IBM X-Force 威脅情報季報：2015 年第 2 季

不論是惡意或是人為疏忽的內部威脅，均足以危害企業關鍵價值並造成重大傷害。探究內部威脅的解決方法。

IBM

目錄

高階主管概觀

我們在今年首份的 IBM® X-Force® 季報中，提供了 2014 年安全事件簿，內容提及產業與基本架構受到危害之嚴重程度，以及面對益發精巧的攻擊技術，我們如何改變安全防護措施。

隨著威脅與資料外洩的規模不斷升級，我們的第二季季報把焦點放在內部威脅，並探討內部威脅難以察覺且常被輕忽的原因。

根據最新的 IBM Security Services 2015 Cyber Security Intelligence Index，內部威脅仍舊是所有攻擊類型中的首位。 外部威脅在 2014 年的攻擊記錄中佔了 45%，而可存取組織系統內部之人員所造成的攻擊事件，則佔 55%。[1]

我們在報告中檢視此類威脅如何演變以及公司該如何降低風險。 內部威脅可能代表許多不同意義，例如心懷不軌的員工惡意傷害公司、或者使用者不慎按下可疑電子郵件附件而讓系統（可能是公司網路）遭受惡意軟體的威脅。 今天大多數的垃圾郵件出自營利業者，其可在垃圾郵件訊息中附加任一種惡意軟體。 不論是基於犯罪意圖或財務利益，任何競爭對手都有足夠的動機僱請垃圾郵件業者，透過自訂的行銷活動誘騙使用者開啟附件或按下連結，以致公司網路遭到勒索軟體或惡意軟體的感染。

此外，我們也聚焦探討所謂的「類內部人員」，例如被認為可信賴合作廠商之員工。 其中包括有機會進入實際工作場所或可存取公司網路的電氣技師、營建工人、電話或其他種類的維修人員。 以美國 Target 賣場的資料外洩事件為例，若不當管理合作廠商的存取權限，攻擊者很容易能竊取認證資料並存取公司網路。

大多數組織都體會到保護關鍵資料與資源安全的重要性，而我們的職責在於提供最佳實務作法與相關建議，促使讀者開始思考如何有效杜絕風險。

本報告的結論說明了安全情報（尤其是識別方面）如何協助偵測內部威脅，以及提高系統與網路現況分析的效果。

去年一整年的教訓，讓企業瞭解防備措施對於電腦、網路及實體安全的重要性。公司針對受到內部或外部威脅的網路評估可能風險，可在未來面對威脅時知道如何應變。

內部威脅破壞信任鏈

您知道誰在存取您的資源嗎？ 探索如何在變動不已的商業環境中保護您的關鍵資產。

對大多數公司而言，「內部威脅」往往肇始於員工心生不滿或漫不經心，以實體或電子形式損害公司資產。 然而，近十年來企業和國家間諜活動層級升高，現在的公司若想保護資產安全，必須考量數種可能情況。

許多公司在評估內部威脅風險時，會將注意力放在「可信任」的員工，特別是權限等級較高的員工。 公司取用及處理重要業務與現金資產時，必須信賴這些員工會恪守隱私要求。 而權限等級高的使用者應受規範約束，不得擅用強大的存取權限。 因此，在高風險的業務環境下，公司必須在信任使用者的程度與對其授予之存取權限間，適度取得平衡。

即使組織期望員工均可信賴，但仍須確認組織高價值資產的運用情形；這些企業關鍵資產包括智慧財產、財務資料、產品設計及達成業務目標的其他關鍵資訊。 由於此類資產具備高價值，其資料自然成為內部威脅覬覦的目標。

現代職場上，員工為求更好發展而經常轉換跑道，對於當前的雇主未必盡心盡力。 公司員工轉換至競爭對手後，在公司內還是有朋友可存取資源。 只要離職員工心懷不滿或貪圖暴利，公司發生資安事故便不足為奇。 離職員工可能在離開公司前就設好「後門」，進到新公司後，就可從外部存取隱藏帳戶或機密資料。 這對業界來說雖不是什麼新花樣，不過幾乎每天還是有公司通報類似資安事件。 為了保持警覺，有必要設立經常性流程來檢閱存取記錄與網路活動，進而偵查「後門」或任何其他異常行為。 或者可考慮使用自動化監測服務，但如何執行則須權衡風險與公司的成本。

現實中，保護客戶資料已無輕鬆簡便的方法。 即便是善於維護客戶隱私資料庫的大型企業，近來也飽受內部威脅的危害。 舉例而言，去年就有全球性電信企業的顧客資料遭竊（包括出生日期與美國社會安全號碼），元凶是合作廠商的惡意內部人員，其利用這些資訊解鎖行動電話並於黑市轉售。[2]

含有重要資產的電腦網路應該審慎監控，確認資產未被有心人士透過網路連線、電子郵件、USB 裝置或其他類似方式加以外洩。 公司不僅要限制私人資料（包括顧客資料）的存取權限（只限職務需要的員工存取），也應監控異常的員工活動。

另一方面，客戶應在廠商要求提供私人資料時，保持警覺。客戶將私人機密資料提供給公司後，便受制於公司的資料保護政策與實務運用，但卻難 以評估和理解箇中意涵。

許多組織在發生重大資安事故前，皆忽視安全措施的升級，等到事故發生再來花錢補救或制定相關政策，才發現為時已晚。 組織常忽略升級安全措施的重要性，不論是技術資產、資料或實體資源皆然，因為確保安全性所需的成本對企業來說，不一定有利於營收。

從實體安全到社群工程，威脅無所不在。

不少人認為，IT 相關的安全性只限於公司的電腦網路與各種附加裝置或科技。 然而，數位威脅絕不僅止於 IT。 許多實例說明，透過數位網路也能存取企業的實體安全系統。

無庸置疑，數位威脅可影響警報系統，尤其對網路式遠端監控系統的影響更甚。 此外，數位威脅也可從組織內外影響網路電話系統。 幾年前，研究人員證明從世界任一處，都能輕鬆地遠端開啟電話的擴音器和竊聽器。[3] 如果網路電話 (VoIP) 配有網路攝影機，他們也能神不知鬼不覺地啟動攝影機。[3]

本研究顯示，評估電腦網路威脅時，實質審查所有系統極為重要。 比方說，電腦的影印機與傳真機可能就存在層級較低的威脅。 大部分此類機器都搭載記憶體或硬碟，通常可與內部網路連結。 維修技師這類具備適足技術知識的人員，即可迅速存取上述儲存設備並竊取重要資料。這些儲存設備也可經由網路加以儲存。

事實上，研究人員發現從 eBay 便能買到內含機密文件的影印機硬碟，其他像是二手公司設備與政府設備拍賣購得的影印機也有相同隱憂。 此種情況甚至無須動用電腦駭客入侵技術，只要知道如何取出硬碟並裝入電腦即可。 設計與 Linux 或 Microsoft Windows 搭配使用的硬碟很常見。 您要 替換影印機或傳真機時，請務必確定公司（而非第三方）已保留資料或將其銷毀。

「類內部人員」是另一種型態的企業安全威脅，層級不高卻不容忽視。 此類威脅屬於間諜慣用伎倆，早在電子連線功能問世前便出現。 許多公司向維修、營建及清潔公司聘請工作人員，即使是下班時間或週末假日仍允許其進入公司。這些聘僱人員通常未經審查即可進出整個公司，甚至可能包括高階主管與董事辦公室。

Target 資料外洩事件就是一個例子，其允許協力廠商人員進出，結果蒙受損失。 詳細情況是，攻擊者盜用冷藏及空調系統廠商人員的認證資料，進而竊取約 1.1 億份個人與財務資訊，相關資料量高達 11 GB。此案例說明除了監控公司網站與網頁伺服器的「前門」進出外，還有其他方面值得多花時間和成本去留意。 很多公司也需要注意其他可能開放給經銷商、承包商及合作夥伴使用的進入點。

