IDC
Analyze the Future

INSIGHT

從勾稽追蹤到完全舉證：台灣金融業的「智能資安」之路

Peipei Wu

贊助商：NETIQ

IDC 觀點

在大環境不確定性升高、全球經營情勢快速變化以及各國資安法規頻頻修訂的趨勢下，企業面臨的法律責任不斷擴張，各類 IT 環境與相關風險也日益複雜。這迫使台灣的金融機構，就像其他亞太國家一樣，在顧及成本考量與提高安全性的前提下，必須轉向更聰明的智能安全解決方案，來改善他們的操作管理，使組織的資訊安全更有效落實。

IDC 最近與台灣金融機構的對話，幫助我們進一步了解近幾年來金融業評估遵法成本以及企業經營衝擊等方面的挑戰。就新版「個人資料保護法」(個資新法)要求的告知義務、資料保護與證據留存等三大重點來看，台灣金融機構在前兩項的準備已相對完善。但對於經常需要徵信資料處理交換服務的銀行、保險公司，以及每日互通大量個資的證券商、金融資料供應商乃至證券交易所而言，使用紀錄的深度、軌跡資料的規則建立與呈堂分析(forensic analysis)等證據留存的處理措施，將會是短期未來的最大挑戰與首要任務。這與 IDC 最近進行的 2012 台灣 CIO 調查結果不謀而合：超過七成(72.9%)以上的台灣企業認爲，未來一到兩年內最重要的資安課題，就是規劃與部署具有自動改善(automatic improvement)、流程一致性(process consistency)與智能資安(intelligent security)等功能的安全和弱點管理 (Security and Vulnerability Management, SVM) 。

本文首先將描述台灣金融機構目前所面臨的各種挑戰與需求概況，再說明 SVM 市場的最新發展，並爲金融業提供有關「注意事項」的指導意見。以下是本文的相關要點：

- 過去台灣的金融機構主要是以控制和法規遵循導向來執行相關的資安專案。隨著金融機構越來越依賴資訊系統的運作，以及政府不斷修訂相關法規，資訊安全管理的健全性已經成爲同業競爭的重要籌碼。
- 企業在資安管理實作措施上遭遇到的挑戰，連動了 SVM 市場近兩年來的快速成長。企業必須在顧及成本以及業務衝擊的前提下，考量安全管理的機制；SVM 則爲企業提供成本效益更高的風險管理，並能自動化評估合規活動的上升成本。
- SVM 業者若希望市場持續擴張成長，必須持續朝智能資安的方向努力。
- 在個資新法正式上路的這個時機，金融機構應該給 IT 更大的發揮與更高的自主權，將安全管理深根於整體的營運環境，並進一步引導企業創新。

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

Filing Information: November 2012, IDC #undefined
: Insight

關於本文

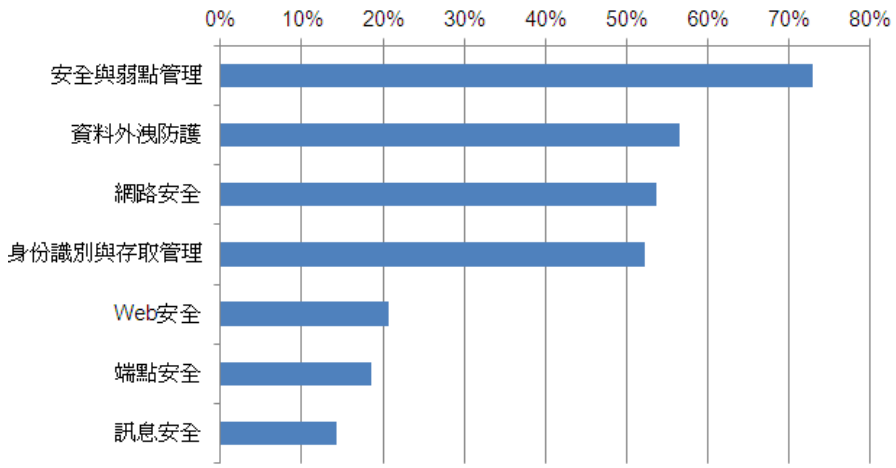
近幾年來，有鑑於數位資料流失、企業聲譽風險和國家安全威脅的迅速擴大，亞太地區的許多國家都開始(或重新)制定法律與法規，以建立(或加強)資料保護和以產業爲主的資訊安全標準。台灣也不例外。個資新法 於 2010 年 4 月底立法院三讀通過後，2012 年 10 月終於正式上路。個資新法的規範對象不分產業，公家機關或私人企業；但由於金融業向來都是高度控管的行業，因應腳步相對較快，態度也相對嚴謹與積極。儘管如此，有關金融機構因應措施遭遇瓶頸，認爲新法過於嚴苛或難以落實的批評，仍然時有所聞。本文描述台灣金融機構面臨行政院金融監督管理委員會(金管會)提出的勾稽追蹤與定期查核，以及個資新法規範的使用紀錄與證據留存等要求，在實作層面所遭遇的各種挑戰。透過 IDC 最新一期的 SVM 市場分析報告，提供建議給相關業者，並幫助金融機構評估與策略發展的參考。

