Y 五財團法人台灣網路資訊中心因公出國人員報告書 109 年 3 月 16 日

報告人 姓　名	林志鴻、曲承則	服務單位及 職稱	組長、工程師
出國期間	2 月 22 日-2 月 29 日	出國地點	舊金山
出國事由	參加 RSA2020 會議		

報告書內容包含：
一、 出國目的
二、 會議行程
三、 考察、訪問心得
四、 建議意見
五、 會議議程

授　權 聲 明 欄	本出國報告書同意貴中心有權重製發行供相關研發目的之公開利用。 授權人： 林志鴻(簽章) 曲承則(簽章)

註二、請於授權聲明欄簽章，授權本中心重製發行公開利用。
附一、請以「A4」大小紙張，橫式編排。出國人員有數人者，依會議類別或考察項目，彙整提出報告。

一. 出國目的:

參加 RSA Conference USA 2020 會議

二. 會議行程:

詳如會議網站 https://www.rsaconference.com/usa

議程 https://www.rsaconference.com/usa/agenda

RSA 網站 https://www.rsaconference.com/

參與會議的行程安排如下表列:

日期	時間	議程
109/02/22(六)	19:50	桃園機場出發(BR18)
	14:50	抵達舊金山國際機場
109/02/23(日)	08:30 - 17:00	Registration
109/02/24(一)	08:30 - 17:00	RSAC Seminars
109/02/25(二)	08:00 - 17:30	RSAC Seminars
	18:00 - 20:00	Non-Profits On The Loose
109/02/26(三)	08:00 - 12:00	RSAC Seminars
	13:00 - 16:00	拜訪 Synopsis
109/02/27(四)	08:00 - 17:30	RSAC Seminars

109/02/28(五)	08:00 - 11:45	RSAC Seminars
109/02/29(六)	109/02/29(六) 15:45	舊金山國際機場出發 (BR27)
	109/03/01(日) 20:15	抵達桃園機場

三. 考察，訪問心得

A. 前言

RSA 會議為全球最大規模資安會議之一，由美國資安公司 RSA 舉辦近 30 年，每年平均吸引約 45,000 人參加。

本次會議為 RSAC 第 29 次會議，於 2020 年 2 月 22 日(六)至 2020 年 28 日(五)在美國舊金山招開，總計為期七天的會議。本次參與會議人數高達 36,000 人次。具近 30 場 Keynotes，超過 500 場次會議、700 位講者及 650 間廠商參展。

RSAC 會議可分成五大類型: 資安議題演講，特定資安議題探討，資安專家經驗分享，贊助商演講，資安教程以及資安交流與人脈拓展。其主題共分為以下 24 大項目: 分析、情資與應變 (Analytics, Inteeligence & Response)，反詐騙 (Anti-Fraud)、加密貨幣&區塊鍊 (Applied Crypto & Blockchain)、資安商業創新 (Business)、雲端安全&虛擬化 (Cloud Security & Virtualization)、加密 (Cryptography)、資安與商務威脅趨勢 (C-Suit View)、資安開發

與應用 (Devsecops & Application Security)、駭客&威脅 (Hackers & Threat)、人為因素 (Human Element)、企業與顧客身分控管 (Identity)、法律面向 (Law)、機器學習與人工智慧 (Machine Learning & Artificial Intelligence)、移動設備與 IoT 安全性 (Mobile & IoT Security)、開源工具 (Open Source Tools)、政策與法治 (Policy & Government)、隱私 (Privacy)、產品安全 (Product Security)、專業成長與人員管理 (Professional Development & Personnel Management)、資料保護 & 供應鏈生態 (Protecting Data & The Supply Chain Ecosystem)、危險評估與法治 (Risk Management & Governance)、安全策略與架構 (Security Strategy & Architecture)、以及科技基礎設施與運作 (Technology Infrastructure & Operation)。提供與會者透過多元參與，掌握最新的資安發展、技術與趨勢。

本中心參加此次會議的主要目的為促進 TWNIC 之 TWCERT/CC (台灣網路危機處理暨協調中心) 的情資分享、資安事件分析與通報業務並掌握資安威脅趨勢，因此主要參與及了解各資安領域現況與威脅發展趨勢相關議程，包括勒索軟體、網路釣魚、資料隱私保護、威脅預防與規劃、惡意文件興起趨勢、惡意程式、社群媒體駭客偵防、事件應變分析與自動化、瀏覽器資料洩漏、漏洞

