以數據存取治理改變遊戲規則

每年，組織面臨著不斷增加的駭客攻擊和其他存在的惡意威脅，其目標就是要入侵公司以獲得對其系統和數據的存取。事實上，自2013年以來，針對性攻擊幾乎倍增。雖然組織用盡心力處理風險使其運作更安全，但似乎每天都有許多新的問題出現。

這些猖獗的數據入侵給組織具風險性的非結構化數據因子帶來長久且廣泛的衝擊。但控制這些數據的存取安全實具挑戰性；若缺乏一個遊戲計畫，僅了解你如何陷入風險也不足以保護你。將數據存取治理計畫整合到身份存取管理(IAM)整體策略中更能保護你組織的安全。也就是說，誰能存取你的數據和他們用這些數據做甚麼，以此角度來管理您的數據資料。

數據洩漏的衝擊

這樣的事情似乎每天發生：又有一家公司被入侵了；它的資料被竊走了；它的秘密被揭露了，而後果可能是非常嚴峻的。當法國的Orange Telecom公司在2014年被入侵兩次，有超過180萬的客戶紀錄被竊取。姓名、電郵、地址 、電話號碼和生日都被竊走了，而這些資訊都可輕易被用來做網路釣魚詐騙。雖然想到若是你的組織被入侵就會感到非常恐懼，但要知道這些風險遠比你想像得還要普遍。

- 直接影響財務成本：或許最為人知且最為公開的事實就是數據洩漏是非常昂貴的資安攻擊事件。但這所涉及的不僅只是監管罰款和對被洩露資訊客戶的賠償。一個公司經歷資料外洩後，其責任險費率飆升200-400%是時有所聞的。
- 信任/名譽的損失：當數據洩漏發生時，新聞媒體會好幾天到現場報導，特別是當這個組織牽涉到大眾孰悉的品牌名稱時(或如Ashley Madison的例子，非常有爭議)。即使無需面對這樣的公共關係(PR)夢魘，數據洩漏可導致客戶失去信任，且大多數情況下是無法挽回的。
- 審查要求增加：發生入侵後，對公司內部及外部的審查要求大幅增加是常見的事。這樣的額外負擔可延續數年之久，因而增加管理和驗證安全控管的時間和成本。

非結構化數據是下一個戰場

只處理企業IT環境這部分已顯不足；絕無法僅對控管結構化系統存取的安全。這也不只是因為傳統的應用程式和系統易受到攻擊。握有非結構化數據的系統(電郵伺服器、檔案分享、雲端儲存應用等)必須是你整體規劃的一部分。

不同於儲存在結構化系統中的資訊 ，這些資訊可用標準的身份和存取方法來管理。非結構化數據以許多不同格式存在於不同地方，而這樣的複雜性使得對其控管和治理變得具有高度挑戰性。

企業運作安全意味著管理所有用戶經由所有應用程式對結構化及非結構化數據的存取。

了解非結構化數據的挑戰性

非結構化數據存取的安全維護對任何企業而言都是一個挑戰。這個安全作業可分為兩部分：如何控管存取，以及如何治理這些控管。

控管存取

控管存取是首要的挑戰，包括三個部分：對任何企業而言，這些數據存在於許多地方，且在建立、修改或刪除這些數據時幾乎沒有監管控制。

- 組織在許多的地方儲存其數據，且每年都有許多新增的儲存點。微軟的SharePoint、 Dropbox、Office 365、 Exchange、內聯網、檔案系統等都含有非結構化數據，且變得愈來愈難管理，因為數據不斷地累積，系統也不斷增加。這些系統存在於企業內部，也會儲存在雲端，而每個企業各自有其不同的儲存組合，使得”一體適用”的方案不可行。

- 非結構化數據是由使用者所掌控，而非IT人員。結構化系統會有數據架構師設計存取模式以保護敏感資料，但大部分的非結構化數據系統讓使用者自行建立、修改和刪除現存的資料 ，無需經過正式的核可。這情況讓使用者可大幅度掌控資料儲存於何處；但使用者在建立資料時通常不會考慮到安全風險，只希望將資料儲存於方便的地方，即使並不安全。

