Part 2：綜合座談

別幫駭客開後門─資安法下的「風險預測」及「防禦提煉」時代

2019 BSI InfoSec Standards 國際資安標準管理年會

責任編輯 徐瑋琳 | 內容修訂 黃純郁 | 採訪撰文 鄭詠中

第十七屆 BSI 國際風險管理年會於 2019 年 11 月 22 日舉行。本屆主題聚焦於「資安法下的『風險預測』及『防禦提煉』時代」，道盡時下面對的挑戰與處境。大會今年首度舉行「資安管理劇場大探討」綜合座談，邀請揚名海內外的資安高手、國家資安政策掌舵者及國際標準制定者進行座談，精選來賓投稿的資安劇情，由不同專業領域的專家現場解讀資安病徵，指處出改善方向，優化資安管理績效。座談重點內容整理如下：

綜合座談【你的情境，我的借鏡】

資安管理劇場大探討

主持人：BSI 英國標準協會東北亞區 蒲樹盛（Peter Pu）總經理

與談人：行政院國家資安會報技服中心 吳啟文主任、iThome 吳其勳總編輯、 DEVCORE 戴夫寇爾 翁浩正（Allen）執行長、BSI 英國標準協會台灣分公司 謝君豪（Joe Hsieh）營運長

「你的情境，我的借鏡」是本次資安管理劇場大探討的中心概念與用意，主持人 Peter 妙語如珠介紹各位與談貴賓。待大家在台上一字排開坐好，螢幕上一個個題目出現，主持人 Peter 用白話替大家直搗核心，聚焦在產業當務之急，並指定在場專家回應。

「資安管理劇場大探討」，左起：BSI 台灣營運長 Joe、DEVCORE 執行長 Allen、技服中心主任吳啟文、iThome 總編輯吳其勳 ，以及 BSI 東北亞區總經理 Peter。

Q1 資安法公布後，對適用機關的資安人力均有明確要求，資安人才頻頻被挖角，部門內的人力技術能量與經驗都不夠，資安業務出狀況也多只能找外援，或將責任歸咎於供應商....（Peter 白話翻譯：人力短缺怎麼辦？）

吳主任：人力短缺的問題，政府是重視的。資通安全管理法上路之後，各級單位按規定要配置到位的資安人才數量，目前統計公部門短缺人才數達一千人。專法施行有過渡條款，暫時兩年內可作委外。由技服中心[1]主辦的資安技能競賽「金盾獎」，向下紮根行之有年，當年有從國高中開始參賽的學生，也因參加得獎的成績加分進入交大資工；除了可從學校尋求，也可從職場合適背景的人才，訓練擔任資安工作，將因應資安法的職能分為策略、管理、技術三個面向，要求政府資安人才依據職能訓練藍圖取得證書。

吳總編：人才短缺的問題，是全球性的問題，其中更看見資安人才角色日趨複雜化（管理、稽核、技術專業），缺人是事實，人才流動也會更快速。**建議大家從不同角色切入，看企業需求去找才—之前提到的國際標準 NIST Cybersecurity Framework 內含界定人才的介面可供參考。當大家都在搶人才，你不見得搶得到，就試著把原來的人才訓練成你要的人才。**有研究統計，長期來看，發現團隊原來的成員經過訓練之後，比委外廠商做資安做得更踏實，可見自己培訓人才有其必要性。

Peter：兩位專家從公部門立場與媒體觀察角度分享，藉此歸納出兩個重點：1.不可能找到全才，但可以按需求找到最需要的單一人才。2.國際間大的資安主管多半不是資安背景出生，但透過訓練，足以擔當現任職務，就看組織是否有合適的資安訓練。

Q2 國外企業組織或機關在資訊安全的作為與觀念都較為先進且開放，爆發資安事件後的反應與態度也較為積極，相信民族性、企業文化與資源策略的關聯性甚大。（沒錢的情況下怎麼做資安？）

Allen：如果希望資安預算能夠調整，首先要創造成功的經驗。資安預算無法增加，可能來自於組織過去投入預算但效果不彰。IT、資安人員要讓「資安意識」到「風險控制」建立正循環，說老闆聽得懂的話，像是：「這個事情做了之後，我們和主要競爭對手的差異化就出來了」，做好向上管理。如何精用預算？此時就突顯了框架的重要性，從管理面和實作面去看，幫助我們找到最需要投入資源的關鍵點，然後循著 P.D.C.A，創造資源，活用資源。

