出國報告（出國類別：考察）

澳洲資訊安全及數位鑑識作業參訪

服務機關：財政部財政資訊中心

姓名職稱：林榮輝分析師、翁緯宏設計師

派赴國家：澳大利亞

報告日期：106 年 2 月 10 日

出國期間：105 年 11 月 6 日至 105 年 11 月 13 日

摘　要

為瞭解國外數位鑑識及資訊安全相關作業規劃，本中心於 105 年 10 月初規劃選派人員赴澳大利亞參訪。經評估後由本中心綜合規劃組及資通營運組各派 1 員，於 105 年 11 月 6 日至 11 月 13 日前往澳大利亞參訪數位鑑識及資訊安全相關作業規劃，參訪機關包括澳大利亞稅務局(Australian Taxation Office；以下簡稱澳洲稅務局)、思科系統公司澳大利亞分公司(Cisco System,Inc；以下簡稱思科澳洲分公司)及澳大利亞資誠企業管理顧問公司(PricewaterhouseCoopers Australia)等 3 個機關(構)。

第一個行程是參訪思科澳洲分公司，考察其規劃建置的一套攻防演練模擬環境，該模擬環境之第一個特點是採用 Splunk 這套工具收集各種不同設備的紀錄檔(log)，並建立索引，之後再透過指令等方式檢視相關事件，以確定是否遭受某種網路攻擊。該資深工程師說明，Splunk 工具架構與一般傳統型 SOC 監控告警之最大差異，在於這套工具可以透過指令方式交叉比對不同設備之紀錄檔(log)，能更精準的確認是否遭受攻擊以及是遭受哪種型態的攻擊。第二個特點是這些設備不限於只有使用於該公司之產品，也與不同廠商的資安設備合作與整合，並將各設備所監控的事件及紀錄(log)統一收至分析工具進行分析，以利及早偵測出所受攻擊並找出來源端。

這套模擬環境之攻擊端是由思科系統公司對客戶執行攻擊，讓客戶學習如何檢視各種防禦設備紀錄檔(log)之特徵，以訓練客戶學習如何判斷受到何種攻擊。**綜上，考量現今網路攻擊手法複雜，需透過整合型防禦網路，以即時發現攻擊行為，建議可考慮建置攻防演練模擬環境，提升資安人員防禦技術能力。**

第二個行程是參訪資誠企業管理顧問公司，考察該公司協助客戶處理資安事件之標準作業流程，如何做好數位證據保全及鑑識分析作業。該公司表示，目前

政府單位或企業組織所建置的各種資安設備，著重於防範外對內威脅，至於內對內威脅及內對外威脅則疏於防範，事中(During)的證據保全及入侵及時偵測變得非常重要，這也是政府單位或企業組織應該需要特別留意的地方，唯有如此，企業才能在事故發生的當下及時應變。

然而，要有公信力的證據，事前的資料保留也是非常重要的課題，許多客戶也沒有規劃「事件發生前要留什麼資料？」等到事件發生後，才苦於無相關證據。至於事先要保留哪些資料，資深顧問建議，重要的稽核軌跡均應保留，以利事發後有跡可循。

對於數位鑑識的程序中，該公司特別提醒我們應注意「對於已開機的電腦(或主機)不要關機，對於已關機的電腦(或主機)則不要開機」，其目的是不要讓資料的修改日期受到改變。對於已開機的電腦(或主機)則立即使用特殊工具將記憶體(RAM)裡面的資料複製出來，因為記憶體(RAM)是屬於揮發性的記憶體，一旦電源關閉後資料就消失了。此外，對於嫌疑電腦(或主機)的拍照則要注意不同角度都要拍，尤其是排線連結狀況、螢幕顯示內容都要清楚拍照。此外，對於發生駭客入侵或資料外洩的案件時，千萬不可立即拔除網路線，而是應以數位鑑識方法保全證據，因為要證明無故意或過失需要證據，事發時若立即拔除網路線，則可能導致證據被湮滅。

至於在鑑識軟體方面，該公司表示他們所使用的採集或鑑識軟體都是使用付費之商業軟體，而且這些軟體都是經過認證的。此外，由於數位環境日新月異，各種新型的數位媒體所需使用之工具及軟體也都需不斷採購及更新，因此更新這些鑑識工具每年均投入許多資金。

綜上，建議(1)事前規劃重要軌跡保存，以利事後數位證據蒐集及分析。(2)建置專業且經認證之數位鑑識分析工具，且需每年更新所需之鑑識工具，以提升數位證據能力並獲法院採信。

第三個行程是參訪澳洲稅務局，考察稅務機關如何保護稅務資料，以及資安事件數位證據保全及鑑識分析作業。澳洲政府如同所有西方國家一樣，相當重視資訊安全標準，並已撰擬完整且詳盡的資訊安全手冊，亦規範每個政府機關資訊安全作業應負權責(參考本報告第 19-21 頁)；目前我國是以任務編組方式推動資安政策及規範，與澳洲政府尚有些許不同。

澳洲稅務局在數位鑑識作業很早就規劃及執行，其數位鑑識團隊(Forensics & Investigations team) 於 1999 年就成立至今，目前專責人員約 30 位，隸屬於該局 IT 安全部門，主要任務是維護該局數位稅務資料之機密性及完整性。另該團隊於坎培拉、雪梨、墨爾本及布里斯班皆設有數位鑑識實驗室，並配備相關蒐證及鑑識分析設備，該團隊曾經服務對象包括該局等 36 個政府機關(構)。本中心於 105 年 10 月成立資安健檢及數位鑑識小組成員共 17 位，其中專責人力只有 1 位，除本中心 13 位成員外，亦包括關務署、國有財產署及台灣銀行等加入 4 位成員，後續將於預算及專責人力允許下，逐步建置資安健檢及數位鑑識能量。

最後該局介紹有關澳洲政府降低網路入侵或減災的防範機制，目前澳州政府共規劃 35 個減災策略，每項策略皆可透過關鍵字連結相對應技術手冊，以指導澳洲政府機關如何自行完成相關評估及執行作業，澳洲稅務局人員表示按規範遵循前 4 大減災策略(包括應用程式白名單、應用程式漏洞修補、作業系統漏洞修補及限制管理者權限等)，即可降低 85%的網路攻擊或災損。

政府機關如要實施前 4 大減緩策略，該局人員建議先從最可能遭受網路入侵的伺服器實施，慢慢擴散到所有伺服器，並評估透過其他減災措施補強，直到達到該施行機關可接受風險。澳洲政府並從總體安全有效性、外部阻力、前期成本(員工，設備，技術複雜性)、維護成本(主要員工負荷)、…等 8 個構面，對所有 35 個減災策略做前置分析，以作為澳洲政府機關導入參考(參考本報告第 28-31 頁)。

澳洲稅務局所採行 35 個防止網路入侵的減災策略，其中部分項目本中心雖已採用，例如排名第 10 的網段隔離、第 11 的多重因子認證、第 17 的電子郵件內容過濾、第 18 的 Web 內容過濾…等，惟未如澳洲政府有系統及完整之評估，且前述有關 IT 系統管理員在典型 Windows 環境中規劃和實施前 4 大策略的技術指導，係因澳大利亞大多數政府業務的個人電腦及伺服器大部分使用 Windows 作業系統；本中心前端個人電腦係使用Windows作業系統,後端的伺服器大部分使用AIX-Unix 或 Linux 作業系統，故無法全面套用，建議可參考澳洲政府規範網路入侵 35 個減災策略之內涵，於本中心 AIX-Unix 或 Linux 作業系統訂定相關技術手冊。

綜上，建議(1)規劃評估網路減災策略，以減緩網路入侵災損。(2)參考澳洲稅務局數位鑑識機制，逐步建置資安健檢及數位鑑識能量。(3)建立資安技術文件瀏覽機制，以利搜尋及閱讀。

目　錄

壹、 前言

行政院於 102 年 12 月 25 日函頒「行政院於國家資通訊安全發展方案(102 年至 105 年)」，在該方案附錄 2：「行動方案執行要點與績效指標說明」之行動方案 3.3.1「完善數位證據保全及相關標準作業程序」中，請法務部於 103 年制定數位證據保全標準作業程序規範。據此，法務部擬訂「政府機關(構)資安事件數位證據保全標準作業程序」草案，於 103 年 12 月函報行政院，行政院並於 104 年 8 月 4 日院臺護字第 1400036611 號函頒所有政府機關照案實施。

為符合行政院資安事件數位證據保全標準作業規範，並期本部及所屬機關於資安事件發生時，第一線人員能透過工具執行數位證據識別、蒐集、擷取、封緘及運送作業，本中心於 105 年 10 月規劃成立資安健檢及數位鑑識團隊，初步辦理本中心資安事件數位證據保全作業，以作為財政部所屬機關(構)表率。後續並將資安事件數位證據保全作業，逐步推廣至財政部所屬機關(構)，以符合行政院「政府機關(構)資安事件數位證據保全標準作業程序」規範。

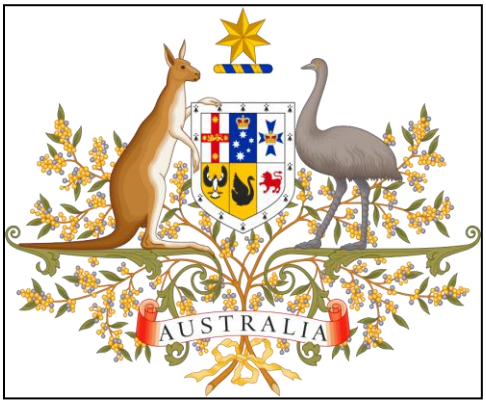
本中心掌管財政部所屬各機關資訊預算及業務，目前財政部擁有全國最多、最完整的財政、稅務、關稅及所得財產等資訊資源，為有效保管及運用這些資源，本中心與所屬機關(單位)建立了綿密的網路連線及資訊系統，更肩負財政部與所屬機關(構)資訊系統規劃、宣導及評核之責任。鑒於本中心資訊經費逐年減少，又依「政府機關(構)資通安全責任等級分級作業規定」，本中心每年必需辦理 ISMS 第三方驗證、內部稽核、業務持續運作演練、SOC 監控、弱點掃描、滲透測試與資安健診等。因此本中心資安健檢及數位鑑識團隊另一個重要任務，即是逐步推動辦理財政部及所屬機關(構)相關網站滲透測試及弱點掃瞄作業，以進一步提升整體資訊安全防護能力，並節省資訊委外經費；又為推廣本項業務，已邀請關務署、國有財產署及台灣銀行等派員加入，目前團隊成員包括隊長、小隊長及隊員計有 17 位。

