出國報告（出國類別：其他國際會議）

RSA Conference Asia Pacific & Japan 2014
出國報告

服務機關：行政院資通安全辦公室
姓名職稱：周智禾 諮議
派赴國家：新加坡
出國期間：103 年 7 月 20 日至 103 年 7 月 24 日
報告日期：103 年 10 月 21 日

摘　　要

RSA 會議主要係每年度美國、歐洲和亞洲於商業活動上重要的資訊安全活動之一，縱觀其歷史，RSA 會議一直吸引著世界上最好及最聰明的資安領域專才，並透過互動方式讓與會者學習到資安最重要的議題及趨勢，隨著資安領域重要性和影響力的持續增長，RSA 會議扮演著整合的角色，讓世界各地的資安專業人才能有更多機會可以相互交流及學習。

RSA 會議自 1991 年開始舉辦，迄今已 20 餘年，並作為一個論壇，讓密碼學專家收集及分享資安領域最新的知識，目前 RSA 會議及其他相關活動仍然由 RSA 負責統籌管理及相關企業的支持，並由資訊安全從業者及其它相關專家協助規劃會議議程及活動內容。

本(2014)年 RSA 會議訂於 7 月 21 至 23 日假新加坡濱海灣金沙酒店(Marina Bay Sands)召開亞太暨日本地區研討會，並邀請多位資安專家擔任大會 11 場次專題演講(Keynote)，會議分雲端及資料安全、網路犯罪及執法、行動安全、安全基礎設施、威脅與風險管理等分會場(Track)，並設有中日文分會場。

目　　錄

壹、會議介紹

一、會議名稱

2014 年 RSA 亞太暨日本地區研討會(RSA Conference Asia Pacific & Japan 2014)

二、會議時間

2014 年 7 月 20 至 2014 年 7 月 24 日

三、會議地點

新加坡濱海灣金沙酒店(Marina Bay Sands)

四、會議相關文件

會議相關資料請詳見網站(http://www.rsaconference.com/events/ap14)

貳、參加會議目的

RSA[註]會議係資訊安全產業最重要的會議之一，同時也是受到世界矚目的資安盛會，每年除固定於美國舊金山舉辦外，亦於歐洲及亞太等地區召開。資訊安全專家可透過此交流平臺發表最新的系統或軟體漏洞，或是提出資安防護方面的議題，全球各資安廠商亦可藉此機會，向與會者展示最新資安防禦措施。RSA 會議提供資訊安全專家在攻擊或防禦上不同的思考方向，瞭解目前最新的資安技術，作為攻擊或防禦的重要參考依據。

本次參加 RSA Conference Asia Pacific & Japan 2014，主要希望能從這些議題中瞭解最新資安威脅並掌握國際發展趨勢，除了提升本身對資安議題的認知外，亦期望藉由演講中所獲取的新知與技術，瞭解目前駭客最新的技術，增廣資訊安全上見聞，俾提供業務或決策方面上的協助。

註：RSA 為為目前世界上最廣泛使用的非對稱式加密演算法之一，其困難度係基於極大整數因數分解問題，在 1977 年由麻省理工學院的 3 位教授(Ron Rivest、Adi Shamir 及 Leonard Adleman)所提出，以他們 3 人姓氏開頭字母組成其名稱，並成立 RSA 公司提供資訊安全解決方案。

參、會議過程及重點議題

一、會議過程

RSA Conference Asia Pacific & Japan 2014 分為兩部分，第 1 天為教育訓練 SANS Digital Forensics & Incident Response Workshop (7 月 21 日)，後 2 天則會 RSA 正式會議(7 月 22-23 日)，本次出國行程主要參加前揭教育訓練及正式會議。

(一) SANS 數位鑑識與事故回應教育訓練

本場教育訓練由 Nick Klein 擔任主講者，同時他也是澳洲雪梨 Klein & Co. Computer Forensics 的主管(Director)，Nick 在資訊科技領域有超過 15 年的經驗，特別是在數位鑑識調查方面，並於實務上承接多起案件，包括商業訴訟、犯罪偵查、金融詐騙、電腦系統入侵等。課程內容主要透過分析微軟 Windows 作業系統相關內容以取得所需的數位證據，包括鍊結文件(link files)、跳轉列表(Jump lists)、shellbags、回收桶(Recycle bin)、網路歷史紀錄(Internet history)、預先擷取(Prefetch)、Document metadata、地理定位技術(Geolocation techniques)、USB 裝置等，第 1 天議程如表 1。

表 1：7 月 21 日(星期一)會議議程

時間	議程內容
7:30－17:30	Registration - Foyer - Level 5
9:00－17:00	Tutorial SANS Digital Forensics & Incident Response Workshop
14:00－17:00	Interactive / Play Innovation Sandbox (Most Innovative Company Contest)

(二) 2014 年 RSA 亞太暨日本地區研討會

為期 2 天的 RSA Conference Asia Pacific & Japan 2014，共安排了 11 場次的 Keynote 演講，議程分分雲端及資料安全、網路犯罪及執法、行動安全、安全基礎設施、威脅與風險管理等分會場(Track)，並設有中日文及廠商特別議題分會場，議程詳見表 2 及表 3。

