出國報告(出國類別：開會)

國際資訊安全會議
(RSA Conference 2020)
出國報告

服務機關： 國家通訊傳播委員會
姓名職稱： 吳銘仁 高級分析師
派赴國家： 美國 (舊金山)
出國期間： 109 年 2 月 22 日至 109 年 3 月 1 日
報告日期： 109 年 5 月 22 日

摘要

本次參加 RSA Conference 2020 會議，係為瞭解國際最重要的資安議題及攻擊趨勢，並與其他國家資安廠商及人員交流，適時掌握當前資安產業發展方向，RSA 會議是一系列極具影響力的全球頂級安全盛會，其同時提供廠商參展、舉辦各種安全議題會議及 Innovation Sandbox 競賽等活動，讓國際不同領域之資安專業人才得齊聚一堂，共同探討網路安全問題以及新興科技應用。

美國政府極為重視該會議，不僅視為招募、教育、媒合人才、獎勵創新及促進產業資安技術交流的平台，也視為宣導政府關鍵基礎設施保護與網路安全政策的絕佳機會，因此國家安全局、聯邦調查局、國土安全部皆在參展區設置攤位介紹該單位特色，並藉此機會召募優秀人才。

RSA Conference 2020 會議於本(109)年 2 月 24 日至 2 月 28 日假美國舊金山的莫斯康(Moscone)展覽中心召開，會中邀請多位資安專家、學者、廠商及政府機關代表擔任會議的專題演講(Keynote)，包含了雲端服務、行動裝置的安全性、物聯網(IoT)、密碼學、航空安全、工業控制系統安全、智慧手機安全、風險管控及其它新興資安威脅等議題。本次會議主題除了傳統的網站應用安全議題外，人類事件議題亦在此會議中受到相當程度的重視。

本次會議期間，美國在臺協會(AIT)亦主動安排國內與會人員的會外行程會議，除邀請美國政府機構國家科學技術研究院(NIST)人員於聯邦商務部舊金山代表處會談外，另亦安排民間 SPLUNK 等資安公司與我國與會人員交流，分享美國資安標準及資安防護機制最新發展，以促進美臺技術交流與商業合作機會。

目次

壹、目的

本次主要任務為參加今年度國際間最受關注且為期 5 天(2 月 24 日至 2 月 28 日)的 RSA Conference 2020 會議，親自參與會議學習來自世界各國的資安專家、學界代表、資訊安全廠商及相關政府機構組織，所分享的各種資安漏洞攻擊手法、資安技術及不同領域的各種新興議題與挑戰，其中包含資安最新趨勢、軟體安全、資訊/營運技術(Iinformation Technology/Operational Technology,IT/OT)環境安全、隱私與資料保護一般規則(General Data Protection Regulation,GDPR)、惡意文件、社交媒體及其它新興資安威脅等。

本次參加 RSA Conference 2020 會議的目的包括：

一、與美國官員互動，建立交流管道

在美國在臺協會(AIT)馬奎立商務官及陳玫芳商務經理協助下，於會議第一天 2 月 24 日另安排我國李諮委德財率政府相關部會代表，與美國商務部之國家標準與技術研究院(NIST)代表交流，並由 NIST 官員介紹與分享該機構提出之 NIST-CSF 資安架構及個資保護規範等推動情形(2/24)。

二、掌握美國資安公司最新的資安發展

AIT 於 28 日另安排參訪美國 SPLUNK 公司，聽取其在資安與商業情資蒐集方法、服務提供模式及產品之軟、硬架構等發展。此外，會議期間亦抽空參觀各家資安廠商於 RSA Conference 2020 會議期間，設攤展示其提供資安服務及資安技術之亮點，以掌握資安公司最新資安發展。

三、瞭解最新資安研究成果

蒐集不同領域的資安專家、學界代表、資訊安全廠商及相關機構組織於會中分享其研究成果，如在網際網路普及與大數據蒐集應用之創新服務中，如何兼顧企業的隱私風險管理，以確保公、私利益及個人隱私保護。另在工控環境中 Supervisory Control and Data Acquisition / Industrial control systems (SCADA/ICS) 如何降低資安事件，以及如何應用有效工具以防止網路攻擊等議題之研究成果。

貳、活動紀要

一、概述

(一) 會議活動情形

RSA Conference 2020 會議於本年 2 月 24 日至 2 月 28 日在美國舊金山的莫斯康(Moscone)展覽中心召開，會議地點區分 Moscone South、Moscone West、Moscone North 及 Marriott Marquis 等 4 個地方，而大部份的主題演講、小組討論會都在 Moscone South、Moscone West、Moscone North 等 3 個地方，僅有部份特別議題在 Marriott Marquis 進行，主要活動情形如下：