吳總編：當外界發生資安事件時，而自己沒出事，就代表目前的投資是有效的。現在比過去好說服老闆，是因為資安事件越來越多，但除了金融界，大家的預算永遠

[1] 「行政院國家資通安全會報技術服務中心」之簡稱。

是不足的。預算不夠反倒促使思考：如何在資源有限下做正確的決定？**經過 iThome 調查，發現資安最大的問題其實是在人員資安意識不足，所以重心可先放在此，提升整體的資安意識，風險可能就先降很多，這或許是在資安預算到位前可以著手的事。**

Allen：國內外都有很多參考，資安預算比例，政府明文規定至少是 IT 預算的 10%，這可以是個參考值，再按我們實際的需求去調整。當要制訂資安策略時，除了考量預算數字，反而是**建議將資安執行計畫的時間軸拉長，資安不是一次就能做好，若設定三年後組織要導入完成哪些系統，再反推這一、二年我要做到什麼？每一個工作都出來了，預算就能比較精準地被預估出來。**

Peter：Allen 提到了一個很好的概念「建立正循環」，把資安預算當做「好」的預算、「正向」的預算，不要等待出事時才再編列預算，藉由我們怎麼去看待。

Q3 **「領導統御」對資安的重要性不言可喻，甚至資安應該成為董事會的議題。但事實上公司內的高階管理者許多不具備 IT 或資安背景，報告的太少，他們不理解嚴重性，報告的太多，可能聽不懂。**

Peter：公元兩千年以後，所有 ISO 國際標準都增加一章「Leadership」，代表領導作用在成功管理上是不可或缺。如何和高階報告資安計畫是大家時常遇到的問題。藉此先要請教吳主任，政府高層在面對資安議題時會展現出那些不同的 Leadership 思維；再請教吳總編，訪談過這麼多組織高層，受訪者都用哪些態度面對領導作用？

吳主任：有關資安的領導統御，即使政府身為監督單位也是有這樣的難處，在對高階做資安會報時，要講對方聽得懂的話，而且短期內要讓主管有感。資通安全法出現之後，有公務人員獎懲規定，資安責任有可能成為政治問題，因而促使長官對資安問題重視。除了講對方聽得懂的話，還有利用每次月會報時，報告資安成效，例如社交工程演練後的各單位的成績，這個方式是有一定程度的效果。目前我們在推「資安治理」，從策略、管理、技術去評估各級單位的資安成熟度，不同面向要達到的數字也不同，利用法遵要求，透過不同管道讓高層重視與推動資安業務，給予人力與預算，決定優先順序及資源分配。

Peter：謝謝吳主任的分享，剛剛聽到的重點是「在所有人在的時候把資安評估結果公佈出來」，公務機關對資安問題應當是要重視的，目前金管會在上市上櫃公司董監事訓練上，已將資安訓練加入，就此也許**各位也可推薦自己的公司企業，在董監事訓練將資安訓練作為項目，增加高階的資安意識。**

吳總編：建議吳主任開資安會議時可以和 Allen 合作，讓公部門高階意識到：原來我們的資安防禦是如此脆弱（全場笑）。iThome 是一個科技媒體，我們擅長講白話文，編輯團隊會這樣要求編採：**1.站在溝通對象的立場想—將廠商、受訪者說的話，轉成「你要溝通的對象（讀者）聽得懂的話」，如何做到呢？將自己的技術本位歸零，不要無意識直覺性地就拋出專有名詞，理所當然覺得溝通的對象聽得懂。2.好的溝通者要能夠站在總經理的高度—你要講出高層、老闆在乎的事。**如果沒有站在老闆經營的角度去看風險，老闆可能也很難意識到你在說的事情背後的意義是什麼。

Q4 中小企業幾乎多數系統或資訊服務都是外包 (例如：活動網站、服務平台、帳務系統、eLearning 系統...)，但資安事件連環爆，了解後發現這些外包供應商的團隊幾乎很少人懂資安，不要說有沒有驗證了，連甚麼是 ISMS 或 ISO 27001 可能都不知道。

Peter：全台灣有 130 萬家中小企業，平均的壽命是 7 年，人力與預算都吃緊，自然將資安交給委外廠商，這樣到底行不行？資安法通過之後，不同等級的納管單位要將服務委外，需交給等級相當的廠商，這是非常挑戰的。這點請教吳主任，他對供應商管理有些想法；並請教我們的營運長 Joe，怎麼樣確定委外廠商符合需求？

