2010 年度資料外洩調查報告

由 Verizon 事故調查團隊與美國特勤局合作進行的研究。

執行摘要

在某些方面，資料外洩與指紋有許多共同之處。每一個指紋都是獨一無二的，我們在分析構成每個指紋的各種形狀、線條和輪廓後，可以取得很多資訊。但是，指紋的主要價值在於可資辨識特定環境中的特定個人。從這個角度來看，大量研究指紋並不能帶來更多好處。從另一方面來說，綜合分析外洩則有很大好處；我們研究越多，越能做好充分準備來防止外洩。

美國特勤局 (USSS) 對於研究和制止資料外洩也非常感興趣，這一點也不足為奇。這是促使他們決定加入我們進行此《2010 年度資料外洩調查報告》(DBIR) 的主要原因。他們提供數百個自己的案例加入到我們的資料中，因此大幅擴大了我們所能研究的範圍。所提供的還包括兩篇來自 USSS 的附錄。一篇深入研究網上犯罪團體，另一篇則著重於有關網路犯罪的起訴。我們非常感謝他們的貢獻，並相信世界各地的組織和個人都將從中受益。

加入 Verizon 2009 年的全部案例以及 USSS 提供的資料後，DBIR 系列現已橫跨 6 年，包括 900 多個外洩事件以及超過 9 億筆洩露記錄。在這個過程中，我們瞭解到很多資訊，並且很高興有這個機會與您分享這些調查結果。和往常一樣，我們的目標是希望此報告中呈現的資料和分析能對讀者在規劃和安全性方面的努力有所助益。我們先來看看以下列出的一些要點。

誰是資料外洩的幕後黑手？

70% 源自外部間諜 (-9%)

48% 由內部人士造成 (+26%)

11% 牽涉到企業合作夥伴 (-23%)

27% 涉及多方 (-12%)

今年的報告在納入 USSS 案例後，某些地方發生一些顛覆性改變，但是並未動搖我們對全局的觀點。2009 年絕大多數的外洩以及幾乎所有被盜的資料 (98%) 主要由有組織的團體發動，仍是受害者組織以外的罪犯所為。然而，在 USSS 處理的案件中，內部人士卻是更常見的因素，因而大幅提高了資料集中此因素的數據。比起以往任何一年，今年的研究大幅增進我們對內部犯罪的認識。與企業合作夥伴有關的外洩持續減少 (在我們上一份報告中已呈現此趨勢)，並達至 2004 年以來的最低點。

在 2009 年，與內部人士相關的大部份案例中，「濫用」穩居造成外洩的威脅行動清單榜首。這並不代表「駭客入侵」和「惡意軟體」已經絕跡，這兩項仍名列第 2 位和第 3 位，並且 95% 以上的外洩資料都與其相關。過於薄弱或遭竊的身分認證資料、SQL Injection 以及會截取資料的特製惡意軟體，仍持續困擾著試圖保護資訊資產的組織。涉及使用社交手段的案例增加超過一倍，而盜竊、竄改和監視等實體攻擊也增加了不少。

外洩是如何發生的？

48% 涉及濫用權限 (+26%)

40% 源自駭客入侵 (-24%)

38% 利用了惡意軟體 (<>)

28% 採用了社交手段 (+16%)

15% 包含實體攻擊 (+6%)

具有哪些共同點？

98% 外洩的資料來自伺服器 (-1%)

85% 的攻擊不被視為具備高難度 (+2%)

61% 由第三方發現 (-8%)

86% 的受害者在其記錄檔中具有關於外洩的證據

96% 的外洩透過簡單或中度控制即可加以避免 (+9%)

79% 受 PCI DSS 管制的受害者未做到符合規範

與往年一樣，幾乎所有的資料都是從伺服器和應用程式外洩出去。這一點仍是區分資料處於風險中的事件和涉及實際洩露的事件的決定性特徵。由高度精密攻擊造成的外洩比例相對來說是較低，但是每十筆遺失的記錄中，大約有九筆都與之有關。根據這項調查結果，我們認為，大多數的外洩是可以避免的，並且無需複雜或昂貴的控制。是的，雖然有些事後諸葛，但是這些教訓仍然適用；在這場博弈中，罪犯也並非居於絕對領先地位。我們瞭解越多，就越能充分準備。說到準備，許多組織在偵測和回應事件方面仍十分遲緩。大多數的外洩都是由外部人員發現，而這時已過了相當長的時間。