1. 計有 36,000 名與會者，704 位演講者和 658 家參展商於活動期間聚集在 Moscone 中心。本會議透過數百場次主題式演講、相似議題會議、教學課程、研討會及個案活動等方式，以探索人為因素在網路安全的角色。其主要議題包括資安最新趨勢、軟體安全、IT/OT 環境安全、隱私與 GDPR、惡意文件及社交媒體等，相關議程請參閱議程及 RSA 網站。
2. 創新沙盒比賽：最具創新性的創業公司 SECURITI.ai 獲首獎。
3. 第 29 屆年度 RSA 會議。
4. 數學領域傑出獎頒獎：獲獎者 Professor Joan Daemen and Professor Vincent Rijmen。
5. CISO 新手訓練營：超過 130 位 CISO 新手參加本訓練營一天半的活動，促進與高級安全領導人之間的對話。
6. RSAC 學院：此機制則為大學生和畢業生探索職業選擇，並媒合工作機會。
7. 會後提供 RSAC onDemand，讓與會者可以隨時觀看錯過的會議。

(二) 議程

1.RSA Conference 2020 會議-2 月 24 日(一)議程

MONDAY EVENTS & ACTIVITIES

MONDAY

8:00 AM – 9:00 AM | Various locations
CONTINENTAL BREAKFAST*
Full Conference Pass holders, head directly to your RSAC Seminar.

8:30 AM – 5:00 PM
RSA CONFERENCE SEMINARS**
See following pages for details and room locations.

8:00 AM – 5:00 PM
PARTNER ALL-ACCESS SEMINARS
See following pages for details and room locations.

8:00 AM – 5:00 PM | Moscone West Street Level
BROADCAST ALLEY
Watch top security publications shoot live and record exclusive interviews.

9:00 AM – 5:00 PM | Moscone South Level 3
TUTORIALS & TRAININGS
See previous pages for details and room locations.

1:30 PM – 4:30 PM | Moscone South Level 2, RSAC Sandbox
RSAC INNOVATION SANDBOX CONTEST
The RSAC Innovation Sandbox Contest has crowned innovative companies who build cutting-edge technologies to minimize cybersecurity risk for the past 15 years. Witness the 2020 Top 10 Finalists battle it out for the coveted title of "Most Innovative Startup." See page 20 for a detailed agenda.
Exclusive RSAC Innovation Sandbox Media Sponsor:
WSJ PRO CYBERSECURITY

4:00 PM – 5:00 PM | Moscone West 2005
FIRST-TIMERS ORIENTATION & NETWORKING RECEPTION
This event is open to Full Conference Pass holders and features a 30-minute presentation followed by a 30-minute networking reception with light refreshments.

5:00 PM – 7:00 PM | Moscone South Lower Level
RSAC SECURITY OPERATIONS CENTER
Take a tour of a working SOC! Head to the Moscone South Lower Level for the RSA Conference Security Operations Center. See what's really taking place on the Moscone Wireless Network in real time.
Sponsored by: cisco RSA

5:00 PM – 7:00 PM | North & South Expo
WELCOME RECEPTION
Join your peers in the Expo while kicking off RSA Conference in style at the Welcome Reception. Enjoy drinks and light fare from 5 to 7 PM. Get exclusive access to the exhibitors you've been waiting to meet; network with peers as you preview cutting-edge products from more than 650 leading information security companies.
Sponsored by:
AT&T Cybersecurity · BlackBerry CYLANCE · Check Point · F5 · ixia · JUNIPER · mimecast · splunk> · TeleTrusT IT Security Made in Germany · tenable · THALES · VARONIS · verizon · vmware Carbon Black · WEBROOT

圖 1　RSA Conference 2020 會議議程(一)

2. RSA Conference 2020 會議-2 月 25 日(二)議程

TUESDAY EVENTS & ACTIVITIES

TUESDAY

6:30 AM – 8:00 AM | Moscone West
CONTINENTAL BREAKFAST*
Full Conference Pass holders, breakfast is available in Moscone West.

Locations and Times Vary
RSAC CYBREW CAFÉ
A full-service coffee bar in the RSAC Sandbox, RSAC Engagement Zone and West Level 3.

KEYNOTES†
Keynote abstracts can be found on pages 34 – 35.
† On Tuesday morning, the West Stage Keynotes are open to Full Conference Pass holders only. South Stage Keynotes are open to Full Conference and Expo Plus Pass holders.