揭露與協調。此外 TWNIC 亦藉本次會議，與其他資安公司、情資分享單位進行交流，拓展未來潛在的情資分享來源與合作夥伴。

所有會議主題及議程皆可於 RSA Agenda 找到完整列表與細節。

Full Agenda:

https://www.rsaconference.com/usa/agenda/full-agenda?location=USA&year=2020

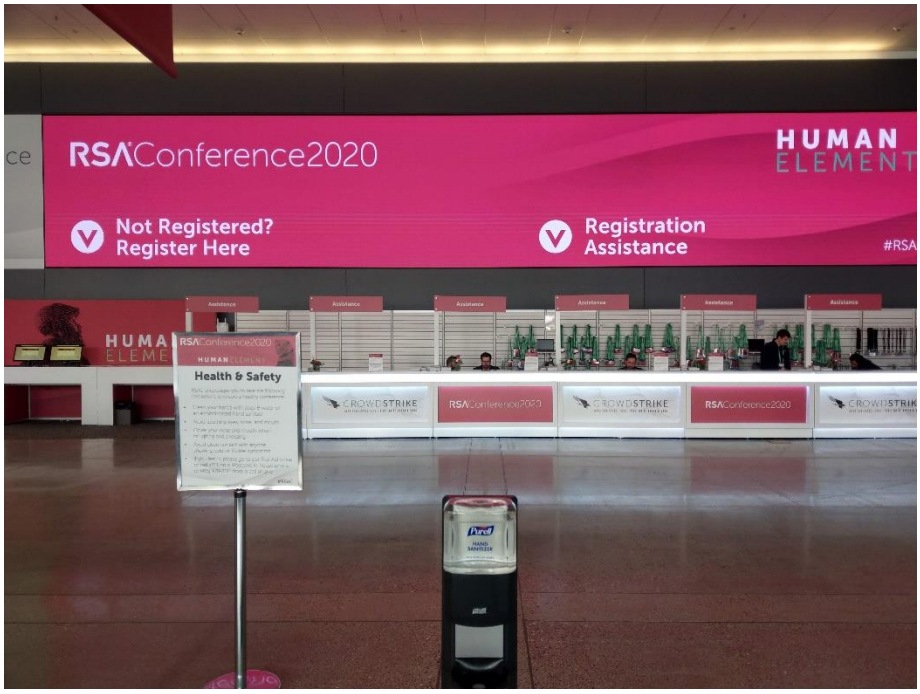

圖 1: RSA 2020 大會報到處

圖 2: TWNIC 曲承則工程師於 RSA 2020 USA 報到

圖 3: RSA 2020 Keynote 會場

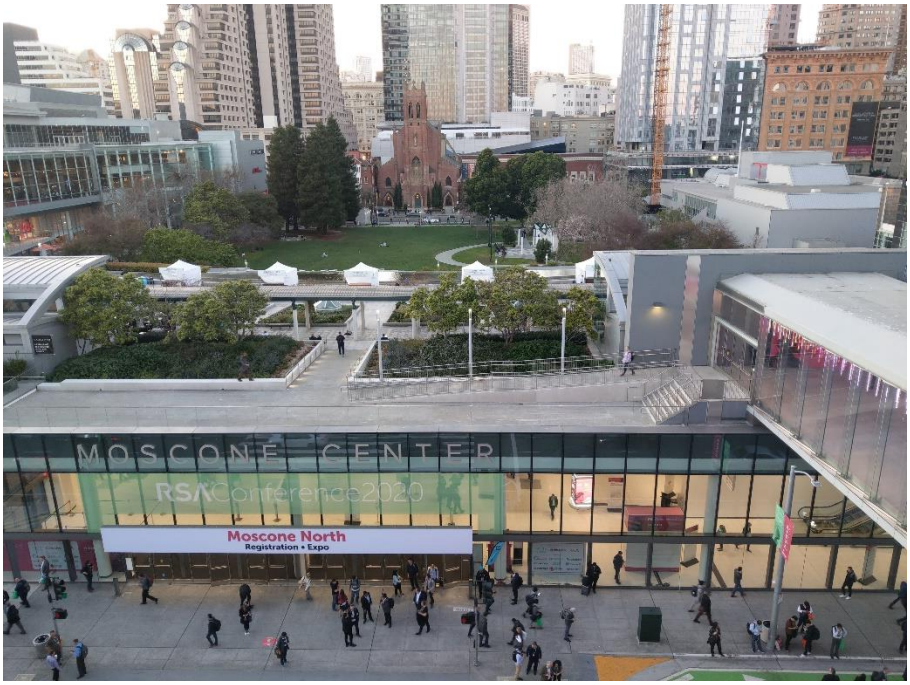

圖 3: RSA 2020 北會場

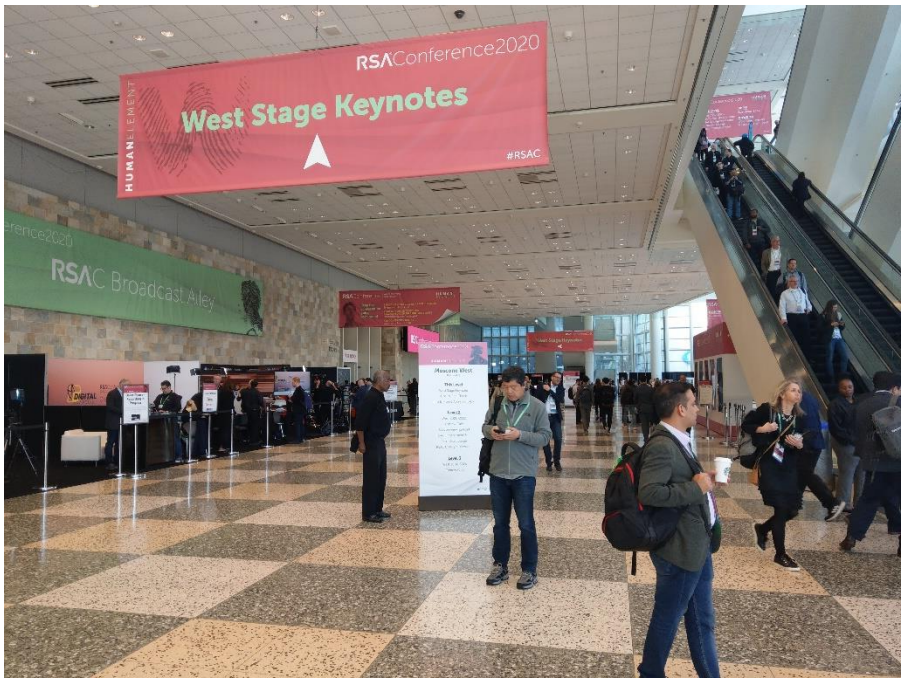

圖 4: RSA 2020 西會場

圖 5: RSA 展場會場

B. 參與主題與摘要

本次會議中主要參與的各項會議主要議題之觀察與建議，分述如下：

1. Lessons from America's two largest cities on preparing for cyber attack

   此演講為 LA 資訊安全長與 NYPD 中尉根據美國最大的兩個都市(紐約與 LA)之資安防護能量與過去資安事件經驗進行分享。其中提及包括 911 恐攻的資安處理經驗以及預計今年(2019 年) 11 月總統大選的資安預防與考量。為了提升資安防護能量與人材培育，美國長期投入許多人力與資金於建設交流平台，提供各年齡層與各技

術能力之資訊安全人員之聯結與交流，進而成熟化美國的資安生態系統。

Reference:

https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/17617/2020_USA20_SEM-M03A_01_Lessons-from-Americas-Two-Largest-Cities-on-Preparing-for-Cyberattack.pdf

2. Ransomware Spread Through Various Distribution Methods from 2018 to 2019

此演講針對 2018 至 2019 年之勒索軟體樣態進行解析分享。勒索軟體包括 wannacry、gaudcrab 等之傳播途徑常為釣魚郵件。釣魚郵件因常採用社交工程提高成功率，具有千變萬化的樣態。釣魚郵件的內容近年常藉由使用拉丁文特殊字母取代英文字母，逃避釣魚郵件偵查。另外甚至有出現冒充知名設計師身分發布釣魚郵件誘導受害者點擊聯結，甚至從雲端下載勒索軟體。

Reference:

https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/17619/2020_USA20_SEM-M03B_01_Ransomware-Spread-through-Various-Distribution-Methods-from-2018-to-2019.pdf