- 有時候，在嘗試處理上述兩個問題所產生的許多安全間隙時，IT人員所採行的存取管控模式反而增加了維護非結構化數據安全的複雜度。因為存取非結構化數據的管理通常是使用群組成員資格以簡化管理程序，而這樣的作法會對什麼人可存取敏感資料產生盲點。

治理管控

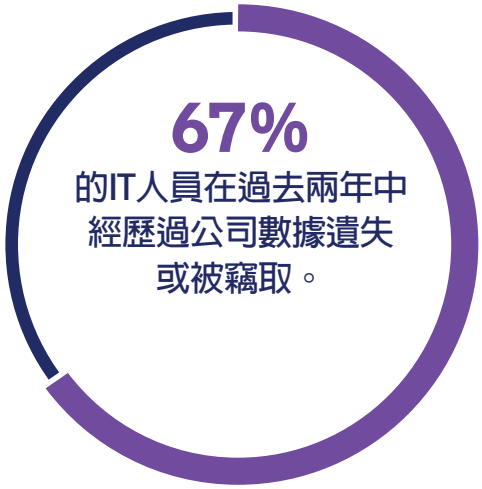
非結構化數據的第二個挑戰—治理存取管控，也有三個部分：數據存在的企業整體可見度、規律性的數據存取檢視和審查對非結構化和結構化數據的非對稱性管控。

- 在大多數組織中，甚麼樣的非結構化數據儲存在哪些地方之類的完整"圖像"根本不存在 。而這樣的數據有三個不同的資訊需要知："有哪些資料?" 、"儲存在哪裡?"、"是敏感資料嗎?"

這使得事情變得更複雜了。若無法解答這三個問題，就不可能有效的管理這些數據和管理誰能存取這些數據。

- 每個企業都需要能夠回答"誰能存取哪些數據"。雖然大多數的組織都有系統可協助回答這問題，但大多數的非結構化數據儲存於這些系統處理範圍之外。這情況使得規律性檢視員工的資料存取變得幾乎不可能。再加上企業通常不清楚資料儲存於何處，嚴重的安全風險就出現了。

- 就像非結構化數據其它面向的挑戰，要安全就需要整體的行動。當然審查亦是如此。過去幾年裏，維護非結構化數據安全的嚴重不足事件其數量大幅飆升。



將身份和存取管理(IAM)延伸到非結構化數據以改變遊戲規則

一旦了解治理非結構化數據的挑戰，你就可開始建置一個遊戲計畫來保護這類數據的安全，並確保你組織整體的安全。在今日的世界，數據是你所做每件事情之開端，即使它不是全部的面貌。人則是其它的變數。在一天結束時，你的目標是要維護你的資料安全，且讓需要的人能夠使用這些數據從事業務目標。幸運地是所有存取數據的人都可與身份結合。

連結數據和人這兩個結點的就是存取。我們在做身份治理時以可見的且完整結構化的存取模式將數據與人做連結。數據存取治理應用了相同的原理 。只有對你的數據、人和其相關存取執行了下面重要的動作後，你才能夠建置一個數據存取治理程序，並有效應用於你的組織。

數據

要實施一個強韌的數據存取治理策略，你必須以數據本身作為起點。

1. 數據在哪裡？要確保你有一切所需的資訊以建立安全系統，首先你必須知道數據存在於何處。這通常包括與數據應用程式擁有者的討論以了解他們使用甚麼類型的數據，以及他們通常將數據儲存於何處。使用工具可加速這些理程序，以掃描典型的非結構化數據之儲存位置：電郵系統、檔案分享、偕同入口網站，以及雲端應用程式，例如 Dropbox和Office 365。

2. 內容是甚麼？一旦知道數據儲存於何處，你就可以依據所含資訊種類將其歸類。這對於辨識最敏感數據的儲存位置是相當重要的，讓你能夠集中精力於最高風險的區域。智慧財產檔案、客戶/員工資訊、和其它種類的資訊代表最高的安全風險；以類別將數據歸類可使管理和改善安全較容易處理。

