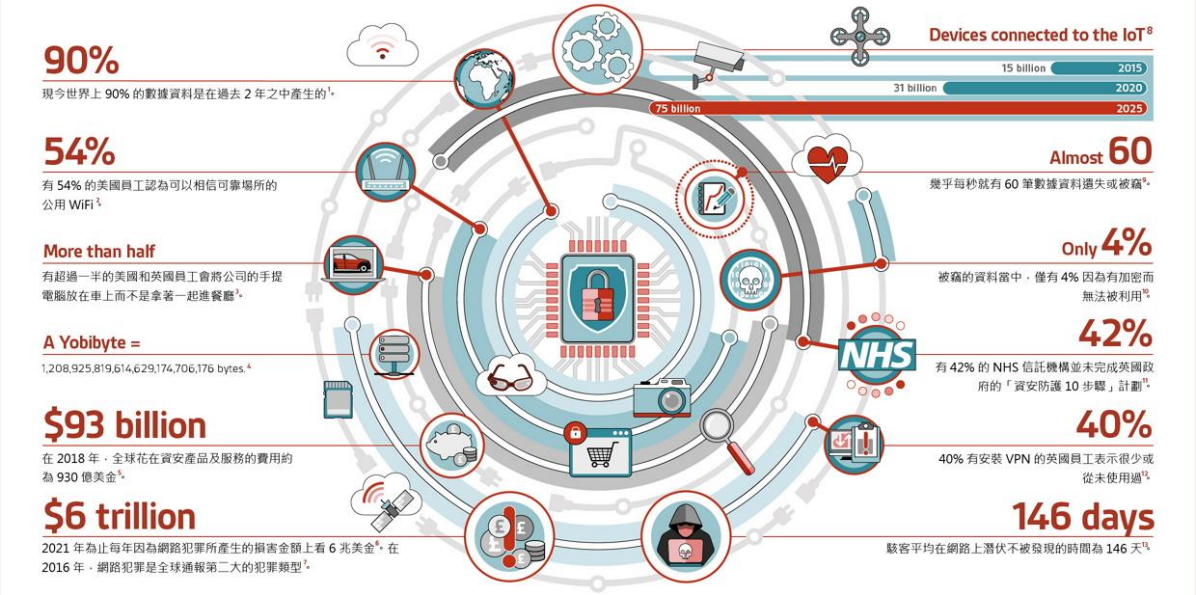
# 有效降低網路安全風險的管控對策 後篇

## 關鍵基礎設施與個資保護

數位科技在 90 年代末期和 20 世紀初快速地發展，隨之而來的網路攻擊及資料盜取事件也層出不窮。經過一個世代的時間，網路安全這個概念已經從有些模糊變成國際間重要的議題；網路安全已經從原本的學術性實驗變成經濟、城市、政府層面的問題了。我們可以從〈圖一〉看到網路安全的趨勢和現況數據。

對各國政府而言，針對連接網路的關鍵基礎設施，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網路的安全，則數百萬人的生活將首當其衝。而個人資料保護則是網路安全的另一個重要議題，駭客威脅的複雜性和資料盜取的情形已大幅增加。對企業組織而言，好的資料管理、加強資料保護已成為不容忽視的議題。相對的，能證明善盡資料管理和保護責任能幫助企業獲得利害關係人和客戶的信任，因此對企業組織來說也是一個提高聲譽的機會。

「標準」做為公認的最佳實務，為企業組織提供了架構，協助這些組織滿足各式規範的要求、降低風險及提升防禦力。繼〈有效降低網路安全風險的管控對策 前篇〉找出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）安全到人為失誤相關的標準，本篇將提出能夠提升關鍵基礎設施與個人資料保護的相關標準與 BSI 的觀點。



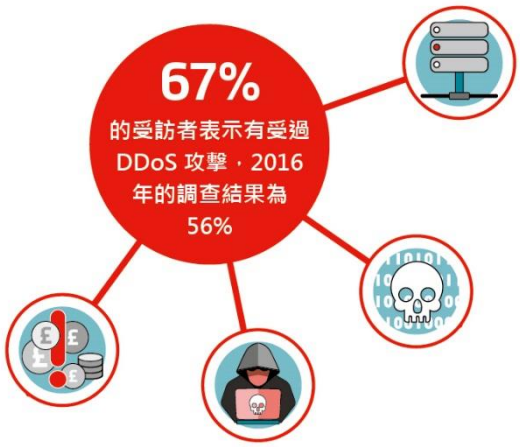

〈圖一〉網路安全趨勢與統計數據（點此放大）

## 提升網路安全 保護關鍵基礎設施

電力、通訊、暖氣、醫療保健及交通網路是一個運作正常的社會中的必要資產，政府一般都會將其定義為關鍵基礎設施。上述這些設施只要其中一個或數個失效的話，就會立即影響到數百萬人民的生活，哪怕只是短時間失效。

在現今的國家基礎建設中，都是環環相扣、相互依賴─互享資訊以提昇效率及管控力。然而，這也同時揭露了整個系統的弱點，意即只要其中一個環節出錯/失效，就將在整個連結的網路中發生骨牌效應。從網路安全的觀點來看，持續性的風險評估及減輕風險是提昇防禦力的不二法門。

關鍵基礎設施往往成為網路攻擊的首要目標。除了這些設施有其重要性外，會吸引駭客的原因還有當中隱藏了許多可進行滲透的管道。例如，2017 年完成的一份全球性的基礎設施調查中顯示，有67%的受訪者表示遭受過多向性阻斷服務攻擊（multi-vector DDoS），2016 年的調查結果為 56%;而這些攻擊結合了流量攻擊、應用層攻擊與網路協定層攻擊的元素讓系統更難以抵禦[1]。