3. Targeted Ransomware: A Potent Threat Begins to Proliferate

近年勒索軟體之攻擊趨勢顯示，2018-2019 年勒索軟體攻擊減少 37%，但針對性勒索軟體卻成長 62%。其中最大受害國家為美國。為未來所可能發生之勒索事件，應定期進行資料備份並更新 OS 與軟體。企業可檢視郵件保護機制，並規劃演練以提升員工遭受勒索軟體攻擊時的應變處理能力。

Reference:

https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/17635/2020_USA20_SEM-M03D_01_Targeted-Ransomware-A-Potent-Threat-Begins-to-Proliferate.pdf

4. IOT Monetization Schemes from the Cybercrime Underground

近年 IOT 攻擊具有增加的趨勢。智慧家電因被駭，進而形成之殭屍網路的攻擊，可具癱瘓能源供給設施等大規模破壞性的影響。而在商場隨處可見的攝影機被駭之後，可竊取客戶刷卡資訊，甚至揭露店家所採用之刷卡系統，型號等機敏資訊。

Reference:

https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/17621/2020_USA20_SEM-M03E_01_IOT-Monetization-Schemes-from-the-Cybercrime-Underground.pdf

5. Ransomware: Partnering for Recovery

   此演講經由過去美國資安事件經驗談(2018 samsam 勒索軟體攻擊，導致 Colorado 州宣布史上第一次的州規模僅擊資安事件)，探討多方面合作(state agencies, federal partners, vendor partners 等)對於資安事件協處與恢復的重要性。

   Reference:

   https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/17623/2020_USA20_SEM-M03F_01_Ransomware-A-Tale-of-Two-CISOs.pdf

6. Protecting Data from Ransomware and Breaches: Demos and Designs

   此演講為 FBI 說明針對資料機敏保護所擔任的角色，以及如何辨識與保護，偵測與處理，恢復遭受勒索軟體攻擊之企業機構的機敏資料。

   Reference:

   https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/17625/2020_USA20_SEM-M03G_01_Protecting-Data-from-Ransomware-and-Breaches-Demos-and-Designs.pdf