表 2：7 月 22 日(星期二)會議議程

時間	議程內容
7:30 – 18:30	Registration – Foyer - Level 5
8:45 – 9:25	Keynotes United We Stand, Divided We Fall
9:25 – 9:45	Keynotes Get Real: Operationalizing an Intelligence Driven Security Program
9:45 – 10:05	Keynotes Cybercrime – Where Did We Go Wrong?
10:05 – 10:25	Keynotes The First Casualty of the Cyber Cold War
10:30 – 18:30	Expo Demo Theatre Presentations – Exhibition - Level 5
10:30 – 18:30	Expo Open – Exhibition - Level 5
10:30 – 11:00	Tea / Coffee Break – Exhibition - Level 5
11:00 – 11:45	Cybercrime and Law Enforcement IP and Telephony Crime Has Converged – Wake Up, Wise Up & Get Protected! Cloud and Data Security From Data to Wisdom: Big Lessons in Small Data Mobile Security Mobile Payment Services: Security Risks, Trends and Countermeasures Threats and Risk Management Brothers In Arms: How the Financial Sector Fought the Brobot Attacks Sponsor Special Topics Whose IP Is It Anyways: Tales of IP Reputation Failures Sessions in Japanese 企業が直面する「脅威の現実」と「セキュリティ対策の現実 - The 'Real Threats' We Face Today vs. The 'State of Reality' (Threats & Risk Management) Security Infrastructure APIs – The Next Hacker Target, or a Business and Security Opportunity?

11:45 – 13:00	Lunch – Exhibition - Level 5
13:00 – 13:45	**Sponsor Special Topics** Accelerate Your Security Operations With Machine Speed Responses to Cyber Attacks **Cybercrime and Law Enforcement** Project 2020 - Preparing Your Organization for Future Cyber Threats, Today **Security Infrastructure** Is Your Fridge Conspiring Against You? IoT Attacks and Embedded Defenses **Sessions in Mandarin** 解开安全的锁链：软件 定义安全的战略和实践 - Security Unchained - Thoughts and Practices around Software Defined Security (Cloud and Data Security) **Cloud and Data Security** Software Defined Perimeter: Securing the Cloud to the Internet of Things **Mobile Security** Practical Attacks Against MDM Solutions **Threats and Risk Management** Cyber Early Warning and the Commonality of Cyber Warfare and Electronic Warfare
14:05 – 14:50	**Security Infrastructure** Memory Forensics & Security Analytics: Detecting Unknown Malware **Threats and Risk Management** Application Security - The Invisible Onslaught Gets Worse **Mobile Security** Cyber-Espionage Using an Android Spyphone **Cloud and Data Security** Cloud Trust Redefined: Eight Essential Steps in a Strong Defense **Sponsor Special Topics** Using Big Data to Uncover Sophisticated Attacks, and Secure Your Organization **Cybercrime and Law Enforcement** Understanding and Defending Against the Modern DDoS Threat **Sessions in Mandarin** APIs - 下一个黑客目标，或是业务与安全的机

	会？（安全基础结构）- APIs – The Next Hacker Target, or a Business and Security Opportunity? (Security Infrastructure)
14:50 – 15:10	Tea / Coffee Break – Exhibition - Level 5
15:10 – 15:55	**Sponsor Special Topics** Out-Connect the Threats **Security Infrastructure** Continuous Delivery and Risk Assessment **Cloud and Data Security** The Impact of National Laws on International Cloud Deployments **Sessions in Japanese** IP 及び電話機能を利用した犯罪の多発－手口を知って賢い対策を！（サイバー犯罪と法執行機関）- IP and Telephony Crime Has Converged – Wake Up, Wise Up & Get Protected! (Cybercrime and Law Enforcement) **Threats and Risk Management** Small Data Analysis - Malware Under Magnifying Glasses **Mobile Security** Minimizing the Threat of Mobile Banking Cybercrime **Cybercrime and Law Enforcement** The Role of the ISACs in Critical Infrastructure Resilience
16:15 – 17:00	**Mobile Security** Split and Conquer: Don’t Put All Your Keys in One Basket **Security Infrastructure** Combat Sophisticate Threats – How Big Data and Open SOC Could Help **Sessions in Japanese** クラウド環境の信頼性の見直し：攻撃をしっかり防ぐための８つの基本ステップ－（クラウド及びデータセキュリティ）- Cloud Trust Redefined: Eight Essential Steps in a Strong Defense (Cloud and Data Security) **Cybercrime and Law Enforcement** Son of SpyEye – a Crimeware Soap Opera

	Threats and Risk Management Securing Secure Browsers Cloud and Data Security Whose Cloud Is It Anyway? Exploring Data Security, Ownership and Control
17:00－18:30	Welcome Reception － Expo

表 3：7 月 23 日(星期三)會議議程

時間	議程內容
7:30－17:00	Registration － Foyer - Level 5
8:45－9:30	Keynotes The Second Machine Age
9:30－9:50	Keynotes The History of Internet Failures and How We Might Break the Cycle
9:50－10:10	Keynotes The Analytics Enabled SOC - Best Practices for Improving Incident Response and Breach Investigation
10:10－10:30	Keynotes New Approaches for Defending IT in Today’s Threat Landscape
10:15－17:00	Expo Demo Theatre Presentations － Exhibition - Level 5
10:15－17:00	Expo Open － Exhibition - Level 5
10:30－10:50	Tea / Coffee Break － Exhibition - Level 5
10:50－11:35	Cybercrime and Law Enforcement Current and Emerging Trends Within the Cybercrime Ecosystem Sessions in Japanese あなたの冷蔵庫があなたを陥れようとしている？ IoT 攻撃と セキュリティソフトの埋め込み－（セキュリティインフラストラクチャー）- Is Your Fridge Conspiring Against You? IoT Attacks and Embedded Defenses (Security Infrastructure) Mobile Security Leave the App Alone! - Attack and Defense of Android App Hijack Threats and Risk Management A Strategic Approach to Threat

