2014 年 RSA Conference 研討會紀要

沈柏村 / 金融聯合徵信中心 資安部

現今的世界已經是高度依賴網路及資訊科技，政府、機構組織及公司企業都在網路上提供各種服務，隨著科技的演進，存取服務的方式也從個人電腦普及至平板電腦與智慧型手機；網路及資訊科技提供了使用者便捷的服務，但提供服務的資訊系統也可能存在著弱點與風險，有機會讓不懷好意的有心人士侵入而造成破壞及損失，網路犯罪的型態也在不斷的改變，手法日新月異的翻新，資訊系統的安全防護也需要時時檢討及改進，才能有效的防堵各種可能的威脅與風險。爲了解國際上資訊安全議題與發展趨勢參加本次RSA Conference研討會(以下簡稱RSA大會)，希望藉由考察後報告介紹的各種資訊安全策略及實例，可以提供作爲規劃資訊安全架構及執行機制之參考。

RSA 是一種公鑰加密演算法，在1977 年由「麻省理工學院」的 Ron Rivest、Adi Shamir 與 Leonard Adleman 三人所共同設計出來，演算法名稱以三人的名字(Rivest, Shamir, Adleman)的第一個字母命名爲RSA；三人於1982年成立RSA Security公司，並於1991年開始舉辦以「密碼學、標準與公共政策」爲主的密碼學家論壇。該論壇自1993年開始成爲一年一度的盛事，並命名爲RSA Data Security Conference，至2000年簡化名稱爲RSA Conference。RSA Security公司於2006年被EMC公司收購，成爲EMC公司的資訊安全事業部(RSA, the Security Division of EMC)，雖然RSA Security公司被收購成爲部門，但每年度的會議仍由該部門舉辦，RSA Conference名稱仍持續延用。RSA Conference的歷史已有20多年，已是每年度全球之資訊安全重要會議，現在每年都在美洲、歐洲及亞洲分別舉辦。

會議內容

2014年在美國舉辦之RSA大會（RSA Conference 2014)，會議地點在舊金山Moscone Center會議中心，會議時間為2月24日至28日，24日主要是大會註冊，還有一些提前進行的研討會課程及歡迎酒會，25日至28日會議議程主要為「專題演講」(Keynotes）與「資訊安全課程」(Class Tracks)；「專題演講」(Keynotes）邀請知名企業高階主管以及大學教授等專家蒞臨演講，而「資訊安全課

程」(Class Tracks)議題包括雲端安全和虛擬化、資料安全和隱私、駭客與威脅等，講師為各議題的專家；另外有RSA、Checkpoint、Juniper、Fortinet、Symantec、McAfee、Cisco、Microsoft、IBM等超過百家廠商展出其資訊安全解決方案，下面就本次參加的內容摘要說明。

(一)大會主題

2014年RSA大會會議的主題是Share · Learn · Secure—Capitalizing on Collective Intelligence (分享 · 學習 · 安全—運用集體智慧)，此主題要描述的是現今大家正面臨著變革與創新，而所有創新都不是憑空產生，是各種想法、觀點、見解和創意，從分享、學習、整合而成的結果，如果我們充分利用集體智慧，每一個進展都會推動創新，循序漸進的不斷創新會演變為真正的變革。

現今大家面臨的危機是駭客們變得越來越有組織、集體的開發出攻擊的新方法，所以網路安全防護已不是僅依靠幾家網路安全軟、硬體產品的廠商就可以達成；RSA大會致力要大家實現知識及資源分享，並即時交換互相學習，以提升網路安全防護強度，建構保護未來安全的平台。

(二) 專題演講 (Keynotes)

本次RSA大會共有16場「專題演講」(Keynotes)，本篇報告分享參與的其中幾場演講的摘要內容：

1. Finding a Path Forward in an Increasingly Conflicted Digital World.

講者：Arthur W. Coviello

資歷：Executive Chairman, RSA

摘要：

我們正處於使用資訊技術的基礎轉變之中，這個轉變對我們的社會和文化的未來有著巨大的影響。資訊技術迅速擴張和民主化帶來了政府、企業和個人共同崩潰的競爭議題，我們需要社會規範來引導我們的數位世界。