7. Deep Fakes are Getting Terrifyingly Real - How Can We Spot Them?

   此演講針對 Deep Fake 所產生之影像的分辨方式進行解說。其中包括觀察眼部扎眼模式，不自然頭部姿勢，高斯分布處理與肉眼可觀察到的影像細節。另外也針對一位於哥本哈根的住宿網站詐騙案例解說。該網站結合 AI 所產生之假圖片與文字說明，仿真程度極高，一般人甚至無法分辨真偽。

   Reference:

   https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/17629/2020_USA20_SEM-M03I_01_Deep-Fakes-Are-Getting-Terrifyingly-Real-How-Can-We-Spot-Them.pdf

8. Ransomware's Threat Over Critical Infrastructure and Industrial Production

   此演講針對關鍵基礎設施，產業製造等 OT 遭受勒索軟體攻擊所產生影響進行說明。2019 Johannesburg 城市的能源供應商就曾遭受勒索軟體攻擊，導致客戶無法於官網進行購買，付款，使用能源。

   Reference:

   https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/17631/2020_USA20_SEM-M03J_01_Ransomwares-Threat-

Over-Critical-Infrastructure-and-Industrial-Production.pdf

9. Prioritizing Threats: What Would Threat Researchers Do (WWTRD)

   此演講從威脅研究家的角度探討如何預防與規劃威脅處理。包括情資收集分析與分享之循環。另外也針對APT41 網軍進行案例分享。

   Reference:

   https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/17633/2020_USA20_SEM-M03K_01_Prioritizing-Threats-What-Would-Threat-Researchers-Do-WWTRD.pdf

10. Reality Check: The Story of Cybersecurity

    Abstract:

    資訊安全議題一直以來對於人為因素以不完整且過於簡化的方式探討，在此會議中讓我們一起探討人為因素對於資訊安全的重要性。

    Reference:

    https://www.rsaconference.com/usa/agenda/reality-check-the-story-of-cybersecurity

11. Time to Tell

    Abstract:

McAfee 首席技術官 Steve Grobman 將帶領我們探討，現有的防禦措施與傳統免疫學方法有著太多的共同點。是時候改變作法並及時採取行動改變未來。

Reference:

https://www.rsaconference.com/usa/agenda/time-to-tell

12. We the People: Democratizing Security

Abstract:

業界仍基於過時的模型來構建安全性。現在我們需要向全球移動用戶提供安全性。我們應該如何適應？我們必須改變思想和技術。安全民主化意味著對我們應該針對不同服務人持有不同看法。用戶不是“最薄弱的環節”。它們是強大的行業驅動力。我們必須放棄過去的信念和控制方式。現在是進行徹底改革的時候了。

Reference:

https://www.rsaconference.com/usa/agenda/we-the-people-democratizing-security

13. The Cryptographer’s Panel

Abstract:

每年，密碼學領域的創始人和領導人都參加 RSA 會議的主題演講，討論和討論網絡安全行業和我們日益數字化

的社會所面臨的最緊迫的問題。而且每年的重要性似乎都越來越高。在 2020 年主題圍繞選舉安全性，個人隱私和數字系統的安全性討論。讓我們一起探討 2020 年最重要的資安事情。

Reference:

https://www.rsaconference.com/usa/agenda/the-cryptographers-panel

14. Cybersecurity Has a Posse

Abstract:

網絡安全和基礎設施安全局（CISA）主任 Christopher C. Krebs 將與我們一起討論 CISA 作為國家風險顧問的廣泛作用，以及他的機構如何在政府和行業之間建立合作夥伴關係，以領導國家協助改善美國網絡安全的工作。

Reference:

https://www.rsaconference.com/usa/agenda/cybersecurity-has-a-posse

15. Fighting a $26 Billion Phishing Problem

Abstract:

通過非技術性社交工程方法（例如被入侵的企業電子郵件帳戶）進行網絡釣魚，現在使企業每月花費超過 7 億

美元。本次會議涵蓋了網絡犯罪分子如何發展其策略以利用組織最薄弱的防御手段-基本人類行為。我們將回顧對 BEC 攻擊的整個攻擊週期的研究，然後討論主動防禦和情報共享如何成功影響 BEC 生態系統。

Reference:

https://www.rsaconference.com/usa/agenda/bec-fighting-a-26-billion-phishing-problem-agari

16. Coordinating a Competitive 5G Strategy among freemarket democracies

Abstract:

華為在 5G 市場中的潛在統治地位將帶來重大的經濟和國家安全風險。中國對不公平貿易行為和 5G 網絡受損的擔憂交織在一起。這兩個問題需要獨立處理。遏制不公平的貿易做法，但還要製定明智的產業政策，以鼓勵對 5G 和外國 5G 設備進行國家安全審查。

Reference:

https://spfusa.org/wp-content/uploads/2019/12/TCSC-National-Security-Strategy-for-5G-Dec-2019.pdf

17. Malicious Documents Emerging Trends: A Gmail Perspective

Abstract:

每天，Gmail 防禦都會分析數十億個附件，以防止惡意文檔進入用戶端或公司用戶的收件箱。本講座將對針對用戶和公司收件箱的惡意文檔進行全面分析，並對攻擊者使用的最新反偵測策略及其 Google 的處理方式進行深入分析。

