數位化時代，企業該如何做好資料外洩防護？

The better the question. The better the answer.
The better the world works.

EY 安永
Building a better working world

前言

「葉舟瓠壺浪如屋，暗樁觸船船版折」，浪上行舟，一個暗樁便會惹得船毀貨損。外部暗樁尚可透過經驗避開而行，內部暗樁想排除難如登天，等到發現時，已如朽木一般無法補救。

現代企業便如這浪上之舟，怎知自己公司中沒有被暗樁滲透？怎知核心資訊沒有被暗樁洩露？

然而，從古至今，防範內部主動或被動洩密都不是一個容易的課題。

在數位化時代，資料成為一個企業創新與發展的核心，已無法透過枷鎖式的方式來進行管控。資料在整個產業生態中的流轉以及在新興業務場景下的使用，促使企業需要採用更靈活的方式來對資料進行管控。資料外洩防護（Data Loss Prevention, DLP）技術應運而生並且日臻成熟，在不同的產業，尤其是具備敏感的研發或客戶資料的企業中被廣泛應用。

DLP 技術日趨成熟，越來越多的安全產品包含了 DLP 功能，比如雲端存取安全代理（Cloud Access Security Broker, CASB），然而，全球企業資料外洩安全事件仍層出不窮。美國針對醫療健康保險業的 HIPPA、歐盟的 GDPR 等法規對資料安全也提出了更嚴格的要求。目前，我們看到很多企業選擇較為傳統的 DLP 工具，也看到市場上一些科技創新，如利用人工智慧進行內容識別。雖然很多企業部署 DLP，卻無法很好地發揮其效用，要麼事件累積擱置不管，要麼花費大量人力進行運維，這都與 DLP 實施的每一個環節息息相關，本次報告將針對企業部署推廣 DLP 提出一些方法和注意觀點。

資料外洩防護技術能實現什麼？

資料外洩防護是透過一定的技術手段，防止企業特定資料或資訊、資產以違反安全性原則規定的形式流出企業的一種策略。

對很多新興科技企業而言，研發部門往往是企業的核心部門，掌握著大量敏感性資料。關於企業內部洩密有很多大家耳熟能詳的例子：

- 研發工程師在離職前，將核心技術原始程式碼下載至個人電腦，並加入競爭對手公司或創立自己的公司
- 自主設計的產品資訊被發現在黑市交易，例如，原始程式碼、設計圖、技術規範等
- 企業員工將高敏感度的公司資訊（如企業策略、行銷計畫、研發產品資訊等）上傳至公共論壇或社交網站上

以上例子只是資料洩露的冰山一角，資料外洩防護對於很多企業來說至關重要，並且能夠直接為企業停止損失。傳統的 DLP 系統可以在資料儲存和傳輸過程中進行即時掃描，識別這些資料是否違反現有策略規則，進而對資料外洩事件進行稽核、隔離可疑檔案、加密資料或直接阻攔傳輸。

DLP 實施前要提前做好什麼工作？

為了更精準地保護企業的敏感性資料，提升 DLP 後續運維的效率，在實施 DLP 專案之前，有幾件需要提前做好的工作：

- 資料分類分級：

  企業需要針對自身所持有的資料進行分類分級，而後對特定等級的資料進行 DLP 策略的實施。如：企業將資料分級為絕對機密、機密、內部、公開四個等級，並僅針對絕對機密和機密資料實施外洩防護。某些產業可能有專門針對資料分類分級的政策規定或指導，企業可根據國家規定、產業實際做法進行相應的資料分類分級工作。

- 人員角色和職務權責定義：

  一般情況下 DLP 產品會讀取企業的 AD（Active Directory）網域資訊來進行管控，如果企業實施精細化管理，AD 網域的準確性將會是一個影響 DLP 管理效果的重要因素，否則企業人工維護人員資訊需要投入的人力成本將會非常高。

- 內部溝通：

  由於有很多企業會部署終端 DLP，這將需要在員工電腦上安裝軟體並且可能會影響到員工的日常操作流程，管理層的重視與支持，由上而下進行推廣，對於一個 DLP 專案的成功實施相當重要。同時實施過程中的資料識別、運維階段的事件處理，都離不開業務部門的支援，這都需要在實施前進行充分的溝通。