8:00 AM | West Stage
Opening

8:10 AM – 8:35 AM | West Stage
Reality Check: The Story of Cybersecurity
&Rohit Ghai, President, RSA

8:35 AM – 8:55 AM | West Stage
Time to Tell
***Steve Grobman**, Senior Vice President and Chief Technology Officer, McAfee*

8:55 AM – 9:15 AM | West Stage
We the People: Democratizing Security
***Wendy Nather**, Head of Advisory CISOs, Cisco*

9:15 AM – 9:20 AM | West Stage
Excellence in the Field of Mathematics Award
Please join us for the announcement of this year's RSAC Math Award recipients for their outstanding contributions to the field of cryptography

9:20 AM – 10:05 AM | West Stage
The Cryptographers' Panel
*MODERATOR: **Zulfikar Ramzan**, Chief Technology Officer, RSA*
*PANELISTS: **Whitfield Diffie**, Cryptographer and Security Expert, Cryptomathic; **Arvind Narayanan**, Associate Professor of Computer Science, Princeton University; **Tal Rabin**, Head of Research, Algorand Foundation; **Ronald Rivest**, Professor, Massachusetts Institute of Technology; **Adi Shamir**, Borman Professor of Computer Science, The Weizmann Institute, Israel*

10:05 AM – 10:30 AM | West Stage
Cybersecurity Has a Posse
***Chris Krebs**, Director, Cybersecurity and Infrastructure Security Agency*

11:00 AM – 11:50 AM | South Stage
Fear and Loathing in Cybersecurity: An Analysis of the Psychology of Fear
***Dr. Jessica Barker**, Co-Chief Executive Officer, Cygenta*

1:00 PM – 1:50 PM | South Stage
A Forward Look at the Cyberspace Solarium Commission
*MODERATOR: **Nicole Perlroth**, Investigative Journalist, New York Times*
*PANELISTS: **Frank Cilluffo**, Director, Auburn University McCrary Institute for Cyber & Critical Infrastructure; **John C. (Chris) Inglis**, Looker Distinguished Visiting Professor of Cyber Studies, United States Naval Academy; **Suzanne Spaulding**, Senior Adviser for Homeland Security in the International Security Program, Center for Strategic and International Studies*

2:20 PM – 3:10 PM | South Stage
Rocked to the Core
*MODERATOR: **Donna Dodson**, Chief Cybersecurity Advisor, National Institute of Standards and Technology (NIST)*
*PANELISTS: **Marene Allison**, Chief Information Security Officer, Johnson & Johnson; **Paul Kocher**, Security Entrepreneur and Researcher; **Phil Venables**, Board Director and Senior Advisor Cyber, Goldman Sachs*

3:40 PM – 4:30 PM | South Stage
Effective Leadership and Motivation: What It Took to Race around the World
***Tracy Edwards MBE**, Round the World Sailor, Author and Social Activist*

9:00 AM – 5:00 PM | Moscone West Street Level
BROADCAST ALLEY
Watch top security publications shoot live and record exclusive interviews.

9:00 AM – 4:30 PM | Moscone West Level 2
RSAC ENGAGEMENT ZONE*
Debuting at RSAC 2020, the RSAC Engagement Zone makes it easier than ever to connect with peers from around the world for meaningful interactions—ranging from informal to structured, and one-on-one to group settings. RSAC Engagement Zone events for Tuesday include Braindate, Cooperative Learning, Problem Solving, Speed Networking. Hours of each vary.

10:00 AM – 6:00 PM | Moscone South Lower Level
RSAC SECURITY OPERATIONS CENTER
Take a tour of a working SOC! Head to the Moscone South Lower Level for the RSA Conference Security Operations Center. See what's really taking place on the Moscone Wireless Network in real time.
Sponsored by: cisco RSA

TUESDAY EVENTS & ACTIVITIES

10:00 AM – 6:00 PM | Moscone North & South Lower Levels
EXPO
Come see how RSA Conference 2020 exhibitors offer you the latest technological solutions, provide hands-on learning opportunities and demonstrate how they can help you better secure your organization.

10:30 AM – 4:10 PM | Moscone North & South Lower Levels
EXPO BRIEFING CENTER
See the following pages for abstracts and a complete schedule on pages 115–119.

11:00 AM – 11:50 AM & 1:00 PM – 4:30 PM | Locations vary
TRACK SESSIONS
See detailed information on the following pages for descriptions and badge access.

11:00 AM – 11:50 AM & 1:00 PM – 4:30 PM | Moscone West 2004
SESSION VIEWING POINT*
Can't make it to a session of interest? Visit Moscone West Level 2, Room 2004 and choose from up to eight different sessions to watch on a large screen. Provided headphones allow you to hear only the session you want.

11:00 AM – 2:00 PM | Yerba Buena Gardens Terrace
FOOD PAVILION
With options for all tastes, the Food Pavilion is the easy way to fuel up between sessions. Open to all RSA Conference badge holders for cash or credit transactions.

11:00 AM – 11:50 AM & 1:00 PM – 5:50 PM | Moscone West 3006
LAW TRACK SESSIONS*
See detailed information on the following pages for descriptions.

