊，可說是金融業今年的內憂外患！」國泰世華銀行營運長章光祖解釋，客戶資料是金融業的資產，以往尚未實施新版個資法前，對於保護個資已不遺餘力；但資料處理很難避免外洩發生，倘若真發生事故，新版個資法很重視業者是否有善盡管理人的責任，也就是到底是否缺乏適當管理才造成憾事。再加上金融業因為握有龐大個人資料，本來就屬於駭客眼中攻擊目標，因此防止資料外洩，變成金融業最關注的資安課題。

章光祖笑著說，在七十、八十年代時，常可以看到銀行報表被中式早餐業者拿來包油條，這其實就是資料外洩了，但當時個資並未被視為有價值，因此不受重視；隨著資訊系統從封閉式走向開放，網路的興起、雲端計算的運用等，當資料取得更加容易，且駭客更加猖獗，使得保護資料避免外流更刻不容緩。

保護資料避免外洩 要從企業作業流程做起

「個人資料保護與資訊安全的工作不僅關係到IT部門，還牽涉到其他業務單位，因此不能視為資訊議題，而必須要從企業整體的流程開始檢視。」章光祖認為，保護資料外洩必須要從整體的作業流程著手做起，而不是單靠某一個防毒軟體、應用程式或系統就可以保護，雖然資安業者可提供客製化的產品，但光靠買配備來增強戰力是不夠的，必須從強健體魄做起，先檢視自己目前的身體狀況，再來練身體，當身體練好了，自然就不怕外來的威脅。因此國泰世華在資料防衛戰的作法，首先就是進行ISO 27001:2005資訊安全管理制度(Information Security Management System)的認證，藉由在認證過程當中，檢視企業作業流程，是否有達成「機密性」、「完整性」、「可用性」的資訊安全管理目標。

當取得ISO 27001資安認證後，國泰世華進一步聘請外部資安顧問團隊針對個資法的規範與資訊系統的因應，作進一步的資安設備投資，優先導入個人資料含量最高的客服中心、存匯系統以及信用卡中心等三大部門。

資安設備加上資安教育 才能打造完善的防護力

「資安防護無法做到100%！」章光祖解釋，資安投資永無止盡，儘管今年花費大量投資預防做到90%的防護，但隨著新科技的興起再加上駭客魔高一丈的侵略行動，事隔兩三年後，現在的資安防禦能力就會迅速下降到五、六成，屆時又將要投資新資安設備來維持防護力。因此，資料保護除了依賴資安設備外，最重要的還是對員工進行資安教育與配合資安政策，尤其是業務單位的配合，假如第一線的業務同仁不配合，則有再好的防護也很容易引狼入室。國泰世華資訊總管理處副理陳慶儒補充，個資安全政策由IT、法務、風險管理與人資部門等籌組的委員會來制訂，訂出那些規範一定得遵守，而哪些資料非執掌同仁不能碰觸，並引進稽核進來擔任內稽，確保徹底執行個資安全政策。舉例來說，業務單位可能會查閱客戶資料，瀏覽資料庫裡的報表等使用行為，但若超過自己權限的使用範圍時，或是異常性重複查詢某些資料時，IT單位就會做Log Control Code來做資料流的控制，把重要資料與異常使用的Log檔留存下來，作一個報表分析提供給主管單位知曉，若真的發生資料外洩，至少也能快速因應與防堵。

章光祖強調，資安教育訓練是一項成本最低的卻最需要確實做的投資，國泰世華的新鮮人在新人訓練時，都會加強資安課程，此外也在e-learning國泰學習網規劃資安議題課程，透過教育訓練宣導，希望同仁可以確切落實資安政策。

三階段措施 預防APT攻擊

隨著智慧型手機與平板電腦的使用愈來愈普及，個人裝置BYOD（Bring-Your-Own-Device）盛行，行動資訊安全成為企業另一個重視的資安議題。章光祖表示，目前國泰世華並未限制同仁使用個人裝置，如智慧型手機或平板電腦等，但私人的設備無法連到企業內部網路，也無法讀取公司郵件，確保公司資訊不會透過私人裝置流到外部。此外，除了有業務需要外，基於安全的考量，國泰世華也不開放員工使用社交網絡，以免提供駭客攻擊的跳板。

章光祖說，去年繼日本Sony遭到駭客APT進階持續性滲透攻擊（Advanced Persistent Threat），造成數百萬客戶資料外洩，因此對於APT議題也相當重視。國泰世華資訊總管理處襄理賴彥廷解釋，APT的防護共分成事前、事中與事後三階段作法。由於在APT的入侵管道中，電子郵件通常是攻擊的最佳點，最常見的方式就是冒名發寄送以假亂真的郵件，並夾帶惡意程式檔，因此當外部郵件有夾帶執行檔或是可疑的文件檔，事前在系統端一律會被過濾機制擋下來。若在事前無法即時攔截下來的惡意程式，則在事中持續監測威脅擋下；若不幸到事後發生入侵時，也能儘速修復漏洞恢復系統穩定。

「商譽是無價的，也是企業最重要的資產。」章光祖強調，面對個資法的實施，正是企業檢視資訊安全系統的最佳時機。資訊安全保護不只是技術層面，而是經營者的體認以及同仁能否確切遵守資安政策。若是管理者瞭解個資保護與企業營運息息相關時，一定會投資足夠資源與心力做到滴水不漏的資安防護。

趨勢科技專家觀點

現今企業面對資訊安全主要有兩大層面，其內憂指的是即將上路的新版個資法，企業如何保護客戶個資不外洩；至於外患就是日益猖獗的APT攻擊。APT攻擊之所以難以防範，主要是APT是一種計畫縝密且具有長期目標的攻擊活動，具有低調、持續性、與潛伏期長等特性，因而很容易躲過一般的資安防護。以往的防護方式主要是透過管控邊界網路(Gateway)和用戶端(Client)；但這並不足以防止APT所構成的全方位威脅。面對APT，趨勢科技建議，企業首先要評估當前的暴險程度，以及對抗APT攻擊情境與防禦能力；接下來，再提升關鍵安全控管措施與流程藉此強化偵測、矯正與事件應變能力。最後則是主動減少漏洞以縮小攻擊面。

想了解更多APT的防護之道，請至http://www.trendmicro.com.tw/apt/tw/