我們在此報告的「結語和建議」一節新增了一些建議，此外，右欄中的內容與我們從一開始即宣揚的訊息類似。這不是因為我們不想長篇大論一番；只是根據我們面前的資料，這裡面的所有要點仍然適用。這項研究總是提醒我們，我們的專業具備完成此工作所必要的工具。我們所面臨的挑戰在於為手頭上的工作選擇正確的工具，並且不讓它們隨著時間而遲鈍生鏽。證據顯示，發生上述情況時，我們的敵人會迅速抓住此時機。以某些方式惡意利用身分認證而導致的資料外洩數量是一個問題。在我們上一份報告中，問題在於預設的身分認證資訊；今年則是被盜和/或過於薄弱的身分認證。也許這是因為駭客知道大多數的使用者都具有過多的權限。也許這是因為他們知道我們並未認真監控使用者活動。也許這就是開啓大門最簡單的方式。不論是什麼原因，我們需要採取一些措施。如果我們不能區分誰是好人、誰是壞人，無論我們的防衛如何堅固也無濟於事。惡意軟體越來越難以偵測和預防 (特別是駭客佔有系統後)。因此，我們要針對感染後惡意軟體造成的損害加以防護，而如果輸出流量受到限制，則可減輕多數此類損害。最後，監控 (或者應該說「挖掘」) 記錄的價值無以言喻，非常重要。跡象就在那裡；而我們只需要提高辨識能力。

應在哪些方面加強防護措施？

- 清除不必要的資料；密切注意留下的資料
- 確保做到基本控制
- 再次檢查上述措施
- 測試並檢查網路應用程式
- 查核使用者帳號以及監督得到授權的活動
- 過濾輸出流量
- 監控和挖掘事件記錄

研究方法

人們常常說，科學的作用是解釋自然界中事物的「原理」。我們覺得這是一個適當的描述，並要讚揚那些研究者，他們致力於探究我們所在領域中錯綜複雜的世界，以追求更清楚的認識。本著這種精神，《2010 年度資料外洩調查報告》(DBIR) 是我們持續致力於闡明電腦犯罪世界中事物「原理」的第三部曲 (如果加上補充報告，則為第五部曲)。

透過嚴謹的觀察來收集資料，當然是任何科學嘗試的其中一個基石。雖然我們認為我們的研究方法非常嚴謹，但不能說保持完全一致。2008 年度的 DBIR 進行了大規模的資料搜集，回顧 Verizon 自 2004 至 2007 年四年間的全部案例。涵蓋範圍很廣，但是由於時間有限，分析的深度有點受限。2009 年度的 DBIR，分析的來源從歷史資料轉為持續收集的資料，為我們打開更主動觀察、更多詳細資料以及新研究領域的大門。針對今年的報告，當然可以再次採用這種研究途徑，以保持統一性，這對於研究方法來說，是一項好的特質。然而，我們的終極目標不是統一性；而是知識程度，是要去瞭解和解釋「原理」。

由於這個原因，我們再次做了一些顛覆，在 2010 年度的 DBIR 中，納入完全由外部提供且非常不同 (但仍非常可靠) 的資料集。我們欣喜歡迎美國特勤局 (USSS) 對本年報告的貢獻 (包括資料和專業知識)。這不僅僅放大了我們對資料外洩世界的視野，同時也提供了一個新的角度來瞭解這個世界。正如下文中將會看到的，我們雙方負責的案例有相似之處，但也有一些關鍵不同之處。兩者都深具啓發性，而我們堅信，合作的力量將帶領我們更接近上述目標。