2:20 PM – 4:20 PM | Moscone South Level 3
LEARNING LABS*
Learning Labs provide highly interactive, facilitated learning experiences and are very hands-on and small group oriented. Seating is limited; use Reserve a Seat to schedule your participation. You can only reserve one Learning Lab on your schedule, so choose carefully from our great offerings. ***Note: Press is not permitted in Learning Lab sessions.***

4:00 PM – 6:00 PM | Moscone South Level 2
RSAC SANDBOX**
Join hands-on learning and fun through a wide range of interactive cybersecurity challenges and networking opportunities. Explore 12 sandboxes each focusing on a unique topic including aerospace, biohacking, car hacking, ICS, IoT, medical devices, supply chain and voting; The Lab featuring SANS NetWars and other capture-the-flag challenges; and 30-minute talks with industry experts.
Exclusive RSAC Sandbox Media Sponsor:
TechTarget | SearchSecurity

Moscone South Level 2, RSAC Sandbox
RSAC EARLY STAGE EXPO**
The RSAC Early Stage Expo is the perfect megaphone for emerging cybersecurity startups. Meet 51 of the industry's most promising newcomers and learn about their innovative products and solutions, and check out the RSAC Early Stage Expo Briefing Center (details on pages 178 – 185).
Exclusive RSAC Early Stage Expo Media Sponsor:
crunchbase

4:00 PM – 6:00 PM | RSAC Sandbox & RSAC Early Stage Expo
CYBEER OPS NETWORKING RECEPTION**
Delight in local California craft beers and nonalcoholic drinks as you network and mingle with peers. CyBEER Ops opens the RSAC Sandbox and RSAC Early Stage Expo where you can check out 51 up and coming startups and participate in hands-on interactive experiences.

5:00 PM – 7:00 PM | Marriott Marquis Yerba Buena 9
WOMEN'S NETWORKING RECEPTION
Join us in celebrating the continued development of women in cybersecurity. All RSA Conference Pass holders are welcome to attend.
Sponsored by: cisco RSA

6:00 PM – 8:00 PM | Moscone South 302
NON-PROFITS ON THE LOOSE
Meet and mingle with industry and government leaders while enjoying food and drink at the Marriott Marquis, just blocks from the Moscone Center. The Anti-Phishing Working Group (APWG), the Center for Threat-Informed Defense and the Cyber Threat Alliance (CTA) invite you to join us for the tenth Annual Non-Profits on the Loose for great food, fun and networking. Thank you for supporting our passions; stop by and discuss how we can improve cybersecurity together.
Attendees must have an RSA Conference badge.

7:00 PM – 9:00 PM | Marriott Marquis Yerba Buena 9
***MAIDEN* MOVIE SCREENING**
Immediately following the Women's Networking Reception, stay put for a screening of *Maiden*, featuring our own RSAC keynote speaker, Tracy Edwards. Watch as she leads the first all-female crew in the Whitbread Round the World Race, a grueling yachting competition that covers 33,000 miles and lasts nine months.

圖 2　RSA Conference 2020 會議議程(二)

3. RSA Conference 2020 會議-2 月 26 日(三)議程

WEDNESDAY EVENTS & ACTIVITIES

WEDNESDAY

7:00 AM – 8:00 AM | Moscone West — CONTINENTAL BREAKFAST*
Full Conference Pass holders, breakfast is available in Moscone West Levels 2 & 3.

7:00 AM – 8:00 AM | Moscone West 2018 Overlook — FIRST-TIMERS MEET-UP*
Start the day with a meet-up with other RSAC first-timers. Grab your complimentary breakfast, and enjoy this time to regroup, share takeaways and, of course, caffeinate.

7:00 AM – 5:00 PM | Location and Times Vary — RSAC CYBREW CAFÉ
A full-service coffee bar in the RSAC Sandbox, RSAC Engagement Zone and West Level 3.

KEYNOTES**
Keynote abstracts can be found on pages 36 – 37.

8:00 AM – 8:50 AM | South Stage — Hacking Exposed: Global Threat Brief
***Dmitri Alperovitch**, Co-Founder and Chief Technology Officer, CrowdStrike; **George Kurtz**, Co-Founder and Chief Executive Officer, CrowdStrike; **Elia Zaitsev**, Vice President of Sales Engineering for the Americas, CrowdStrike*

9:20 AM – 10:10 AM | South Stage — Genomics: A New Frontier for Privacy and Security
*MODERATOR: **Rajeev Chand**, Partner and Head of Research, Wing Venture Capital*
*PANELISTS: **Dr. Patrick Courneya**, Chief Medical Officer, Kaiser Permanente; **Kathy Hibbs JD**, Chief Legal and Regulatory Officer, 23andMe; **Sharon F. Terry**, President and CEO, Genetic Alliance; **Mike Wilson**, Former CISO, Molina Healthcare and McKesson*

10:30 AM – 10:55 AM | West Stage — Rethink the Way You Secure Your Organization with Intrinsic Security
***Carrie Mills**, Senior Manager, Cybersecurity, Southwest Airlines; **Patrick Morley**, SVP/GM Security Business Unit, VMware; **Sanjay Poonen**, Chief Operating Officer, Customer Operations, VMware*

