有效降低網路安全風險的管控對策

從 BYOD 個人自帶裝置、IoT 物聯網和人為失誤談起

人們普遍認為多年前芝加哥某所高中的學生，與史上第一件網路駭客的事件有關。在 1967 年，Evanston 城區高中的電腦社團透過 IBM 當時所捐贈的一台以 TTY 為基礎的終端機，駭入 IBM APL 網絡系統。數年後，Creeper(史上第一隻病毒)在 ARPNET（網際網路的先趨）上擴散開來。它在電腦間不停地複製並且留下「我是 Creeper，有本事的話，來抓我啊」的訊息。

1984 年，「病毒」這詞首次在南加大 (University of Southern California) 出版物內的一則網路安全相關文章中出現。隨著 80 年代邁入 90 年代，人們對於網路攻擊對整個社會的影響也有越來越清晰的認知與理解。第一屆 DEF CON 駭客大會首次於 1993 年召開，並且很快地成為一年一度的例行網路安全盛會。

隨著數位科技在 90 年代末期及 20 世紀初快速地演進，網路攻擊及資料盜取事件也層出不窮。社群媒體的出現、行動裝置在家庭及工作場所中的普及，以及電子商務的快速成長，這些應用開發都成為不肖份子的新犯罪機會；善意使用者也可能因一時失察而付出昂貴的代價。

從企業組織的角度來看，網路安全早就不再只是 IT 部門的責任了。在企業組織中，每個人的日常作業皆需對網路安全有正確的觀念並受到規範，採用國際認可的網路安全系統設計標準並進行教育訓練，將可提升資料保護層級，同時也符合相關法令法規的遵循性要求。

找出能夠優化組織網路安全防禦力的標準是關鍵且實用的第一步，以下將從保護使用個人自帶裝置 (BYOD) 辦公的員工、快速成長的物聯網 (IoT) 安全到人為失誤，提出相關的應用標準與 BSI 的觀點：

一、自帶裝置（BYOD）之安排及管控

依據MarketsandMarkets的研究報告估算，BYOD及企業行動裝置市場在 2021 年前將成長至 733 億美元[1]。但市場對BYOD仍然有兩極的意見看法;有些人認為BYOD具有生產面的收益及節省成本的潛力，另一些人則是比較擔心資料被竊取的問題。

組織面臨的風險高低，取決於員工對於 BYOD 安全責任的體悟與了解。只是單純地假設全體員工都會做好自我教育以符合標準要求並不足夠，組織應當定期地將最佳實務對各部門及各層級人員做溝通才是重點。如果希望達到最低程度的保護等級，可以開始考慮如何清楚地制定 BYOD 政策，像是根據 ISO/IEC 27001 資訊安全管理及 ISO/IEC 38500（組織之 IT 治理）標準的規範。

組織要確保每個人員都能在相關程序上盡一己之力，同時也都能提供反饋與建議，在日常的運作中，就要定期提醒員工「資安維護，人人有責」的觀念。最理想的狀況就是指派一些受過良好教育訓練的積極員工擔任種子人員，為彼此及組織多加留意，並在適當情況下提供諮詢及介入。

BYOD 政策除了需與新進員工的教育訓練內容結合外，對於即將離職的員工，相關的程序也該納入。特別是當員工非自願離職時，這部份的程序制定更顯重要。組織可針對離職員工要求他們執行某些程序，例如刪除特定檔案等，但這必須要在 BYOD 政策內有明確的定義才行。

同時也該釐清該程序是否能信賴離職員工自行操作，或需要透過 IT 部門執行。一旦有員工確定要離職，就一定要迅速地依該政策內容執行相關程序。由於離職員工極有可能在新公司使用自己的行動裝置，在這種情況下，後續若要去取得任何相關資訊就會變得更為困難。

在設計或更新BYOD政策也該將法令法規的變化納入考量，例如：2018 年 5 月上路的歐盟一般資料保護規範（GDPR），就針對組織在蒐集、處理、利用及傳輸個人資料的流程方式要求做了相關的新增與變更，組織的相關政策應要能反映並回應GDPR的最新要求[2]。

組織可以利用 BS 10012:2017 新版的個人資訊管理標準，展現自身在 GDPR 重要條款及要求的個資保護能力。透過維護良好的管理系統來區分 BYOD 上的個人檔案或公司檔案，其效益不僅僅是能夠降低資料外洩的風險，依據標準所制定的 BYOD 政策則能持續提供最佳保護。