為瞭解國外有關數位鑑識及資訊安全作業規劃，本中心於 105 年 10 月初規劃選派人員赴澳大利亞參訪。經評估後由本中心綜合規劃組及資通營運組各派 1 員，於 105 年 11 月 6 日至 11 月 13 日前往澳大利亞參訪數位鑑識及資訊安全相關作業規劃，參訪機關包括澳洲稅務局、思科澳洲分公司及澳大利亞資誠企業管理顧問公司等 3 個機關(構)。

貳、 澳大利亞簡介

澳洲聯邦（Commonwealth of Australia）為聯邦制國家，主要為新南威爾斯，昆士蘭，南澳洲，塔斯馬尼亞，維多利亞，西澳洲斯等 6 州。澳洲聯邦通稱澳大利亞（Australia，縮寫為 AU、AUS），在臺灣常使用「澳洲」代替「澳大利亞」，澳洲是全球面積第六大，大洋洲面積最大及南半球面積第二大的國家。澳洲國土包括澳洲大陸，塔斯曼尼亞島及數個海外的島嶼，面積和美國本土相似。澳洲是全球第 12 大經濟體，生活素質，健康，教育，經濟自由度，公民自由度與政治權利等評比項目在世界各國中名列前茅。

澳洲國徽以盾牌為中心，盾面的圖案代表的是組成澳洲聯邦的六個州，盾牌上方是藍白相間的花環和七角星。左右兩側各有袋鼠和鴕鵝(鴕鳥)站在桉樹枝上，背後襯托著澳大利亞的國花—金合歡。前面所提起左右 2 側的袋鼠及鴕鳥，我們一般人都以為這 2 種動物只是象徵澳大利亞特有的物種，經過當地人解說才了解，這 2 種動物的腳都無法後退，在澳洲國徽上代表的是澳大利亞勇往直前的精神。



本中心前往澳大利亞參訪澳洲稅務局、思科澳洲分公司公司及澳大利亞資誠企業管理顧問公司等 3 個機關(構)期間，適逢當地紀念陣亡將士紀念節日(英文：Remembrance Day)，依據澳洲稅務局人員解說每年的 11 月 11 日 11 時，澳大利

亞人會準時地停止所有正在進行的活動，向第一次世界大戰以來在戰爭中陣亡士兵們默哀 10 分鐘。因為澳洲屬大英國協成員國，因此於第一次世界大戰爆發時，雖然當時澳洲人口不足 500 萬，卻有 41 萬 7000 千名澳洲人應徵入伍，33 萬 2 千人被派往海外，15 萬 2 千人受傷，6 萬 1 千人再也沒能返回家園。(摘錄自維基百科)

當然戰爭造成悲劇是一場無法挽回的記憶，但是避免戰爭則是我們這一代須肩負的使命，目前世界紛亂難免，所幸無大規模的戰爭。惟網路攻擊卻是時刻在上演的戲碼，澳洲政府堅信雖無法將所有的網路攻擊阻擋，但是如何透過事前防範機制，以降低入侵機會及損失，卻是參訪人員在與澳洲稅務局資訊安全及數位鑑識部門對話時，他們一再提起重點。

參、 參訪人員與行程安排

一、行前準備及致謝

為規劃辦理此次參訪計畫，透過外交部聯繫我駐澳大利亞代表處協助，並在該處積極協助下，在極短時間內洽妥安排參訪澳洲稅務局、思科澳洲分公司及澳大利亞資誠企業管理顧問公司等 3 個機關(構)，使得本中心參訪人員得以順利完成此行任務，在此謹向外交部及我駐澳大利亞代表處致謝忱。

又時正值我國積極推動新南向政策，駐澳大利亞代表處及駐雪梨台北經濟文化辦事處人員皆忙於執行推動該項政策相關事宜，惟林公使維揚、蕭秘書伊芳及潘秘書琪祿等人於公忙之餘，均不辭辛勞在食宿、交通及參訪行程上，皆給予最大的協助，不勝感荷。尤其是蕭秘書伊芳陪同參訪人員協助參訪澳洲稅務局協助提問，宵旰勤力協助參訪人員完成任務，讓本次參訪行程收穫豐碩。

二、行程安排

日期	時間	參訪單位	參訪說明
11月6日(日)	23:05	台灣桃園國際機場第二航站出發	
11月7日(一)	11:20	抵達澳大利亞雪梨國際機場	
	14:00-17:00	準備參訪資料	
11月8日(二)	09:30-17:30	思科澳洲分公司 (Cisco Australia)	討論網路資安防禦架構、權限及業務執行概況
11月9日(三)	09:00-12:00	準備參訪資料	
	14:00-17:00	澳大利亞資誠企業管理顧問公司 (PricewaterhouseCoopers Australia)	討論澳大利亞該公司數位鑑識之作業
11月10日(四)	10:55-11:50	雪梨機場出發 抵達坎培拉國際機場(國內線)	
	13:00-15:00	拜會駐澳大利亞代表處及餐敘	
11月11日(五)	09:00-13:00	澳大利亞稅務局 (Australian Taxation Office)	澳大利亞資訊安全推動各項相關議題，包括資安規範、緊急應變程序、數位鑑識作業之推動現況
	15:00-15:55	坎培拉機場出發 抵達雪梨國際機場(國內線)	
11月12日(六)	22:10	雪梨國際機場出發	雪梨→桃園
11月13日(日)	04:30	抵達台灣桃園國際機場	抵達桃園

肆、 參訪機關

一、思科澳洲分公司

(一) 參訪對象

11 月 8 日拜訪思科澳洲分公司之網路安全研究團隊。

【思科系統公司簡介】

思科系統公司於 1984 年由史丹佛大學的兩位學者創立，企業總部位於美國加州聖荷西，為全球網路設備領導廠商，目前在全球 67 個國家已有超過 400 個以上的分支機構，擁有約 7 萬名員工，其於 1994 年分別在澳洲雪梨、中國北京、香港、韓國漢城與新加坡等地相繼成立分公司，至今已在亞太地區主要的 13 個國家中設有辦公室及 3 個技術支援中心(Technology Assistance Center ; TAC)。思科澳洲分公司是其眾多分公司中第一個成立網路場域(Cyber-Range)模擬駭客攻擊手法，並研究如何從某些特徵值(Features)來判斷是何種攻擊並加以防禦之實驗機房。

思科系統公司早期是以研發並生產網路設備為主，近年來除投入在互聯網之整合外，更積極致力於網路安全之攻防研究，該公司目前已是全球領先的互聯網設備供應商。該公司善用其專長的網路設備和應用方案將世界各地的人、計算設備以及網路聯結起來，使人們能夠隨時隨地利用各種設備傳送信息。該公司網路安全解決方案「化被動為主動」，引進主動式安全防禦網路(Self Defending Network)，並配合網路存取控制方案(NAC)來達到加成乘效益，確保政府及企業組織之網路安全。

(二) 參訪目的

1. 由於本中心成立「資安健檢及數位鑑識團隊」，希望藉由這次參訪，了解思科系統公司如何對於網路攻防建置模擬環境，以及在模擬環境中如何能檢視是否被攻擊。

2. 隨著網路應用日益普及，意圖不軌的駭客透過網路進行攻擊、資料竊探、竄改資料、破壞系統及勒索等行為，其手法也日新月異，使政府及企業組織對於駭客之不法行為之防範，亦隨攻擊手法不斷創新而更加困難。希望藉由本次參訪網路領域中之領頭羊思科系統公司，實地了解並學習該公司在網路環境如何提升網路安全之解決方案，並就該公司之網路資安產品進行了解及意見交換，並實地參觀其實驗機房環境，以作為本中心未來在規劃建置網路安全防禦機制上之重要參考。

(三) 參訪過程

來到思科澳洲分公司，該公司安排了網路安全研究室幾位資深工程師引領我們至會議室進行該公司之網路資安防禦架構介紹並與我們進行意見交流。

首先說明該公司在近年來致力於網路環境攻擊防禦之研究，並與許多資安設備之廠商進行合作，設計出一套整合型之資安防禦架構，這套架構可以協助客戶及早發現潛在的網路攻擊，例如分散式阻斷攻擊(DDoS Attack)、勒索贖金攻擊(Ransomware attack)、惡意軟體攻擊(Malware Attack)、進階持續性滲透攻擊(APT Attack)等。

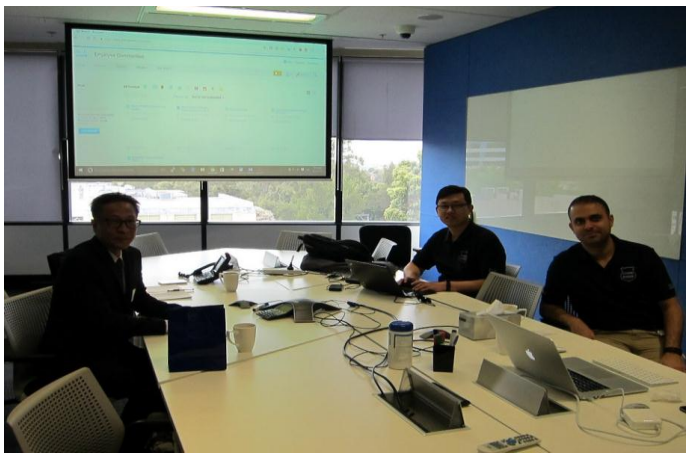


圖 1、聽取 Cisco 公司介紹及意見交流

為何需要整合各種資安設備之資訊呢？該資深工程師表示，從單一資安設備並不易發現是否已經遭受攻擊，必需藉由整合不同的網路資安設備之記錄檔(log)，透過交叉比對及分析其連線行為或特徵值，才能正確判斷是否已經遭受到駭客攻擊。

在這套防禦架構中，分別整合了事前、事中及事後所需之各式資安設備。該資深工程師另表示，該防禦架構特點在於這些設備不限於只有使用於該公司之產品，也與不同廠商的資安設備合作與整合，並將各設備所監控的事件及紀錄(log)統一收至分析工具進行分析，以利及早偵測出所受攻擊並找出來源端。下圖為資安防禦整體架構示意圖：