Reference:
https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/18534/2020_USA20_HTA-T10_01_Malicious-Documents-Emerging-Trends-A-Gmail-Perspective.pdf

18. Repurposed Malware: A Dark Side of Recycling

Abstract:

本次會議將討論攻擊者顛覆現有惡意軟件的方法，並說明如何通過傳統的檢測方法仍無法檢測到這種“舊惡意程式再利用”的威脅。

Reference:
https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/17809/2020_USA20_HT-T11_01_Repurposed-Malware-A-Dark-Side-of-Recycling.pdf

19. Rob, Replicate and Replace: China's Global Technology Theft and How to Confront It

Abstract:

我們應該如何重視中國的網絡威脅？國家安全助理總檢察長 John Demers 和國家反情報與安全中心主任 William Evanina 將描述這種不斷演變的威脅的性質，討論私營部門可以採取哪些措施緩解其脆弱性以及政府正在採取何種措施應對威脅。

Reference:
https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/17723/2020_USA20_PNG-T12_01_rob-replicate-and-replace-chinas-global-technology-theft-and-how-to-confront-it.pdf

20. Enabling and Reducing the Barriers for Collective Cyber-Defence

Abstract:

集體網絡防禦的概念正在蓬勃發展。這個由關鍵威脅情報共享專家組成的多元化小組將討論集體網絡防禦及其益處。小組還將討論為提高共享威脅情報的動機而做出的努力，並使中小型組織也能夠使用和共享威脅情報。

Reference:
https://www.rsaconference.com/usa/agenda/enabling-and-reducing-the-barriers-for-collective-cyber-defense

21. Combatting Cyber Sexual Predators

Abstract:

網絡性犯罪者破壞了受害者的生命，造成的危害與其他網絡犯罪不同。這些巨大的傷害針對的是人類而不是數據，而“deep fake”，加密和其他工具的出現擴大了他們造成傷害的潛力。我們須了解這種線上性暴力的新形式，以及如何避免/應變，成為受害者。

Reference:

https://www.rsaconference.com/usa/agenda/combatting-cyber-sexual-predators

22. Phishing mobile Devices for Fun and Prison

Abstract:

現在有三名網絡罪犯被關進聯邦監獄。他們進行了一項耗資數百萬美元的網絡犯罪行動，該行動利用虛假短信誘騙數千名受害者。本講座將探討他們使用的工具和技術，如何對其進行追查以及 FBI 如何抓獲並定罪。探討透過智能手機攻擊人們的防範策略。

Reference:

https://www.rsaconference.com/usa/agenda/phishing-mobile-devices-for-fun-and-prison-3

23. Creepy Leaky Browser

Abstract:

您是否擔心 Internet 上的隱私？如果是這樣，您的瀏覽器可能洩漏了可用於識別您的數據。本講座將探討當今一些最受歡迎的瀏覽器，並比較/對比洩漏的數據量。

Reference:

https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/18272/2020_USA20_HT-R02_01_Creepy-Leaky-Browsers.pdf

24. Beyond the Ballot Box: Securing America's Supporting Election Technology

Abstract:

我們如何確保選舉系統的安全性?一起來聽 Center for Internet Security 的分享，了解如何保護和驗證美國的網絡選舉技術。驗證試驗項目的結果將被分享和討論。

Reference:

https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/18047/2020_USA20_SBX1-R5_01_Beyond-the-Ballot-Box-Securing-Americas-Supporting-Election-Technology.pdf

25. Incident Response Analysis vs. Automation

Abstract:

我們一直提倡需要將自動化構建到事件應變中，但是我們會做得太多嗎？讓我們討論如何平衡兩者，分享好與壞的方法，以及如何透過同時使用兩者來改善我們的資訊安全事件應變能力。

Reference:

https://www.rsaconference.com/usa/agenda/incident-response-analysis-v-automation

26. What Really Happens When Hackers Attack Medical Devices

Abstract:

本次會議將回顧以醫療保健機構為切入點的駭客行為。一起探討 FDA 的指南和進展，以了解醫療器械的監管方式。最後將演示駭客 demo 來對 HDO 網絡的攻擊。

Reference:

https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/18223/2020_USA20_SBX1-R10_01_What-Really-Happens-When-Hackers-Attack-Medical-Devices.pdf

27. Human Dimension of Active Defence

Abstract:

主動防禦通常僅作為技術操作來討論。本次會議將重點討論以人為導向的對策，其中涉及情報收集和取回被盜

的資料。利用實際案例和美國司法部的新指南，當從犯罪來源收集資訊並重新取回被盜資料時，訂定法律上的底線和政策考量。

Reference:

https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/18170/2020_USA20_PNG-R09_01_human-dimensions-of-active-defense.pdf

28. The 5 Most Dangerous New Attack Techniques and How to Counter Them

Abstract:

攻擊者使用的最危險的新技術是什麼？它們如何運作？如何阻止他們？接下來會發生什麼，您該如何準備？快節奏的簡報會由三位最能提供答案的人組成：美國 mobile forensics 的頂級專家，Internet Storm Center 的負責人和美國頂級的 Hacker exploit 專家。