RSA的執行主席Arthur W. Coviello在開幕致詞中指出，隱私、政府以及民間如何一起參與合作而非麻痺或衝突，然而若政府模糊了防禦和情報收集的角色界線，這將導致隱私安全產業、顧客與政府間的信任崩解，並產生問題。他主張美國國家安全局(NSA,National Security Agency)和世界各地情報機構，都需更清楚區分防禦角色和情報收集角色。

Arthur W. Coviello在會場上說明，在現今社會，資訊已越來越垂手可得並更具價值，大眾對於政府、企業以及個人競爭利益的緊張情勢已是意料之內。我們身處於對未來社會及文化具有重大影響的歷史性轉變中，然而資訊技術的快速擴張及民主化，若缺乏社會規範，將帶來不同群體的牴觸與衝突，並產生不可預知的後果。他提到「資訊

技術使用的歷史性轉換」，數位技術、巨量資料(Big data)和萬物聯網(Internet of Things)的出現是關鍵因素。現今的數位技術能解決很多問題，但亦有毀滅性的力量，所以必須為數位技術的利用制定合理的規範準則。

Arthur W. Coviello在演講中呼籲，所有國家應採行下列四項原則：

(1) 放棄網路武器，以及放棄藉由網路發動戰爭。

我們必須像憎惡核子武器和化學戰爭一樣憎惡網路戰爭。不同於核子武器，網路武器易於傳播並吸引開發者，Arthur W. Coviello並擷取一句名言，「Those who seek military advantage riding the back of the tiger will end up inside.」說明若採用網路武器發動戰爭，最終將自取滅亡。

(2) 國際間合作研發及制裁網路犯罪。

各國政府如果試圖在網際網路上一爭高下，那麼獲利的只會是網路罪犯。網路罪犯近年越發猖獗，國際間越是缺乏及時性、持續性的合作，越是提供這些罪犯一個安全無虞的犯罪天堂。

(3) 確保網路中的經濟活動能自由進行以及全球重視智慧財產權。

商業、研究及通訊所帶動的經濟活動大有價值，因此需達有合作協定，相關法律規範必須明文制定。

(4) 尊重並確保個人隱私。

在這數位世代，個人資料已成為真正的貨幣，個人的基本自由要得到保護；政府在處於開放、公平及透明的前提立場下，越有責任確保個人權利(individual rights)在集體安全(collective security)中取得平衡。

Arthur W. Coviello另外表示我們需要持續開發資訊技術架構以實行智慧化安全，期望未來自動應對0 day安全威脅、隔離危險並防止損害。他也說明未來將是用戶定義IT的時代(user defined IT)，需要用更具智慧的方法識別系統，使資安團隊能夠平衡用戶和IT部門的需求，同時仍然能夠跨使用者設備執行安全政策。身份管理必須能夠在移動設備和雲端環境中管理。

Arthur W. Coviello闡明，儘管國與國之間存有不同的利益與差異性，但上述四項原則無庸置疑地是以所有國家及人類的利益作為出發點，國際間應致力於付諸實行，共同打造更安全、更可信賴、更理想的數位世界。

2. Conundrums in Cyberspace：Exploiting Security in the Name of, well, Security.

講者：Scott Charney

資歷：Corporate Vice President, Trustworthy Computing, Microsoft

摘要：

政府監控計劃遭廣泛的揭露使得資訊技術的信任已經被嚴重的破壞，限制政府存取隱私資料的重大的公眾議題仍在持續爭論，客戶，政府及大眾需要知道的資訊技術供應商的立場在哪裡。

Microsoft公司的Trustworthy Computing副總裁Scott Charney談論因為國家安全局（NSA,National Security Agency）的監控計劃遭公開揭露，已經嚴重損害了大眾對資訊技術的信任。他表示業界和政府應有責任保護大眾，但在稱為國家安全的前提下，大眾的資料隱私往往被忽視，直到發生了事件後才會被重視。他指出有必要對政府的監控建立規範，他認為大眾必須參與建立規範，以確保資料的隱私，防止資料遭政府洩露濫用。

Scott Charney談到創新與安全，供應商不僅需提供先進的技術，以滿足大眾的數據通信和Internet網路的需求，供應商同時也有責任確保他們的產品和服務不會有任何明顯的漏洞讓大眾處於風險當中。