這不僅僅放大了我們對資料外洩世界的視野，同時也提供了一個新的角度來瞭解這個世界。正如下文中將會看到的，我們負責的個案有相似之處，但也有一些關鍵不同之處。

將這兩個資料集結合在一起，對雙方都是頂艱鉅的挑戰，此節剩下的部分將說明我們是如何做到這一點的。

Verizon 資料收集方法

Verizon 使用的基本方法仍與往年無異。所有結果均以 Verizon 在 2004 至 2009 年之間所進行之付費鑑識調查所收集的第一手證據為依據。2009 年的全部案例是報告的分析重點所在，但是整個報告中均廣泛參考了整個範圍的資料。雖然調查反應 (IR) 團隊處理了各種各樣的案例，但是在此資料集之中，只包括那些涉及已證實的外洩事件的案例。為有助於確保得到可靠而統一的資料，所有調查者均使用「Verizon 企業風險和事件分享」(VERIS) 架構來記錄案例資料和其他相關詳細資料。以 VERIS 收集的資訊之後會送交給事故調查團隊成員，以進一步驗證和分析。案例資料的集合儲存庫經過淨化，不包含可能使他人查證客戶身分的資訊。

USSS 資料收集方法

由於上面一直提到「做了一些顛覆」，讀者可能會推斷今年的報告拋棄了統一的原則。情況並非如此。在資料收集方面，USSS 的方法與 Verizon 沒有什麼差別。為進行此研究，USSS 以 VERIS 為基礎，建立一個內部應用程式。從 USSS 於 2008 和 2009[1] 年間處理的上千案例中，研究範圍縮小為僅限那些涉及已證實組織資料外洩[2]的案例，以與 DBIR 的重點保持一致。然後，研究範圍又進一步縮小，僅包括那些未由 Verizon 進行鑑識調查[3]的案例。在這些案例中會抽取樣本，並傳送輸入資料的要求給處理各個案例的 USSS 工作人員。如此一來，這些工作人員會利用調查記錄、受害者和其他鑑識公司提供的報告，以及他們自己在處理此案例時所得到的經驗。最終產生了 257 個符合條件的案例，在針對此報告設定的時間範圍內，可以收集這些案例的資料。產生的資料集會清除掉任何可能辨識出涉及此案例的組織或個人之資訊，然後提供給 Verizon 的事故調查團隊進行分析。

總而言之，我們想要重申一點，此報告的調查結果並不能夠代表任何時候所有組織中的所有資料外洩的情況。即使合併的 Verizon-USSS 資料集 (可能) 比兩個單獨的資料集更能貼近反映現實，這仍只是一個樣本。雖然我們相信，此報告中展示的許多調查結果適合套用於一般情況 (而我們對這點的信心也隨著時間不斷強化)，無疑地還是會有偏差存在。即便如此，這裡包含了豐富的資訊，並且不乏有效清楚的收穫。和任何其他研究一樣，讀者最終會決定哪些調查結果適用於其組織。

關於 VERIS 的概要介紹

VERIS 是專門設計的架構，提供一種通用語言，以結構分明和可重複的方式描述安全性事件。它採用「誰對什麼或誰做了什麼，得到什麼結果」的敘述，並轉換為您在此報告中所看到的資料類型。由於許多讀者詢問 DBIR 背後所使用的方法，而我們希望促進更多資訊流通來分享安全性事件，因此在今年稍早發布 VERIS 供公衆免費使用。在我們網站[4]上提供了 VERIS 的簡短概述，完整的架構可從 VERIS 社群 wiki[5] 取得。兩者都是此報告的絕佳輔助參考，有助於瞭解術語和背景知識。

1 USSS 所收集的資料範圍為 2008 和 2009 年。但是，2008 年所處理的案例中，有超過 70 件涉及到在 2007 年發生的外洩事件。由於這是一個足夠大的樣本並可進行三年趨勢分析，因此我們將其與 2008 年外洩案例分開，單獨進行研究。

2 USSS 處理的許多與盜竊和詐欺相關的案例並不包括在此報告中。例如，針對消費者而並不涉及組織或其資產的犯罪行為，則並不包括在內。在資料遭竊後發生的犯罪活動 (例如，「白卡詐欺」和身分盜用) 也不包括在此研究的範圍內。

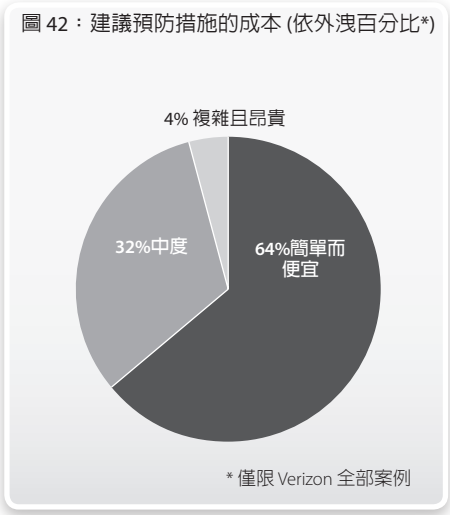
3 USSS 經常以某種方式參與 Verizon 所處理的案例 (特別是較大的案例)。為減少重複，這些案例已從 USSS 樣本中移除。當 Verizon 和 USSS 都處理同一個案例時，使用 Verizon 提供的資料。