Reference:

https://www.rsaconference.com/usa/agenda/the-5-most-dangerous-new-attack-techniques-and-how-to-counter-them

29. Coordinated Vulnerability Disclosure: You've Come a Long Way, Baby

Abstract:

安全研究人員和公司之間在揭露軟件漏洞時發生了許多衝突的例子，但是很少有可量化的數據來研究漏洞披露。在有關協調披露的新研究數據的幫助下，本演講將由安全研究人員和組織的觀點，分享行為，偏好和既定做法。

Reference:
https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/18540/2020_USA20_KEY-F01S_01_Coordinated-Vulnerability-Disclosure-Youve-Come-a-Long-Way-Baby.pdf

30. Your Democracy Needs You: Taking On Digital Dictatorships

Abstract:

民主受到攻擊，它需要聰明的捍衛者。該小組將描述鎮壓政權進行資訊戰的人為代價，權威者如何進行和隱藏其活動，揭露它們的方法以及當前研究的局限性。我們需要盡快將資訊安全與人權聯繫起來，學習如何保護用戶免受於受到資訊獨裁者的攻擊。

Reference:
https://www.rsaconference.com/usa/agenda/your-democracy-needs-you-taking-on-digital-dictatorships

31.You Can Stop Stupid

Abstract:

當用戶造成損害時，原因常被歸咎於缺乏認知。現實情況是，因某項操作導致損失的應是系統的設計失敗。引用資訊安全和反恐科學的研究，我們應為用戶打造周圍環境的策略，以防止損害的發生，並在用戶採取可能有害的行為時減輕損害。

Reference:

https://www.rsaconference.com/usa/agenda/you-can-stop-stupid

32. Protect Privacy in a Data-Driven World:

Privacy-Preserving Machine Learning

Abstract:

將 AI 和隱私結合起來不一定是零和遊戲，本演講探討新興的隱私保護機器學習（PPML），可以在保持數據隱私下進行 AI 的分析。這些技術需要更高的計算和存儲要求，因此要如何克服這些議題，使技術具有可行性是近期研究的重點。

Reference:

https://www.rsaconference.com/usa/agenda/shodan-20-the-worlds-most-dangerous-search-engine-goes-on-the-defensive-3

33. Nowhere to Hide: How HW Telemetry and ML Can Make Life Tough for Exploits

Abstract:

硬體(HW)可以在指令層級，克服惡意程式的隱匿機制，發掘其執行情況。本演講詳細介紹如何使用 CPU 遙測和機器學習構建，運行時威脅和異常檢測解決方案。

Reference:

https://www.rsaconference.com/usa/agenda/nowhere-to-hide-how-hw-telemetry-and-ml-can-make-life-tough-for-exploits

34. 2020 ATT&CK Vision: Correlating TTPs to Disrupt Advanced Cyberattacks

Abstract:

Shodan 是資安人員最常使用的搜索引擎之一，透過關鍵字搜尋與操作，可以迅速得知具有漏洞的物聯網裝置分布概況。本演講利用 Shodan，提供針對關鍵基礎設施人員易於使用，開放源始碼的網路防禦工具，同時展示並分享他們的試驗結果。

Reference:

https://www.rsaconference.com/usa/agenda/2020-attck-vision-correlating-ttps-to-disrupt-advanced-cyberattacks

35. Alice Ain't Home: Detecting and Countering Foreign Hackers on Social Media

Abstract:

駭客通常透過虛假社群媒體，散布不實訊息進行社交工程攻擊，來影響他國的政經情勢，或協助洗錢等其他多種任務。本演講將討論打擊虛假線上帳號的作法與概況。

Reference:

https://www.rsaconference.com/usa/agenda/alice-aint-home-detecting-and-countering-foreign-hackers-on-social-media

36. The Industrial Cyberthreat Landscape

Abstract:

工業控制系統(ICS)的威脅隨著新的攻擊手法、新的漏洞、新的思維演進，以及從事件應變案例的經驗，而持續不斷變化。該演講介紹工業控制系統（ICS）社群的- Dragos 的年度報告中的新案例、威脅及經驗分享。

Reference:

https://www.rsaconference.com/usa/agenda/the-industrial-cyberthreat-landscape-2019-year-in-review

37. Measuring Vulnerability Remediation Strategies with Real-World Data

Abstract:

本演講概述四種以數據為依據的漏洞管理程序措施，這些漏洞管理措施包括：涵蓋範圍、效率、速度和能量。講者亦比較這些措施在數百個組織的執行概況，並展示組織如何將這些措施應用於他們的專案中。

Reference:
https://www.rsaconference.com/usa/agenda/measuring-vulnerability-remediation-strategies-with-real-world-data