Scott Charney認真傳達微軟沒有為政府設後門軟體的立場，因為這樣做是不道德的行為，且對微軟也沒有好處；他提及以前有流傳Windows NT系統含有名為_NSAKEY的金鑰，並說明這樣命名是因為國家安全局監管加密技術出口，必需符合美國法規才這樣命名，他表示假如微軟設置後門，絕對不會將之命名為_NSAKEY；他提到“如果微軟在產品植入後門軟體，市值會一夜之間變為零”，那是瘋子的自殺行為，所以微軟不可能有後門軟體。

Scott Charney表示微軟在一個範圍限度內會幫助政府的執法，但微軟不會參與非法的搜查，如果政府需要從微軟的雲端客戶取得資料，微軟不會直接提供，微軟會引導政府向該客戶直接獲取資料。

Scott Charney指出為了讓國外的政府相信微軟不存在後門軟體，微軟把自己的原始程式碼交給其他國家的政府檢查，如果有發現存在缺陷，微軟會修復缺陷，以獲取客戶的信任，並證明微軟是安全的。

3.The Next World War Will be Fought in Silicon Valley

講者：Nawaf Bitar

資歷：Senior Vice President and General Manager, Security Business Unit, Juniper Networks, Inc.

摘要：

Juniper Networks公司的資深副總裁兼安全業務部門總經理Nawaf Bitar表示網路攻擊所造成的破壞比蓋達恐怖組織活動更具威脅性；他指出，儘管我們的隱私正一點一滴受到入侵，資訊被侵犯竊取，但大眾卻仍習慣性地認為網路的安全與自身毫不相關。

Nawaf Bitar認為大眾的冷漠加深了網路攻擊的威脅性，掩蓋了當前形勢的嚴重性，然而我們往往只會在我們真正在乎的實質價

值 (例如：家庭與金錢) 受到威脅時才會有所反應。Nawaf Bitar並點明所謂第一世界的怒火 (first-world outrage)，並無助於網路安全的實踐，人們在Facebook或Twitter上不斷分享連結或是以按讚來表達自己憤怒的情緒，實際上這是一件毫無意義的事。

Nawaf Bitar呼籲大眾重新評估隱私對於個人的價值，他表示資料是我們最為寶貴的財產之一，我們也應該建立起這樣的價值意識。

Nawaf Bitar講述Semmelweis Reflex (意指拒絕新的知識僅僅是因為它違背了既定的規範，信仰或做事的方式)，早期醫師不認為男人的手會傳染疾病，因而造成產婦分娩過程中的死亡率相當高，直到匈牙利醫生Ignaz Semmelweis發現為產婦接生前先洗手，可以大大減少產婦分娩過程中的死亡率，Ignaz Semmelweis的一個新的想法與實驗，改變他們的工作方式，減少了生命的死亡；這種精神同樣的適用於安全性的創新，通過實現簡單的安全行為，使之成為習慣常態，我們可能會大大降低我們的資料被破壞或竊取的風險。

Nawaf Bitar節錄愛因斯坦名言，I don't know what weapons will be used in the next world war, but the one after will be fought with sticks and stones. (戰爭造成毀滅使一切重新再來)，說明我們應該要將憤怒化成具體行動，有所作為並反轉情勢，否則消極的作為可能換來下一波在矽谷的世界大戰。

4. The Future of Security

講者：Stephen Trilling

資歷：Senior Vice President of Security Intelligence and Technology, Symantec Corp.

摘要：

如何停止有無限資源的攻擊者危害企業最重要的資料和服務? 部署50台單機資安產品和僱用昂貴的專家穩定的監測它們？這種做法不恰當，有太多的盲點且方法太昂貴。那麼有什麼解決辦法？讓我們展望看看未來。

Symantec公司的安全情報與技術高級副總裁Stephen Trilling談到“我們正在打一場不對稱的戰鬥”。他說目前的確是有些比較好的資安產品可以阻擋一些網路攻擊，可是因為攻擊者一樣可以買到同樣的產品，並了解產品的弱點，攻擊者有資源以及耐心，可以多年策劃和調整攻擊，即便是最好的資安產品，也無法擋住一些攻擊甚至多數攻擊。

Stephen Trilling認為在資安的縱深防禦策略，企業仍需要繼續部署資安產品來做防禦 (如防火牆、電子郵件過濾系統及防毒系統等)，但問題在於這些資安產品每個都像是一個孤島，各自有自己的平台，在自己有限的範圍內檢測防護，並無法做到互相關聯

溝通；儲存這些設備的資料也是一個成本，管理設備也是複雜且需要許多人力參與的事情，大多數企業都面臨這些問題，不僅如此，現有大多數企業都是只顧做好自己的防禦，也讓每個企業形成是一個個孤島。

