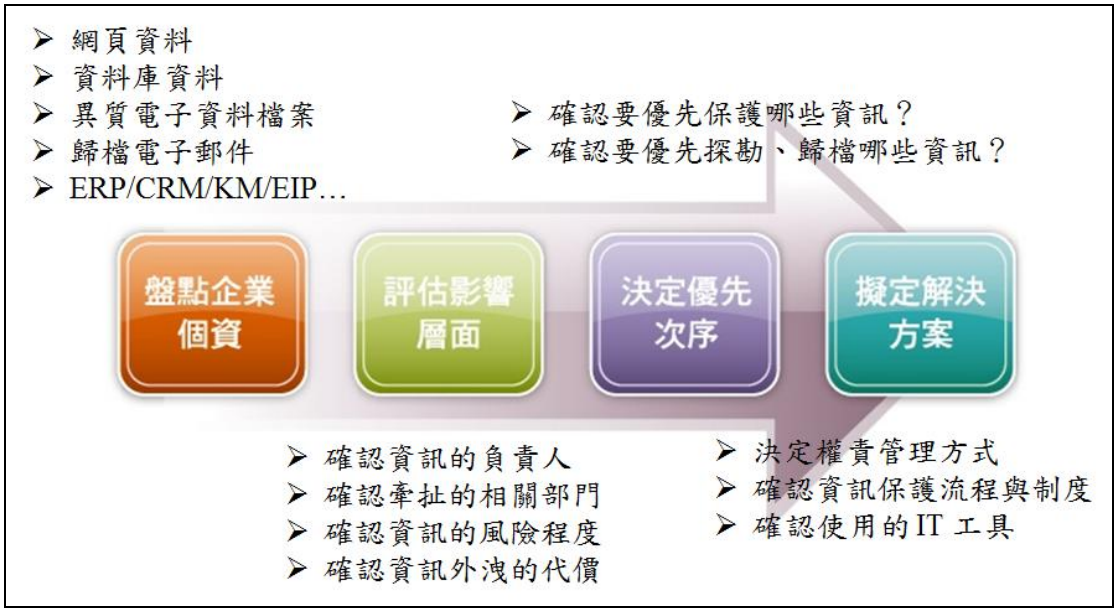
個資法準備上路了，到底我該做什麼？

Peter Liao

新版個人資料保護法的施行細則，已於今年六月底送交行政院審查，預計在近期即將完成審閱。由於新版個資法規定，未來不論企業規模大小、個資數量多寡，都受到新版個資法嚴格規範，加上舉證責任倒置，企業必須負起證明企業本身無過失及盡善良管理的舉證責任，這部以「優先保護個資來源者」為思維導向的法典，不但在國內引起震撼，更帶來一連串資安產品的吹捧效應潮。

發展已久但沈寂多時的各式各樣 DRM、DLP、NAC、Log Analyze 產品，開始以「雨後春筍」的曝光風格瘋狂露出，以一副「只要買了我，你就可以搞定個資法」的態度行走江湖。事實上這是一個個資防護的繆思，到底僅做好外洩這件事，是否就能防範個資外洩的威脅呢？在問這一個問題之前，其實應該先思考，既然要防止外洩，那麼，我們要防止什麼資訊外洩？如果說我們連要防止外洩的目標都不清楚，那麼購置了 DRM、DLP 等產品的個資防護政策執行部門，又要從何防起？

因此，企業面對個人資料保護法的第一步，即為個資盤點，也是企業進行個人資料外洩風險防範的第一步。唯有透過個資盤點，清楚發掘並標定個資的所在，才能識別個人資料的擁有者、資料流、影響程度以及相關牽涉部門，並進行後續的評估、保護計畫，並擬定相關的對應策略，才能精準地因應個資外洩、官司纏身的風險，並讓後續因應保護政策而使用的外洩防護工具發揮最大的防護效用。



【企業個資盤點與防護解決方案流程圖】

透過安全度量，確認個資風險所在

透過個資盤點產出個資探勘資料報表的過程，不但可以發掘企業過去歷史資料中潛藏的個人資料（風險所在），同時也可以透過盤點網站、電子檔案、資料庫、歸檔封存郵件等電子化資訊的過程，理解企業資料的資料流程（Data Flow Diagram），進一步釐清資訊的負責人、牽扯相關部門、風險程度以及如果這些個人資料外洩了，公司會付出多少有形以及無形的代價？擁有這樣完整、清晰的個資盤點分析報告，也有助於負責個資防護策略的專人或小組，在公司內以有系統且量化的數據，將個資防護的議題擴大討論，並提昇討論階層至營運階級主管（CEO、CFO、CTO）的程度，更進一步有效率的以 PDCA 的精神，從上而下地訂定個資保護框架，並且確認該保護計畫獲得公司有效的資源支持以達到有效執行的目標。