10:55 AM – 11:15 AM | West Stage — Drive Security into the Fabric of Your Business by Investing in Your People
***Roland Cloutier**, Senior Vice President and Chief Security Officer, ADP; **Mary O'Brien**, General Manager, IBM Security, IBM; **Wendi Whitmore**, IBM Security Vice President, X-Force Threat Intelligence*

11:15 AM – 11:45 AM | West Stage — Record-Breaking: My Life and Career with NASA
***Peggy Whitson**, Record-Breaking Astronaut; **Mike Massimino**, Former NASA Astronaut*

1:30 PM – 2:20 PM | South Stage — Fireside Chat with the Department of Energy's Karen S. Evans
***Karen Evans**, Assistant Secretary, Office of Cybersecurity, Energy Security and Emergency Response, US Department of Energy; **Marty Edwards**, VP Operational Technology Security, Tenable*

2:50 PM – 3:40 PM | South Stage — How to Reduce Supply Chain Risk: Lessons from Efforts to Block Huawei
*MODERATOR: **Craig Spiezle**, Founder, Agelight Advisory and Research Group*
*PANELISTS: **Katie Arrington**, Cyber Information Security Officer of Acquisitions, US Dept of Defense / OUSD for Acquisitions; **Donald (Andy) Purdy**, Chief Security Officer, Huawei Technologies USA; **Bruce Schneier**, Security Technologist, Researcher and Lecturer, Harvard Kennedy School; **Kathryn Waldron**, Fellow, R Street Institute*

4:00 PM – 4:25 PM | West Stage — Why Your People Are Still Your Best Cyber-Defense
***Ann Johnson**, Corporate Vice President, Cybersecurity Solutions Group, Microsoft*

4:25 PM – 5:00 PM | West Stage — Insights from Kara Swisher
***Kara Swisher**, Co-Founder and Editor-at-Large, Recode*

8:00 AM – 10:10 AM & 1:30 PM – 3:40 PM | Locations Vary — TRACK SESSIONS
See detailed information on the following pages for descriptions and badge access.

8:00 AM – 10:10 AM & 1:30 PM – 3:40 PM | Moscone West 2004 — SESSION VIEWING POINT*
Can't make it to a session of interest? Visit Moscone West Level 2, Room 2004 and choose from up to eight different sessions to watch on a large screen. Provided headphones allow you to hear only the session you want.

8:00 AM – 10:10 AM & 1:30 PM – 3:40 PM | RSAC Engagement Zone Moscone West 2020 — BIRDS OF A FEATHER
It's our popular Birds of a Feather format—with an Engagement Zone twist. Participate in published, planned topics facilitated by some of our speakers, or take advantage of open, non-scheduled space all day to have free-form discussions. You never know where the conversation may lead! ***Note: Press is not permitted in Birds of a Feather sessions.***

8:00 AM – 5:00 PM | Moscone West Level 2 — RSAC ENGAGEMENT ZONE*
Debuting at RSAC 2020, the RSAC Engagement Zone makes it easier than ever to connect with peers from around the world for meaningful interactions—ranging from informal to structured, and one-on-one to group settings. RSAC Engagement Zone events for Wednesday include Birds of a Feather, Braindate, Cooperative Learning. Hours of each vary.

WEDNESDAY EVENTS & ACTIVITIES

8:00 AM – 5:00 PM | Moscone West 3006 — LAW TRACK SESSIONS*
See detailed information on the following pages for descriptions.

8:00 AM – 4:00 PM | Moscone South Level 2, RSAC Sandbox — RSAC EARLY STAGE EXPO**
The RSAC Early Stage Expo is the perfect megaphone for emerging cybersecurity startups. Meet 51 of the industry's most promising newcomers and learn about their innovative products and solutions, and check out the RSAC Early Stage Expo Briefing Center (details on pages 178 – 185).
Exclusive RSAC Early Stage Expo Media Sponsor: crunchbase

8:00 AM – 5:00 PM | Moscone South Level 2 — RSAC SANDBOX**
Join hands-on learning and fun through a wide range of interactive cybersecurity challenges and networking opportunities. Explore 12 sandboxes each focusing on a unique topic including aerospace, biohacking, car hacking, ICS, IoT, medical devices, supply chain and voting; The Lab featuring SANS NetWars and other capture-the-flag challenges; and 30-minute talks with industry experts.
Exclusive RSAC Sandbox Media Sponsor: TechTarget | SearchSecurity

8:00 AM – 5:00 PM | Moscone West Street Level — BROADCAST ALLEY
Watch top security publications shoot live and record exclusive interviews.