	Intelligence **Security Infrastructure** Cisco Unified Security Metrics: Measuring Your Organization's Security Health **Sponsor Special Topics** Revenge of the Full Proxy **Cloud and Data Security** The Perimeter is Dead! Birth of the Elastic Network
11:55 – 12:40	**Cybercrime and Law Enforcement** Cybercrime Layers – How Cybercriminals Defeat Security Measures **Sessions in Japanese** 「アンドロイド端末用スパイフォンを使ったサイバースパイ」(モバイルセキュリティ) - Cyber-Espionage Using an Android Spyphone (Mobile Security) **Mobile Security** Mobile Security Attacks: A Glimpse From the Trenches **Cloud and Data Security** How to Hadoop Without the Worry: Protecting Big Data at Scale **Sponsor Special Topics** Infrastructure Complexity – a Business Puzzle Worth Solving **Threats and Risk Management** Learning Malware Languages: Fun with Dick and Jane's Malware **Security Infrastructure** EAS-SEC Project: Securing Enterprise Business Applications
12:40 – 13:40	Lunch – Exhibition - Level 5
13:40 – 14:25	**Threats and Risk Management** One Failure Leads to Another: Developing Leading Indicators for Security Threats and Risks **Mobile Security** Mobile Devices Security: Evolving Threat Profile of Mobile Networks **Security Infrastructure** Is the Security Industry Ready for On

	Appliance SSL Decryption Features? Sessions in Mandarin 离我的 App 远点儿！ - Android 应用劫持的攻与防 Cybercrime and Law Enforcement DDoS Past, Present, and Future Sponsor Special Topics Next Generation Enterprise Security Cloud and Data Security Building and Breaking Privacy Barriers
14:25－14:45	Tea / Coffee Break － Exhibition - Level 5
14:45－15:30	Sessions in Mandarin 了解并抵御现代 DDoS 的威胁(网络犯罪与执法) - Understanding and Defending Against the Modern DDoS Threat (Cybercrime and Law Enforcement) Security Infrastructure EITC Lessons Learned: Building Our Internal Security Intelligence Capability Threats and Risk Management Will Your Company Be to Intellectual Property What Mt. Gox Was to Bitcoin? Mobile Security Third Party Components in Applications: Understanding Application Security Cloud and Data Security Restoring Trust After a Data Breach Cybercrime and Law Enforcement IP Challenges in Asia: Keeping Your Data Safe from Malware & Other Threats Sponsor Special Topics Supply Chain: The Exposed Flank
15:45－16:05	Keynotes Securely Enable the Open Enterprise
16:05－16:25	Keynotes Combatting Cyber Attacks Through Advanced Analytics & Intelligence
16:25－17:30	Keynotes The Fall of Lance Armstrong and the Importance of the Truth