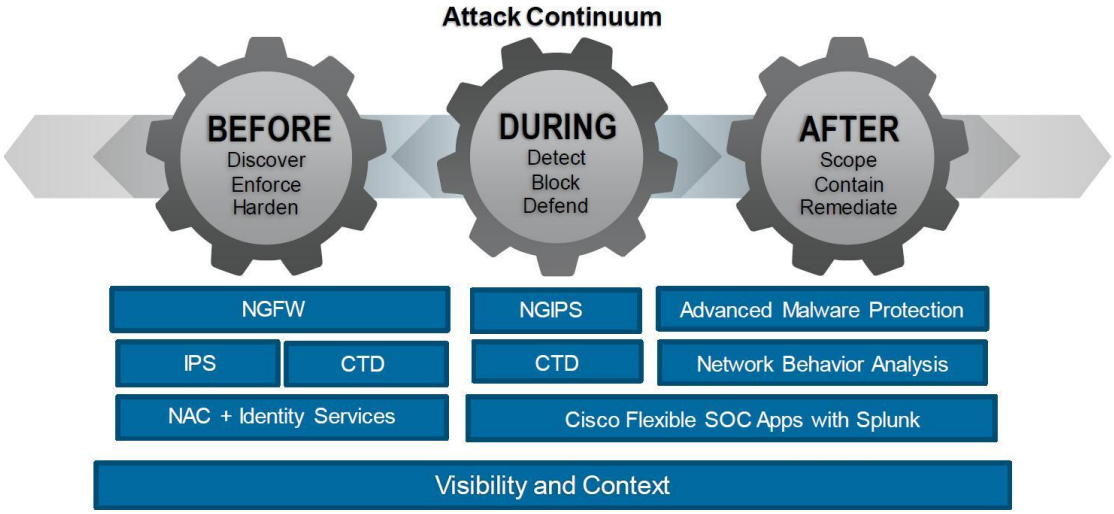


圖 2、Cisco 網路安全解決方案之整體架構

其中，NAC 為 Network Admission Control(網路存取控制)之縮寫，其功能是允許網路管理者在有線、無線和遠端存取用戶及其終端裝置存取網路前，能先對其機器的狀態進行驗證、授權、評估和矯正。它能識別出如筆記型電腦、桌上型電腦或其他相關公司資產的連網設備，是否符合安全性政策，並在其進入網路存取前修補漏洞。

上圖所列設備僅為一示意，真正參與整合運作的設備可以包含很多，至於想要整合哪些設備則可視機關組織之需要來規劃設計，一些最重要的資安設備如下所示：

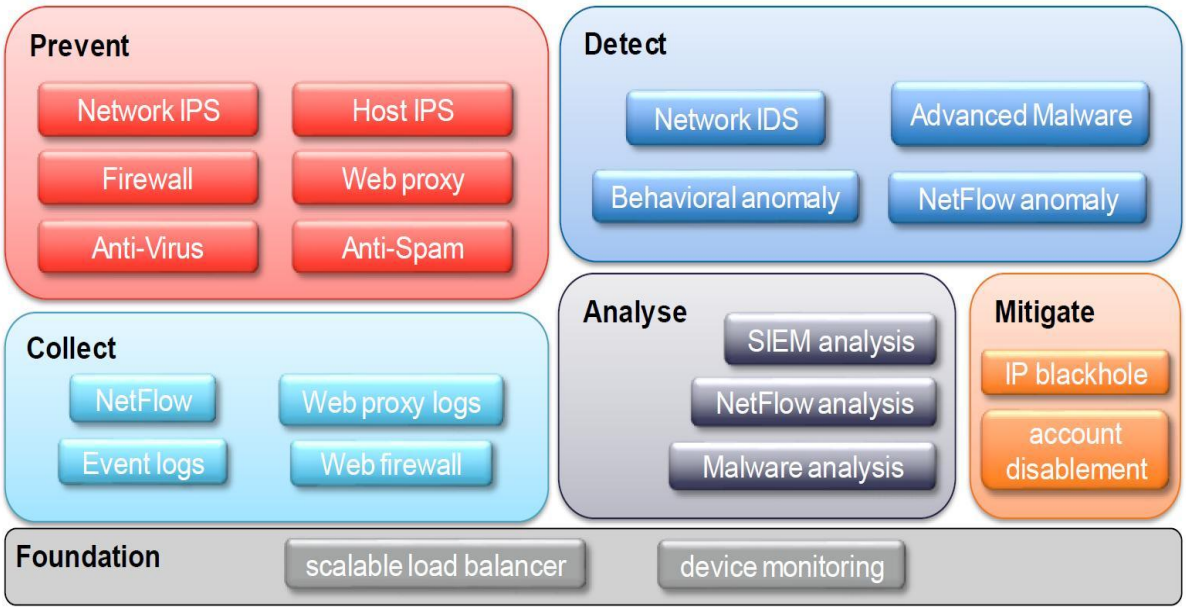


圖 3、Cisco 網路安全解決方案之資安設備與類別

該公司的網路安全防禦架構中，是採用 Splunk 這套工具收集各種不同設備的紀錄檔(log)，並建立索引，之後再透過指令等方式檢視相關事件，以確定是否遭受某種網路攻擊。

該資深工程師說明，Splunk 工具架構與一般傳統型 SOC 監控告警之最大差異，在於這套工具可以透過指令方式交叉比對不同設備之紀錄檔(log)，能更精準的確認是否遭受攻擊以及是遭受哪種型態的攻擊。其架構如下：

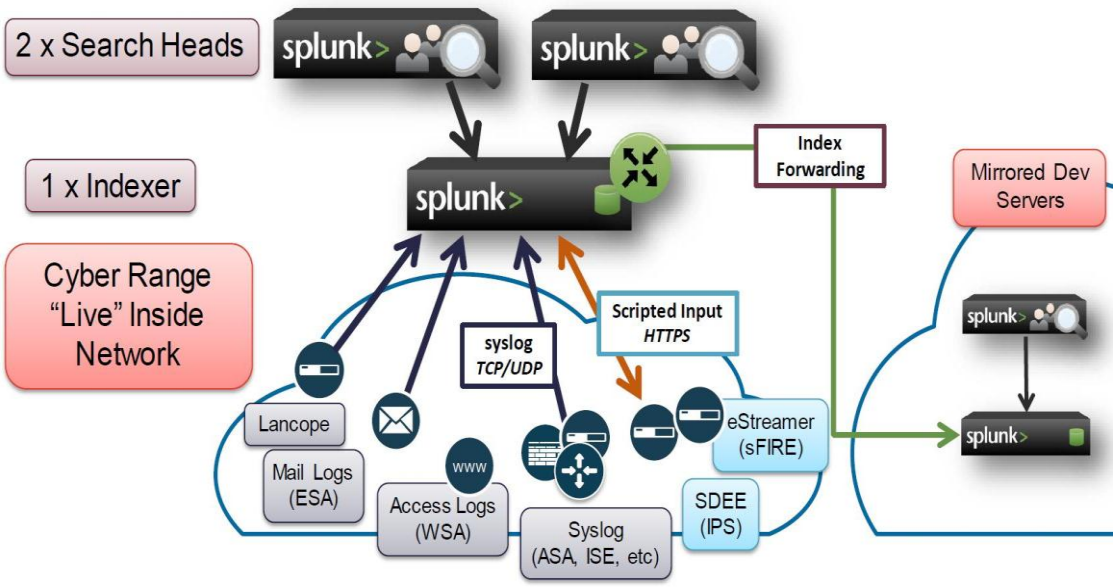


圖 4、Splunk 工具之架構

若購置該套網路防禦架構的客戶，該公司會以模擬對客戶系統發動攻擊之方式，讓客戶學習如何檢視紀錄檔(log)之特徵來判斷是否知道何種攻擊。也就是說，在該數位攻防架構中的攻擊腳本是由該公司統一錄製，再對客戶進行模擬攻擊，讓客戶學習如何判讀紀錄檔(log)，提升客戶端的防禦能力。