Beginning at 9:00 AM | Moscone North Street Level — RSAC YOGA & MEDITATION
Take a break from your busy RSAC schedule for a brief 15-minute guided meditation session (at 9 and 9:45 AM) or chair yoga session (at noon and 12:45 PM) led by the professionals from Office Meets Yoga.

9:20 AM – 11:20 AM & 2:00 PM – 4:00 PM | Moscone South Level 3 — LEARNING LABS*
Learning Labs provide highly interactive, facilitated learning experiences and are very hands-on and small group oriented. Seating is limited; use Reserve a Seat to schedule your participation. You can only reserve one Learning Lab on your schedule, so choose carefully from our great offerings. ***Note: Press is not permitted in Learning Lab sessions.***

9:30 AM – 2:20 PM | RSAC Early Stage Expo — RSAC EARLY STAGE EXPO BRIEFING CENTER**
See page 185 for a schedule of presentations.

10:00 AM – 6:00 PM | Moscone South Lower Level — RSAC SECURITY OPERATIONS CENTER
Take a tour of a working SOC! Head to the Moscone South Lower Level for the RSA Conference Security Operations Center. See what's really taking place on the Moscone Wireless Network in real time.
Sponsored by: cisco RSA

10:00 AM – 6:00 PM | Moscone North & South Lower Levels — EXPO
Come see how RSA Conference 2020 exhibitors offer you the latest technological solutions, provide hands-on learning opportunities and demonstrate how they can help you better secure your organization.

10:30 AM – 4:10 PM | Moscone North & South Lower Levels — EXPO BRIEFING CENTER
See the following pages for abstracts and a complete schedule on pages 115–119.

11:00 AM – 2:00 PM | Yerba Buena Gardens Terrace — FOOD PAVILION
With options for all tastes, the Food Pavilion is the easy way to fuel up between sessions. Open to all RSA Conference badge holders for cash or credit transactions.

11:30 AM – 1:00 PM | Moscone South 303 — EXECUTIVE WOMEN'S FORUM MEET & GREET AT RSA CONFERENCE 2020
The Executive Women's Forum and Accenture Security are hosting a Meet & Greet for all the amazing women attending RSA Conference 2020. Enjoy the company of your peers—some of the brightest minds at the event—for a fun, relaxed, professional get together. Engage and connect with the most dynamic personalities; the women in information security who make it happen. Join in interactive discussions and get to know each other over light lunch. We look forward to meeting you!

12:00 PM – 1:00 PM | Moscone North Street Level — RSAC SECURITY SCHOLAR POSTER BOARD EXHIBITION
RSA Conference Security Scholar connects the brightest up-and-coming cybersecurity students to leading experts, peers and Conference attendees. We are offering the RSAC Security Scholars the opportunity to demonstrate their work at a poster board exhibition. Drop by, provide feedback and meet the RSAC Security Scholar Class of 2020!

WEDNESDAY

圖 3　RSA Conference 2020 會議議程(三)

4. RSA Conference 2020 會議-2 月 27 日(四)議程

THURSDAY EVENTS & ACTIVITIES

THURSDAY

7:00 AM – 8:00 AM | Moscone West — CONTINENTAL BREAKFAST*
Full Conference Pass holders, breakfast is available in Moscone West Levels 2 & 3.

7:00 AM – 8:00 AM | Moscone West 2018 Overlook — FIRST-TIMERS MEET-UP*
Start the day with a meet-up with other RSAC first-timers. Grab your complimentary breakfast, and enjoy this time to regroup, share takeaways and, of course, caffeinate.

7:00 AM – 5:00 PM | Locations and Times Vary — RSAC CYBREW CAFÉ
A full-service coffee bar in the RSAC Sandbox, RSAC Engagement Zone and West Level 3.

KEYNOTES**
Keynote abstracts can be found on pages 38 – 39.

8:00 AM – 8:50 AM | South Stage — The Industrial Cyberthreat Landscape: 2019 Year in Review
***Robert Lee**, CEO, Dragos, Inc.*

9:20 AM – 10:10 AM | South Stage — Hacking Society
***Bruce Schneier**, Security Technologist, Researcher and Lecturer, Harvard Kennedy School*

10:30 AM – 10:55 AM | West Stage — 20 Years In: Security's Grand Challenges, Then and Now
***Andy Ellis**, Chief Security Officer, Akamai Technologies, Inc.*

10:55 AM – 11:25 AM | West Stage — The Future of Transportation Relies on Strong Cybersecurity
***Mary T. Barra**, Chairman and Chief Executive Officer, General Motors Company*

1:30 PM – 2:20 PM | South Stage — Geopolitical Risks, Elections and Cybersecurity
***Admiral James Stavridis,** Retired Four-Star Officer, US Navy; **Juliette Kayyem**, Professor, Harvard's Kennedy School of Government*

2:50 PM – 3:40 PM | South Stage — Hacking Stress in Cybersecurity Operations
***Dr. Celeste Paul**, Researcher, National Security Agency*