二、重點議題

(一)SANS: Digital Forensics & Incident Response Workshop

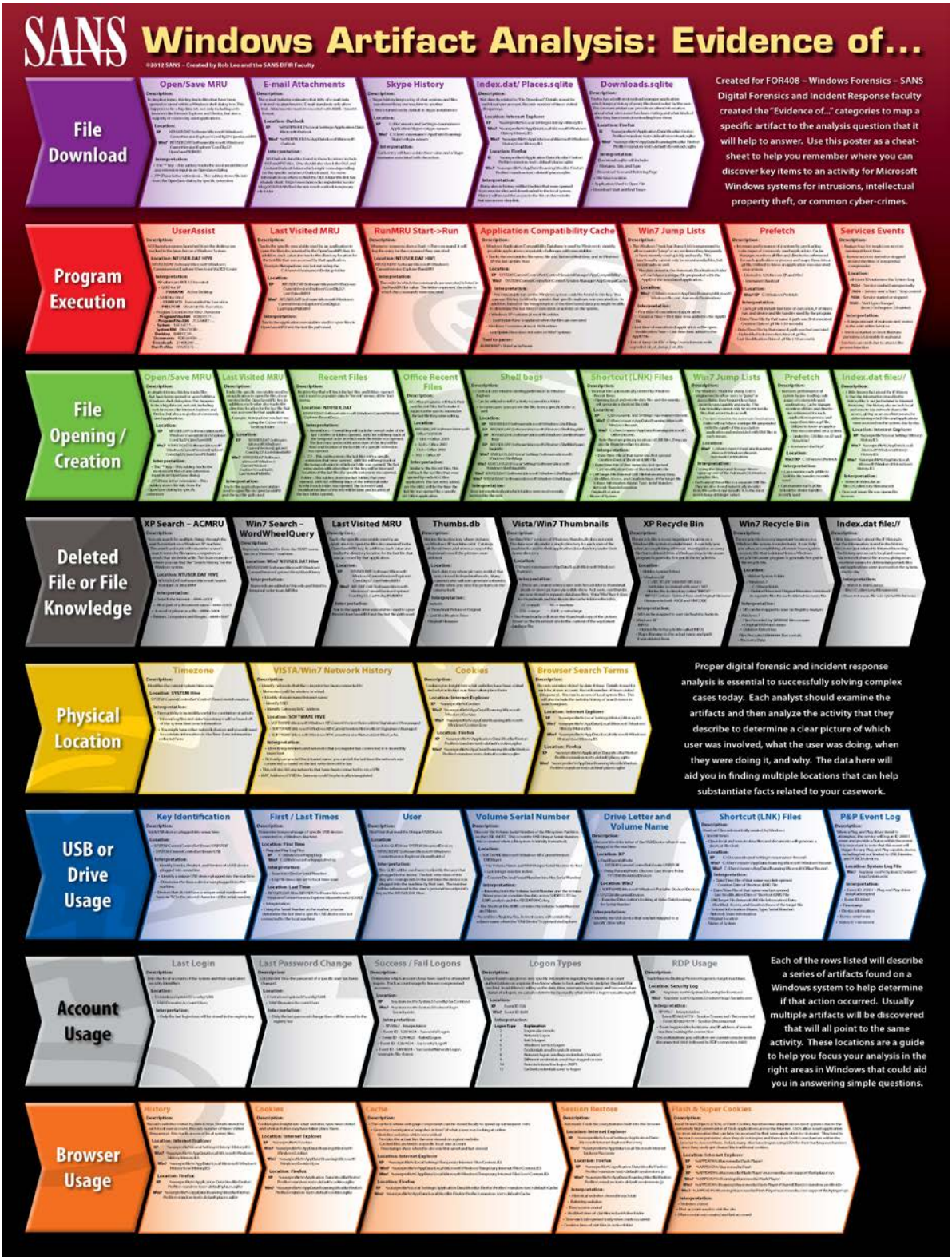

圖 1：Windows 作業系統數位鑑識項目

SANS 數位鑑識與事故回應教育訓練課程內容主要透過分析微軟 Windows 作業系統相關內容以取得所需的數位證據，包括下列各項：

1、Recycle Bin

使用者在電腦中刪除檔案時，檔案會被放進 Recycle Bin(Windows 95/98 稱為 RECYCLED，Windows 2000/NT/XP/2003 稱為 RECYCLER，Windows Vista/7/8 則稱為 $Recycle.bin)，刪除檔案的名稱及時間會被記錄在隱藏檔(INFO2 或是$I、$R 檔案)中，此部分說明如何使用相關工具(FTK 或 rifiuti)找出使用者刪除了哪些檔案。

2、Shortcut / Link Files

當我們開啟本機端或遠端的資料檔案或文件時，Windows 將會自動產生副檔名為.lnk 的 Shortcut 檔案，其內容包括檔案的 MAC 時間、標籤(Volume)資訊、網路分享資訊、原始位置及系統名稱等，我們可以使用免費工具(lp.exe)來分析多個.lnk 檔案，該工具同時也支援從原始檔案(如 dd image)直接剖析.lnk 檔案，讓我們可以得知使用者開啟過什麼檔案，同時我們可能從這些檔案及其位置找出部分所需資訊。

3、Jump Lists

Windows 7 工具列(task bar)允許使用者跳轉(jump)或存取(access)他們時常或最近曾使用過的檔案，使用者透過應用程式開啟過什麼檔案，Windows 的跳轉列表(Jump lists)由 Destination(可以是檔案、資料夾、網站等)和 Task(實際上為 lnk)所組成，我們可以利用 jmp.exe 工具分析 Custom 及 Automatic Destination 檔案，並將結果輸出為 csv 檔，以瞭解使用者透過應用程式開啟過什麼檔案。

4、Recent Docs

在 Windows 的 Registry 裡，可以很容易找到 RecentDocs 項目，並使用 Access Data’s Registry Viewer 剖析其內容，以瞭解使用者開啟過什麼檔案以及何時開啟。

5、Shellbags

Windows 使用 Shellbag 儲存使用者對 Windows Explorer 的目錄顯示偏好設定，包括顯示(圖示、詳細資料及列表等)及排序方式，而在 Windows Registry 中，BagMRU 則記錄使用者最近瀏覽過哪些目錄的資訊，包括本機端(ShellNoRoam)及遠端(BagMRU)的目錄，我們可以使用者 sbag.exe 工具瞭解使用者存取過本機端、遠端及移除式裝置中的哪些目

錄。

6、USB Devices

USB 資訊儲存在 Windows Registry(System.dat、Software.dat 及 Ntuser.dat)、Setupapi.log(Plug and Play Log)及事件紀錄(Event Logs)中，其資訊包括廠商、製造者、版本、序號(Unique Serial Number)，甚至是使用者活動行為紀錄，如最近一次使用的磁碟機代號、標籤名稱、使用者名稱、第 1 次使用時間、最近 1 次開機後的第 1 次使用時間、最後使用時間，我們可以使用 usbHistory.exe 工具找出曾連接到該電腦的 USB 裝置相關資訊。

7、Document Metadata

說明如何利用 Metadata 分析文件的內容，主要利用 Exif Parsing 工具，分析 Microsoft Office 相關檔案及 PDF 檔，如找出文件的作者(Author)、建立日期(Creation Date)、建立者(Creator)、修改日期(Modification Date)及標題(Title)等資訊。

8、Network Connections

列出電腦中所有的網路介面卡，以及網路使用歷史紀錄，可得知使用者曾使用哪個網路上網，此外，可以進一步使用 MAC 或 SSID 搭配 http://wigle.net 網站，找出網路的實際地理位置。

9、E-mail Geolocation

從電子郵件的標頭(Headers)，除了寄件者所聲明的 To、CC、BCC、Subject、Date 等欄位外，可藉由解析 Message-ID、Received、IP(或 X-IP)及 X-Mailer 等 4 個欄位，找出電子郵件從哪裡被寄出的。