此外，該工具也可以將統計結果以畫面的方式呈現(如下圖所示)。

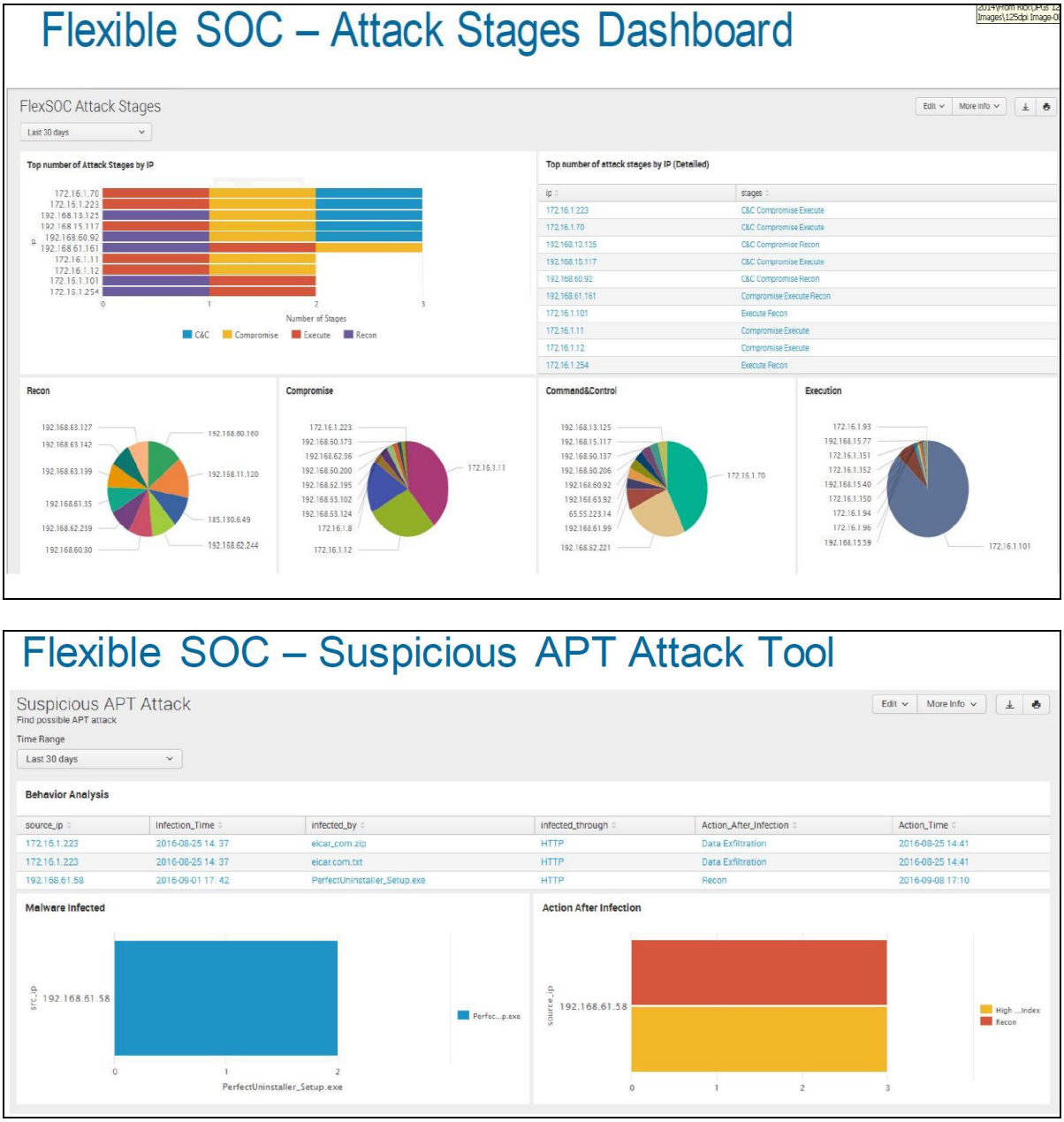


圖 5、分析工具之畫面呈現

最後，我們也參觀思科澳洲分公司實驗機房，該機房主要為建置模擬各種攻擊手法並研究如何從蛛絲馬跡中提早發現。

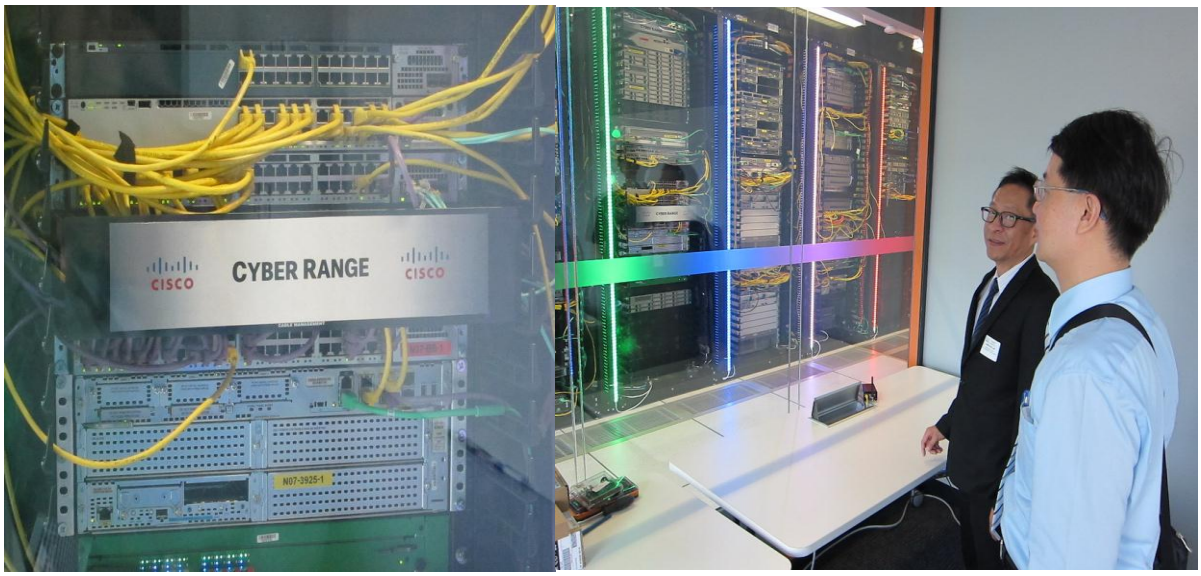


圖 6、參訪 Cisco 公司之機房

在我們與資深工程師們一起合影後，結束此次參訪。

圖 7、與 Cisco 資深工程師們結束前合影

二、資誠企業管理顧問公司(PwC)澳洲分公司

(一) 參訪對象

11 月 9 日拜訪資誠企業管理顧問公司澳洲分部之數位鑑識團隊。

【資誠企業管理顧問公司簡介】

資誠企業管理顧問公司(PwC Taiwan)創於 1970 年，提供產業專精的整合性專業服務，包括審計、稅務、財務顧問服務、管理顧問諮詢服務、人才與變革管理服務、法律暨智財管理等服務。

該事務所近年來對於數位證據保全及鑑識的研究與服務亦投入相當多的資源，積極培養數位證據鑑識專業人才，成立「數位鑑識實驗室」，建構數位證據鑑識標準作業程序。除協助客戶導入證據保全及數位鑑識相關的認證，例如 ISO20037、ISO20041 ~ ISO20043 等專業認證外，亦協助客戶進行專業的數位證據採集鑑識工作，以提升法院對於數位證據之採信度。

(二) 參訪目的

希望藉由這次參訪能獲取一些該事務所在協助客戶採集數位證據時之實務作法及經驗分享，以提升本中心數位鑑識之專業能力。

(三) 參訪過程

11 月 9 日拜訪澳洲資誠企業管理顧問公司(PwC)，該所Martin 主任引導我們至會議室與多位數位鑑識部門同仁一同座談，並由該所的資深顧問進行簡報。簡報內容主要在介紹數位證據之採集、記錄、保存及鑑識各階段應特別注意的地方及經驗分享。

資深顧問表示，近年來該事務所服務客戶調查及鑑識的大宗案件分類為「資料外洩」及「駭客入侵」。網路犯罪事件成長了 38%，隨著網絡攻擊的頻率不斷加快、造成了嚴重的損失及廣泛的影響。例如著名的 SWIFT(Society for Worldwide Interbank Financial Telecommunication)

銀行國際匯款竊盜案，駭客利用一封電子郵件，不到 40 天內盜取孟加拉央行共 9 億 5 千 1 百萬美元。近幾年相關個人資料外洩事件持續發生，企業內營業秘密及機密資料外洩事件層出不窮，許多企業不知道如何因應，或者沒有足夠資源應付網路罪犯。高達 46%的經濟犯罪案件來自內部員工，其中超過 5 成犯案者為中高管理階層，原因為內控機制存有潛在弱點。

目前政府單位或企業組織所建置的各種資安設備，著重於防範外對內威脅，至於內對內威脅及內對外威脅則疏於防範，事中(During)的證據保全及入侵及時偵測變得非常重要，這也是政府單位或企業組織應該需要特別留意的地方，唯有如此，企業才能在事故發生的當下及時應變。

數位鑑識係利用科學驗證方法調查數位證據，經由資料還原、擷取、分析等過程，還原案情原貌，做為法庭訴訟之依據，資深顧問表示，在接受客戶委託協助調查時，特別要注意一定要先簽「授權委任書」，之後要對現場進行錄影、拍照或現場蒐證等證據採集。

圖 8、數位證據採集常用工具

該資深顧問表示，值得特別一提的是「對於已開機的電腦(或主機)不要關機，對於已關機的電腦(或主機)則不要開機」，其目的是不要讓資料的修

改日期受到改變。對於已開機的電腦(或主機)則立即使用特殊工具將記憶體(RAM)裡面的資料複製出來，因為記憶體(RAM)是屬於揮發性的記憶體，一旦電源關閉後資料就消失了。此外，對於嫌疑電腦(或主機)的拍照則要注意不同角度都要拍，尤其是排線連結狀況、螢幕顯示內容都要清楚拍照。

此外，對於發生駭客入侵或資料外洩的案件時，千萬不可立即拔除網路線，而是應以數位鑑識方法保全證據，因為要證明無故意或過失需要證據，事發時若立即拔除網路線，則可能導致證據被湮滅。記憶體鑑識主要採集的項目則如下圖所示：

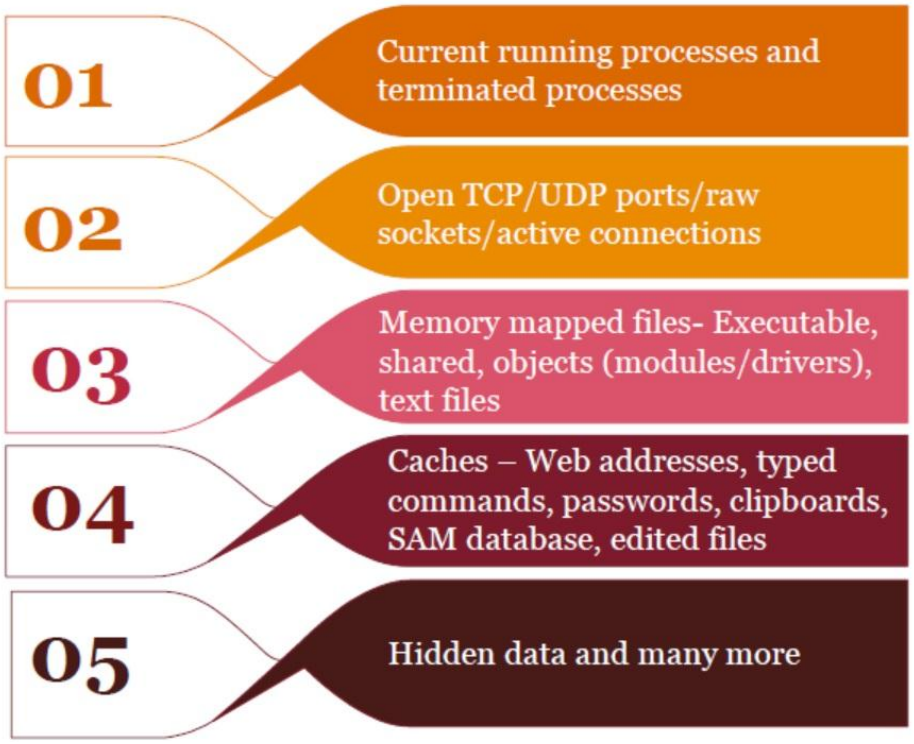


圖 9、記憶體鑑識主要採集的項目

資深顧問表示，許多客戶於事件發生時不知要怎麼蒐集證據以及將其保存，甚至第一時間人為直接操作電腦，未以證據保全及封存程序進行處理，違反鑑識原則之「不得再對電腦設備或儲存媒體中的數位資料造成任何改變」，造成證據無法被法院採信。然而，要有公信力的證據，事前的資料保留也是非常重要的課題，許多客戶也沒有規劃「事件發生前要留什麼資料？」