內部威脅的攻擊變形

滲透實體系統的數位進入點：攻擊者可利用警報系統、影印機和傳真機，以及網路電話系統作為存取機密資料的進入點。

合作廠商人員：維修工人、駐點服務技師及清潔人員未經審查即可隨意進出，不僅系統易遭竄改，取得員工的工作場所密碼亦非難事。

除此之外，國際環境因缺乏監管機制而安全漏洞頻傳，替競爭國家或對手製造暗中滲透並取得公司資產的良機。訓練有素的間諜不出幾分鐘便能在高階主管或董事辦公室植入監聽裝置。 其訓練可能僅是「把監聽器置入牆壁並設法遮蔽」，也有可能更為精密複雜。

短短幾分鐘，未經授權的人員便能翻遍員工的辦公桌，並從抽屜、筆記本或其他辦公位置找到密碼。若未經授權的人員可從內部（如員工工作場所）存取公司網路，便能對公司造成重大傷害而不被察覺。他們還可迅速替換或複製影印機和傳真機的儲存裝置並下載內容。雖然機器可透過鎖定或裝上防篡改標籤來加以保護，仍無法完全免除威脅。高階主管與董事辦公室的資料當然也難以倖免。

不論資料外洩是起因於企業或國際間諜活動，或者純粹個人 貪圖利益所致，公司均可在潛在風險下採取適當防護步驟。 舉例而言，位於公用大樓的企業需要留意大樓的所有人是誰。另外也應清楚公司隔壁、樓上及樓下是哪些人在使用。您必須掌握並保護資料所在的實體位置。過去經驗顯示，來自鄰處的攻擊特別難防。

最終考量和建議事項

現代商業環境中，要防止公司關鍵資產遭到竊取或移轉，十分困難；來自內外部的對手為求突破存取限制，不但充滿意圖與耐心，更掌握相關資訊及資源。公司應當配置預算以阻絕資訊盜竊。相關防護措施包括適當控制實體安全以及科技運用，同時對於組織的員工和約聘人員需有充分的瞭解，不論其為工作人員或組織代表人皆不例外。

組織想要保護關鍵資產安全免於數位威脅時，使用合作廠商評估或可帶來明顯幫助，卻常忽略可存取關鍵資產的內部員工或約聘人員所帶來的潛在威脅。很多人具備專業知識與技能，能夠在觀察組織後提供建議並向您說明顯而易見的安全漏洞；不過企業通常對其看法難以置信。許多專業人士曾在軍方或政府服務多年，習得之技能組合使用在參與或調查間諜與反間諜活動時，十分派得上用場。

外部人員要進入含機密資料或設備的區域時，派公司員工緊隨在側是個簡單有用的解決方案。或許有人認為此作法加重公司資源的負擔或浪費，但與系統入侵或資料竊取所造成之數百萬美元關鍵資產損失比較，長期來看相對值得。在特定的政府機關，任何約聘人員進入辦公場所時必須有人跟隨或進行背景檢查。

針對機密性職位僱用及留住最適員工時，或約聘可存取公司重要資料的人員時，聘僱流程最好納入背景考核。大多數公司會針對特定職位於僱用前執行藥物檢測及犯罪背景查核。

內部人員與持續不斷的垃圾郵件威脅

經由垃圾郵件傳播惡意軟體已愈來愈常見。瞭解如何保護您的企業，同時讓使用者保持警戒

威脅可能源自組織外部人員，也會來自未經授權的惡意內部人員，然而內部人員即使立意良善，也可能不慎按下網路釣魚郵件的惡意連結而助長攻擊威脅。若要防止相關情事發生，組織安全團隊必須能辨識垃圾郵件所散布的惡意軟體威脅，並採取相關步驟予以阻絕。每位使用者應當保持警覺，瞭解即便最單純之動作也能引入威脅。

資訊安全專家有時將平凡的垃圾郵件視為一般困擾而非威脅。 畢竟，諸如網路釣魚或魚叉式網路釣魚、惡意或分散式阻斷服務 (DDoS) 攻擊等威脅，足以讓他們忙到喘不過氣。 據最近 IBM X-Force 進階研究 (IBM X-Force Advanced Research) 的分析，垃圾郵件的威脅持續成長，因而需要多加留意。

若要深入檢視目前的垃圾郵件活動，可先從瞭解垃圾郵件發出的國家開始。圖 1 顯示近兩年垃圾郵件來源國家的趨勢。

我們從這張圖表可檢視各年內的起伏情形，以及依每年查看變化。 觀察重點包括：

- 在 2015 年第 1 季，美國是最多垃圾郵件的來源國，僅佔總數 8% 以上，顯示垃圾郵件來源極為分散。
- 越南去年排在首位，今年則退至第二。
- 西班牙兩年內多次拿到垃圾郵件來源國的第一名，目前則排第三。
- 最近一季中，源自其他參與國的垃圾郵件量各佔全球總數的 6.1% 到 1.1% 之間，而在近兩年內起伏劇烈。