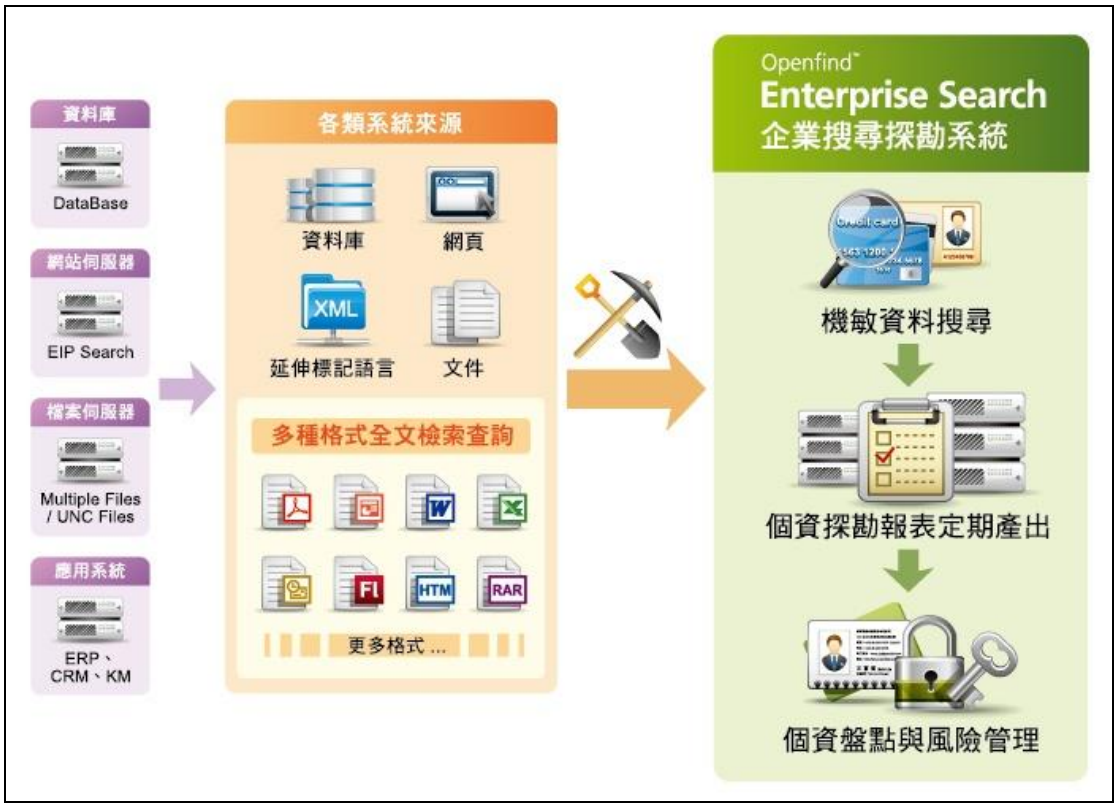
針對 IT 工具，做法律導向的個資防護設定

大部分的 DRM、DLP、NAC、Log Analyze 產品，是屬於 IT 工具的範疇，也是個資保護流程的最後一環，以規劃和採購的 Timeline 而言，這是最後一件需要執行，而且僅是需求導向的執行事項。因此，不是昂貴的 IT 工具投資就能解決個資防護的問題。透過個資盤點確認防護需求的過程，就有能力選擇符合不同個案對個資防護需求的 IT 工具，並且針對外洩防護和舉證做法律導向的思考防護設定策略，也就是以阻斷外洩資訊的「不當事實、資料」、「行為資訊」、「當事人」、「損害因果關係」，作為基礎的外洩偵測或個人資料遮蔽設定原則。如此，才能真正有效降低個資外洩，進而引起官司成立的風險。

法務、IT、稽核，到底誰要來做？

在個資防護策略的擬定和進行中，每個人都應了解，個資防護不僅是 IT 議題，更是一個法律上的問題，但僅由法務部門進行組織內的推動角色，對於今日 e 化程度極高的企業或組織而言，則是不切實際的想法。個資防護是一個跨部門的重要議題，必須具備明確的主管組織、完整的個資盤點、好的資訊保護框架、IT 工具，才能落實執行力。而 IT 部門的重點任務則為盤點、歸檔、報表、警示、舉證，而非背負洩漏責任，應當讓權責和管理行動，落在個人資料擁有者與使用者(部門)身上，才能有效的將個資防護變成全體共同議題。而回歸個資防護計畫的原始出發點，這一切都必須仰賴個資盤點後的分析報告，以有力的證據和事實來作為驅動的原點，由此可見個資盤點對於個資保護計畫的重要性。

OES 3.0 SP2 協助企業進行個資盤點！



【OES 3.0SP2 個資盤點解決方案示意圖】

OES 3.0 Service Pack 2 (SP2)，可協助企業針對常見的異質資料源如資料庫、文件、網頁（網站）、檔案伺服器等進行個資盤點，產出個資探勘報表，方便個資權責單位擬定後續的個資保護計畫，以預防更勝於治療的態度，將個資法的衝擊降至最低。有別於 OES 3.0 SP1 的既有功能，新版本 SP2 在個資檢測部份，支援各式英數字及中文的資料形式，並預設內建了身份證字號、信用卡號、手機號碼、家用住址、Email、家用電話及生日等七種探勘規則，可協助企業有效率的篩選出具有特定格式的個人機敏資料。管理者也可自行設定符合公司內部政策的個資探勘規則，定期在系統中查找出機敏資料與回報，並利用探勘後產生的個資盤點報表，有效並立即制定大量的機敏個資保護政策，避免公司員工可以任意讀取，有效的抵制外洩風險。

回顧近年來層出不窮的個人資料外洩事件，不僅嚴重影響社會治安，更重創企業商譽，而隨著個資法的施行細則即將公布，未來在資料搜尋的安全防護上，也必須從被動發現轉為主動檢測，若缺乏縝密的安全管理，容易使企業內部重要的內容資產曝光。OES 3.0 SP2 獨有的特徵值比對技術，可協助企業探勘出任何隱含個人資料的異質資料源，管理者也可即時從公共查詢結果中移除相關機敏檔案，以幫助企業完整掌握凌亂分散在各伺服器與資料庫中的龐大個人資料，並有效的控管企業內的風險來源，有效達到個資外洩的主動預防，真正做到防範於未然。