Stephen Trilling說到資安產品SIEM (Security Incident and Event Monitor)，SIEM的好處是它可儲存許多資安產品的log資料，但目前只適合在數分鐘至數小時的限定時間內做資料關聯分析，現有的瓶頸是那些週、月甚至是年的分散時間資料目前並沒有一個方式做相關聯分析，而且SIEM價格昂貴，通常是有非常多資安產品且願意投資人力與金錢的企業，使用SIEM才會有規模經濟。

Stephen Trilling談及理想解決方案的未來計劃，他認為最重要的是在巨量資料(Big data)層面的整合，他表示未來企業應該會採用委外服務來保護他們的資料安全，因為服務的廠商能提供各企業符合其需求的資安產品與資料關聯分析，可充分利用規模經濟做安全管理，以開發模型智慧分析在跨行業的許多企業公司與機構的資料檢測攻擊模式，整合為安全服務並自動化的通知企業客戶，例如自動連續尋找異常活動(在Internet的A伺服器在分析後是被認定有惡意程式的，服務廠商能自動連續尋找過去有連接至A伺服器的所有企業並給予通知)；未來許多複雜的攻擊將在數分鐘或數小時內檢測發現攻擊者，如此企業不再侷限在有限的範圍內檢測防護，資安產品與企業不再會像孤島，而是形成了一個區域聯盟，分享、智慧的保護企業安全。

(三)資訊安全課程(Class Tracks)

本次RSA大會「資訊安全課程」(Class Tracks)包含雲端安全和虛擬化、資料安全和隱私、駭客與威脅、產業專家、行動裝置安全、技術基礎架構、安全分析、應用程式安全、密碼學、安全趨勢和創新等23個議題，此次參與了雲端安全和虛擬化、資料安全和隱私、駭客與威脅議題，本篇報告分享參與的其中幾場的內容摘要說明：

1. Hacking Exposed： Day of Destruction

講者：Dmitri Alperovitch

資歷：Co-Founder & CTO, CrowdStrike, Inc.

摘要：

破壞性的攻擊仍然是相對較少發生的；然而，對此有興趣的攻擊者越來越多。破壞性攻擊的歷史回顧，包含 fork炸彈、CIH病毒、Stuxnet、Wiper、Narilam、Maya、Korean/DarkSeoul attacks、Ransomware、Shamoon。

大多數的攻擊，做好資料備份仍可復原，下一代的攻擊主要是攻擊硬體，給與最大的衝擊和最難恢復的狀態，目前的大多數

的攻擊仍然是可復原的，硬碟資料被破壞、硬碟資料被加密，做好資料備份就可復原；硬碟開機磁區MBR被破壞，做好硬碟備份，並有開機磁區還原程式就可復原；BIOS被破壞，做好備份重新安裝就可復原，雖然造成了某種損害，我們總是有辦法恢復系統或恢復資料。

下一代的攻擊是永久性的破壞，主要是攻擊硬體，試想一下，如果下列系統被破壞會有什麼影響：你在公司建築內但你的識別證不能用、冷暖空調處於關閉狀態、監控攝影機關機、50,000台顯示器屏幕閃爍顯示“系統磁碟錯誤”、電話系統及視訊會議無法使用、電子郵件伺服器停機、VPN網路關閉、不能買到咖啡，因為信用卡讀卡機失效。

會場演示情境為蘋果電腦有SSL弱點，使用社交工程讓受害者更新了偽造的蘋果電腦韌體，重開機後使電腦關閉風扇，CPU溫度上升至沸水水平，造成的影響可能是燒傷使用者、永久損壞電子元件或電子元件短路引起火災。

對於此種破壞性攻擊的對策是韌體需做簽章，以確認韌體是供應商所開發提供，在Windows 8中包含EFI(Extensible Firmware Interface)簽章(NIST BIOS保護準則)，所有的供應商應需簽署其所有韌體。我們正在進入針對性的破壞性攻擊的新時代，從資料洩露到資料系統被破壞，有意圖的駭客者將從DDOS攻擊轉移到破壞系統，我們要了解攻擊對手會做破壞的活動，而所有提供更新的韌體需做簽章是緊急必要的。