C. 參加 NGO 交流會議

此交流會議為 RSA 主辦，欲促進 RSAC 參與者與政府及產業高層人員交流互動。其中與 TWNIC 業務相關的主要無營利組織有 The Anti-Phishing Working Group (APWG 反釣魚工作小組)和 Cyber Threat Alliance (CTA)。APWG 反釣魚工作小組長期與 TWNIC 具密切的合作關西，進行網路釣魚情資分享及事件通報協處。CTA 為 2017 年由六個權威資安公司(Check Point Software Technologies Ltd., Cisco, Fortinet, McAfee, Palo Alto Networks 及 Symantec)共同成立的無營利組織，其目的為分析及分享跨產業之珍貴資安威脅情資。目前 CTA 已具超過 20 個資安公司包括如 NEC，NTT，Juniper Networks 等。TWNIC 藉由此交流機會，

維持與 APWG 良好的合作關係，並與 CTA 討論未來資安威脅情資交流與合作關係。

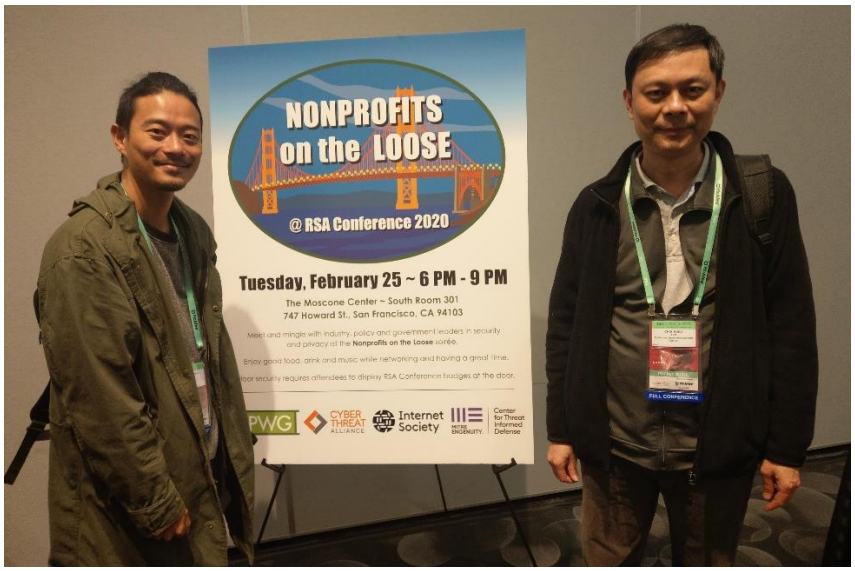

圖 6、左至右: TWNIC 曲承則工程師與 TWNIC 林志鴻組長

D. 參訪新思科技(Synopsys)

TWNIC 藉由此次機會與資安會等相關單位，拜訪舊金山思科參訪，並與 Don Davidson (Director), Jonathan Knudsen (Technical Evangelist)及 Joe Jarzombek (Director for Government & Critical Infrastructure Program) 等進行交流，介紹台灣 TWNIC 及 TWCERT/CC 運作狀況，並針對新思在資訊安全性評估等相關主題交換意見。

新思科技是全球排名第一的電子設計自動化(EDA, Electronic Design Automation) 廠商；新思科技致力提供技

術領先的半導體設計、驗證平臺和 IC 製造軟體產品，協助半導體及電子相關產業的業者，進行複雜的積體電路(IC)設計、系統晶片(SoCs)等產品的開發與生產。

此外，新思科技亦發展成為提供軟體品質及安全測試的領導廠商。不論是針對開發先進半導體 SoC 的設計工程師，或正在撰寫應用程式且要求高品質及安全性的軟體開發工程師，新思科技都能提供所需的解決方案，以協助完成創新、高品質並兼具資訊安全性的產品。Synopsys 在北美、歐洲、日本和亞洲等 90 多個地區都設有分公司及辦事處 。

圖 7、左至右: TWNIC 曲承則工程師，Joe Jarzombek (Director for Government & Critical Infrastructure Programs, Synopsys)，以及 TWNIC 林志鴻組長。

四. 建議意見:

建議事項

- ☐ 建議持續關注資安各領域的發展與趨勢。
- ☐ 勒索軟體近年的針對性勒索軟體具大幅度成長趨勢，並經常透過釣魚郵件傳播，社交工程提供成功率，甚至有藉由特殊拉丁字母等方式躲避偵測機制。建議持續關注相關攻擊手法及偵防機制，強化我國資安防護能量。
- ☐ 網路安全除了威脅研究外，在事件通報的業務上有相關建議措施議題討論，建議持續關注事件應變分析與處理的相關發展，以掌握資訊安全相關技術，並強化網路資訊安全的防護機制。
- ☐ 惡意程式樣態變化日新月異，建議持續關注惡意程式相關技術發展，以掌握新形態惡意程式樣態，強化網路資訊安全偵防能量。

- ☐ 建議持續關注社群媒體駭侵手法，以掌握最新相關駭侵趨勢。
- ☐ 建議持續關注隱私與資料洩漏等狀況以及相關建議應變措施，以提升我國資安事件協處效率。
- ☐ 建議持續關注漏洞揭露規範與建議處理方式，作為強化未來漏洞揭露流程基礎。
- ☐ 建議持續關注資安工作小組、非營利組織與企業等，以拓展未來多元情資來源管道與合作夥伴。