等到事件發生後，才苦於無相關證據。至於事先要保留哪些資料，資深顧問建議，重要的稽核軌跡均應保留，以利事發後有跡可循。

至於在工具使用方面，資深顧問表示他們所使用的採集或鑑識工具都是採用付費之商業軟體，而且這些軟體都是經過認證的，因為這樣採集或鑑識的證據才會被法院所採信。

資深顧問引導我們實地參觀他們鑑識團隊的辦公室及數位證據採集工具：

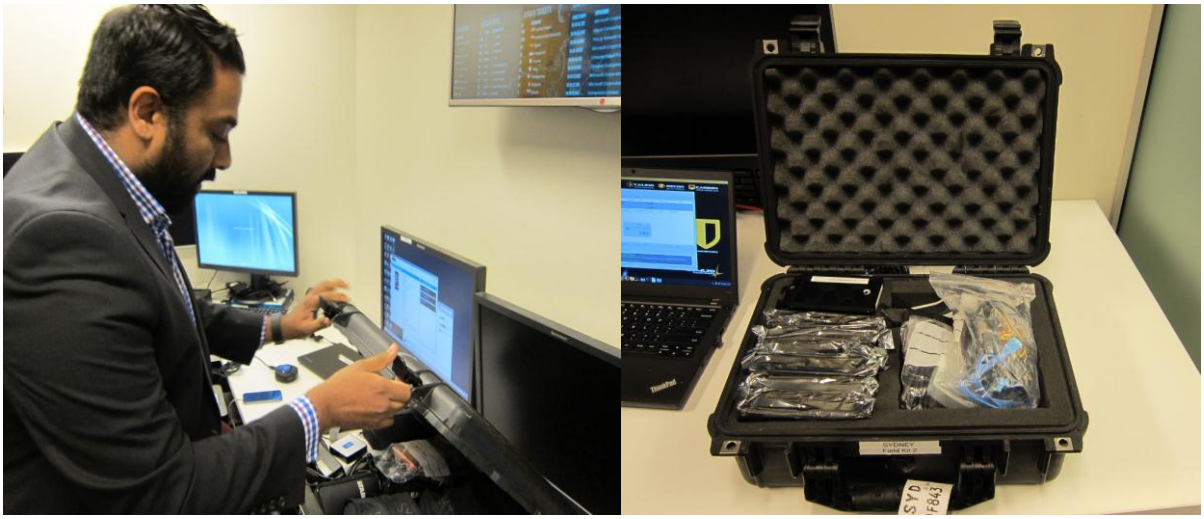


圖 10、資深顧問使用數位證據保全工具及鑑識分析

最後，我們與資深顧問們一合影，並結束這場參訪。

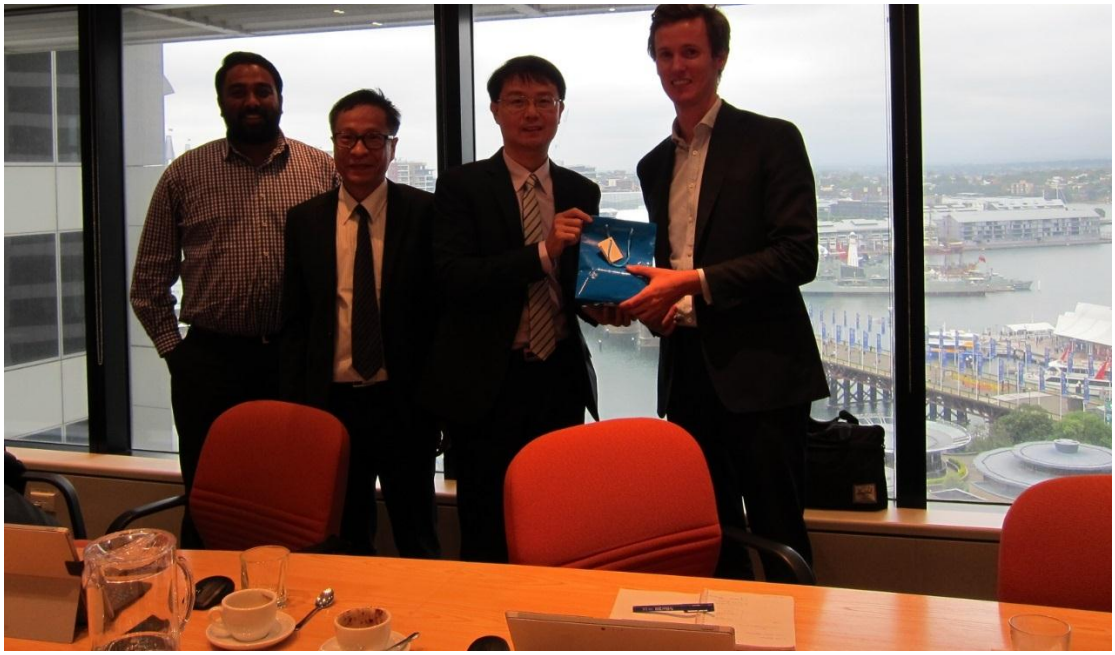


圖 11、與資誠公司資深工程師結束前合影

三、澳大利亞稅務局(Australian Taxation Office；ATO)

(一) 參訪對象

澳大利亞是一個聯邦制的國家，主要實行分稅制的財政管理體制，聯邦、州和地方政府根據憲法和法律規定的職權，徵收各自的稅費。澳大利亞的稅收徵收權主要集中在澳洲稅務局，澳大利亞稅收以直接稅為主，包括公司所得稅、個人所得稅、消費稅及貨物與勞務稅(GST)等。另由州、地方政府徵收的稅費主要為工薪稅、土地稅、博採稅；此外，州地方政府還徵收菸稅、油稅和其他收入。

澳洲稅務局它的前身是聯邦稅務局(Commonwealth Taxation Office 及 Federal Taxation Office)，於 1910 年 11 月 11 日成立至今，它掌握澳大利亞稅務政策、徵收實務及稅務資料，是澳大利亞政府的主要稅捐稽徵機關。負責管理澳大利亞聯邦稅務制度、稅務立法和其他相關事宜，是澳大利亞在聯邦財政最重要的一環，平均雇用 22,022 人(摘錄自維基百科)。

(二) 參訪目的

澳洲政府如同所有西方國家一樣，相當重視資訊安全標準，並已撰擬完整且詳盡的資訊安全手冊，亦規範每個政府機關資訊安全作業應負權責。以下是澳洲政府各機關資訊安全的權責區分：

表 1、澳洲政府各機關資安職責彙整表

AGENCY OR BODY(機關)	SERVICES(權責)
ttorney-General's Department (AGD) 澳大利亞聯邦檢察總署	Responsible for information security policy and cyber security incident preparedness, response and recovery arrangements across government.
Attorney-General's Department—Protective Security Training College 總檢察長辦公室 - 防護安全培訓學院	Provides protective security training to government agencies and contractors.

Australian Federal Police(Cybercrime) 澳大利亞聯邦警察（網絡犯罪）	Law enforcement in relation to electronic andother high tech crimes.
Australian Cyber Security Centre(AC SC) 澳大利亞網絡安全中心	The role of the AC SC is to lead the Australian Government’s operational response to cyber security incidents, organise national cyber security operations and resources, encourage and receive reporting of cyber security incidents, raise awareness of the threat to Australia and study and investigate cyber threats.The AC SC includes representatives from ASD, theAustralian Crime Commission (ACC), the Australian Defence Force (ADF), the Australian Federal Police (AF P), the Australian Security Intelligence Organisation (ASIO), the Computer Emergency Response Team (CERT) Australia and the Defence Intelligence Organisation (DIO).
Australian National Audit Office (ANAO) 澳大利亞國家審計署	Performance audits on information security.
Australian Security Intelligence Organisation (ASIO) 澳大利亞安全情報組織（ASIO）	ASIO is responsible for collecting, analysing and reporting intelligence on threats to security.
ASIO - T4 Protective Security T4 防護安全	ASIO - T4 Protective Security section provides advice and training, technical surveillance countermeasures, physical security certifications, protective security risk reviews and physical security equipment testing.
CERT Australia 澳大利亞 CERT	Provides the private sector with informationand assistance to help them protect their Information and Communications Technology(ICT) infrastructure from cyber threats andvulnerabilities. CERT Australia also provides acoordination role during a serious cyber incident

Cyber Security Operations Board 網絡安全執行委員會	Provides strategic direction and oversight of operational cyber security matters. Chairmanship and Secretariat support provided by the AttorneyGeneral’s Department.。
Cyber Security Policy and Coordination Committee 網絡安全政策和協調委員會	Coordinates the development of cyber security policy for the Australian Government.
Department of Communications 通訊部	Responsible for initiatives to educate and protect home users, students and small business from electronic intrusions and fraud.
Department of Finance 財政部	Development and oversight of whole-of government policy on the Australian Government’s use of information and communications technology.
Department of Foreign Affairs and Trade 外交貿易部	Policy and advice for security overseas.
Department of the Prime Minister and Cabinet 總理內閣部	Coordination of cyber and information security policy and activities across government.Responsible for implementation of the National Security Information Environment Roadmap: 2020Vision.
National Archives of Australia 澳大利亞國家檔案館管理局	Provides standards and advice on capturing and managing records to ensure their integrity as evidence is maintained. The National Archives also authorises the disposal of all Commonwealth records, including those relating to ICT and security processes and incidents.
Protective Security Policy Committee 安全防護政策委員會	Coordinates the development of protective security policy. Chairmanship and Secretariat support provided by the Attorney-General’s Department.
Security Construction and EquipmentCommittee 安全架構評估委員會	Oversees the evaluation of physical security equipment.