3. 儲存位置正確嗎？一旦知道數據在哪裡及其內容後，最後一步是決定它的儲存位置是否正確。使用者通常會將數據儲存於方便的位置，但可能是安全脆弱的地方。辨認這樣的組合是否正確是整體策略中關鍵的一環。當你將過度暴露(數據儲存於未被授權者可存取之處)與敏感數據結合，結果就是高風險的情勢。一旦數據儲存於正確的位置，管理和安全維護就容易得多了。

案例：
Sony Pictures

當Sony Pictures被入侵時，發現員工的帳號和密碼儲存在Word、PDF和Excel檔案中。 甚至在此入侵過程中，特權帳號和密碼也被曝露。因為敏感數據儲存在不安全的位置，這種毒害的組合導致比我們所見過更廣泛的洩漏，但如果這些文件當時有適當的安全維護，就不會出現此嚴重洩漏的情況。

人(即身份)

在找到數據的位置之後，將它們分類並驗證的作業就需要檢視哪些人可以存取這些數據。

1. 你的使用者是哪些人？ 就如同知道你有哪些資料一般重要，你也需了解你的使用者是哪些人。員工、承包商、供應商、業務夥伴和其他使用者都可能存取你的非結構化數據系統，且會以不同的方式來使用和存取這些數據。

2. 哪些人使用你的數據？事實上，數據管理是維護敏感數據資產安全上很重要的一部分。太多的使用者會單純地假設他們所建立的數據資料是安全的，因為這些資料都儲存在組織內的系統和應用程式上。此外，對於保護敏感資訊的存取，常見自由放任的態度，因此數據資料的儲存總以方便為考量。找出企業中誰使用這些數據是很重要的，這樣才得以變更處理程序並維護數據安全。這也是下一步驟關鍵的部分。

3. 誰是數據擁有者？除了要找出組織中誰管理數據，明確標示出這些資訊的數據擁有者也是必要的。數據擁有者變成維護和管理數據存取安全的第一道防線。因為可以感受到個人的責任，這些數據擁有者會積極確保數據儲存在正確的地方且只有適當的使用者可以存取。當然，找出這些擁有者會花一些時間，也可能會有很多挫折。利用使用者社群和"群衆外包"手法做擁有者篩選處理可大幅降低所需的時間並增加找到最適當擁有者的機率。

存取

一旦辨識出數據和人之後，就可用存取將這兩者連結。

1. 哪些人可以存取哪些數據？首先要將數據和人做配對，以決定誰可以存取甚麼數據。你必須先將重點放在最敏感的數據上。要記得，當你建立使用者模型和定義其與企業的關係時，所收集到的數據對此配對作業也會有影響。辨識出最具風險區域的確實資訊可在你處理整個非結構化數據作業時提供指引。

2. 如何授權存取？使用者如何存取數據的這類最基本問題會在組織建立存取授權時浮現。在此作業期間，許多先前討論過的挑戰都會出現。雖然此步驟是以了解存取是直接或間接的授權做為開端，但過程中可能會需要在存取模型中針對問題做修正以改進安全。

3. 如何驗證存取？計畫若無法確保其未來的成功就是不完整的計劃。清除存取許可，找到過度暴露的數據，並修復在此過程中出現的其它問題會給企業帶來極大的益處，但也會很容易讓企業掉入這處理程序中而變得不安全。建立規律性的存取檢視以及適當的存取型態和方法，以利偵測異常或不適當的行為，可保護企業抵禦潛在的安全風險。這類問題愈早被發現就可愈快速佈署降低風險的策略，並得以限制(甚至預防)數據洩漏所帶來的損害。

結論

今日組織會面對比以往更多的惡意威脅，但很幸運地，用來保護企業目前和未來資產的工具也不斷演化精進。雖然IT人員需面對一堆令人畏懼氣餒的挑戰，數據治理是保護企業血脈安全的重要部分。從整體角度了解(結構化和非結構化)數據儲存於何處、誰可存取甚麼數據、以及這些人如何使用這些數據，可幫助偵測問題、降低風險，並保護組織的安全。

未來不必是一片灰暗；將你的組織帶往好的方向移動，讓IT安全人員藉由通用的工具和處理程序來管理所有的數據存取。以所有這些數據資料作為你決策的基礎，並使用基本原則來保護你的數據。結合身份和存取管理架構，你就可確保一個更安全和穩定的企業。