市場現況概述

根據 IDC 2012 台灣 CIO 調查結果顯示，超過七成(72.9%)以上的台灣企業認爲，未來一到兩年內最重要的資安課題，就是規劃與部署「安全與弱點管理(SVM)」。台灣企業賦予 SVM 的重要性比重，相較於其次的資料外洩防護(Data Loss Prevention, DLP)、網路安全(Network Security)以及身分識別與存取管理(Identity & Access Management, IAM)，有 15-20%的差距。(見圖一)

圖 1

台灣 2012-2013 最重要的資安課題 (依「前三大」列舉統計)



N = 140

Source: IDC, 2012

這個結果與過去幾年有明顯的差異(2010 年與 2011 年台灣最重要的資安課題分別是網路安全以及身分識別與存取管理)。改變的原因與主要的驅動力，其實都與這幾年的技術和產業發展息息相關。

挑戰

相較於各大產業，台灣金融機構向來面臨較多金管會法令規範，上市櫃企業受證交所稽核或與美國企業有業務往來者，則須配合一定的安全等級。自 2008 年起，包括網路商店在內，凡接受信用卡刷卡付費的組織，都必須符合「支付卡產業資料安全標準(Payment Card Industry Data Security Standard, PCI DSS)」。適用對象包括發卡銀行以及接受信用卡付款的商店。尤其每年的刷卡交易達 6 百萬筆以上者，還須接受經由認可的第三方單位稽核與安全檢測。爲了符合這些規定與通過檢測，台灣金融機構從 2008-2011 年間積極部署與強化各類網路安全以及帳號整合管理工作。其中，包括中國信託、台新銀行、第一銀行、華南銀行與土地銀行等超過 15 家大型金融機構，皆陸續分階段採用 NetIQ/Novell 的 Identity 和 Security 相關解決方案，來進行各系統間身分和資安稽核的整合性管理，在台灣金融業界的採用率第一。

然而，除了帳號整合管理之外，依照個資新法的規範，經由各項程序所產生的任何形式記錄，企業皆需妥善保存，以利日後舉證之用。此外，金管會更要求金融機構在許多業務的處理程序上，須符合稽核與日誌管理驗證或關聯性舉證等勾稽追蹤。這意味著金融機構要將動輒數千台以上伺服器與網路設備所執行的各種應用系統、資料庫、作業平台、流量監控等，在運作或存取過程中所產生的日誌紀錄，統一收集管理並進行足以舉證「沒有外洩客戶個資，或已善盡保管責任」的呈堂分析報告。對企業來說，這在具體實作措施層面，還涉及幾項挑戰：

- 首先，企業的網路、應用程式、資料庫、伺服器等產出的日誌紀錄，在時間上是否同步？在格式或欄位上是否能互相參照對應？舉例來說，側錄網路封包所產出的時間格式，往往無法與應用系統日誌紀錄中時間欄位的資料相互參照。