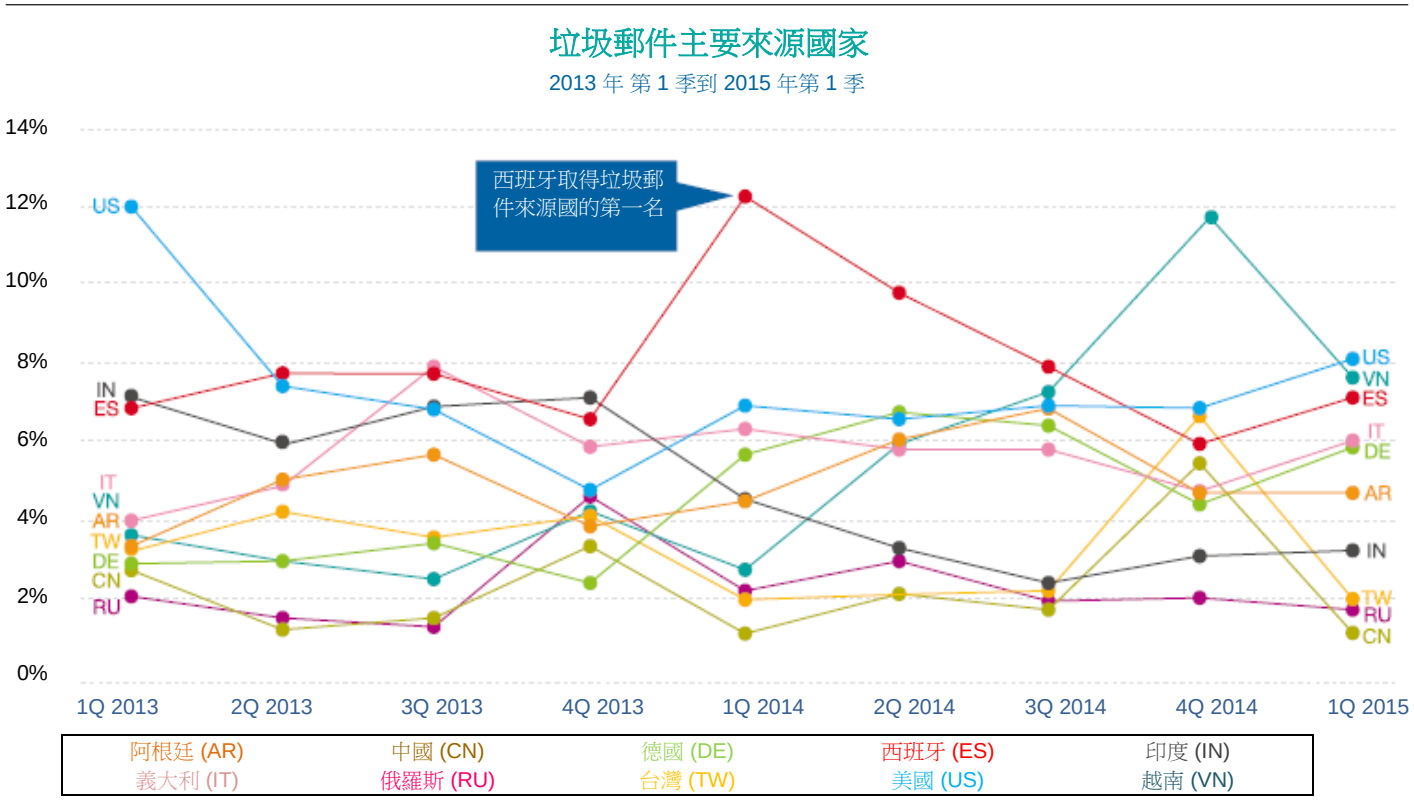


圖 1. 垃圾郵件主要來源國家（2013 年第 1 季到 2015 年第 1 季）

查看下列數據後，可能沒有特別的新發現。

可能和檢視近兩年垃圾郵件量（如圖 2 所示）的印象差不多。

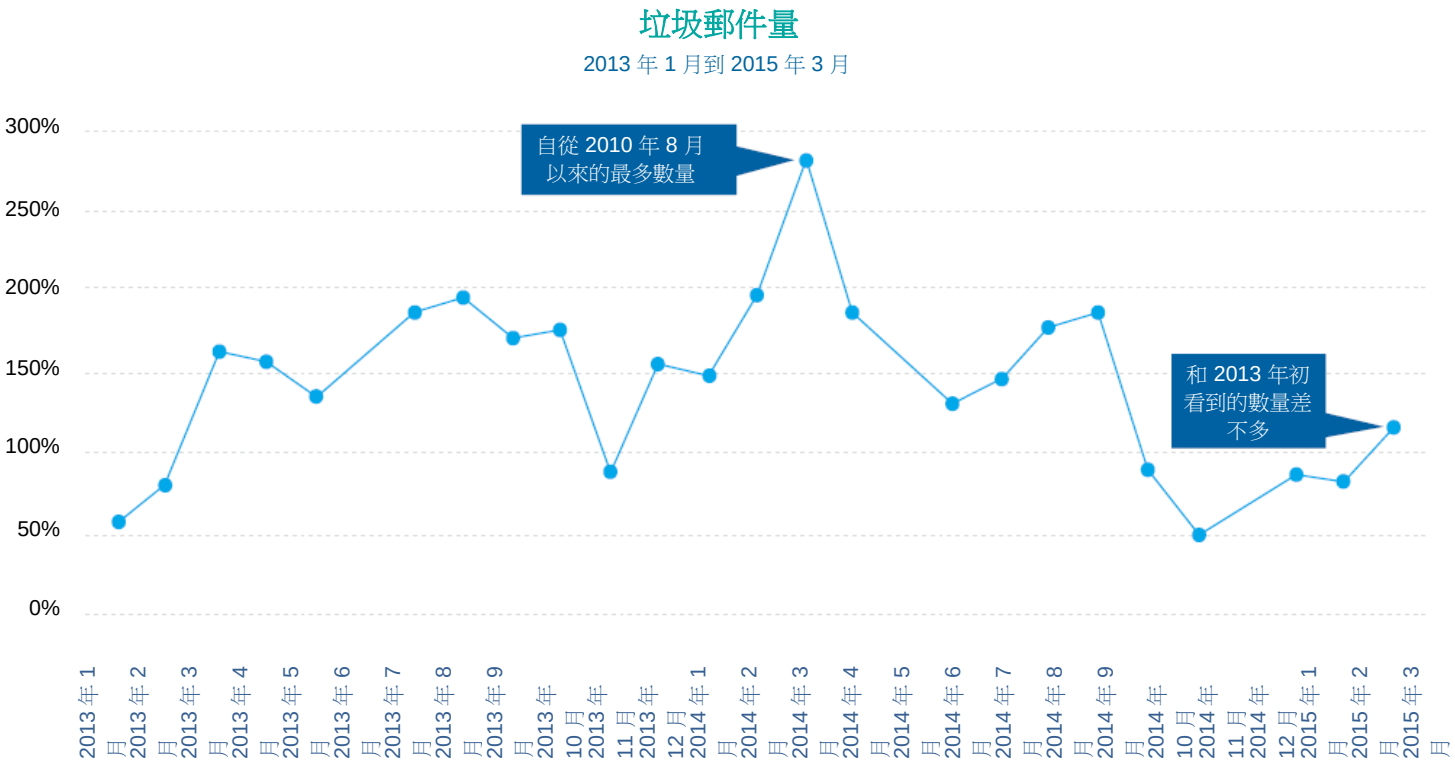


圖 2. 垃圾郵件量（2013 年 1 月到 2015 年 3 月）

雖然我們檢視的是近兩年整體垃圾郵件數量的起伏趨勢，但也適用於目前的垃圾郵件數量。

不過，不能就此認為垃圾郵件的性質變化不大。圖 3 為垃圾郵件含惡意附件的百分比，藉此可看出主要變化。

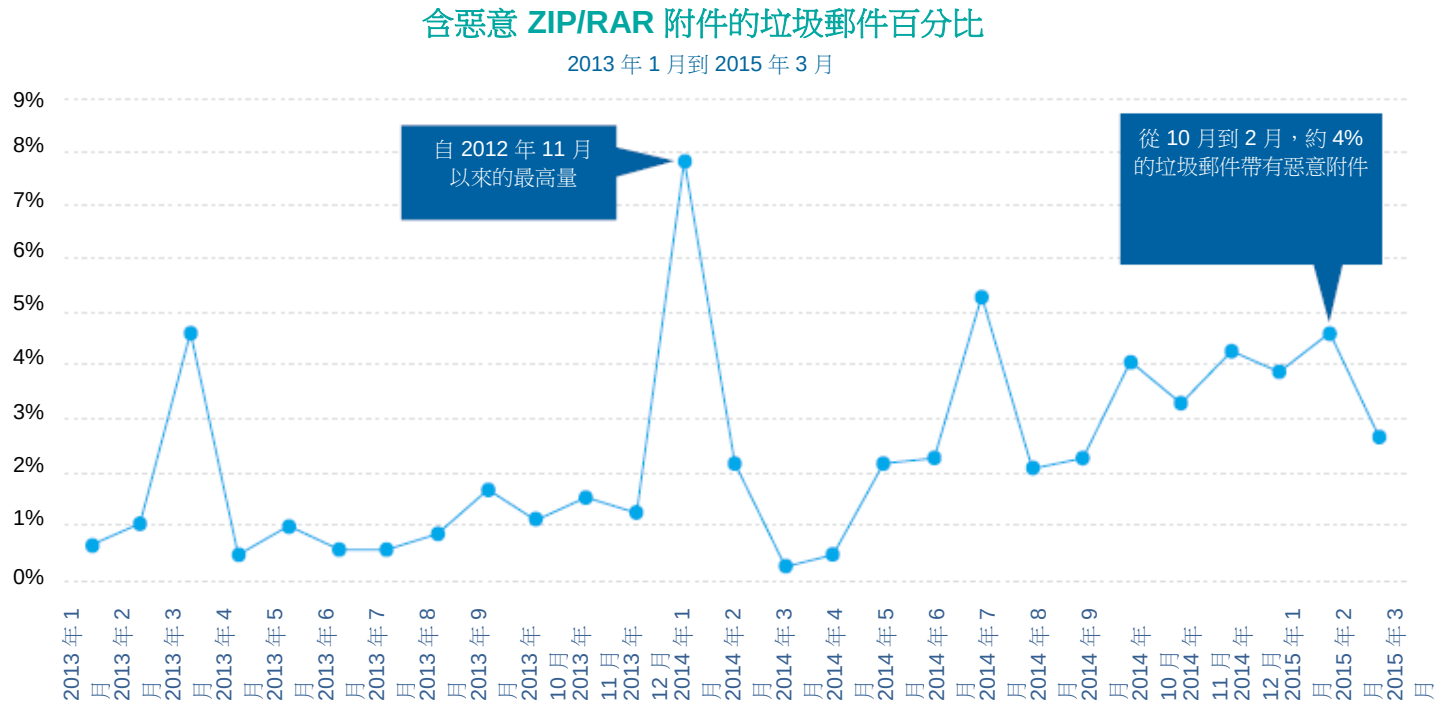


圖 3. 含 ZIP/RAR 惡意附件的垃圾郵件百分比（2013 年 1 月到 2015 年 3 月）

2013 年夏季之前，帶有惡意軟體的垃圾郵件鮮少超過 1%。 但在同年的秋季開始大幅增加。到 2015 年的前幾個月，含惡意附件的垃圾郵件百分比約 4%。即使近兩年整體的垃圾郵件量變化不大，垃圾郵件製造者現在利用此管道散布惡意軟體的情況，比以往嚴重。