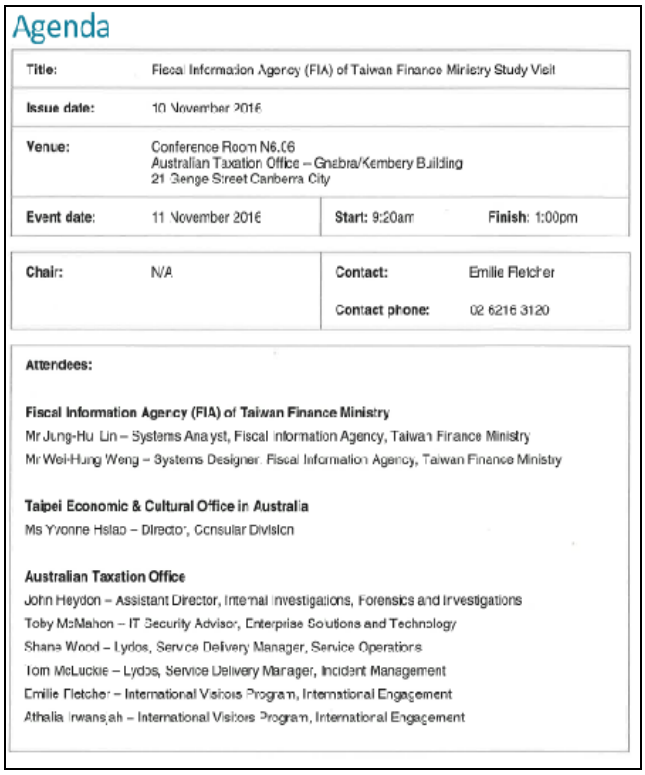
所以參訪澳洲稅務局的主要目地，是想了解該局的資安組織、政策及資安事件應變作業流程，以及該局數位鑑識團隊人員規劃、教育訓練及數位鑑

識作業。

（三）參訪過程

感謝外交部駐澳大利亞代表處戮力協助，澳洲稅務局於本中心參訪人員出發前，已將該局的參訪議程表(如下圖)透過外交部轉給本中心，讓參訪人員有更充裕時間準備與該局的對話：

表 2、參訪澳洲稅務局議程表



Agenda

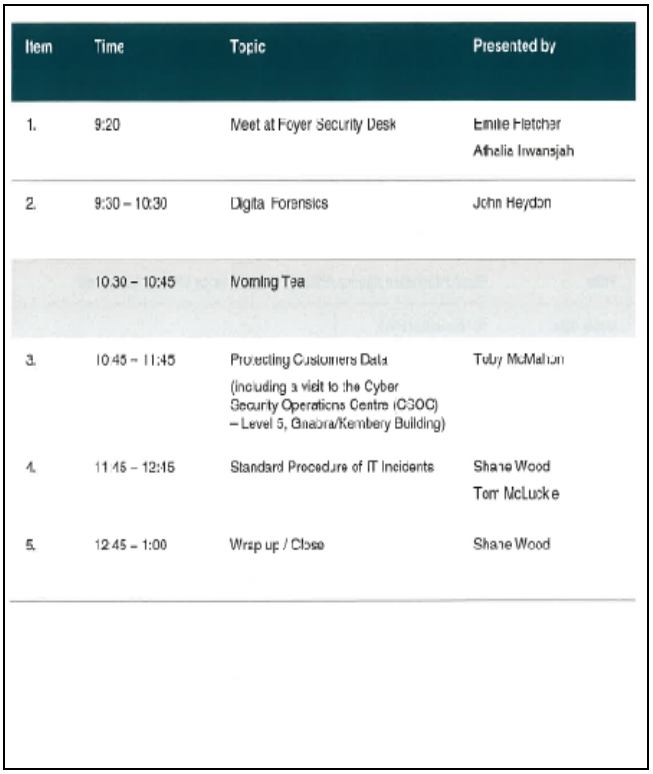
Title:	Fiscal Information Agency (FIA) of Taiwan Finance Ministry Study Visit		
Issue date:	10 November 2016		
Venue:	Conference Room N6.06 Australian Taxation Office – Ghabra/Kembery Building 21 Genge Street Canberra City		
Event date:	11 November 2016	**Start:** 9:20am	**Finish:** 1:00pm
Chair:	N/A	**Contact:**	Emilie Fletcher
		Contact phone:	02 6216 3120

Attendees:

Fiscal Information Agency (FIA) of Taiwan Finance Ministry
Mr Jung-Hu Lin – Systems Analyst, Fiscal Information Agency, Taiwan Finance Ministry
Mr Wei-Hung Weng – Systems Designer, Fiscal Information Agency, Taiwan Finance Ministry

Taipei Economic & Cultural Office in Australia
Ms Yvonne Hsiao – Director, Consular Division

Australian Taxation Office
John Heydon – Assistant Director, Internal Investigations, Forensics and Investigations
Toby McMahon – IT Security Advisor, Enterprise Solutions and Technology
Shana Wood – Lydos, Service Delivery Manager, Service Operations
Tom McLuckie – Lydos, Service Delivery Manager, Incident Management
Emilie Fletcher – International Visitors Program, International Engagement
Athalia Irwansah – International Visitors Program, International Engagement



Item	Time	Topic	Presented by
1.	9:20	Meet at Foyer Security Desk	Emilie Fletcher Athalia Irwansjah
2.	9:30 – 10:30	Digita Forensics	John Heydon
	10:30 – 10:45	Morning Tea	
3.	10:45 – 11:45	Protecting Customers Data (including a visit to the Cyber Security Operations Centre (CSOC) – Level 5, Gnabra/Kembery Building)	Toby McMahon
4.	11:45 – 12:45	Standard Procedure of IT Incidents	Shane Wood Tom McLuske
5.	12:45 – 1:00	Wrap up / Close	Shane Wood

澳洲稅務局數位鑑識團隊(Forensics & Investigations team)於 1999 年就成立至今，目前成員約 30 人，隸屬於該局 IT 安全部門，主要任務是維護該局數位稅務資料之機密性及完整性。該局數位鑑識人員表示，澳洲稅務局資料不得提供給任何第三方或傳輸到海外，除承包商在存放或傳輸之前經該局書面核准。因此如有違反相關規範，該局數位鑑識團隊亦會介入調查。澳洲稅務局數位鑑識團隊架構圖如下：

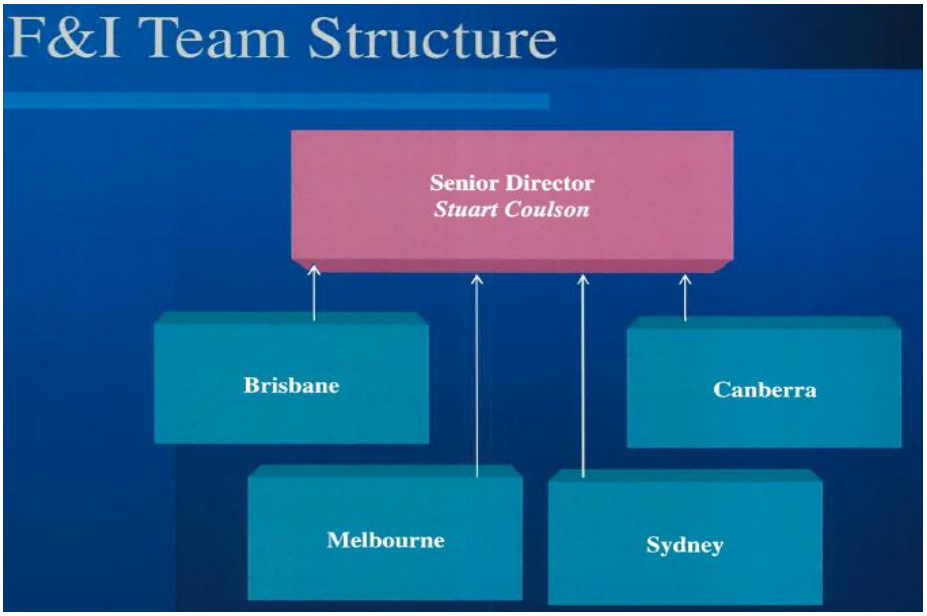


圖 12、澳洲稅務局數位鑑識團隊架構圖

該團隊除於首都坎培拉(Canberra)設立數位鑑識實驗室外，另在雪梨(Sydney)、墨爾本(Melbourne)及布里斯班(Brisbane)也設有數位鑑識實驗室，主要提供澳洲稅務局業務面內部調查和資安鑑識技術支援，包括澳洲稅務局所有資訊系統內部舞弊調查，如稅務作業不當行為或濫用資訊系統服務(包括稅務資料外洩、竄改或營業人逃漏稅)，另亦支援其他政府的鑑識服務，包括其他政府機關內部和外部資安事件調查。

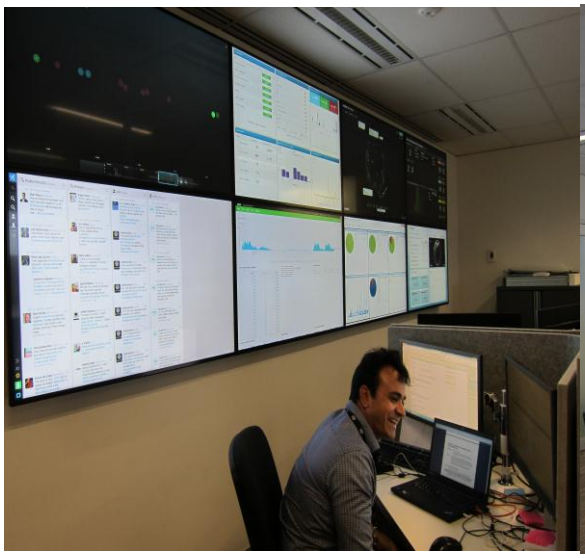
該局數位鑑識人員表示，其執行澳洲稅務局內部和外部的一系列數位鑑識工作時，需要高水準的數位鑑識專業技術能力，因此他們必須不斷進修及訓練。執行數位證據蒐證時，有時必須進入納稅人處所蒐證，故須澳大利亞聯邦警察配合協助執行搜查。當他們執行前述作業時，為確保蒐證期間之數位證據可以保留作為法庭上之證據力，爰嚴格執行數位證據保全標準作業流程。

為執行上述數位鑑識作業，每位數位鑑識調查員都須接受符合國家標準之數位鑑識培訓作業，並配備了各種高規格之數位鑑識的現場蒐證工具。例如為順利辦理現場蒐證及存取資料作業，所使用之工具必須可以蒐集硬碟、