吳主任：政府機關的資安大部分是委外，最近也發生許多來自供應鏈的資安攻擊，像是駭客先入侵共用系統開發商，再進而攻進政府機關，另外也可能透過防毒軟體或其他軟體來攻擊。隨著資安事件頻繁，政府在對資安防護和委外廠商的要求也升高。當然資安風險管理是沒辦法一下子就做到一百分，目前是透過「資通安全責任等級」來分，風險屬高等級單位的委外廠商，可能就要通過 ISO 27001 的驗證，而且單位本身要對委外廠商做資安稽核，以廠商驗證和對廠商稽核這兩種方式做資安風險管理。**公部門在制定標案時，除了要規定廠商通過哪些驗證，還要特別注意通過驗證的範圍是否包含你委外的服務；另一個是行政院資安處有推廠商資安評鑑，每年都會更新評鑑結果，將廠商分級，利用客觀公正的方式作出評鑑，讓不同等級的單位得以依據選擇委外廠商。**

Joe：公務機關和民間企業遇到的挑戰是不一樣的。公務機關在於人力緊迫，若要監督委外廠商，相關的人力一定要先建立起來，並且清楚知道要要求廠商什麼，否則只能繼續高度依賴廠商。民間企業就看主管機關的力道夠不夠，金融和電信這兩個產業的主管機關要求是相對嚴格的，這兩個產業在委外廠商管理上力道也比較足夠。當然，**對於委外廠商的管理，永遠要回來思考：組織請這樣的人力過來，是期待對方能給出什麼貢獻？若這點意識不夠，都使用制式合約，無法認知自己面臨的風險，在委外初期所做的評估會是很大的弱點。**以金融業為例，在資源足夠的情況

下，程式委外開發一定是做駐點開發，風險才能相對控管；若資源不足只能作非駐點開發，你僅能依靠合約來管理，這又回到你是否清楚你的風險在哪？而駐點廠商管理要管理得好，首先要知道如何要求駐點廠商？你期待對方做出什麼樣的貢獻，以此去要求對方。

Q5 網路攻擊手法推陳出新，許多組織缺乏安全防護機制，更談不上防禦縱深與網路安全架構的能力。

Peter：要請教吳主任和 Allen，就中小企業來講，目前主要有哪些網路攻擊手法？以及，從技術面的角度，中小企業有哪三件最重要的技術保護合作？

吳主任：以資安攻擊面向來看，目前政府遇到是以 e-mail 為主，民間除了 e-mail 還有透過 excel，偽造轉帳帳務文件的，真實程度讓人足以信以為真，而被詐騙輕信轉帳。台灣現在有很多無店面業者或電商業者，是一個人就出來開業，以為裝防毒軟體就夠，反映出欠缺資安防護觀念，目前也透過經濟部中小企業處進行資安防護的推廣。拿現在很流行的 NIST Cybersecurity Framework V1.1 的架構來分享，一般分事前、事中和事後三個階段：事前來看，目前中小企業很多都沒有防毒軟體只有防火牆，或者有裝防火牆但沒有設定，佈署不足。事中監控這一塊，對中小企業來說真的是有困難，即使是低流量的企業，一年就是幾萬塊的監控軟體監控成本對他們來說也是負擔—近幾年券商被攻擊（被勒索）的很嚴重，主關機關就要求券商提高監控與防護，等於是提高駭客成本，當駭客發現投資成本太大時他們就會撤退。事後就是情資通報，透過情資分享避免事端擴大，但以中小企業來講真的也是不容易。會建議從自己核心業務使用的系統弱點開始加強，再來是防毒軟體的加強，還有遇到資安事件時該如何因應。

Allen：現在全世界做資安，不應該說自己能做到百分百的防禦，因為沒有一個組織不會被駭。既然談到防禦，除了預防，如何應變也是重點。發生資安事件後重點在於，如何在最短的時間做應變，所以剛才主任講的事後情資分享是有其必要性。很多從政府機關到大型乃至中小型企業被駭，都是因為帳號被竊取，我會想和大家說的是，**「做資安不等於要花大錢」，方法其實很簡單只是大家都做不到**，像是不要使用已經使用過的密碼，一旦有一組密碼被破解，你所有的帳號也都可能受影響。呼應今天的主題，有些心法可用：**1.帳號管理：**一定要用雙因子認證或二階段驗證做帳號管理，駭客若是取得密碼但沒有 PIN code 或 key 也沒有用，這是所費不貴但優先可做的。**2.備份：**這兩年有幾波勒索軟體得以成功，是因為沒有做好備份，或者備份沒有做驗證，以至於備份回復之後無法使用。**3.漏洞管理：**這對中小企業可能有點難度，當有一個新的漏洞出現，當知道廠商在更新，漏洞/攻擊就可能發生（駭客時時在監控全世界每個 IP 或每個網站），漏洞修補時間越短受到威脅的