- 其次，目前大型金融機構一般會有數千台伺服器執行上百種的應用系統，要如何決定收集對象的優先順序？一但收集之後，如何制定異常的關聯性分析規則？

- 最重要的是，針對關鍵任務系統進行大量的使用紀錄，勢必造成業務營運上的衝擊，這又要如何評估？

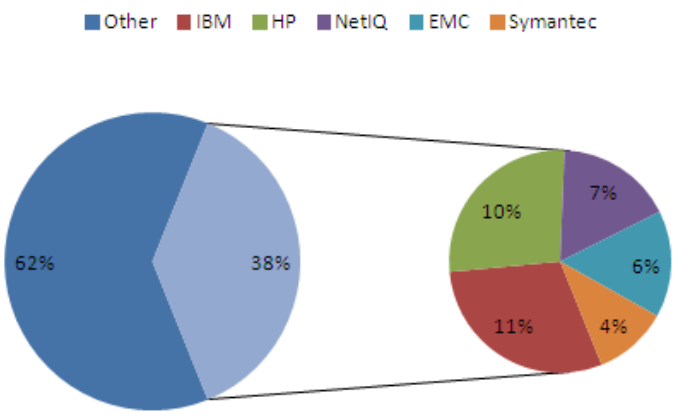
台灣的金融機構明白企業內的系統、儲存運作、網路連接與端點等基礎架構以及應用系統都需要有一定程度的安全管控。最理想的狀況，是安全管理的機制與所有的基礎架構和應用系統完善整合；但這必須顧及成本考量以及業務衝擊。這就是 SVM 近來受到企業青睞的最重要背景。SVM 在符合風險管理目標方面扮演非常關鍵的角色，因爲它提供了資安政策與法規的背景脈絡(context)、弱點資訊與補救措施，爲企業的風險管理呈現出全貌性的觀點。SVM 爲企業提供成本效益更高的風險管理，並能自動化評估合規活動的上升成本。它可以簡化管理多個安全解決方案的複雜性，同時提升自動化、效率以及主動(proactive)保護。

解決方案

從供應商來看，SVM 市場中的業者目前呈現極端多樣化的風貌。根據 IDC 最近出版的全球 SVM 市場報告，2011 年有超過 40 家以上的知名廠商銷售具有安全管理與弱點評估的各類工具，功能上包括有安全智能與事件管理(Security Intelligence and Event management, SIEM)、主動式端點風險管理(Proactive Endpoint Risk Management, PERM)、鑑識與事件調查、政策與發規遵循、安全裝置系統管理(Security Device System management, SDSM) 、裝置弱點評估以及應用系統掃描等，但只有市佔約 38%的前五大的業者能夠提供較完整的 SVM 解決方案。(見圖二)