手機…Xboxes 及 iPods 等任何能保存數據之媒體，且蒐證之數位證據必須接受法庭上檢驗，因此鑑識人員亦須於法庭上以專家證人身分出席。所以他們位於布里斯班、坎培拉、墨爾本及雪梨等四個數位鑑識實驗室，皆配備了高級鑑識分析工作站和伺服器，以提供鑑識分析這些蒐證和存取的證據。

該局數位鑑識人員表示，澳洲稅務局數位鑑識團隊曾經服務的對象包括澳洲稅務局(ATO)、澳大利亞聯邦警察、環境部、農漁業和林業部、外交和貿易部、教育部、海關/移民邊境大隊、昆士蘭警察、維多利亞警察、NSW 警察、NT 警察、昆士蘭州國家稅務局、澳大利亞犯罪委員會、就業部、澳大利亞體育反藥物管理局、國防部(包括四個機構)、廉政公署、衛生和公眾服務部、社會福利部、律政司、澳大利亞選舉委員會、財政部、國際刑警、ASIC、ACCC、雪梨市、社會服務部、NSW 環境保護局、NSW 公平貿易局、護照發行辦事處、總理和內閣辦公室、澳大利亞技能局、護照發行辦事處、外交和貿易部及犯罪和腐敗委員會等 36 個機關(構)。只要其他政府機關提供車馬補助費，他們基於機關互助，皆會提供數位鑑識相關服務。

另澳洲稅務局資安監控中心(SOC)針對網路流量、防火牆、入侵防禦系統、應用程式防火牆、防毒軟體中控台等監控(資安監控儀表如下圖)，據該局人員表示對於委外廠商存取紀錄及網路社群網站對於澳洲稅務局好壞評分，也會特別監控，並以笑臉及哭臉表示社群網站目前評分現況。



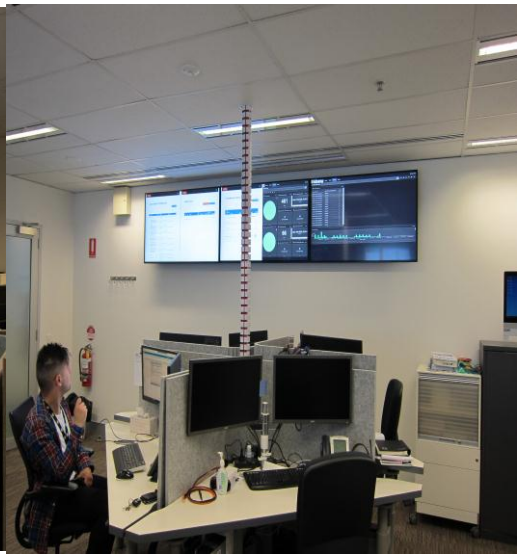


圖 13、澳洲稅務局資安監控儀表

目前該局資安監控儀表並未全面整合，據澳洲稅務局人員表示預計於106 年他們 IT 部門搬到新大樓時，將會全面整併資安監控儀表，以全面掌握資安事件動態狀況，並互相勾稽資安現況。

澳洲政府規定，每個政府機關皆要制定「營運持續及災難回復計畫」(Business Continuity and Disaster Recovery Plans)，避免災害發生時，關鍵系統無法於短期內提供使用，並且須定期測試備份資料，演練災害發生之回復過程，以確認其計畫有效性。

我們參訪澳洲稅務局適逢陣亡將士紀念日(英文：Remembrance Day)，他們為紀念第一次世界大戰於 1918 年 11 月 11 日上午 11 時結束，於每年 11 月 11 日當地時間 11 時，當地人皆會放下手中工作，就地默哀 10 分鐘。當然戰爭造成悲劇是一場無法挽回的記憶，但是避免戰爭的發生則是我們這一代須肩負的使命。目前網路攻擊時刻在上演，他們堅信雖無法將所有的網路攻擊阻擋，但是如何透過事前防範機制，以降低網路入侵或減緩災害，是澳洲稅務局資訊安全及數位鑑識部門一再提起的重點。所以澳洲政府對於降低網路入侵或減災的防範機制，目前總共規劃 35 個減災策略(參閱下表)，按規範遵循前 4 大減災策略，約可降低 85%的網路攻擊或災損。

表 3、澳大利亞 35 個減緩網路入侵策略評估彙整表

Strategies to Mitigate Targeted Cyber Intrusions (Originally published 18 February 2010, updated for February 2014)									
Rankingfor 2014(2012)排名	Mitigation Strategy 防災策略	Overall Security Effectiveness 整體安全有效性	User Resistance 外部阻力	Upfront Cost 前置成本	Maintenance Cost 維護成本	HelpsDetectIntrusions 有助於檢測入侵	HelpsPreventIntrusion Stage 1 有助於防止第 1 階段網路入侵	HelpsContainIntrusionStage 2 有助於防止第 2 階段網路入侵	HelpsContainIntrusionStage 3 有助於防止第 3 階段網路入侵
1(1)	Application whitelisting of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers.	Essential	Medium	High	Medium	Yes	Yes	Yes	Yes
2(2)	Patch applications e.g. Java, PDF viewer, Flash, web browsers and Microsoft Office. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications.	Essential	Low	High	High	No	Yes	Possible	No
3(3)	Patch operating system vulnerabilities. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest suitable operating system version. Avoid Microsoft Windows XP.	Essential	Low	Medium	Medium	No	Yes	Possible	No
4(4)	Restrict administrative privileges to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.	Essential	Medium	Medium	Low	No	Possible	Yes	No
5(18)	User application configuration hardening, disabling: running Internet-based Java code, untrusted Microsoft Office macros, and unneeded/undesired web browser and PDF viewer features.	Excellent	Medium	Medium	Medium	No	Yes	No	No
6(N/A)	Automated dynamic analysis of email and web content run in a sandbox to detect suspicious behaviour including network traffic, new or modified files, or other configuration changes.	Excellent	Low	Medium	Low	Yes	Yes	No	Possible
7(21)	Operating system generic exploit mitigation e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).	Excellent	Low	Medium	Low	Possible	Yes	Possible	No

8(11)	Host-based Intrusion Detection/Prevention System to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence.	Excellent	Low	Medium	Medium	Yes	Yes	No	Possible
9(5)	Disable local administrator accounts to prevent network propagation using compromised local administrator credentials that are shared by several workstations.	Excellent	Low	Medium	Low	No	No	Yes	No
10(7)	Network segmentation and segregation into security zones to protect sensitive information and critical services such as user authentication by the Microsoft Active Directory service.	Excellent	Low	High	Medium	Yes	No	Yes	Possible
11(6)	Multi-factor authentication especially implemented for remote access, or when the user is about to perform a privileged action or access a sensitive information repository.	Excellent	Medium	High	Medium	No	No	Possible	No
12(8)	Software-based application firewall, blocking incoming network traffic that is malicious or otherwise unauthorised, and denying network traffic by default.	Excellent	Low	Medium	Medium	Yes	Yes	Yes	No
13(9)	Software-based application firewall, blocking outgoing network traffic that is not generated by a whitelisted application, and denying network traffic by default.	Excellent	Medium	Medium	Medium	Yes	No	Yes	Yes
14(10)	Non-persistent virtualised sandboxed trusted operating environment, hosted outside of the organisation's internal network, for risky activities such as web browsing.	Excellent	High	High	Medium	Possible	No	Yes	Possible
15(12)	Centralised and time-synchronised logging of successful and failed computer events, with automated immediate log analysis, storing logs for at least 18 months.	Excellent	Low	High	High	Yes	No	Possible	Possible
16(13)	Centralised and time-synchronised logging of allowed and blocked network activity, with automated immediate log analysis, storing logs for at least 18 months.	Excellent	Low	High	High	Yes	No	Possible	Possible
17(14)	Email content filtering, allowing only whitelisted business related attachment types. Preferably analyse/convert/sanitise hyperlinks, PDF and Microsoft Office attachments.	Excellent	High	High	Medium	Yes	Yes	No	Possible
18(15)	Web content filtering of incoming and outgoing traffic, whitelisting allowed types of web content and using behavioural analysis, cloud-based reputation ratings, heuristics and signatures.	Excellent	Medium	Medium	Medium	Yes	Yes	No	Possible

19(16)	Web domain whitelisting for all domains, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.	Excellent	High	High	Medium	Yes	Yes	No	Yes
20(19)	Block spoofed emails using Sender ID or Sender Policy Framework (SPF) to check incoming emails, and a "hard fail" SPF record to help prevent spoofing of your organisation's domain.	Excellent	Low	Low	Low	Possible	Yes	No	No
21(22)	Workstation and server configuration management based on a hardened Standard Operating Environment, disabling unneeded/undesired functionality e.g. IPv6, autorun and LanMan.	Good	Medium	Medium	Low	Possible	Yes	Yes	Possible
22(25)	Antivirus software using heuristics and automated Internet-based reputation ratings to check a program's prevalence and its digital signature's trustworthiness prior to execution.	Good	Low	Low	Low	Yes	Yes	No	No
23(24)	Deny direct Internet access from workstations by using an IPv6-capable firewall to force traffic through a split DNS server, an email server, or an authenticated web proxy server.	Good	Low	Low	Low	Yes	Possible	No	Yes
24(23)	Server application configuration hardening e.g. databases, web applications, customer relationship management, finance, human resources and other data storage systems.	Good	Low	High	Medium	Possible	Yes	No	Possible
25(27)	Enforce a strong passphrase policy covering complexity, length, expiry, and avoiding both passphrase reuse and the use of a single dictionary word.	Good	Medium	Medium	Low	Possible	No	Yes	No
26(29)	Removable and portable media control as part of a Data Loss Prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.	Good	High	Medium	Medium	No	Yes	Possible	Yes
27(28)	Restrict access to Server Message Block (SMB) and NetBIOS services running on workstations and on servers where possible.	Good	Low	Medium	Low	No	Yes	Yes	No
28(20)	User education e.g. Internet threats and spear phishing socially engineered emails. Avoid: weak passphrases, passphrase reuse, exposing email addresses, unapproved USB devices.	Good	Medium	High	Medium	Possible	Possible	No	No
29(26)	Workstation inspection of Microsoft Office files for potentially malicious abnormalities e.g. using the Microsoft Office File Validation or Protected View feature.	Good	Low	Low	Low	Possible	Yes	No	No
30(25)	Signature-based antivirus software that primarily relies on up to date signatures to identify malware. Use gateway and desktop antivirus	Good	Low	Low	Low	Possible	Possible	No	No

	software from different vendors.								
31(30)	TLS encryption between email servers to help prevent legitimate emails being intercepted and used for social engineering. Perform content scanning after email traffic is decrypted.	Good	Low	Low	Low	No	No	No	No
32(32)	Block attempts to access websites by their IP address instead of by their domain name, e.g. implemented using a web proxy server, to force cyber adversaries to obtain a domain name.	Average	Low	Low	Low	Yes	Yes	No	Yes
33(33)	Network-based Intrusion Detection/Prevention System using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.	Average	Low	High	High	Possible	Possible	Possible	Possible
34(34)	Gateway blacklisting to block access to known malicious domains and IP addresses, including dynamic and other domains provided free to anonymous Internet users.	Average	Low	Low	High	Possible	Yes	No	Yes
35(35)	Capture network traffic to/from internal critical asset workstations and servers as well as traffic traversing the network perimeter, to perform post-intrusion analysis.	Average	Low	High	Low	No	No	No	No
This document and additional information about implementing the 35 mitigation strategies is available at http://www.asd.gov.au/infosec/top35mitigationstrategies.htm									