可能性就會降低—如何縮短漏洞修補時間？或者確認自己有沒有做修補？不用買很貴的軟體，用 excel 去做追蹤管理就可以。**4.提升資安意識：**雖然是老生常談，但請多從資安事件和資安的攻擊面去了解，不是去看別人的損失有多慘重，而是要看是件是怎麼發生的，如果今天換作你會發生嗎？所以要多看 iThome。

Peter：駭客最怕我們換密碼，我們也最怕換密碼。

Q6 **有關開放銀行（Open Banking），10 月政府宣布啟用金融開放 API 平臺，第一階段的公開資料查詢 API 正式對外開放了，第三方服務（TSP）業者也宣稱盡力做資安。多數 TSP 業者對法律遵循、風險控管與資訊安全管理的認知有限，較缺乏完善、嚴格的法規與管理機制。在有限的預算與人力下，TSP 業者在資安控管與防護上，與金融業者有很大的落差。**（※ 由於時間關係，本題係請專家會後以文字方式回答）

Peter：Open Banking TSP 業者如何滿足銀行端的資安要求？如何評估 API 的安全性？若要針對 TSP 業者做紅隊演練，您會鎖定哪幾個部分進行攻擊呢？

Allen：

- **Open Banking TSP 業者如何滿足銀行端的資安要求？**

  這個部分需要根據每個銀行的資安要求而定。TSP 業者比較難以在銀行的資安管控之內，銀行在開放 API 的時候必須要做好嚴格的管控，而 TSP 業者在存取資料的時候，也需要以最高規格執行。包含資料的取得、處理、存放、刪除，都需要確認每個環節是否有符合資安要求。

- **如何評估 API 的安全性？**

  API 的設計通常一定需要謹慎，因為通常 API 會是企業的疏失，並且是攻擊者嘗試的入口。通常在 App、新型網站的設計中，多半都使用 API 的方式做資料的傳遞。但因為 API 在使用者介面背後執行，不少企業會認為攻擊者無法透過這些地方進行攻擊。但實際上恰恰相反，透過封包的側錄或者是逆向工程，馬上可以知道 API 的介面，並且透過 API 的設計缺失直接進行資料的撈取或者是進一步更嚴重的攻擊。建議幾個最優先需要注意的點如下：

  (1) 完善 API 文件及盤點進入點：API 文件需要完整謹慎的撰寫，在撰寫的過程也可以一併進行 API 進入點的盤點，例如有哪些 URL、Parameter、Key/Value，每一個的使用方式、接受的值範圍、型態、身份認證授權與否等等。這樣的盤點可以幫助企業確保 API 的設計完善以及預期接受的數值範圍，也能針對這樣的設計做好防禦、過濾。

(2) 身份認證、授權：如何驗證使用者的身份、如何確認使用者的帳號有權限操作某些特定的 API、如何避免使用者繞過檢查讀取其他使用者的資料，這些都是 API 常見的問題。企業必須確保 API 在呼叫的時候，哪些需要認證、哪些需要特殊的權限，嚴格進行管控。

(3) 最小權限原則：API 在設計的時候，給予資料必須做權限、資料最小化。例如確認 TSP 需要使用怎樣類型的資料、或者是申請使用某些資料，設計時就只給予他們需要的資料就好，避免給予過多不需要的資料。

(4) 漏洞檢測：設計好 API 界面之後，在正式上線之前，務必要進行漏洞檢測，例如滲透測試等。經過檢測，可以避免帳號的權限問題、參數特殊字元攻擊等風險。透過攻擊者的思維來進行盤點、修補相關的漏洞。

也可以參考 OWASP API Security Top 10 所描述的議題來盤點安全性。

- ✓ https://www.owasp.org/index.php/OWASP_API_Security_Project
- ✓ https://github.com/OWASP/API-Security