2. Let Go of the Status Quo：Build an Effective Information Protection Program

講者：Daniel Velez

資歷：Director of Insider Threat Operations, Raytheon Cyber Products Company

摘要：

內部威脅是指組織內已授權的存取，因為員工受到詐騙、蓄意的破壞、盜竊、或是缺乏知識的作業錯誤等因素，對企業造成損害。

管理內部威脅的一般原則包含：留存日誌紀錄、監控管理、員工的作業稽核檢查、存取敏感文件的稽核檢查、員工正常工作範圍以外的活動偵查、帳號建立及系統管理員更改密碼之稽核檢查。

一個完整的內部威脅計劃可協助降低企業風險，建構一個完整的內部威脅計劃所必需的程序：

(1) 建立一個內部威脅計劃：由上向下的指導和宣傳，並建立願景(提高意願;降低拖累)。

(2) 業務導向： 讓計畫是對應組織的業務案件。

(3) 編制工作成員： 成員的素質比技術更為重要，必要時需篩選和審查。

(4) 利益相關者參與： 組織的利益相關者需提早參與，以了解利益相關者的需求。

(5) 教育訓練： 多舉辦內部教育訓練。

(6) 治理： 計畫需治理和監督，以及執行效果的測驗。

(7) 活動文件化： 將組織的原則、假設、需求都文件化，依5W1H規則提供明確的指導。

(8) 工具： 選擇一個適合組織的工具 (如：支援內部威脅計畫的資訊技術系統)

(9) 實行： 必需實行計劃，實行過程的阻礙須予以擊敗克服，因企業文化的不同，要與使用者溝通實行計劃的方向內容，組織要相信實行後的效果是對組織有益的，而實行內部威脅計劃並不是一勞永逸，要持續改善稽核檢查政策。

3. Hijacking the Cloud：Systematic Risk in Datacenter Management Networks

講者：Michael Cotton

資歷：Chief Security Architect Digital Defense Inc.

摘要：

側通道攻擊 (side-channel attack) 是間接地觀察硬體在運作時所洩漏出來的資訊，而不是傳統的直接破解方法，此攻擊方式可打破傳統的安全控管，完全繞過現有保護機制，但側通道攻擊有一個很大的限制條件，那就是通常情況下，需要「實體接近」才能進行。

但網絡基板 (Baseboard controllers) 攻擊已不需「實體接近」，會場演示經由伺服器基板管理控制器 (BMC, Baseboard Management Controller) 插槽進行網絡偵察、位址欺騙、執行惡意代理程式取得密碼、植入後門程式。

對於此種攻擊的對策是需確保管理網絡的完整性，注意網絡的管理與設定 (VLAN 存取、防火牆規則、共享網路卡、用戶端通訊協定、驗證密碼長度)，另外架構系統需注意國際安全組織CVE (Common Vulnerability and Exposure) 公布的漏洞，其他漏洞與一般設定的弱點。

結論與建議

(一) 培養資安意識成為習慣常態

聽了Nawaf Bitar的演講，有感目前多數的大眾仍認為資訊安全是提供服務的業者應該要做的，或是機構組織內負責管理安全的單位應該要幫大家做好的，大眾仍覺得資訊安全與自身毫不相關，除非自身已受到損失或傷害後才會有所領悟與改進。

想起小的時候，父母、幼兒園及小學的老師都會教導道路安全規則，例如：走路要靠右邊走，對面迎來的行人也靠右邊走，就可減少衝撞人的機會；過馬路前要先看左邊及右邊，確認沒有車子要經過再過馬路。有一次沒有照

著安全規則做，過馬路時急著衝過去，不巧就被摩托車撞飛而受傷，所幸只是皮肉擦傷，從那次以後過馬路都會特別的注意照著安全規則做。

其實資訊安全就如同道路安全，經由教導安全規則，實現簡單的安全行為，使之成為習慣常態，就可以大大降低風險，例如電子郵件社交工程教育訓練，教導同仁使用電子郵件的安全規則，只要同仁確實執行電子郵件軟體的安全設定，並於開啓郵件時確認一下寄件者的來源，不明來源就馬上刪除信件，這樣就可以大大降低資料被破壞或竊取的風險。

交通安全，人人有責，同樣的，資訊安全，人人也有責；降低資訊安全風險是每個人應該做的，大眾應學習培養將資訊安全規則變成一種意識，將遵守資訊安全規則成為習慣常態，如同「走路靠右邊、過馬路前要看左邊及右邊」的安全習慣，以共同防範網路攻擊，降低個人與機構組織的損害。