10、Thumbnail Forensics

在 Windows XP 中，圖片檔所在目錄會有一個名為 thumbs.db 的隱藏檔，用以記錄圖片最後修改時間及原始檔名等資訊，即使圖片檔被刪除；而在 Windows 7/8 中，則是為 Thumbcache_xx.db，其中可分為 4 種大小(Small、Medium、Large 及 XL)、日期/時間不會儲存，我們可以使用 Thumbcache Parser/Recovery 或 FTK 工具找出被使用者刪除的圖片檔。

11、Deleted Registry Keys

可以使用 YARU(Yet Another Registry Utility)工具瞭解使用者是否曾試圖刪除

Registry keys 以清除軌跡。

12、Prefetch

Windows XP/Vista/7/8 為了減少應用程式的啟動時間以及作業系統開機時間，使用一種稱為 Prefetch(預先擷取)的機制，當使用者執行一個 X 應用程式時，會建立一個 X.pf 的檔案，記錄應用程式載入到記憶體中的索引排序，以及有關它們被載入的順序資訊，我們可以使用 pf.exe 工具知道使用者是否曾在電腦中執行過清除或可疑的程式。

(二) Keynotes

1、United We Stand, Divided We Fall

- ✧ 主講者：Arthur W. Coviello
- ✧ 職稱/公司：Executive Vice President, EMC Corporation, Executive Chairman, RSA
- ✧ 內容：雖然有許多因素導致數位領域越來越複雜，然而，似乎令我們最掙扎的因素是我們相互依賴關係以及我們國家，企業和個人間的縱橫交錯關係，如果我們想要安全，我們政治及企業的領導人必須採取適當政策和技術，並取得兩者間的平衡點，而不是避免這種相互依存關係。

2、Get Real: Operationalizing an Intelligence Driven Security Program

- ✧ 主講者：Amit Yoran
- ✧ 職稱/公司：SVP, Products, RSA
- ✧ 內容：組織想要充分利用雲端，行動和其它數位技術取得其競爭優勢，同時，這些技術也代表對手的攻擊能量及的威脅，雖然毫無疑問地，智能驅動型安全(Intelligence Driven Security)是未來的方向，但是很少人提出如何實現這個願景，現在應該是談談智能驅動型安全如何面對現實的時候了。

3、Cybercrime – Where Did We Go Wrong?

- ✧ 主講者：Steve Lam
- ✧ 職稱/公司：Partner, Ernst & Young Advisory
- ✧ 內容：儘管現今已有更好的技術，同時各界也在資安經費及網路犯罪議題上增加

許多努力，然而，我們卻仍然看到入侵事件發生以前所未有的速度逐漸增加。在這個會議上，我們認為組織所採取的網絡安全管理辦法，似乎從一開始就註定為什麼他們會失敗的原因。

4、The First Casualty of the Cyber Cold War

- ✧ 主講者：Kevin Kennedy
- ✧ 職稱/公司：Senior Director of Product Management for Security Business Unit, Juniper Networks
- ✧ 內容：我們的隱私正受到侵犯，我們的智慧財產權正被竊取，而這些攻擊是無限制的，我們現在正在目睹一個網絡冷戰的開始，將對我們造成重大傷亡。

5、The Second Machine Age

- ✧ 主講者：Andrew McAfee
- ✧ 職稱/公司：Principal Research Scientist, Center for Digital Business, MIT Sloan School of Management and Fellow, Harvard Law School, Berkman Center for Internet and Society
- ✧ 內容：我們生活在輝煌科技的時代，汽車可以自行驅動；危險且強大的超級計算機;便宜具彈性且好用的機器人;3D 列印機器。他們正在把我們帶入了一個 second machine 時代，為工業革命以來最偉大的時代，本次演講，McAfee 博士將討論我們以科幻小說般的科技技術正在創造的世界，其所帶來的巨大潛力及棘手挑戰。

6、The Analytics Enabled SOC - Best Practices for Improving Incident Response and Breach Investigation

- ✧ 主講者：Haiyan Song
- ✧ 職稱/公司：Vice President of Security Markets, Splunk
- ✧ 內容：對抗現代資安威脅需要一種新的方法，參加本次會議可以看看 SIEM 技術正在如何改變，企業如何提供強大和動態分析功能給每個 SOC 成員，以及全球性威脅的團隊如何對抗現代網路攻擊，瞭解如何有效地利用企業級的數據資料管理現在的企業風險，這包括已知及未知的威脅、APT、內部威脅和欺詐等。

7、The History of Internet Failures and How We Might Break the Cycle

- ✧ 主講者：Wolfgang Kandek

- ✧ 職稱/公司：Chief Technical Officer, Qualys
- ✧ 內容：在過去的幾十年來，我們已經看到許多引起網路問題的重大事件，包括蠕蟲、病毒以及最近的 Heartbleed，每一次我們齊心協力來解決這個問題，但卻沒有深入去瞭解我們應如何擺脫這種不斷重複發生的問題(break and fix)，本次演講主要是要讓大家一窺網路發生問題的歷史記錄，並討論我們如何可以做得更好。