➢ **若要針對 TSP 業者做紅隊演練，您會鎖定哪幾個部分進行攻擊呢？**

TSP 業者跟銀行 API 的關係類似大型企業跟供應商間專線或是跨國公司子公司的網路架構。所以對紅隊演練來說目標可以設定成「TSP 業者與銀行對接的系統或網路」，而攻擊的方式與對一般企業進行紅隊並無差異。若經過銀行授權一同檢測，攻擊的焦點之一也會是 API 介面，因此對 App 的逆向工程、銀行 API 的各種攻擊檢測都會是首要進行的。透過攻擊 API，或許有機會進入到銀行的內部網路，進而取得更多機敏的資料。

Q7 隨著 5G 時代來臨，電信業者開始採用許多 IT 技術，如網路功能軟體化、虛擬化等，也將面臨資安漏洞或安全威脅。面對 5G 的超高速、低延遲反應能力的特性，還有節點爆增、異質網路銜接機會倍增。電信商和 5G 應用開發商將面臨哪些資安弱點？需要重新審視哪些管控措施還有政策？（※ 由於時間關係，本題係請專家會後以文字方式回答）

Allen：5G 時代來臨對開發商跟企業來說最麻煩的課題是 IoT 漏洞的管理以及網路邊界的擴大。以往不會暴露在外的系統很容易接上網際網路成為攻擊的對象，而對企業來說這些難以控管的 IoT 設備更成為可能被利用的跳板。擴大的網路連線能力造成攻擊面積擴大，因此企業需要加強盤點與網路連接的伺服器及設備，並且確認這些設備的組態設定、安全性問題無誤，並同樣遵循權限最小化原則。

而在 5G 的新架構、新設備之下，漏洞及攻擊的掌握度一定需要更高。世界上駭客組織及資安團隊會針對這些新架構進行研究，看有無可能找到新的漏洞或攻擊手法。因此需要多注意系統的更新狀態，及時進行更新修補。

可以參考 US DHS 對於 IoT 資安強化的策略建議（Strategic Principles for securing the Internet of Things），幾個比較實用的點包括：

- ✓ 考慮潛在影響並且考慮適當的安全控管措施(如：對連上網路的 IoT 設備進行驗證、了解設備的用途和環境、建立紅隊演練模式，從應用層、網路層、資料層和實體層檢驗）
- ✓ 建立公認的安全操作方式：參考已有的準則（通報、稽核）、縱深防護、建立漏洞分享平台
- ✓ 強化安全更新跟漏洞管理：修補方式盡可能透過網路和自動化機制更新、建立第三方供應商的更新機制協助消費者更新、找白帽駭客協助找漏洞、訂定 IoT 的使用期限，如 OS 停止支援多久後不使用該 IoT 裝置
- ✓ 設計階段考慮安全：如禁用預設密碼、使用新版本的 OS、硬體式安全、設計時考量中斷或例外處理等。

※ 延伸閱讀→〈別幫駭客開後門─資安法下的「風險預測」及「防禦提煉」時代─Part 1：會後報導〉

BSI 資訊安全與網路安全系列課程

資訊安全	個資管理	雲端安全	品質管理	營運持續	產業資安
ISO 27001 資訊安全管理系統 基礎課程 建置課程 風險評鑑課程 內部稽核員課程 主導稽核員課程	ISO 27701 隱私資訊管理系統 基礎課程 建置課程 稽核員轉換 主導稽核員課程	雲端服務資訊安全管理系統 Cloud 主導稽核員課程	ISO 20000 服務管理系統 基礎課程 建置課程 內部稽核員課程 主導稽核員課程 稽核員轉版課程	ISO 22301 營運持續管理系統 基礎課程 主導稽核員課程	PCI DSS 支付卡產業資料安全標準 以 PCI DSS 強化電子支付服務的資訊安全管理及法規遵循課程 內部稽核員課程 主導稽核員課程
資通安全管理法 稽核課程	BS 10012 個人資訊管理系統 基礎課程 建置課程 主導稽核員課程	ISO 27017 & ISO 27018 建置課程		BSI 營運衝擊分析(BIA)課程	ISO 27799 健康醫療資安基礎課程
GDPR 歐盟一般資料保護規範 基礎課程	ISO 29100 隱私框架 基礎課程 主導稽核員課程	NIST 網路安全框架 建置課程			

課程詳情請洽 BSI 訓練學苑：
T: 02-26560333
E: training.taiwan@bsigroup.com