4:00 PM – 4:25 PM | West Stage — On the Edge of Something Big: Security's Next Frontier
***Ken Xie**, Founder, Chairman of the Board and Chief Executive Officer, Fortinet*

4:25 PM – 5:10 PM | West Stage — The 5 Most Dangerous New Attack Techniques and How to Counter Them
*MODERATOR: **Alan Paller**, Research Director and Founder, SANS Institute*
*PANELISTS: **Heather Mahalik**, Senior Instructor, SANS Institute and Director of Digital Intelligence, Cellebrite; **Ed Skoudis**, Instructor, SANS Institute; **Johannes Ullrich**, Dean of Research, SANS Technology Institute*

8:00 AM – 10:10 AM & 1:30 PM – 3:40 PM | Various Locations — TRACK SESSIONS
See detailed information on the following pages for descriptions and badge access.

8:00 AM – 10:10 AM & 1:30 PM – 3:40 PM | Moscone West 2004 — SESSION VIEWING POINT*
Can't make it to a session of interest? Visit Moscone West Level 2, Room 2004 and choose from up to eight different sessions to watch on a large screen. Provided headphones allow you to hear only the session you want.

8:00 AM – 10:10 AM & 1:30 PM – 3:40 PM | RSAC Engagement Zone Moscone West 2020 — BIRDS OF A FEATHER
It's our popular Birds of a Feather format—with an Engagement Zone twist. Participate in published, planned topics facilitated by some of our speakers, or take advantage of open, non-scheduled space all day to have free-form discussions. You never know where the conversation may lead! ***Note: Press is not permitted in Birds of a Feather sessions.***

8:00 AM – 3:30 PM | Moscone South Level 2 — RSAC SANDBOX**
Join hands-on learning and fun through a wide range of interactive cybersecurity challenges and networking opportunities. Explore 12 sandboxes each focusing on a unique topic including aerospace, biohacking, car hacking, ICS, IoT, medical devices, supply chain and voting; The Lab featuring SANS NetWars and other capture-the-flag challenges; and 30-minute talks with industry experts.
Exclusive RSAC Sandbox Media Sponsor: TechTarget | SearchSecurity

THURSDAY EVENTS & ACTIVITIES

8:00 AM – 3:00 PM | Moscone South Level 2 — RSAC EARLY STAGE EXPO**
The RSAC Early Stage Expo is the perfect megaphone for emerging cybersecurity startups. Meet 51 of the industry's most promising newcomers and learn about their innovative products and solutions, and check out the RSAC Early Stage Expo Briefing Center (details on pages 178 – 185).
RSAC Early Stage Expo Exclusive Media Sponsor: crunchbase

8:00 AM – 5:00 PM | Moscone West Street Level — BROADCAST ALLEY
Watch top security publications shoot live and record exclusive interviews.

8:00 AM – 5:10 PM | Moscone West Level 2 — RSAC ENGAGEMENT ZONE*
Debuting at RSAC 2020, the RSAC Engagement Zone makes it easier than ever to connect with peers from around the world for meaningful interactions—ranging from informal to structured, and one-on-one to group settings. RSAC Engagement Zone events for Thursday include Birds of a Feather, Braindate, Cooperative Learning. Hours of each vary.

Beginning at 9:00 AM | Moscone North Street Level — RSAC YOGA & MEDITATION
Take a break from your busy RSAC schedule for a brief 15-minute chair yoga session (at 9 AM and 12:45 PM) or guided meditation session (at 9:45 AM and noon) led by the professionals from Office Meets Yoga.

9:20 AM – 10:20 AM | Moscone West 3006 — RSAC SECURITY SCHOLAR POSTER PITCH-OFF
Learn about the cutting-edge research coming out of top universities as three selected RSA Conference Security Scholars give 5 minute pitches to government, research and cybersecurity veterans.

9:20 AM – 11:20 AM & 2:00 PM – 4:00 PM | Moscone South Level 3 — LEARNING LABS*
Learning Labs provide highly interactive, facilitated learning experiences and are very hands-on and small group oriented. Seating is limited; use Reserve a Seat to schedule your participation. You can only reserve one Learning Lab on your schedule, so choose carefully from our great offerings. ***Note: Press is not permitted in Learning Lab sessions.***

10:00 AM – 3:00 PM | Moscone South Lower Level — RSAC SECURITY OPERATIONS CENTER
Take a tour of a working SOC! Head to the Moscone South Lower Level for the RSA Conference Security Operations Center. See what's really taking place on the Moscone Wireless Network in real time.
Sponsored by: cisco RSA

10:00 AM – 3:00 PM | Moscone North & South Lower Levels — EXPO
Come see how RSA Conference 2020 exhibitors offer you the latest technological solutions, provide hands-on learning opportunities and demonstrate how they can help you better secure your organization.