許多大型的基礎建設網路也未被適當地保護。一份 2017 年的調查報告指出，在英國的 338 家關鍵基礎設施機構中，有 42%的國家醫療服務（National Health Service, NHS）信託機構並未全數完成英國政府的「資安防護 10 步驟」計劃（該計劃於 2012 年開始）；而且當中有超過一半的機構忽略了在他們的網路中迅速又隱密的 DDoS 攻擊會帶來的風險──一般包含植入惡意軟體、勒索軟體及竊取資料[2]。

除此之外，在許多國家中，這些關鍵基礎設施的網路都由各式不同的私人機構營運並且與政府單位在地方、區域及國家層級的面向上做緊密配合。由於當中牽涉到為數眾多的團體與利害關係人，採用相關單位都認同的最佳方式做為網路安全的佈署基礎是有其必要的。

BSI 會透過定期召集會議、委員會和工作小組來結合政府和負責關鍵基礎設施的事業單位，以便用大家都認同的方式來開發及維護一個國際級的最佳執行方式。當初，ISO/IEC 27000 系列標準也是用這樣的模式開發出來的。

---

[1] http://www.darkreading.com/cloud/7-things-to-know-about-todays-ddos-attacks/d/d-id/1329758?piddl_msgid=329347&image_number=3

[2] www.scmagazineuk.com/critical-infrastructure-not-ready-for-ddos-attacks-foi-data-report/article/684838/

採用公認的標準為關鍵基礎設施架構一個具有韌性的防護網，能夠向社會大眾展現保障網路安全的承諾；這同時也代表著，有一套適當的管控機制在其中運作。此外，這些關鍵基礎設施的供應鏈成員是否採用公認的安全標準並取得驗證也是相當重要的。這讓供應鏈中的潛在夥伴可以放心地分享及傳遞他們的安全憑證，並且提供一個可持續改善、進行品管稽核以及驗證流程的架構。

除了可緩和來自外部的網路攻擊力道外，以標準為基礎、用來保護關鍵基礎設施的作為也可降低人為錯誤所帶來的風險。專業的訓練及績效評估都可協助組織的重要部門建立資訊安全意識，以維持一定水準的管理責任。另外，在網路安全事件的調查中，若可證明組織的管理政策符合受認可的國際標準，那麼就可能在消除「專業疏忽」這類的指控上成為決定性的因素。

最後，我們需要理解制定新的法令規範往往曠日廢時，但狡猾的駭客變化莫測並且持續進行破壞攻擊；國際社會透過長期的合作，開發及維護大家認同的標準則會是在全球保護這些關鍵基礎設施及資訊相當有效的方式。

## 個人資料保護、GDPR 與遵循性

2018 年的歐盟一般資料保護規範( GDPR )取代了 1995 年頒布的資料保護法令；因為舊的法令對於保護涉及 Google 或 Facebook 這類網路及雲端巨人相關的個資已經不敷使用了。

立法的腳步難以跟上科技發展的速度以及科技所催生的社會及商務轉型。GDPR 則是立法慢慢趕上科技發展的一個最佳範例。在 GDPR 初次問世 ( 2011 年 ) 和實際執行 ( 2018 年 ) 之間的幾年間，我們見證到智慧型手機、語音搜尋和物聯網 ( IoT ) 成為主流的過程。然而，與此同時，駭客威脅的複雜性和資料盜取的情形也大幅增加，所幸，良好的資料管理這樣的基本原則依然是不變的最高指導原則。

對於不合規的行為，GDPR 祭出更嚴格的罰則與罰金，並且明確地唯組織是問；這使得歐盟居民和公民能夠對其個資擁有最大的掌控權力。這個歐洲半世紀以來資料隱私法的最重大變更在 2018 年 5 月正式實施前，其實在主流媒體上已獲得大量的討論。

儘管如此，別忘記還有超過 100 種不同的區域性資料隱私法規─每一種都有不同的要求與規定。企業組織以標準為本的資料治理作為，將是持續實現全球合規的最佳基礎。

使用公認的標準來為資料保護流程提供資訊，可幫助組織了解他們眼前和潛在的風險規模，並且提供一個可被管理或減少風險的管控架構。驗證有助於獲得利害關係

人和客戶的信任，以及證明他們的個資是受到保護的。事實上，許多具有前瞻思維的企業將 GDPR 視為可藉此建立聲譽的最佳機會。

BS 10012 為企業組織提供了定義 GDPR 風險和合規要求的途徑，然後以最適合其企業組織的方式實施個資管理系統。系統到位後，組織可以申請獨立驗證，以證明他們已對個資進行有效的管理，及確保流程已維持並能持續改善。

最後，針對受認可的資料管理標準進行驗證還可向所有主管機管保證適當的管控措施皆有到位，並確保供應鏈的各層級皆能各司其職、各付其責，進而提高供應鏈各夥伴之間的合作透明度。

## 關於資料的 5 個議題及其他相關標準

BS 10012 能協助企業管理關於資料的 5 個議題：

| | | | | |
|---|---|---|---|---|
| 1 Whose | 2 Why | 3 Where | 4 When | 5 What |
| 誰的資料？ | 為何我們需要處理這些資料？ | 要在何處保存這些資料或是要轉送到哪去？ | 要保存這些資料到何時？ | 建置了哪些安全防禦機制？ |

其他相關標準包括

ISO/IEC 27018：保護公有雲端中的個人身份資訊
ISO/IEC 29151:2017：提供與 ISO/IEC 27001 協同運作的一系列額外管控
BS ISO/IEC 38505-1:2017：用於資料治理和資訊流的管控
ISO/IEC 27002：為延伸 ISO/IEC 27001 的新標準，用於資訊科技領域的資安管理
ISO/IEC 27552：包含對隱私管理的要求和指引

## 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