[1] https://www.marketsandmarkets.com/Market-Reports/enterprise-mobility-334.html

[2] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

除此之外，員工在外的行為也應該納入考量。例如：當使用行動裝置的人員在公司以外的場所時，他們會認知道自己已經離開公司的資安政策 / 架構的保護範圍，因此對於網路釣魚這類威脅的敏感度將會提高（員工在接觸非工作相關之內容時，則比較容易忽略安全責任）。

當真的發生失誤時，教育訓練是不可或缺的，這點請銘記在心。組織若能維護良好的「事件回應計劃」將可釐清責任歸屬，並且確保危害事件發生時能採取正確的方式來因應，其重點就在於依循可靠的標準持續進行風險評估及測試，以確保 BYOD 政策仍然有效。

二、「安全標準」是讓物聯網（IoT）成功發展的關鍵因素

雖說物聯網（IoT）在效率、自動化及整體的優化這些面向上都為我們的生活帶來極大的改善，但仍需要發展專門的安全標準以保護個人、組織及他們的資料，因為 IoT 所涵蓋的範圍之廣，「網路安全」勢必成為一大挑戰。例如，為了最大化資訊分享及自動化的效率，企業可能會讓數個系統都接上網際網路（如暖氣、通風、冷氣系統、機械、大樓保全及感應器除了連至 IoT 系統外，彼此之間也可能互相連結），這將會讓安全問題變得更為複雜、風險變得更大，同時也會增加駭客得以入侵的「後門」數量及方式。

西烏克蘭的電網在 2015 年曾遭受到攻擊，進而造成 25 萬居民斷電長達 6 小時，該攻擊侵入SCADA（資料採集與監控系統）並中斷其遠端操作的功能 [3]。另一個近期案例則是廣為人知的一個叫做「未來」的惡意軟體，該軟體在 2016 年底入侵許多防禦力不強的IoT裝置，並發動大規模的網路攻擊行動 [4]。而在數位領域之外，CAV（連網的自駕車）駕駛或車輛的安全可能在預謀的網路攻擊中遭到威脅，讓實體弱點顯而易見。

為了贏得大眾的信任，IoT 市場需要的是廣為接受的網路安全最佳實務與標準。重要的是如何確保那些蒐集、分享與處理的資料之安全性，當然 IoT 裝置本身的安全性也同樣重要。每個月都有新的 IoT 產品上市，然而每家製造商確保其安全性的方法也都不同；若無法遵循像 ISO/IEC 27001 這類的國際標準規範，實在很難向廣大的市場保證在產品設計階段就有導入適當地的安全管控機制。

在這樣一個成長快速的新興市場，對於每一個準備好上市的 IoT 裝置，我們的確該思考這些問題，例如：

- 雲端服務供應商通過哪些資訊安全驗證？

[3] https://www.incapsula.com/blog/critical-infrastructure-cyber-security.html
[4] https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/

- 製造商是否有花心力教育潛在使用者，讓他們獲得基本且重要的資訊安全認知，例如：變更預設密碼…？
- 資料傳輸是採用哪種加密標準？存取管控及使用者授權的方式又是如何？

BSI 是 IoT 安全領域的領頭羊，協同 Hypercat 聯盟共同開發了 PAS 212 物聯網資源自動發現的標準，而與其高度關聯的還有「智慧城市」標準，像是 PAS 182 智慧城市概念模型，以及 PAS 183 智慧城市決策框架指南，都是值得被關注的重要標準。

PAS 182 標準描述了如何定義來自許多不同領域（如健康、教育和交通）的資料含義，以便更容易地共享資料並在各個領域間共享；PAS 183 為適當的使用資料制定方針，並闡明了哪些類型的資料可以被揭露和共享，以及哪些又應該被保密，定義出各城市間資料分享的架構。

長遠來看，這些標準對於個人及組織如何因應及降低 IoT 風險是非常關鍵的。物聯網的成長是全球性的，而這樣的特質需要的是在安全標準的開發與維護上，能夠有一套放諸國際社會皆準的協定方式。為了面對這樣的挑戰，BSI 致力於開創出一個全球性的聚落，同時也期望能夠加速國際社會對於 IoT 安全標準的採用。