8、New Approaches for Defending IT in Today’s Threat Landscape

- ✧ 主講者：Bret Hartman
- ✧ 職稱/公司：Vice President and Chief Technology Officer, Security Business Group, Cisco Systems, Inc.
- ✧ 內容：為了對抗網路攻擊，IT 專業人員必須配合現代網絡環境的複雜性和部署無處不在的防禦，以保護他們的基礎設施，現在先進的且針對性的攻擊在其頻率、嚴重程度及複雜性均已大幅成長，惡意軟體為攻擊者所選擇的武器，並可以以多種形式呈現，行動化和雲端運算應用在新的攻擊，讓我們無法預期。要對抗這些複雜的威脅，資安長(CISOs)及資訊長(CIOs)必須以攻擊者的角度思考才能保護自己，而要實現這一點的關鍵處，首先須瞭解現代威脅環境，以及如何提高威脅防禦的功效，主講者Bret 提供當今不斷變化的威脅環境的概況，並指出資安長(CISOs)及資訊長(CIOs)在攻擊發生的前中後期，如何保護自己的環境。

9、Securely Enable the Open Enterprise

- ✧ 主講者：Vic Mankotia
- ✧ 職稱/公司：Vice President, Solution Sales, Asia Pacific & Japan, CA
- ✧ 內容：隨著企業以其業務主題的中心開始相互合作，帶來新的世界商業蓬勃發展。安全性問題一直被視為進入門檻，隨著雲端服務、社交媒體和超連結作為民眾間溝通的核心技術，企業必須需要融入合作夥伴的生態系統，行動化、雲端運算和社交媒體所構成的三維世界是應用程序，而應用程序經濟是我們開放式企業的一部分，開放式企業需要安全性才能得以順利推動其業務。

10、Combatting Cyber Attacks Through Advanced Analytics & Intelligence

- ✧ 主講者：Bryan Sartin
- ✧ 職稱/公司：Managing Director, Verizon

- ✧ 內容：針對式攻擊和先進惡意軟體不斷地被創造，即使是最好的安全團隊站可能也擋不了這種網路威脅，本次演講採用數據驅動的方式看看這個問題的科學議題，並談到現實世界的技術如何推動事件偵測的發展，瞭解如何去進攻以進一步得到威脅殺傷鏈。

11、The Fall of Lance Armstrong and the Importance of the Truth

- ✧ 主講者： David Walsh
- ✧ 職稱/公司：Journalist and Chief Sports Writer, The Sunday Times
- ✧ 內容：在 1993 年 7 月，阿姆斯壯在環法自行車賽上首次亮相，在危及生命癌症後的倖存，阿姆斯壯又贏得了環法自行車賽，主講者(大衛·沃爾許)是少數幾個公開質疑阿姆斯壯的勝利真實性的記者之一，沃爾許花費了許多年的時間調查阿姆斯壯，最終取得了真相，阿姆斯壯欺騙了所有他 7 個環法自行車賽冠軍，他被剝奪了冠軍，並終身禁止參加任何體育比賽，沃爾許把這個故事寫成一本暢銷書(Seven Deadly Sins)，同時也被改編成電影。

(三) Tracks

1、Mobile Payment Services: Security Risks, Trends and Countermeasures

行動支付已漸漸取代傳統付款方式成為新的交易模式，一般行動支付是在使用者的行動裝置上安裝電子錢包，近年來，越來越多的方式被提出，包括 NFC Apps、Client Apps(Android、iOS、BB、Windows 等)、Browser based Apps(HTML5、CSS 等)、VAS Apps、QR Code、Telematics Apps、MicroATM/ATM/POS Apps、USSD Based Apps，其所面臨的挑戰如行動支持傳輸政策(Transfer Policy)的標準化、服務提供者和銀行的相依關係、行動支付應用程式和裝置的相容性、行動支付服務安全性、政府政策等。

行動支付服務安全性議題包括詐騙行為、使用弱密碼演算法、應用程式伺服器的威脅、行動支付應用程式資料庫威脅、SIM 卡應用程式攻擊、行動支付應用程式自身安全，對企業所造成的影響包括財務損失、使用者敏感資料外洩等。另，行動應用程式(Mobile App)所面臨的風險包括程式碼隱匿、不安全的本機裝置資料庫、不安全的應用程式權限許可等，同時，在通訊的過程中，也有可能面臨重送攻擊(Replay Attack)。

為了提高行動支付的安全性，安全的軟體開發生命週期(Secure SDLC)日漸重要，其涉及的層面包括傳輸過程、行動裝置上的資料儲存、適當的會議管理(Session Management)、輸出入內容的驗證(特別要過濾一些特殊字元)、落實有效的認驗證機制、安全的網頁服務存取、確保行動裝置遺失或遭竊後之安全性問題。

2、API – 是下一个黑客攻击目标， 还是业务和安全机会？

為什麼我們要談到 API 這個議題，舉一個實務上的例子，僅 Amazon Web Services EC2 就有 148 個 API，開發人員公開提供的 API 亦多達 10,500 個，各個平臺每天 API 被使用多達數十億次，Expedia 的聯盟網路每年僅通過 API 就處理價值超過 20 億美元的交易，然而在 2013 年 12 月 Snapchat API 遭非法入侵，造成大量的電話號碼遭竊，被新增多個假帳戶，並成為垃圾郵件平臺，大家開始注意到 API 安全的重要性。

API 所面臨的威脅包括假冒身份、重送攻擊、中間人攻擊、權限控管問題、注入攻擊、密鑰遭竊等，我們可以將 API 安全分成 2 個層面來看，一個是 API 與後端服務、應用伺服器等連接所可能面臨的洩露議題，另一個則是 API 與前端(行動或 Web 應用程式)溝通的消耗議題，API 的管理解決方案必須解決 API 的不同利益關係者和使用者的安全問題，即包括前面所提到的 2 個議題，我們可以使用雙向 TLS、身份認證、登錄和審核等技術達成。