4 http://www.verizonbusiness.com/resources/whitepapers/wp_verizon-incident-sharing-metrics-framework_en_xg.pdf

5 https://verisframework.wiki.zoho.com/

結語和建議

雖然在 2009 年觀測到的攻擊整體難度比往年稍高，我們的調查結果卻顯示，預防攻擊的難度卻有所下降。僅 4% 的外洩被評定為需要複雜且昂貴的預防措施。圖 43 對此調查結果進行了部份說明，此圖將這些建議的預防措施分為幾個大類。比起大規模重新部署和採購新設備，變更設定和調整現有做法更能解決問題。往年也表明了同樣結果。



這些都涉及到一個有關安全性管理的重要教訓。是的，我們的敵人非常狡猾且資源豐富，但這項研究總是提醒我們，我們的專業具備完成此工作所必要的工具。我們所面臨的挑戰在於為手頭上的工作選擇正確的工具，並且不讓它們隨著時間而遲鈍生鏽。證據顯示，發生上述情況時，我們的敵人會迅速抓住此時機。不要讓他們得逞。

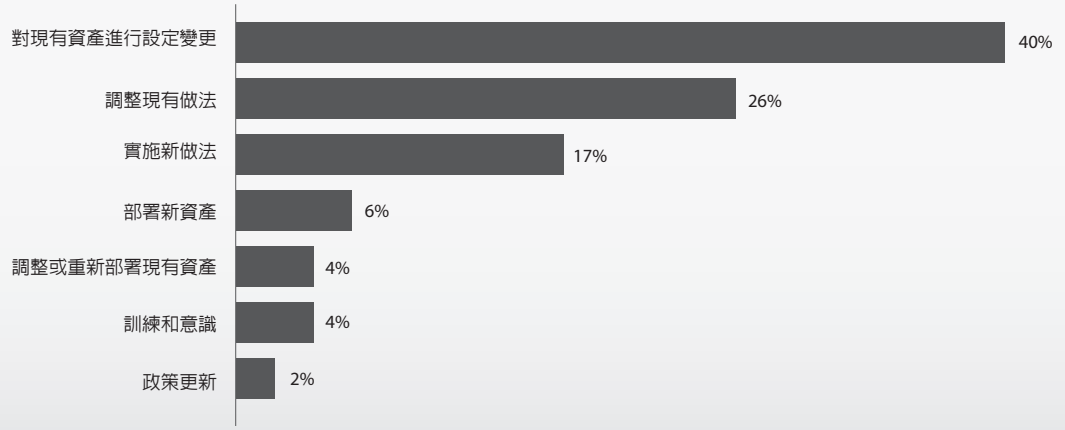
每年發表此報告時，建立一份切實可行的建議清單變得越來越困難。想想看：我們的調查結果隨著時間有所提升進化，但很少是全新或未預期的結果。根據這些調查結果，所提出的建議為何會有任何不同呢？當然，我們可以隨便拼湊並漫談一份很長的「應做事項」清單，但我們發現您在別處也可以找到這樣的東西。我們更注重價值，而不是以量取勝。根據對 2009 年度的分析，我們的確發現一些我們認為有可取之處的新內容 (或舊有內容的擴充)，下面列出了這些建議。當然，我們會繼續推薦我們以往提供的建議 (可在 2008 和 2009 年度的 DBIR 以及 2009 年度補充報告中找到)。