RSAC 下一次會議將於 2021 年 02 月 08 日至 2021 年 02 月 12 日於同地點(舊金山 Moscone Center South)舉行，相關資訊請參考：https://conventioncalendar.com/sanfrancisco/RSA-Security-Inc-Annual-Conference-376512

五. 會議議程:

以下為 RSAC 2020 USA 的議程表:

Saturday, February 22, 2020	
時間	**議程**
1200-1800	Registration

Sunday, February 23, 2020	
時間	議程
0700-1730	Registration
0900-1700	Tutorials & Training

Monday, February 24, 2019	
時間	議程
0700-1900	Registration
0900-1700	Tutorial & Training
0900-1700	RSAC Seminars
0900-1700	Partner All Access Seminars
1300-1600	Innovation Sandbox
1700-1900	Welcome Reception

Tuesday, February 25, 2019	
時間	議程
0600-1800	Registration
0900-1630	Engagement Zone
1000-1800	Expo
1100-1630	Keynotes
1100-1700	Sessions
1600-1730	Sandbox
1600-1730	Early Stage Expo
1600-1730	Cybeer Ops

1700-1900	Women’s Networking Reception

Wednesday, February 26, 2019	
時間	**議程**
0700-1800	Registration
0800-1700	Keynotes
0800-1600	Early Stage Expo
0800-1700	Sessions
0800-1700	Engagement Zone
1000-1800	Expo
1600-1700	Launch Pad
1600-1730	Expo Pub Crawl

Thursday, February 27, 2019	
時間	**議程**
0700-1700	Registration
0700-1730	College Day
0800-1730	Keynotes
0800-1700	Engagement Zone
0800-1600	Sessions
0800-1530	Sandbox
0800-1500	Early Stage Expo
1000-1500	Expo
1800-2100	RSAC After Hours

Friday, February 28, 2019	
時間	議程
0700-1300	Registration
0800-1300	College Day
0800-1130	Keynotes
0800-1130	Sessions
1200-1300	Closing Keynote

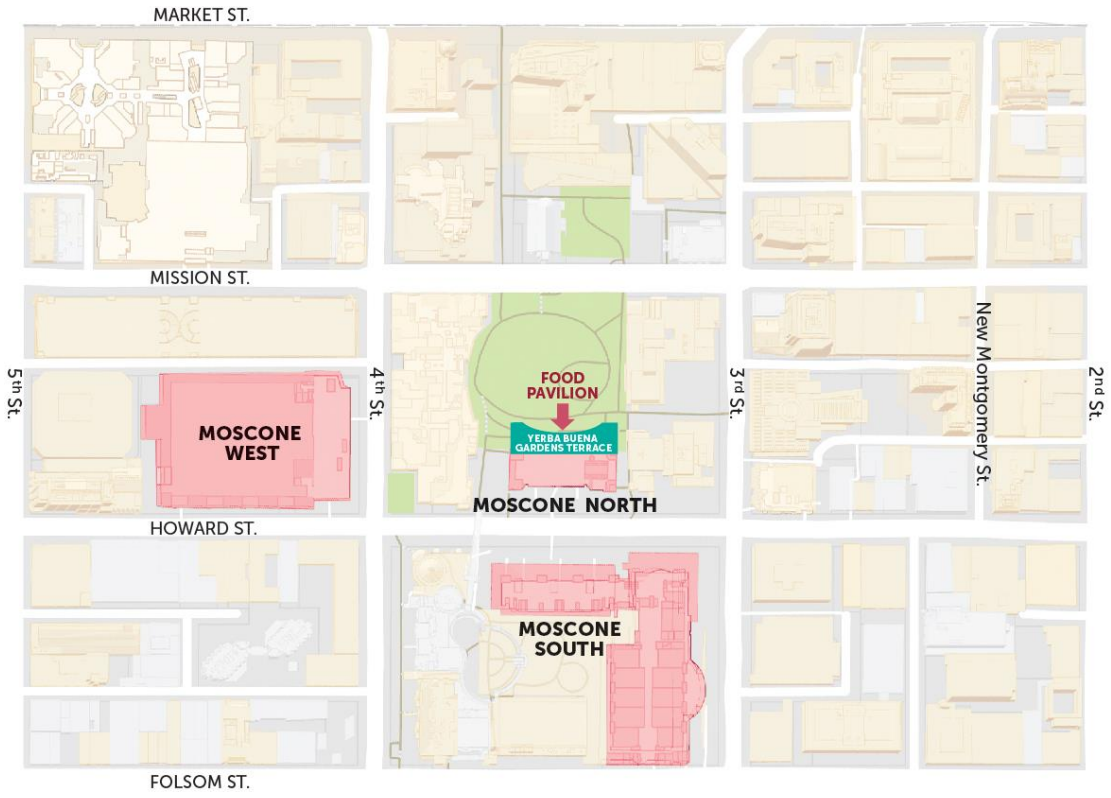

圖 8: 會議場地圖