目前情況反映了 IBM X-Force 威脅情報季報：2015 年第 1 季中呈現的趨勢。當時我們發現惡意軟體是最常見的攻擊類型之一，而含惡意附件的垃圾郵件則提供傳送惡意軟體的途徑，威脅公司網路和使用者電腦。

垃圾郵件可能附加任何種類的惡意軟體，只要含有相關連結即可辦到。許多垃圾郵件製造者屬於營利事業，主要由客戶決定裝載內容，而非垃圾郵件系統業者。任何對手都可僱用垃圾郵件業者，動機從意圖犯罪到財務利得，不無可能。如同個人使用者受到危害般嚴重，企業網路遭到勒索軟體入侵也會對企業帶來極大風險。此外，對手若對您的智慧財產與商業機密更感興趣，可利用垃圾郵件搭配鍵盤記錄和密碼竊取工具，來滲透您的網路。

根據上述觀察，可歸納數個結論。 最值得注意的是，垃圾郵件的數量與威脅與日俱增。過去的垃圾郵件主要企圖誘使受害者購買或參與騙局。然而，隨著時間改變，垃圾郵件逐漸轉向利用惡意軟體感染機器。根據此趨勢，您應在各種網路安全方案中，更加重視垃圾郵件過濾器的可靠度。 再者，由於沒有技術可保證完全有效，我們必須教導使用者不要容易受騙。

建議

以下建議提供給網路管理員，以阻絕惡意垃圾郵件附件。

- 保持垃圾郵件與病毒過濾器的最新狀態。
- 阻擋執行檔附件。在一般商業環境中，傳送執行檔附件屬於異常狀況。大多數的垃圾郵件過濾器可設為阻擋執行檔，即使放在壓縮檔內也不例外。
- 使用的郵件用戶端軟體須支援停用自動轉譯附件與圖形，以及支援停用預載連結，然後確實將其設為停用。

改善使用者的防護功能時，問題更加複雜。關鍵在於使用者能否每次察覺危險並運用常識判斷。開啟電子郵件以及按下連結或打開所含附件之前，使用者應先考慮幾個簡單問題：

- 我認識寄件人嗎？
- 我有預期會收到這封電子郵件和其附件嗎？
- 附件為壓縮檔是否合理？訊息與附件類型的格式是否適當？
- 壓縮檔內的檔案類型為何？若為執行檔、螢幕保護程式或不明檔案類型，就不該打開！

垃圾郵件製造者企圖使其電子郵件偽裝成線上商店、銀行或金融機構發出的標準訊息，或者來自如傳真機與影印機等網路內部系統的訊息。使用者也必須對這類電子郵件保持警覺。

每次資料外洩都需要行動解決方案

認識識別分析如何提供您需要的洞察，以瞭解網路事件現況以及防止威脅所需的步驟。

確保網路免受潛在威脅的過程有如飛行員工作般，99% 無聊加上 1% 恐慌。安全專員也應學習飛行員在飛機故障時的系統反應，在面對網路資產受到威脅時有條不紊地處理。

所謂安全無虞的系統，應該要讓入侵系統所費的工夫遠超過獲利。不過，兩者是依存的變動關係。隨著對手將入侵工具社群化（共用技術並合作攻擊指定目標），入侵組織系統所需的工作減少。而報酬通常足以支持駭客部隊鑽研更精密的軟體，以根據最新發佈的安全漏洞測試與滲透網路。 若公司成為威脅目標，安全專員可於新安全漏洞發表及上述特殊惡意程式進行測試與探索時，監視網路警示情況。

重點並非網路是否會遭到威脅，而是您是否準備妥當以及如何應變攻擊。請想像未曾受過突發狀況訓練的飛行員。結果不可能改善。現在請想像，若網路沒有識別功能。後果一樣堪慮。

舉例來說，當今消費者經常收到保健、金融及電子商務業者關於網路遭受攻擊的訊息，不過這些業者卻無法清楚描述攻擊內容為何。通常唯一的解決方式是要求顧客更改其信用卡與登入身分資料，並重設密碼。然而，真正嚴重的後果是使用者再也無法取回其身分證號碼、地址、電話號碼及其他個人身分識別資料。

原因是遺失單筆個人識別資料並不嚴重，但若網路犯罪取得個人全部的識別資料，便能擁有約 95% 的 必要資料以透過電子方式進行財務竊盜與詐欺，無關乎受害者是否已更改信用卡號碼。 進一步來說，如果業者 無法確認遭受到何種攻擊，便不能保證此攻擊永遠不再發生。

對於電子犯罪所覬覦的任何企業而言，精準辨識威脅乃必備能力。

網路與資產識別

識別是指明確重現及說明系統所受任何攻擊的能力。基本功能包含封包擷取、搜尋、過濾重建與微觀檢查。

封包擷取

「擷取」是指收集與儲存網路所發生每次交易的能力。 其提供識別所需的能見度，且需要龐大的儲存容量。例如，若要儲存以 60% 容量運行的 10 Gigabit 連結網路流量，每天需要約 7 TB 的儲存空間。一般容量 56 TB 的 2U 機架式擷取裝置可提供 8 天的歷史網路資料。此一期間稱為能見度的識別時間範圍。 時間範圍越廣，可用於識別分析的能見度就越大。

由於許多攻擊的持續期間較長，因此能否以最低成本涵蓋最長時間範圍，十分重要。而封包擷取的主要費用為儲存成本，因此在提供長時間範圍的能見度時，能否取得較低成本的儲存設備，至關緊要。儲存設備的主要廠商將其產品導入壓縮技術，藉此增加系統容量多達 4 倍。圖 4 顯示擷取 10 Gigabit 網路流量時，使用及未使用壓縮技術的成本。在此案例中，使用壓縮技術可將成本降至 1/4，等於比未使用壓縮技術的儲存設備多了 45 天的封包擷取作業。

搜尋

識別調查通常目標不明。 因而搜尋引擎在此相當實用，它可提供：

- 簡單熟悉的搜尋介面
- 全部識別資料的百分之百即時能見度

比方說，任何人在網際網路上搜尋包含 support@corporatebank.syzexperts.com 的文件，可立即得到結果。適用於識別的搜尋引擎技術所提供的容量與網路流量擷取相同。 上面範例中的電子郵件地址，很適合作為網路釣魚的郵件地址，因為其中的公司商標名稱 (corporatebank) 內嵌於攻擊者的網域 (syzexperts.com)。正確索引化的搜尋引擎可立即揭露使用該郵件地址的網路交易。

要達到百分之百能見度，需要全部擷取封包內容並經過索引作業。 在索引處理過程中，搜尋引擎會將資料分成各領域以提供高準確性查詢。 例如，網路流量是依照 Web 網域、電子郵件地址、URL、HTTP 錯誤代碼以及上百種其他領域進行索引作業以處理特定查詢。 請思考以下查詢：