DLP 實施應從哪些技術層面進行考量？

目前市場上使用比較多的 DLP 類型有終端 DLP、網路型 DLP 以及郵件 DLP。

- 終端 DLP 會監控終端的資料使用行為，這也是目前應用範圍最廣的 DLP 類型。即使設備在離線狀態，只要策略已經在終端生效，也會實施相應的管控措施。
- 網路型 DLP 一般是放在企業內網出口位置，可以對發送的資訊做第二道審核。同時有些產品為了減輕終端壓力，圖像識別功能（如掃描的圖片、截圖或非文字轉換為 PDF 的文檔）也是放在網路型 DLP 中。
- 郵件 DLP 一般是部署在郵件伺服器上，對於郵件發放進行審核。有的企業電子郵件是在外網可以登入的，此種方式可以減少這種由外網登入企業電子郵件發送資料而產生資料洩露的風險。

DLP 策略是整個實施過程的核心，策略的準確性和覆蓋性會直接影響到 DLP 專案的成敗，可以分為四個面向來進行考慮，分別為：資料的識別規則、策略生效的範圍、安全應對策略和資料傳輸方式。

- 資料的識別規則：
  針對特定密級文檔的識別，也就是需要保護的物件。一般類型的文檔可以使用關鍵字、建立字典或者使用規則運算式等方法來識別，一些特殊的檔案需要針對檔案類型來做相應的識別方法，如 CAD 等圖檔。大部分 DLP 產品中會自帶一些可一鍵使用的識別方式，如身分證字號、個人簡歷、原始程式碼等等，由於這些通用性的策略沒有根據企業實際情況進行客制化，因此必須在調整過程中逐步進行優化。

- 策略生效的範圍：
  指策略生效的終端（人員）。理論上來說，所有策略都需要發出給企業內部所有終端，但某些更加嚴格的策略會需要針對特定群組的員工實施，亦或是有些企業的研發環境與辦公網路環境是隔離的，某些機密檔案的策略只需要針對該部門的員工終端實施。

- 安全應對策略：
  指針對這項策略實施怎樣的應對方式，如稽核、阻攔等等。一般在策略生效之初的優化階段，只會私下對事件先進行稽核以免影響合理的業務往來。當誤報量達到可接受的範圍內時，企業會根據自身需要調整策略，進行發送確認或者阻攔等方式。

- 資料傳輸方式：
  指該類型檔案被允許的傳輸管道，如電子郵件、USB、網路雲端等。企業需要針對每個類型的檔案有清楚的傳輸管道定義，如某機密檔只可以透過內部郵件信箱發送，其餘管道都需要阻攔等。

當然還有其他一些面向，如針對時間進行設置、企業可根據自身要求和產品功能進行相關策略的配置。

從人員及管理方面，應當進行哪些工作來保證 DLP 的有效性？

一、當 DLP 投入正式運維後，需要有一定的組織和人員來保障持續營運，方能及時發現和處理資料外洩事件

一般情況下，除了安全團隊，企業內部還需要以下幾個團隊：

- DLP 運維團隊：
  DLP 運維團隊的所屬部門一般依企業實際情況而有所不同。DLP 系統後臺管理會由基礎架構團隊或者資訊安全團隊負責，部分企業可能由法遵團隊負責，此團隊主要負責 DLP 後臺的運維，諸如後臺帳號建立、事件、日誌審閱等。

- 應急回應團隊：
  此團隊主要工作是在發生資訊安全事件時，進行相關的資料洩露事件回應和處理。團隊成員可包括資訊安全團隊相關負責人、各業務部門相關負責人、法遵團隊負責人、人力資源團隊負責人等等。

- 基礎架構支援團隊：
  從終端 DLP 軟體的推送、網路 DLP 的部署，到伺服器資源配置等，都需要基礎架構團隊的參與，方能從技術上保障 DLP 工具的實施和運維。

- 稽核團隊：
  防範 DLP 管理過程中第二次可能發生資料外洩的事件。

二、有效建立事件審查模式方能保障資料外洩防護的持續效果

目前有三種事件審查模式比較常見：

1. 資訊安全團隊審查：
   完全由資訊安全團隊來審查 DLP 後臺事件。這種模式的優點是由資訊安全團隊專人進行事件處理，效率會比較高。但由於安全團隊人員對於業務理解度不高，可能無法判斷該業務需求是否合理，還需多次與業務部門溝通，或存在事件處理結果不恰當的情況。

2. 業務部門審查模式：
   完全由業務部門來審查 DLP 後臺事件。這種模式優點是各業務部門出於對自身業務的了解，能更加有效地判斷事件是否為真實的資訊安全事件。但是這種模式存在以下幾種缺點：
   - 業務部門調查人員可能存在包庇行為，或業務部門內部解決而不報告安全部門的情況
   - 由於 DLP 實施前期誤報可能比較多，造成業務部門調查人員積極性不高，並且當大量誤報形成時會導致潛在資訊安全事件被淹沒
   - 對調查人員本身及其主管的資訊洩漏事件可能有所缺失