圖 2

全球 2011 年 SVM 市場營收前五大業者市佔率

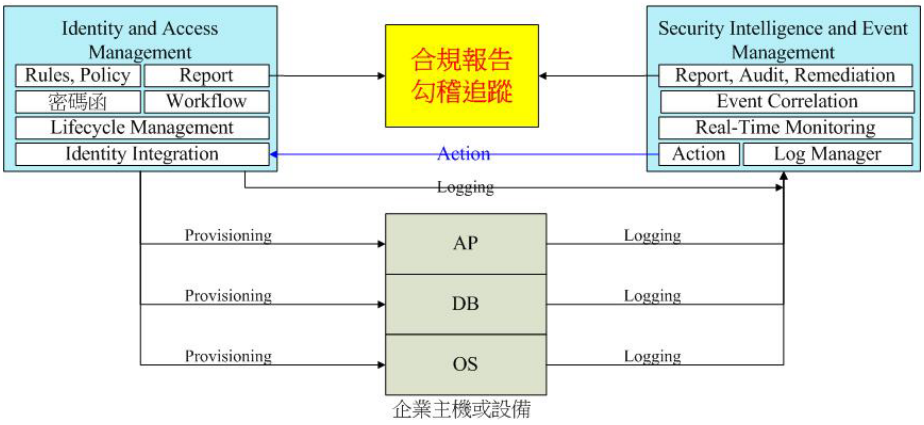


Source: IDC, 2012

其中，前三名的 IBM、HP 與 NetIQ 都是在這幾年內因購併而快速擴大市場。排名第一的 IBM 於去年 10 月買下 Q1 Lab 並於今年年初正式成立資安系統部門之後，在美國先行推出 QRadar Security Intelligence Platform 作爲這塊市場的主力產品，台灣目前尚處於培訓人才與市場宣導初期。第二名的 HP 是在 2010 年 10 月完成對 ArcSight 的收購，目前全球正在進行企業安全產品(Enterprise Security Product, ESP)組織與軟體事業群的整合。而排名第三大的 NetIQ，去年 Attachmate 集團將 Novell 與 NetIQ 的產品線整合，其獨到的身分追蹤技術更能爲企業達成勾稽和智能資安的目標。一個典型的 IAM 和 SIEM 整合的智能資安架構(見圖三)，能有效幫助企業執行標準化的基礎架構與跨平台網路間的身分安全與稽核管理，產生完整的呈堂分析報告。

圖 3

NetIQ 智能資安架構示意圖



Source: NetIQ, 2012

此外，NetIQ 對於產品的在地建置經驗、熟悉程度與支援能力較爲豐富，是所有廠商之最。這對期望順利建置上線，有效發揮產品最大效用的台灣金融業客戶來說，不失爲重要考量因素之一。

目前大多數的 SVM 業者都針對現有的安全管理產品，致力於加強更全面性功能。在這一領域取得成功的關鍵，將是提供主動安全保護的能力，以及提供全面性安全評估資料的知識與智能。

展望未來

IDC 認爲，廠商應該開發新一代的工具，來整合事件紀錄，有效排序事件嚴重性，區隔安全違規與誤報，以及從不同地點、裝置與製造商匯集安全事件等功能。此外，全面性的資安管理架構必須考慮資安政策、法規遵循以及風險管理，並且將資安弱點視爲其中一部分。SVM 解決方案應該讓企業理解到資安弱點是一個問題，它的風險等級以及應該如何修復的方式。SVM 業者若希望市場持續擴張成長，必須持續朝智能資安的方向努力。這包括提供適當的政策管理以自動執行安全政策，這點 PERM 以及 SIEM 市場都會是發展趨勢。特別是在 SIEM 領域，企業必須爲不斷增加的安全資料尋求更有效的處理方式，在其中取得關鍵性的資訊，將智能置於適當的脈絡中。SIEM 對於提供稽核資訊以及確保安全技術的有效利用來說，是非常重要的。此外，能夠提供即時滲透測試 (penetration testing)，精確發現資安缺陷的解決方案，也將受到企業的歡迎。

給金融機構的建議

IDC 這些年來與各國的金融機構進行對話，發現大多數金融機構都同意，追求高獲利的前提，必須要有完善的風險管控與良好的客戶資料管理機制。我們認爲，在個資新法正式上路的這個時機，應該給企業 IT 更大的發揮與更高的自主權，以維護及提升企業安全管理機制的健全性，確認資訊安全在企業整體的運作環境裡扮演者不可或缺的角色，是企業永續經營的根基之一。

- 我們預見在未來以客戶導向的經營，以及以使用者爲中心的終端運算時代，企業的工作環境要能夠安全運作，必須加強資安政策的制定、安全流程與功能自動化以及支援流程等層面的改善。

- 資安爲企業運作的一個環結，資訊總處除了選擇合適的資安解決方案之外，應該扮演監督與落實資安政策與治理的執行中心。

- 企業可以考慮從法規遵循導向轉爲策略導向，以主動性的保護來落實資安。將安全管理深根於整體的營運環境，並進一步引導企業創新。

- 資安的風險考量是企業創新的一大阻力，並且可能連動降低員工生產力。然而明確的資安政策落實，可以讓企業創新與生產力凌駕在較低風險的環境中運行。

- 資安流程改造、智能安全的部署以及新的資安服務團隊的成立都有賴於整個企業組織的支持。這必須取得高階主管的堅定承諾，以確保這些步驟不僅僅是 IT 部門的提議，而能成爲一場全民運動。

Copyright Notice