IPAddress:192.72.68.121 AND Port:880 AND URL:*$^% AND HTTPError:404

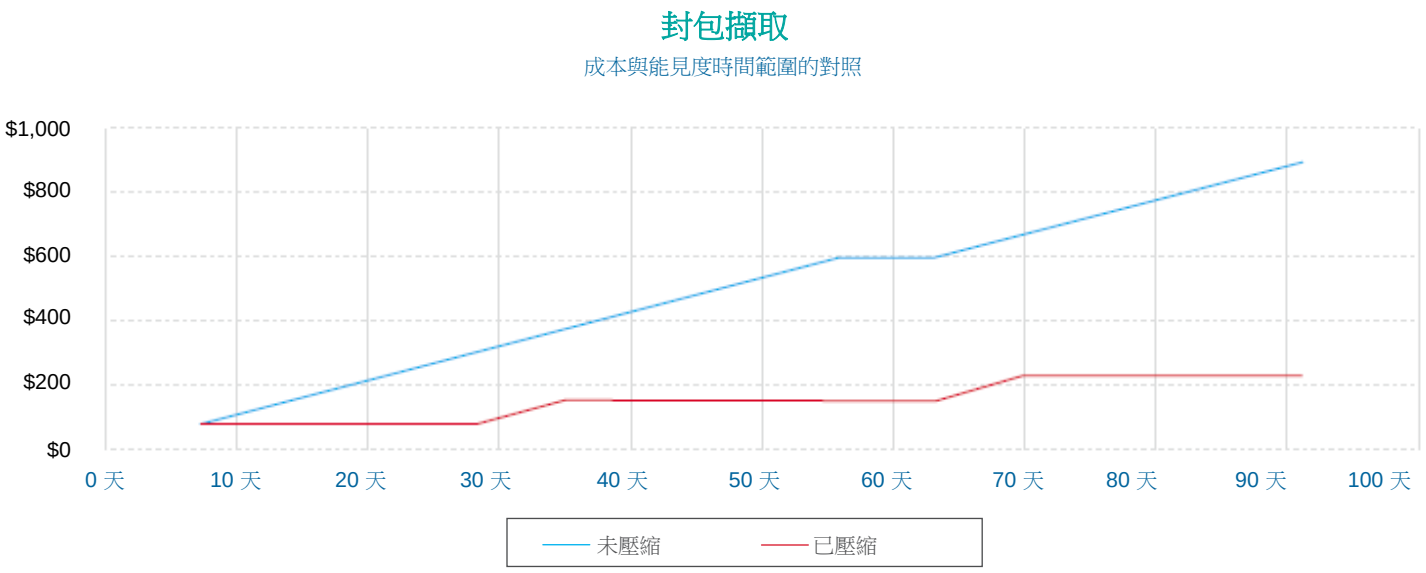


圖 4. 封包擷取、成本 vs. 能見度時間範圍

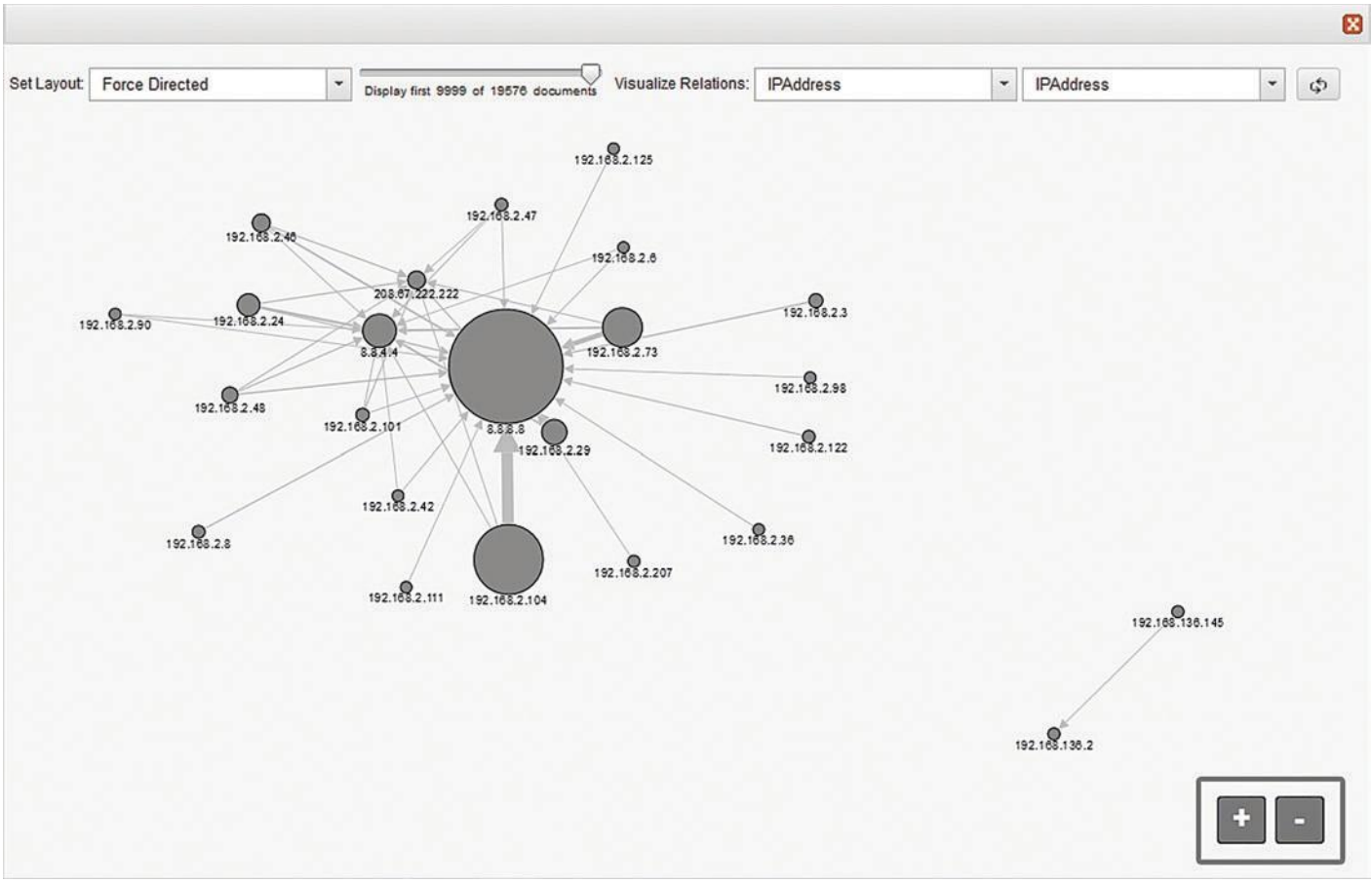
此查詢可讓識別調查人員搜尋任何使用異常字元來搞混表徵性狀態傳輸 (REST) 介面，且意圖混亂 HTTP 應用程式服務的記錄。識別調查員也可縮小搜尋範圍，針對網路釣魚意圖進行搜尋。

From: *syzexperts* AND password

此搜尋可找到郵件名稱含 syzexperts、訊息內容含密碼字詞的任何電子郵件流量。

過濾

搜尋目標不明時，必須判斷重要與不重要的內容為何。識別 能力應包括能否輕鬆進行過濾，並將資料視覺化以便區分重要與否。例如，研究人員可能發現網路內發生某些網域的異常行為。簡易搜尋 DNS 流量並將端點關係視覺化，便能快速找出報告中不易取得的「離群值」。例如，圖表 1 顯示特定查詢的所有 DNS 流量。此視覺化圖表清楚呈現兩個解析異常作業的網域離群值。此種視覺陳述方式提供調查人員檢視離群值的明確起點，反觀標準報告就無法提供。



圖表 1. DNS 網路實體關係

重建

重建可讓組織以人類適讀格式檢視網路交易記錄。儲存系統含有擷取自網路的原始資料流量區塊，一般人難以理解。這些原始資料必須經過剖析和分析，才能重建。顯示對手存取的網頁、相關的完整電子郵件訊息（或執行緒）、遭入侵行為竊取的檔案，甚或全部即時通訊對談內容，都是重建的例子。