3、The Role of the ISACs in Critical Infrastructure Resilience

資訊分享與分析中心(ISAC)是由各個不同領域的個體所共同建立組成的資訊分享平臺，能夠快速分析處理所接獲之資訊，並與各界共同分享關鍵資訊，特別是涉及安全上的議題，目前美國已設立的 ISAC 領域包括 Communications、Defense Industrial Base、Electricity、Emergency Management & Response、Financial Services、Information Technology、Maritime、Multi-State、National Health、Oil and Natural Gas、Over the Road & Motor Coach、Public Transit、Real Estate、Research and Education、Supply Chain、Surface Transportation、Water 等數十種，其他以及未來將建立的 ISAC 包括 Automotive、Aviation、Food & Ag、Nuclear、Chemical、Critical Manufacturing。

以金融 ISAC(FS-ISAC)為例，其於 1999 年由一個非營利的私有部門所成立，主要處

理實體與網路上的犯罪及詐騙等活動，每月可處理數千筆威脅資訊，在 2004 年約有 68 個成員，至 2014 年已有超過 5,000 個成員，其中 DHS、FBI、USSS 及 NYPD 均參與其運作，提供相關資訊來源；其分享的資訊依 Traffic Light Protocol(TLP)亦分有不同等級，Red 表示不與任何人分享，Amber 表示僅與 FS-ISAC 成員分享，Green 表示僅與 FS-ISAC 成員及夥伴分享，White 表示公開可分享的資訊，且透過安全之管道讓各界提供網路事件、實體事件或上傳文件，再由相關成員及時進行初步分析及提出建議，並由 SOC 完成整體分析並向相關成員提供警示訊息。

National Council of ISACs 成立於 2003 年，為一自發性的組織，每月皆定期開會，並致力於促進不同的部門間如何發展信任工作關係，如增加各個部門的參與程度、建立跨部門的資訊分享機制、辦理相關攻防演練等；另由 National Cybersecurity and Communications Integration Center(NCCIC)負責公私部門間的協同合作。

4、Current and Emerging Trends Within the Cybercrime Ecosystem

本議題主要著重於 Point-of-Sale(PoS)惡意程式及網路犯罪行動化威脅(Cybercrime Mobile Threats)，PoS 泛指任何處理付款機制的裝置，大多數的 PoS 系統為一般且版本較舊的作業系統，利用相關技術或工具，如 RegEX、RAM Scrapping、Luhn Algorithm、TOR，有可能對 PoS 系統造成威脅；至於感染的途徑可分為下咧幾種方式，網路公開的服務(如弱點、身份驗證問題、預設密碼、未設定密碼)、實體存取、供應鍊感染、社交工程、滲透合作關係之網絡；如何減低是類攻擊威脅，建議可降低攻擊被利用面向(網路存取、預設密碼、安全性更新)、實作 Chip and PIN(EMV)、應用點對點加密方式(P2PE)、使用裝置和網路監控機制、遵循 PCI-DSS 要求等。

有關網路犯罪行動化威脅方面，近期，行動裝置所面臨的威脅以大幅速度成長，可將行動裝置上惡意程式偵測的方式分為 2 種，一種是動態分析，如瞭解安裝應用程式時開放哪些權限，以及分析 SMS/Network/GPS/NFC 等元件的活動；另一種則是靜態分析，主要查看 APK 檔案的原始資料，對 APK 檔進行反組譯。而行動裝置感染惡意程式的途徑則包括下載安裝不信任的 apps、瀏覽網頁時預載相關元件、透過個人電腦感染、社交工程方式等。如何有效解決前揭議題，在下載安裝應用程式前，應確實檢查各項權限要求，確認開啟「Verify apps」選項，當需要時才開啟 USB debugging mode，不安裝來路不明

的應用程式，定期備份行動裝置資料。

5、了解并防范 Modern DDoS 威胁

有關面臨 DDoS 的威脅，根據 corer 的調查，40%的企業沒有準備，23%的受訪者沒有相關計畫，26%則依賴他們的 ISP 業者，甚至高達 50%從未測過他們 DDoS 的防禦功能。研究人員發現攻擊者發起 DDoS 攻擊的方式在增加，攻擊者逐漸瞭解 DDoS 檢測和防禦的方式，而且不斷的在開發繞過現有防禦機制的新方法。另外，根據 SANS Institute 所作的調查，DDoS 可分為 5 類：網路級別、反射、出站、應用層以及精心設計的網路封包，其防禦方式分別對應至 IP 威脅級別評估、全狀態流量偵測、雙向淹沒檢測、行為分析及協定分析，近年來發生多起重大的 DDoS 攻擊，均使用不同的攻擊手法，甚至混合多種手法，讓機關組織越來越難防禦。特別要注意 Layer 7 的應用層攻擊，攻擊者會不斷嘗試存取網路或其所提供的功能，如主頁、偽裝登入、忘記密碼、隨機關鍵字檢索等，讓應用伺服器疲於回應。為有效解決各類 DDoS 攻擊問題，我們應該僅允許期望的流量，評估流量的數量，實施流量修改，分析流量的完整性，提高對所有不需要的流量之可見性。