(二)可評估加強資安防護事項

1. 資安監控中心

聽完Stephen Trilling的演講，想到資安監控中心作業，除了由專業廠商提供全年無休的資安產品資料關聯分析、通報及協助處理服務，專業廠商在巨量資料(Big data)的分析，是否能有更進一步的加強與精進，可以針對下列內容評估規劃：

(1) 現今駭客對目標的攻擊行為更具恒心和耐力，可以多年策劃和調整攻擊，資料關聯分析是否可以跨多週、多月甚至是多年的分散時間做不同時段的攻擊行為分析。

(2) 分析發現外單位有新型態攻擊行為或黑名單主機，是否可以查找過去的紀錄，給予通報及協助處理服務。

(3) 目前關聯分析大部分仍局限於特徵碼的方式發現攻擊與威脅，是否可以開發模型智慧分析與自我學習機制，建立一個企業專屬的應用模型，經一段時間的自我學習和優化，套用於關聯分析規則；例如建立專屬的企業網路流量正常基準(baseline)模型，如發現企業的網路流量違背了這個基準模型，則發出預警通告或執行安全防護。

2. 韌體簽章

Dmitri Alperovitch在課程演示了攻擊模式正演進為下一代的攻擊，是有針對性的破壞性攻擊，是對硬體的攻擊，會破壞系統造成無法復原的損害，並表示提供更新的韌體需做簽章是緊急必要的，為此對韌體的安裝及更新，可與廠商針對下列內容，做評估規劃：

(1) 提供更新的韌體需由原廠取得，韌體需有原廠的簽章

(2) 安裝或更新韌體時需有檢核程序，確認韌體有原廠的簽章才能進行安裝或

更新。

(3) 系統於安裝或更新軔體時，自動檢核軔體是否有原廠的簽章再進行作業。

3. 實體隔離與虛擬化

實體隔離政策，可以減少或避免許多的風險，例如：營運區與辦公區隔離，可避免辦公區的變更作業影響營運環境運作的風險；禁止使用自有設備連接內部網路，可避免BYOD,Bring Your Own Device (帶自己的行動裝置來上班) 可能造成的管理成本及風險。

然而實體隔離不是只有隔離網路的存取就可使風險降低，Michael Cotton在課程演示了對於基板管理網路之側通道攻擊 (side channel attack)，顯示在實體隔離及虛擬化的建置規劃及維運，為避免此種攻擊，可以進行的檢視與評估方式：

(1) 無論是營運區或辦公測試區的電腦伺服器，從機房、機櫃及伺服器實體都需要加強存取管控，避免非授權人員的「實體接近」。

(2) 建置虛擬化主機時，營運區與辦公測試區必須獨立分開有各自的電腦伺服器及儲存設備。

(3) 檢視管理網絡的完整性，是否有不同網段之IP使用相同VLAN分段。

(4) 虛擬化主機需注意共享網路卡的使用，系統管理與網路管理的網段，不能與其他網段共享網路卡。

(三) 分享、學習、安全

我國行政院國家資通安全會報 (以下簡稱資安會報)，已逐步推動發展「資安資訊分享與分析中心 (Information Sharing and Analysis Center，以下簡稱ISAC)」，目前已建立之ISAC包括行政院國家資通安全會報技術服務中心營運之政府G-ISAC、國家通訊傳播委員會NCC-ISAC與教育部A-ISAC等。

我國政府的目的是希望結合政府與民間機構之力量，透過會員制度之互信關係，統一資安情報溝通格式與即時交換方式，建立資安會報所屬各分組與關鍵資安組織對資安資訊分析與分享之能力，達成資安早期應變與預警。

本次RSA大會的主題「分享．學習．安全—運用集體智慧」與我國政府推動ISAC政策的目的一致，顯示我國政府的資訊科技發展策略與方向早已與國際接軌，並符合未來發展趨勢。

目前金管會為強化與金融周邊單位資安資訊共享機制，以有效防範及預防類似資安事件發生，正評估規劃建立金融資安資訊分享與分析中心 (Financial Information Sharing and Analysis Center，簡稱F-ISAC)，初期將邀請各周邊單位加入試辦，再視推動成果再邀請各金融機構加入，待金管會完成規劃，相關機構應將盡力配合主管機關之政策，以共同加強金融產業資訊安全防護。