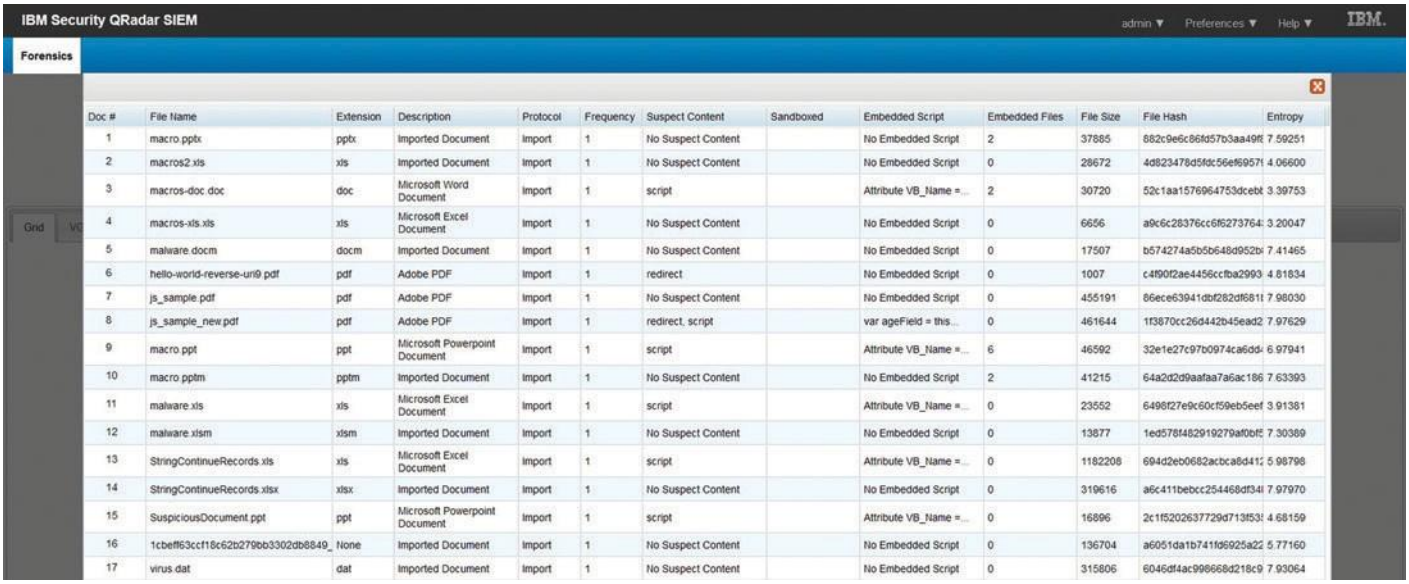
重建過程中，軟體模組「檢查工具」(inspector) 會將網路資料細分為中繼呈現形式，以用於搜尋和重建。檢查工具可透過電子資料流的位元模式辨識網路流量。根據資料模式（非埠號）辨識流量很重要，因為攻擊者會嘗試欺騙通訊協定檢查工具是由分析通訊協定的工程師編寫，他們也會分析擷取關鍵欄位中繼資料的服務。中繼資料則以結構化格式輸往搜尋引擎，可促成網路事件的細節重建。在評估識別解決方案的功用時，必須先瞭解通訊協定識別和通訊協定檢查之間的差異。 許多供應商宣稱有上千組通訊協定識別碼。 識別碼只能標記用過的通訊協定，而檢查工具則可分解通訊協定以用於搜尋和重建作業。

以下為不同類型的重建作業：

- 網頁
- 聊天
- 社群網路
- 網頁型電子郵件
- 部落格
- 檔案傳送
- 附件檔案
- 檔案中繼資料（地理位置、上次更新以及其他類似屬性）
- 檔案流（附加執行檔、JavaScript、巨集、重新導向）

微觀檢查

搜尋與重建可將值得注意的網路交易從數十億筆資料流減少至可管理的資料集。微觀檢查針對策略性識別資訊找出可疑內容或資料，進而對最終分析（如報告內嵌檔案、檔案熵、檔案混淆、檔案沙箱及檔案流、巨集、執行檔等等）進行分解。優良的檢查環境包括以自動方式擷取詳細檔案資訊的功能。在檔案內嵌資訊與檔案以及混淆檔案類型，都是攻擊者主要的手段。



Doc #	File Name	Extension	Description	Protocol	Frequency	Suspect Content	Sandboxed	Embedded Script	Embedded Files	File Size	File Hash	Entropy
1	macro.pptx	pptx	Imported Document	Import	1	No Suspect Content		No Embedded Script	2	37885	882c9e6c86fd57b3aa49f	7.59251
2	macros2.xls	xls	Imported Document	Import	1	No Suspect Content		No Embedded Script	0	28672	4d823478d5fdc56ef6957	4.06600
3	macros-doc.doc	doc	Microsoft Word Document	Import	1	script		Attribute VB_Name =...	2	30720	52c1aa1576964753dcebf	3.39753
4	macros-xls.xls	xls	Microsoft Excel Document	Import	1	No Suspect Content		No Embedded Script	0	6656	a9c6c28376cc6f6273764	3.20047
5	malware.docm	docm	Imported Document	Import	1	No Suspect Content		No Embedded Script	0	17507	b574274a5b5b648d952b	7.41465
6	hello-world-reverse-uri9.pdf	pdf	Adobe PDF	Import	1	redirect		No Embedded Script	0	1007	c4f90f2ae4456ccfba2993	4.81834
7	js_sample.pdf	pdf	Adobe PDF	Import	1	No Suspect Content		No Embedded Script	0	455191	86ece63941dbf282df681	7.98030
8	js_sample_new.pdf	pdf	Adobe PDF	Import	1	redirect, script		var ageField = this...	0	461644	1f3870cc26d442b45ead2	7.97629
9	macro.ppt	ppt	Microsoft Powerpoint Document	Import	1	script		Attribute VB_Name =...	6	46592	32e1e27c97b0974ca6dd	6.97941
10	macro.pptm	pptm	Imported Document	Import	1	No Suspect Content		No Embedded Script	2	41215	64a2d2d9aafaa7a6ac186	7.63393
11	malware.xls	xls	Microsoft Excel Document	Import	1	script		Attribute VB_Name =...	0	23552	6496f27e9c60cf59eb5eef	3.91381
12	malware.xlsm	xlsm	Imported Document	Import	1	No Suspect Content		No Embedded Script	0	13877	1ed578f482919279af0bf5	7.30389
13	StringContinueRecords.xls	xls	Microsoft Excel Document	Import	1	script		Attribute VB_Name =...	0	1182208	694d2eb0682acbca8d41	5.98798
14	StringContinueRecords.xlsx	xlsx	Imported Document	Import	1	No Suspect Content		No Embedded Script	0	319616	a6c411bebcc254468df34	7.97970
15	SuspiciousDocument.ppt	ppt	Microsoft Powerpoint Document	Import	1	script		Attribute VB_Name =...	0	16896	2c1f5202637729d713f53	4.68159
16	1cbeff63ccf18c62b279bb3302db8849_	None	Imported Document	Import	1	No Suspect Content		No Embedded Script	0	136704	a6051da1b741fd6925a22	5.77160
17	virus.dat	dat	Imported Document	Import	1	No Suspect Content		No Embedded Script	0	315806	6046df4ac998668d218c9	7.93064

圖表 2. 網路事件內所有檔案的微觀檢查

識別系統使用各種方式偵查內嵌檔案，包括「魔術數字」及統計分析。 魔術數字為檔案識別屬性，在檔案內檢查多組魔術數字可向調查人員警示可疑的內容。 統計分析測量資料流或檔案內容的常態性，可潛在偵測資料何時注入檔案或資料流。

其他微觀檢查的方法包括檔案反混淆，是指將檔案副檔名與 MIME 和內容類型進行比較。例如，攻擊者經常將執行檔偽裝成影像檔。 附加至文件的檔案流也是一種執行檔案（巨集、JavaScript、執行檔、URL、重新導向等）內嵌式惡意軟體的攻擊手法。

沙箱提供識別分析員絕佳工具，用以判斷攻擊感染主機的方式。圖表 2 顯示針對透過網路流精簡搜尋找到之檔案的微觀檢查功能。

摘要

必須重建網路威脅期間所發生的活動，才能確保網路安全並防止更多傷害。威脅經常難以精準偵查，而優良的識別環境基本上應有搜尋功能。 透過擷取與索引化全部資料以提供網路流量百分之百能見度，可讓調查過程精準明確。輔助工具可提供視覺化、商業智慧及微觀檢查功能，不但大幅減少評估威脅的時間，並可準確描述損害之範圍以及防止更多傷害所需的安全措施與補強工作。

身分管理協助風險管控

您的員工（尤其是具有權限的使用者）也可能威脅系統。瞭解正確工具如何協助管理風險。

對企業資源（包括企業資料的關鍵資源）的威脅可能來自組織內部，不限地點職位。 因此您需要全面性的工具組合來管控風險。您需要可觸及企業每個角落的工具，藉以提供每個動作的洞察，並協助管理可存取公司環境的所有人員。