肆、心得建議

近年來，本院(資通安全)辦公室積極推動多項資安強化機制，如修正「國家資通安全通報應變作業綱要」，要求各級政府機關(構)無論自建或委外資安監控(Security Operation Center, SOC)服務，應配合建立監控情蒐回傳機制，定期回傳予技術服務中心，以建置二線監控機制；為強化政府網際服務網(GSN)骨幹資安，規劃導出並過濾GSN骨幹相關資訊後，進行相關分析作業；為加強重大資安事件事中緊急應變能力，亦積極研擬政府機關資安紀錄保存機制，上述各項工作皆須及時處理及分析大量資訊，爰亟需研究並規劃鉅量資料(Big Data)分析處理系統架構，包括資料傳輸、接收、處理、分析及儲存等技術。本次參加RSA Conference Asia Pacific & Japan 2014，在「Cloud and Data Security」中有幾篇報告均談及鉅量資料分析，可作為後續鉅量資料分析處理相關研究之參據。

資安相關法律亦為本次研討會(Cybercrime and Law Enforcement Cybercrime)的重點之一，依「國家資通訊安全發展方案」(102年至105年)之行動方案1.2.1，本辦公室已初步完成我國資安相關法規之盤點，相關法律與規範主要分為「網路犯罪」、「通訊保障」、「身分認證」、「資料保護」、「資訊公開與機密保護」及「資安治理」等6類；目前刻正參酌國際先進國家立法原則，並考量我國社經環境與法規制度等，研議「資通安全基本法(草案)」中，將從強化國家資安政策、健全資安防護體系、落實資安通報應變、分享多元資安情報、擴大資安人才培育、加強國際資安交流、奠基資安技術能量等面向，以完善我國資通安全發展環境，促進我國整體資通安全。

另外，有關本次研討會部分作者將重點放在行動安全及分散式阻斷服務(DDoS)攻擊，佔了整個會議議程相當高的比例，足見是類議題為現階段國際間所面臨的共同問題，研擬相關的資安技術及標準規範已是刻不容緩的議題。經查，我國目前已對行動安全及DDoS攻擊應變機制訂有相關的參考指引或手冊，然面對資安威脅日新月異不斷演進，必須與時俱進，參考國際目前最新趨勢，據以檢討修正相關規範，此亦為本辦公室近期的工作重點。

伍、會議照片

圖 2：會議地點(Marina Bay Sands)

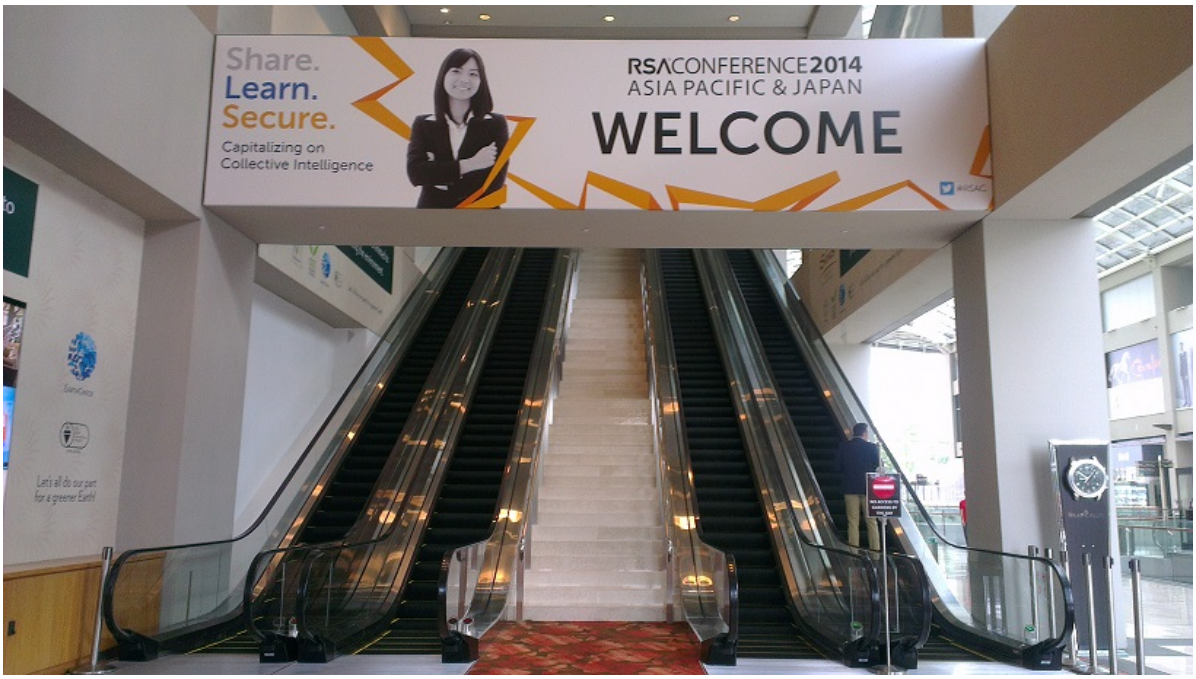

圖 3：會議入口處(Sands Expo and Convention Center)

圖 4：會議 Check-in 處

圖 5：SANS: Digital Forensics & Incident Response Workshop - 會議地點

圖 6：SANS: Digital Forensics & Incident Response Workshop - 會議實況

圖 7：RSA Conference Asia Pacific & Japan 2014 – Keynote 現場

圖 8：RSA Conference Asia Pacific & Japan 2014 – Keynote 實況

圖 9：廠商展覽區(Exhibition)-1

圖 10：廠商展覽區(Exhibition)-2

圖 11：RSA Conference Asia Pacific & Japan 2014 －會議現場

圖 12：RSA Conference Asia Pacific & Japan 2014 －一般 Track

圖 13：RSA Conference Asia Pacific & Japan 2014 －中文 Track