3. 混合團隊審查模式：
   由資訊安全團隊和業務部門混合調查。這種模式主要可以理解為，資訊安全團隊對後臺事件先進行篩選，剔除重複或者明顯是誤報的事件，隨後將各業務部門的潛在安全事件分配給業務部門調查人員進行確認。當然，這種混合型審查模式也是有缺點的，過於依賴資訊安全團隊人員的篩選，分配事件的時間較長，事件調查的時效性會比較差。

三、相關資料外洩防護流程的建立

相對 DLP 技術產品或設備的實施，企業建立相關流程無疑可以保證各個控制節點合作運行，資料外洩防護的流程，需要與其他流程和規範相結合方能更好地執行，如資料分類分級、資料外部發送流程、安全事件回應流程等。資料外洩防護的流程中，可以包括但不限於：各部門及團隊的職責與許可

權、資料外洩防護策略變更、資料安全事件回應與處罰、資料外部發送申請等。

如何從技術方面提升 DLP 營運的效率？

不僅僅是 DLP 產品所覆蓋的環節，對特定敏感性資料和資產進行生命週期管理，將讓資料安全管理人員具有更廣、更具前瞻性的視野。

企業 DLP 在實施完成之後，對於策略以及流程的優化至關重要，能夠大幅降低人力的花費。然而，由於傳統 DLP 系統的局限性，在諸如大量事件分析及用戶操作能見度方面，仍會顯得有些不足，這可以使用某些安全資訊和事件管理（SIEM）解決方案產品，將 DLP 後臺的事件資訊導入，並制定相關規則進行分析。

此外，企業可以使用 UEBA（使用者與實體設備行為分析）的方法對大數據進行分析，對內部使用者訪問資料的數量、關係、序列進行多維度計算，形成用戶正常行為基線，並檢測出偏離正常基線的異常行為，這樣可以更加有效地減少誤報，發現真正可疑的資訊安全事件。

結語

雖然傳統 DLP 工具有一定的局限性，也有不少待解決的資料安全管理困境，但有效的策略配置、優化的管理流程和人員意識教育，很大程度上能夠幫助企業降低員工將核心資料洩露的風險，在識別、處理和回應安全事件上贏得先機。

聯繫安永

涂嘉玲
審計服務部營運長
安永聯合會計師事務所
+886 2 2757 8888 ext. 88810
Lin.Tu@tw.ey.com

劉惠雯
稅務服務部營運長
安永聯合會計師事務所
+886 2 2757 8888 ext. 88858
Heidi.Liu@tw.ey.com

何淑芬
總經理
安永財務管理諮詢服務股份有限公司
+886 2 2757 8888 ext. 88898
Audry.Ho@tw.ey.com

黃孟光
總經理
安永諮詢服務股份有限公司
+886 2 2757 8888 ext. 88867
Mengkuan.Hwang@tw.ey.com

EY 安永 | Assurance 審計 | Tax 稅務 | Transactions 交易 | Advisory 諮詢

關於安永

安永是全球領先的審計、稅務、交易和諮詢服務機構之一。我們的深刻洞察力和優質服務有助全球各地資本市場和經濟體建立信任和信心。我們致力培養傑出領導人才，通過團隊協作落實我們對所有利益相關者的堅定承諾。因此，我們在為員工、客戶及社群各界建設更美好的商業世界的過程中扮演重要角色。

EY 安永是指 Ernst & Young Global Limited 的全球組織，也可指其中一個或多個成員機構，各成員機構都是獨立的法人個體。Ernst & Young Global Limited 是英國一家擔保有限公司，並不向客戶提供服務。有關 EY 安永如何蒐集及使用個人資料，以及相關個人資料保護之權益敘述，請參考網站 ey.com/privacy。如要進一步了解，請參考 EY 安永全球的網站 ey.com。

安永台灣是指按中華民國法律登記成立的機構，包括：安永聯合會計師事務所、安永管理顧問股份有限公司、安永諮詢服務股份有限公司、安永企業管理諮詢服務股份有限公司、安永財務管理諮詢服務股份有限公司、安永圓方國際法律事務所及財團法人台北市安永文教基金會。如要進一步了解，請參考安永台灣網站 ey.com/taiwan。

APAC No. 14004820
ED None

本資料之編製僅為一般資訊目的，並非旨在成為可仰賴的會計、稅務或其他專業建議。請聯繫您的顧問以獲取具體建議。

ey.com/taiwan

加入安永 LINE@好友
掃描 QR code，獲取最新資訊