您的員工可能是最脆弱的一環

今天的許多組織中，最嚴重的安全威脅並非來自外部攻擊，而是可危害或外洩機密資料的內部人員。 企業運算當前的趨勢（社群媒體崛起、雲端、行動性以及海量資料時代來臨）使得員工、約聘人員、合作夥伴及其他具有存取權限之人員所帶來的威脅，更加難以辨別，也讓內部人員有更多方式可取得受保護之資訊而不被發現。

內部威脅來自各式各樣的攻擊者，可讓組織和其資產處於風險狀態。除了惡意員工是明顯的威脅來源外，使用者也可能不慎讓系統暴露於攻擊風險，或因疏忽而讓惡意軟體有機可乘。即使是安全措施嚴密的企業也難以抵擋社群工程的威脅，讓網路犯罪得以竊取存取認證資料。例如，攻擊者寄送帶有惡意軟體的電子郵件給無警覺的員工，以取得廠商顧客資料的存取權限。[5]

向使用者清楚說明可疑通訊與潛在風險的特性，十分重要。不過還需要其他支援才有用，例如功能更強大的自動化威脅防護工具以及全面性的安全原則。

使用 IAM 解決方案降低內部威脅

身分與存取管理 (IAM) 解決方案是對抗內部威脅的關鍵，能協助消除安全威脅，並減少因使用者存取權限過期或不當所致的違規情形。 事實上，當使用者設定檔的資源存取權授予不符目前需求或實際使用模式時，內部威脅的潛在危機更高。意圖發動攻擊的內部人員也可能利用管控不足的管理權限，提升攻擊等級或改變系統以達竊聽目的。使用者存取權限的管控與監視不足，加上權限遭到誤用或濫用時難以發現，造就了成功內部攻擊的有利條件。因此，務必確定存取權限符合既有安全原則，且用於監視使用者行為並執行原則的稽核和報告工具都已就緒。

面臨內部威脅時，保護重要資料與資源不僅止於要求每位使用者擁有一組簡易的使用者 ID 和密碼。您需要根據健全原則施行嚴格驗證以確認身分。如此不但有助於防止組織外部的攻擊，也減少內部人員不慎洩漏資料的機會。另外，此作法還能防止意圖不軌的員工利用管制寬鬆的過期或孤立帳戶來攻擊您的重要資源。

組織也應當使用身分管理解決方案，協助依照角色和存取條件分類使用者，進而設定及施行基於角色的原則以自動化使用者生命週期和密碼管理。僅允許或拒絕應用程式存取仍嫌不足，您還須知道要求存取的人員和原因為何，以及個人被授予存取權限後，會如何運用。IAM 解決方案也應執行監視與嚴格管控，以協助辨別原則違反行為以及可視為內部威脅警訊的濫用情況。

具有權限的使用者常帶來最大的威脅

資料中心整合、雲端運算、虛擬化及委外服務的趨勢，造成今天 IT 基礎架構中，有更多 ID 被授予權限。集中管理並保護具權限之 ID 的需求因此提高，並要注意授予哪些人員具權限的 ID。這些具權限的使用者可藉由其總體存取權，沒有阻礙地控制並運用組織資料、應用程式和端點。若未適當管理具權限的使用者 ID，除了提高資料遭竊的風險外，還可能造成職責歸屬與法規遵循問題。 此外，針對其他群組（權限較低，但風險仍高）的內部人員存取控制也不能馬虎。系統管理員與其他 IT 員工雖能調查內部攻擊事件，也不能免於受監控。如圖 5 所示，最近 IBM 研究中受訪的決策者已注意到管理者和具權限的使用者所帶來的安全威脅。

值得慶幸的是，組織可用多種方式來降低內部威脅。更嚴格的原則管控並提高使用者意識，乃不錯的開始。這意味著確保組織全體員工均瞭解本身在特定作業上的責任與職責範圍，同時知道如何避免攻擊與不當存取。公司方面應確保員工遵守最新法規要求。

這些措施需要有效的安全工具支援。可監視行為與並提供異常偵測功能的安全情報解決方案價值非凡，例如權限身分管理 (PIM) 解決方案便可管控並監視「超級使用者」的存取行為。身分管理工具可幫助確保使用者的存取權限符合該名使用者的工作職責。若情報與管理工具得以整合，就能長期阻絕惡意內部攻擊。

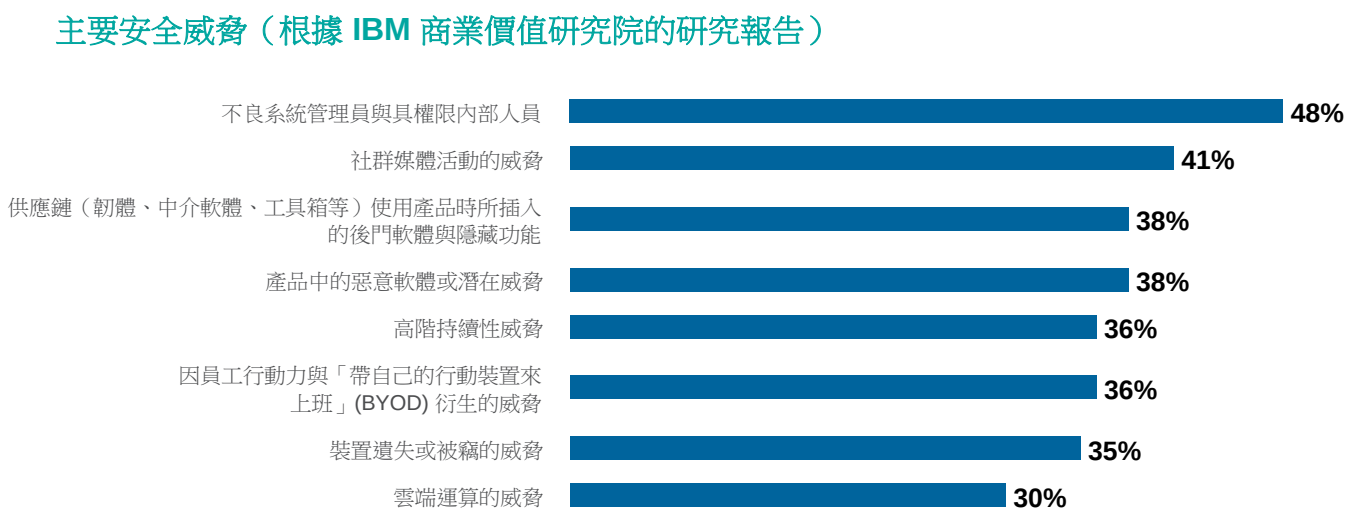


圖 5. 主要安全威脅（根據 IBM 商業價值研究院的研究報告）

資料來源： IBM 商業價值研究院 IT 基礎架構調查；Q7： 您對下列資安威脅的看法？

使用作業情報作為秘密武器

為求有效對抗內部威脅，必須建立並維護對高階主管的存取控制及監視機制，因為他們通常可隨意存取組織最高機密資料而不受拘束。 若缺乏適度監督，幾個月前離開組織的高階主管（甚或是已入侵系統的攻擊者）便 可運用主管權限存取您的伺服器、裝置網路及資料。所謂對這些使用者及其活動監督得宜，是指在機密資訊 遭到不當存取、散佈及下載時，會發出警示。

為了有效確認使用者職責歸屬並降低內部威脅，組織應考量整體採用可支援分析功能與安全情報的 IAM 方式。此種方式可讓組織快速準確地發現異常使用者行為、瞭解使用者角色與群組成員、防止內部人員詐欺並確定遵守快速增長的安全法規。

整合性的身分情報系統也可監視使用者活動，這屬於積極防護 內部威脅的重要一環。 例如，整合運用安全情報分析與報表工具，能取得關鍵功能以稽核使用者活動並發現可疑行為。 藉由安全情報，使用者活動監視解決方案能提供使用者活動及其 影響的全面性透視。

安全情報也能幫助偵查長時間的內部威脅。有些解決方案聚焦於特定事件、資產或交易類型，以便儲存與分析規模較小且易於管理的資料量。如此一來，即使「低調慢性」的內部攻擊亦無所遁形。 安全情報最棒的優勢是協助企業掌握現況，並預測未來可能發生的威脅；組織藉此能防止潛在的資料外洩。