限制和監控具有權限的使用者：由於得到了 USSS 提供的資料，今年，我們前所未有地發現更多內部人士外洩事件。對於內部人士 (特別是具有高權限的人士)，通常難以管理，但也有一些可行的策略。信任，但要查核。透過僱前調查，防患於未然。不要給予使用者多於其所需的權限 (這點非常重要)，並運用職權分立。確定他們都得到指引 (他們知道政策和期望) 以及監督 (確定他們按政策和期望行事)。授權的使用行為應記錄下來，並產生訊息給管理人員。授權的使用行為若不在規劃中，則應產生警示並進行調查。

密切注意「輕微」政策違規：在內部人士這個主題上，我們已多次談到有關「輕微」政策違規和更嚴重的濫用之間的關聯。也許我們應該將其標示為「網路犯罪的破窗理論」。接著，我們建議組織應對政策違規事件提高警覺，並做出適當回應。根據案例資料，如果在使用者系統上出現不法內容、色情內容等 (或其他不當行為)，可視為是未來可能發生資料外洩的合理指標。主動搜尋類似指標，而不是在其突然出現後才加以處理，會更加有效。

採取措施，制止遭竊的身分認證資料：在 2009 年，遭竊的身分認證資料是得以未經授權即可進入組織的最常見方式。不論這只是暫時性問題或一種趨勢，都值得我們採取一些措施來加以防範。將可截取身分認證資料的惡意軟體阻擋在系統之外，是第一號優先任務。請酌情考慮使用雙因素認證。如有可能，實施有使用時間限制的規則、IP 黑名單 (如果大位址區段/區域沒有合法商業目的，請考慮加以封鎖) 以及有限制的管理連線 (例如，僅來自特定內部來源)。使用「上次登入」橫幅，以及訓練使用者在發現可疑情況時報告/變更密碼，也同樣有助於防範。

圖 43：建議防護措施的類別 (依外洩百分比*)



* 僅限 Verizon 全部案例

監控並過濾輸出網路流量：大多數組織都至少做出合理努力，過濾來自網際網路的輸入流量。這可能源自一種 (正確) 觀點，認為外界有很多我們不想讓其進入的東西。許多組織忘記了一點，內部有很多我們不想讓其流出的東西。因此，過濾輸出幾乎沒有得到與過濾輸入同等的重視。我們的調查顯示也許應該同樣重視過濾輸出。在許多外洩案件的事件順序的某一點上，如果阻止了某些東西 (資料、通訊、連線) 輸出，則可能會打破整個事件鏈，而制止了外洩。在對輸出流量進行監控、瞭解和控制之下，組織將能大幅提高消滅惡意活動的機率。

變更事件監控和記錄分析的方式：讓我們快速回顧此報告的一些調查結果，以有助於說明這項建議。1) 大多數的攻擊中，在資料洩露前，受害者有幾天或者更多時間可發現。2) 外洩需要很長時間才會被發現，而且 3) 外洩最終發生時，通常不是由受害者所發現。4) 最後，幾乎所有受害者在其記錄檔中都有洩密的證據。要發現不正常的事物，並不需要花費太多力氣，適當進行一些變更即可。首先，不要將所有蛋放在「即時」的籃子中。IDS/IPS 不應是唯一的防線。您還有時間可依賴更徹底的批次處理和分析記錄。下一步，著眼於明顯的事情 (「草堆」)，而非細枝末節 (「針葉」)。這項工作不一定要付出高昂代價；一個能計算記錄行/長度並在超出容忍範圍時傳送警示的簡單指令碼，即相當有效。最後，確定有足夠的人員、適當的工具和/或充足的處理程序，可辨識和回應異常情況。我們相信此措施可取得良好成效，並能節省時間、精力和金錢。

分享事件資訊：最後這則建議也將是本篇文章最後一段。我們認為此報告證明了可以盡責、安全、有效做到這則建議。我們相信安全方案的成功取決於我們採取的實踐方式。那些實踐方式取決於我們所做的決策。我們的決策取決於我們所相信可以落實的事物。那些信念取決於我們所知道的事情，而我們所知道的取決於我們能夠得到的資訊。資訊的可用性取決於願意收集、分析和分享。如果這條關係鏈成立，則可以說，安全方案的成功取決於大家願意分享的資訊。我們相信這是一個行動號召，並感謝所有付諸行動的人員。

感謝您撥冗閱讀此報告。

verizonbusiness.com

verizonbusiness.com/socialmedia verizonbusiness.com/thinkforward