以下介紹澳洲政府對於降低網路入侵或減災的策略中，最重要之前四大策略：

1. 應用程式白名單

建立允許(或受信任)應用程式白名單的機制，以防止執行惡意或未經批准的程式(包括 DLL 檔案, scripts and installers)，這個策略應優先規劃於最可能遭受攻擊的伺服器執行。該局人員表示應用程式白名單的適當配置，有助於防止不明程式執行造成漏洞，例如從網站下載、電子郵件附件或經由可攜式設備(如 USB)之軟體。尤其在重要的服務器(如 Active Directory 和其他身份驗證伺服器)應嚴格執行應用程式白名單，這策略可避免網絡攻擊者取得管理者權限或密碼。

2. 應用程式漏洞修補

應用程式補 Patch，特別是 Java，PDF 閱覽器，Flash Player，Microsoft Office，Web 瀏覽器和 Web 瀏覽器使用的 ActiveX。網絡攻擊者可能會利用這些漏洞，來執行未經授權程式，以取得管理者權限或入侵電腦系統，故應該在 Patch 公布後 2 天內修補應用程式漏洞，以避免存有漏洞之系統暴露高風險。應提升應用程式至最新版本，最新版本通常包含其他安全防護技術，軟體甚至只能透過升版來修復漏洞。

3. 作業系統漏洞修補

作業系統漏洞修補也是非常重要，例如微軟作業系統的 Patch 修補，澳洲稅務局人員表示同樣應該在 Patch 公布後 2 天內修補完畢，並且使用符合組織業務需求的最新版本之操作系統。例如避免使用 Microsoft Windows XP 和早期版本的 Microsoft Windows，最好使用 64 位版本的 Microsoft Windows 而不是 32 位版本，因為 64 位版本包含其他安全防護技術。

4. 限制管理者權限

管理者權限主要被設計為僅允許受信任的人員配置，用來管理及監

控電腦系統。對於使用者操作時，應該限制其在作業系統及應用程式的管理權限。如果有必要時，可以規範使用者在非管理或有風險的活動，應該使用非特權的帳號及密碼，例如透過網際網路讀取電子郵件或瀏覽網頁等。限制使用者之管理權限可以讓系統管理者更易於管理及維護整個電腦系統，因為可以避免少數使用有意或無意對其作業系統進行重大更改。最小化管理權限使得入侵者更難以在系統隱藏，或被惡意程式利用當作跳板擴散到內部網路。

該局人員表示限制管理者權限策略適用於下列使用者，例如具有網域或本機系統管理權限、具有提升的作業系統權限的帳號、具有連結資料庫帳號及允許承商執行遠程訪問的管理帳號等。

澳洲稅務局人員表示降低網路入侵或減災的前四大策略是該國澳大利亞信號局(ASD)評估，根據他們目前對網絡威脅環境的現況，規劃實施的最有效的安全控制措施。據該局人員表示，如果實施前四大策略將至少阻擋或減輕該組織被入侵 85%的機率。因此該國總檢察長辦公室在澳大利亞政府保護安全政策框架(PSPF)，要求澳大利亞政府機構實施資安的控制措施，需先評估滿足澳大利亞信號局(ASD)的前四大減災策略。

澳大利亞並從總體安全有效性、外部阻力、前期成本、維護成本、有助於檢測入侵、有助於防止入侵(階段 1)、有助於防止入侵(階段 2)、有助於防止入侵(階段 3)等 8 個構面，對所有 35 個減災策略做前置分析，以作為澳洲政府機關導入參考。如果確定要實施前 4 大減緩措施，澳洲稅務局人員建議先從最可能遭受網路入侵的伺服器實施，慢慢擴散到所有伺服器，並評估透過其他減緩措施補強，直到達到施行機關可接受風險。

圖 14、澳洲稅務局參訪合影

伍、 心得與建議

一、 參訪思科澳洲分公司心得與建議

(一) 參訪心得

本次拜訪思科澳洲分公司之網路安全研究團隊，並於聽取該公司的介紹及討論後，更加感受到該公司對於網路安全的專業與投入。該公司除長於網路設備及網路資安設備之生產外，對於整合網路安全設備並提升網路安全也非常專業。

(二) 參訪建議

考量現今網路攻擊手法複雜，需透過整合型防禦網路，以即時發現攻擊行為，建議可考慮建置攻防演練模擬環境，提升資安人員防禦技術能力；或直接導入整合型網路防禦方案，以提升本中心網路整體防禦能力。

二、 參訪資誠企業管理顧問公司(PwC)澳洲分公司心得與建議

(一) 參訪心得

該事務所近年來對於數位證據保全及鑑識的研究與服務亦投入相當多的資源，積極培養數位證據鑑識專業人才，成立「數位鑑識實驗室」，建構數位證據鑑識標準作業程序。

(二) 參訪建議

1.事前規劃重要軌跡保存，以利事後數位證據蒐集及分析

數位證據之證據力及證據能力與事前規劃保存息息相關，數位證據除用戶端電腦外，主機之硬碟、記憶體、日誌紀錄等均為重要來源，因此建議在重要軌跡蒐集，事先須有良好的保存規劃，一旦發生事件時才能有跡可循。

2.建置專業且認證之數位鑑識分析工具，提升數位證據能力

「工欲善其事，必先利其器」，建議採購專業且認證之數位鑑識分析工具，除有效、快速的找出事件發生之原因，透過該工具所採集或分析之證據，亦可被法院所採信。

三、 參訪澳洲稅務局心得與建議

(一) 參訪心得

澳洲政府對於每個機關(構)在資訊安全應肩負的責任，在相關文件皆已明確規範，反觀我國目前是以任務編組方式推動資安政策及規範。澳洲政府將資安相關技術文件指引暨規範及關鍵技術文件暨規範，均公布於網路上，提供政府機關、承商及使用者透過網路連結瀏覽，且易搜尋及閱讀。

另在執行 35 個減災策略的作業，澳洲政府皆已規範相關作業流程，並透過政府事前評估表，讓政府機關可以清楚了解有關減災策略实施成本及使用者的阻力等之評估，以利政府機關根據需求，評估及選擇最佳策略。

(二) 參訪建議

1. 規劃評估網路減災策略，以減緩網路入侵災損

澳洲稅務局所採行 35 個防止網路入侵或減災策略，其中部分項目本中心雖已採用，例如排名第 10 的網段隔離、第 11 的多重因子認證、第 17 的電子郵件內容過濾、第 18 的 Web 內容過濾…等，惟未如澳大利亞有系統及完整之評估，建議參考澳大利亞從總體安全有效性、外部阻力、前期成本(員工，設備，技術複雜性)、維護成本(主要員工)、有助於檢測入侵、有助於防止入侵(階段 1)、有助於防止入侵(階段 2)、有助於防止入侵(階段 3)等 8 個構面評估分析。

前述有關 IT 系統管理員在典型 Windows 環境中規劃和實施前 4 大策略的技術指導，係因澳大利亞大多數政府業務的個人電腦及伺服器大部分使用 Windows 作業系統；本中心前端個人電腦係使用 Windows 作業系統，後端的伺服器大部分使用 AIX-Unix 或 Linux 作業系統，故無法全面套用，而行政院資通安全處提供類似組態設定規範，惟亦未如澳洲政府所制訂全面性規範及參考資料，建議可參考澳洲政府規範網路入侵 35 個減災策略之內涵，於本中心 AIX-Unix 或 Linux 作業系統訂定相關規範。

2.參考澳洲稅務局數位鑑識機制，逐步建置資安健檢及數位鑑識能量

有關澳洲稅務局在數位鑑識作業很早就規劃及執行,其數位鑑識團隊(Forensics & Investigations team) 於 1999 年就成立至今，目前專責人員約 30 位，隸屬於該局 IT 安全部門，主要任務是維護該局數位稅務資料之機密性及完整性。另該團隊於坎培拉、雪梨、墨爾本及布里斯班皆設有數位鑑識實驗室，並配備相關蒐證及鑑識分析設備，該團隊曾經服務對象包括該局等 36 個政府機關(構)。

本中心於 105 年 10 月成立資安健檢及數位鑑識小組成員共 17 位,其中專責人力只有 1 位，除本中心 13 位，亦包括關務署、國有財產署及台灣銀行計派 4 位，建議後續將於預算及專責人力允許下，就資安健檢及數位鑑識所需之設備逐步建置，供該小組成員使用，並須透過人員補充及專業訓練，提升資安健檢及數位鑑識作業能力，將資安健檢及數位鑑識能量從本中心逐步擴大至財政部所屬機關。

3．建立資安技術文件瀏覽機制，以利搜尋及閱讀

澳洲政府資安相關技術文件指引暨規範及關鍵技術文件暨規範,均公布於網路上，提供政府機關、承商及使用者透過網路連結瀏覽，且易搜尋及閱讀。建議本中心參考澳洲政府文件瀏覽機制，將資安技術文件公布於網路上，並建立關鍵字超連結，以利搜尋及閱讀。