建議

幫助企業減少內部威脅並加強合規性的最佳作法為何？

隨著具權限的 ID 持續增加，相關風險的控管也要提升。 組織經常將特定行政管理任務指派給一群員工或約聘人員，不過這些人的職務角色經常變動。此外，諸如應用程式負責人或開發者等員工，可能會要求臨時或一次性的權限，以存取特定資源進行維護工作。 這些 情況皆會造成組織內的 ID 提供數量劇增。允許多位具權限的使用者針對各項資源分享一或多組通用的使用者 ID，或可迅速管控 ID 增長，但這並非絕佳辦法。這種作法雖可避免因使用者來去頻繁以致帳號不斷增加又 刪除的麻煩，但也會破壞使用者的職責歸屬。 除了會破壞使用者職責歸屬外，還有礙法規遵循。 更好的解決方案是部署身份管理系統，藉此提供 IT 工作人員安全便利之方式來共用 ID 權限，同時對個人使用者行為進行稽核追蹤。

授予使用者適當權限並隨時保持更新。 使用者權限需要更新以因應變動，尤其應在工作人員職務變更或離職時更新。每個組織均可採用的簡易最佳方案為依據使用者所需最低存取權限來予以授權，然後定期稽核使用者權限。由於潛在傷害力會隨權限提高而擴大，具權限的 帳戶數目應當保持在最低需要量。 授予 ID 權限時應先詳查，僅限授予真正需要存取權限且擁有必要認證與許可的人員。

針對安全性與合規性管理並監視使用者。 使用者帳戶一旦建立，組織就應謹慎監督並稽核與此 ID 關聯的活動，以注意異常行為或帳戶權限誤用情況。 透過將使用者與應用程式監視功能結合應用層級的網路能見度，組織便能更有效偵查異常活動的偏差，進而阻絕攻擊。

關於 X-Force

進階威脅危機四伏。 讓 IBM 專家的洞見幫您將風險降至最低。

IBM X-Force 研發團隊研究並監控最新的威脅趨勢，包括漏洞、洩漏、主動攻擊、病毒和其他惡意軟體、垃圾郵件、網絡釣魚及惡意的網頁內容。 除了對新興的重要威脅給予客戶與大眾相關建議，IBM X-Force 還提供了安全內容來幫助保護 IBM 客戶免受這些威脅。

IBM Security 協同作業

IBM Security 代表數個品牌，提供廣泛的安全能力：

- IBM X-Force 研發小組發現、分析、監控並記錄大範圍的電腦安全威脅、漏洞及駭客攻擊的最新趨勢和方法。 IBM 的其他團隊則運用此豐富的資料，為我們的客戶發展保護技術。
- IBM X-Force Exchange 為健全的全球威脅情報分享平台，旨在使用、分享並處理威脅情報，並由規模與信譽兼備的 IBM X-Force 提供支援。使用者可以搜尋源自機器生成情報的各種威脅指標，並透過人類智慧增加相關內容，以協作方式進行研究並阻止威脅。
- IBM Security Trusteer® 系列產品提供了一個全面的端點網路犯罪防範平台，能幫助企業組織預防金融詐騙及資料外洩。上百家企業組織跟上千萬名一般使用者都倚賴 IBM Security 的產品來保護他們的網路應用程式、電腦及行動裝置，以避免受到線上威脅（例如進階惡意軟體和網絡釣魚攻擊）。
- IBM X-Force 內容安全團隊透過緩慢、仔細且獨立地搜尋和 IBM 資訊安全代管服務所提供的資訊來獨立搜索、分類網頁。
- IBM 資訊安全代管服務負責監控跟端點、伺服器（包括 Web 伺服器）和一般網路基礎架構相關的漏洞。 這個團隊追蹤了利用網頁及其他如電子郵件和即時訊息而散佈的漏洞。
- IBM 專業安全服務提供各企業安全評估、設計及部署服務，藉以建構有效率的資訊安全解決方案。
- IBM QRadar® 安全情報平台為安全情報及事件管理 (SIEM)、登入管理、配置管理、漏洞評估和異常偵測提供了整合式的解決方案。為人員、資料、應用程式及基礎架構間的安全與法規遵循風險提供了一個統一的儀表板和即時的洞察資料。
- IBM Security QRadar Incident Forensics 的設計是用來讓企業安全團隊能確實掌握網路活動及識別使用者行為。 它可以索引封包擷取 (PCAP) 檔案中的中繼資料及裝載內容，藉以重建工作階段、建立數位印模、凸顯可疑內容，以及促進視覺化的搜尋導向資料探索。 QRadar Incident Forensics 輕鬆整合 QRadar 安全情報平台，而且只需一個 QRadar 主控台管理介面就可以存取。
- IBM Security AppScan® 讓企業組織能夠評估網路及行動應用程式的安全性，加強應用程式安全的管理，並藉由識別漏洞來符合法律規範，以及使用智能修正建議以緩解補救措施。IBM 託管應用程式安全管理服務是一種雲端型解決方案，用以動態測試在試驗性生產及生產環境中使用 AppScan 的網路應用程式。
- IBM Security 身分與存取管理解決方案可在今日的多樣化環境中，透過保護與監視使用者的存取權限來協助改善合規性並降低風險。 如此可藉由相關內容存取控制、安全原則執行及業務驅動式身分管理，進一步保障重要資料與應用程式的安全。

協作者

因為 IBM 全體上下的協同幫助，才得以完成 IBM X-Force 威脅情報季報。 我們要感謝下列的各位，如此重視這份季報，並付出貢獻。

協作者	職稱
Ben Wuest	IBM 安全情報 (IBM Security Intelligence) 高階技術職員
Doug Franklin	IBM X-Force 進階研究 (IBM X-Force Advanced Research) 研究技師
Leslie Horacek	IBM X-Force 威脅回應 (IBM X-Force Threat Response) 經理
Michael Campbell	IBM 安全系統銷售促成 (IBM Security Systems Sales Enablement) 高階安全專員
Pamela Cobb	IBM X-Force 威脅產品組合 (IBM X-Force and Threat Portfolio) 全球市場區隔經理
Ralf Iffert	IBM X-Force 內容安全 (IBM X-Force Content Security) 經理
Robin Cohan	IBM 安全身分管理 (IBM Security Identity Management) 產品經理
Roger J. Hellman	IBM 安全情報 (IBM Security Intelligence) 全球市場區隔經理
Russell Couturier	IBM 網路識別 (IBM Network Forensics) 首席技術主管
Tim Kroupa	IBM 緊急應變服務 (IBM Emergency Response Services) 專案主管
Veronica A. Shelley	IBM 身分與存取管理 (IBM Identity and Access Management) 全球市場區隔經理

更多資訊

如需進一步瞭解 IBM X-Force，請造訪：
ibm.com/security/xforce/

[1] 《IBM Security Services 2015 Cyber Security Intelligence Index》，http://www-935.ibm.com/services/us/en/it-services/security-services/index.html?lnk=sec_home

[2] Sean Michael Kerner，《AT&T Insider Data Breach More Dangerous Than External Hacking》eWEEK，2014 年 6 月 14 日。http://www.eweek.com/mobile/att-insider-data-breach-more-dangerous-than-external-hacking.html

[3] Darlene Storm，《Remotely listen in via hacked VoIP phones: Cisco working on eavesdropping patch》Computerworld，2013 年 1 月 8 日。http://www.computerworld.com/article/2474060/cybercrime-hacking/remotely-listen-in-via-hacked-voip-phones--cisco-working-on-eavesdropping-patch.html

[4] Chris Poulin，《What Retailers Need to Learn from the Target Breach to Protect against Similar Attacks》，IBM Security Intelligence Blog，2014 年 1 月 31 日。http://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers/#.VUtHXPmqjRY

[5] Adam Greenberg，《Home Depot announces 53M email addresses stolen in breach》SC Magazine，2014 年 11 月 7 日。http://www.scmagazine.com/home-depot-announces-53m-email-addresses-stolen-in-breach/article/382144/

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
June 2015

WGL03076-USEN-00