三、降低因人為錯誤所造成的風險

人為錯誤始終是組織網路安全風險中的一部分，而且往往無法被排除。每年層出不窮的資安與資料外洩問題中，人為因素佔大宗，所以「人」經常被視為是網路安全系統中最弱的一環。若是將人為因素納入考量的話，以標準為本的安全意識的教育和訓練之重要性則不容小覷，還有可能將此人為因素轉化成正面能量。

犯罪分子經常尋求機會駭入個人系統而非組織的系統，因為他們了解社交工程技術對於那些可能沒有網路安全意識的忙碌員工是多麼有效。Wombat Security的「Beyond the Phish 2017」報告[5]中顯示有近四分之一（24%）的受訪者無法正確地回答如何識別網絡釣魚威脅，這情況對駭客來說無疑是竊取對方資料和身份的絕佳機會。

公司應該努力協助員工在網路安全鏈中成為更強大的一環──讓他們成為「人員防火牆」，而不是被動式的思維模式。特別是現今在家工作概念的盛行，以及使用 BYOD 工作的員工的普及，這點尤其重要，網路安全意識必須跨出員工的日常工作空間。

根據 Wombat Security 的研究發現，當涉及到所謂的簡單保護措施時，員工普遍缺乏相關意識。例如，超過一半的美國員工認為，在他們認定安全的空間中，可以信

[5] Beyond the Phish Report 2017, published by Wombat Security: www.wombatsecurity.com/beyond-the-phish

任其開放的 WiFi 網路，安裝 VPN 的英國員工有 40%說他們很少或從不使用它，甚至有超過一半的美國和英國員工會將筆記型電腦留在車裡，而不是帶著進餐館。該研究還強調了實體安全面的常見訓練需求，例如：保護門禁卡、紙本文件以及列有供應商詳細資訊的重要文件等。

組織可以透過網路釣魚攻擊的模擬和知識考核，準確地評估所需的教育訓練內容和當前面臨的風險，並根據資訊安全標準 ISO / IEC 27001 幫助組織依循國際認可的最佳實務作法來設計或架構出適用的訓練內容，為員工不同的業務需求，量身定制教育計劃。

除此之外，還應考慮提供網路安全教育訓練的頻率。一年一次的方法是達不到預期效果的，同時也會讓員工覺得這種訓練可有可無。我們建議對員工進行簡短但頻繁的訓練，同時提供內容一致的教材。為了真正改變員工的行為，塑造出一個「實際參與」的企業文化也是相當重要的，因為當員工有機會提供反饋並提出建議，就更能夠提升他們的參與意願。

一轉眼的時間，網路安全已經從模糊不清的概念，發展成各國間重要的議題，也從原本的學術性實驗，成為經濟、城市、政府層面的重要政策。與網路相連結的關鍵基礎設施，政府現在得 24 小時確保其安全；若無法有效地確保重要服務及資源，則數百萬人的生活將首當其衝。即使國際間已有許多網路安全相關標準被廣泛使用，在組織有限的人力與資源下，依據 BSI 鑑別出的 11 個以 ISO 27001 為核心所延伸的網路安全關鍵標準，就能夠著手展開您的網路安全管理升級計畫，確實降低相關風險。

網路安全關鍵標準 Top 11

- ISO 27001：資訊安全管理系統驗證標準，是每個網路安全策略的核心基礎 **相關課程**
- ISO 27002：資訊安全管控之作業規範
- ISO 27003：資訊安全管理系統指引
- ISO 27005：資訊安全風險管理
- ISO 27017：基於 ISO / IEC 27002 的雲服務資訊安全控制作業規範 **相關課程**
- ISO 27018：公有雲個人資料（PII）處理者之個資保護作業規範
- ISO 20000-1：IT 服務管理系統 **相關課程**
- ISO/IEC 27031：營運持續性之資訊與通訊技術準備指南
- ISO/IEC 27032：網路安全指南
- ISO/IEC 27033-1：網路安全概述與概念
- ISO/IEC 27034-5：軟體安全指引

● **洽詢 BSI** ｜ 稽核驗證、產品測試、BSI 訓練學苑、VerifEye 認證平台、BSOL 標準資料庫

BSI英國標準協會
T: +886 2 2656 0333 ｜ E: infotaiwan@bsigroup.com ｜ www.bsigroup.tw