10:30 AM – 12:00 PM | Moscone North & South Lower Levels — EXPO BRIEFING CENTER
See the following pages for abstracts and a complete schedule on pages 115–119.

9:30 AM – 2:20 PM | RSAC Early Stage Expo — RSAC EARLY STAGE EXPO BRIEFING CENTER**
See page 185 for a schedule of presentations.

11:00 AM – 2:00 PM | Yerba Buena Gardens Terrace — FOOD PAVILION
With options for all tastes, the Food Pavilion is the easy way to fuel up between sessions. Open to all RSA Conference badge holders for cash or credit transactions.

6:00 PM – 9:00 PM | Marriott Marquis, Yerba Buena Level — RSAC AFTER HOURS*
Bring back the 80's with RSA Conference and enjoy a night back in time on Throwback Thursday #TBT.
Join your peers and enjoy food, drinks, dancing with a live 80's cover band, throwback games and more.
Return shuttles to official RSAC hotels will run from 6:30 to 9:00 PM.

THURSDAY

圖 4　RSA Conference 2020 會議議程(四)

5. RSA Conference 2020 會議-2 月 28 日(五)議程

FRIDAY EVENTS & ACTIVITIES

FRIDAY

7:30 AM – 8:30 AM Moscone West	**CONTINENTAL BREAKFAST*** Full Conference Pass holders, breakfast is available in Moscone West Levels 2 & 3.
7:30 AM – 12:30 PM Moscone West Level 3	**RSAC CYBREW CAFÉ*** A full-service coffee bar.
8:00 AM – 1:00 PM Moscone West Street Level	**BROADCAST ALLEY** Watch top security publications shoot live and record exclusive interviews.
	KEYNOTES** *Keynote abstracts can be found on page 40.*
8:30 AM – 9:20 AM South Stage	**Coordinated Vulnerability Disclosure: You've Come a Long Way, Baby** ***Katie Moussouris**, Chief Executive Officer, Luta Security; **Chris Wysopal**, Co-Founder and Chief Technology Officer, Veracode*
9:50 AM – 10:40 AM South Stage	**Collaborating to Improve Open Source Security: How the Ecosystem Is Stepping Up** ***Mark Russinovich**, Chief Technology Officer, Microsoft Azure*
11:10 AM – 12:00 PM South Stage	**You Can Stop Stupid** ***Dr. Tracy Celaya Brown**, President, Go Consulting International; **Ira Winkler**, Lead Security Principal, Trustwave*
8:30 AM – 12:00 PM Locations Vary	**TRACK SESSIONS*** See detailed information on the following pages for descriptions.
8:30 AM – 12:00 PM Moscone West 2004	**SESSION VIEWING POINT*** Can't make it to a session of interest? Visit Moscone West Level 2, Room 2004 and choose from up to eight different sessions to watch on a large screen. Provided headphones allow you to hear only the session you want.
8:30 AM – 9:40 AM Moscone West 2018	**JOB SEARCH 2020: INTERVIEW SKILLS & RESUME REVIEW WORKSHOP*** This workshop has two components—the first explores how to best present your skills and self to potential companies and the second is a resume review workshop. ***No Press allowed.***
	CONFERENCE CLOSING** **The Hugh Thompson Show, featuring Penn & Teller and Dr. Lorrie Cranor** ***Penn & Teller**, Magicians; **Hugh Thompson**, Program Committee Chair, RSA Conference; **Dr. Lorrie Cranor**, Director and Bosch Distinguished Professor, CyLab Security and Privacy Institute, Carnegie Mellon University*
12:30 PM – 1:30 PM West Stage	

圖 5　RSA Conference 2020 會議議程(五)

二、與美國官員互動，建立交流管道

美國在臺協會(AIT)於 2 月 24 日安排美國 NIST 資訊技術實驗室之 Amy Mahn、Katie Boecki、Jeffrey Cichonski 及 Katerina”Kat”Megas 等 4 位同仁，在美國國務院駐加州舊金山辦公室，與我國李諮委德財率領政府相關部會代表之參訪團(圖 6)，分享其推動資安框架 Cybersecurity Framework（CSF）、隱私保護等標準規範推動情形，分述如下：

圖 6：我國參訪團成員與 NIST 及美國 AIT 代表合照

(一) NIST 的 CSF 資安框架

NIST 於 107 年 4 月公布新修正之 CSF 1.1 版資安框架，係由識別、保護、偵測、回應與復原等 5 大功能組成(詳圖 7)，NIST 並針對此 5 大功能再展開細分成 23 類別(詳圖 8)及各類別相對映加總計有 108 項子類別之表格(如圖 9)。該框架與前一版最大差異係就供應鏈安全、身份識別與驗證，以及自我評估資安風險等內容進行強化。

CSF 資安框架之推動係採自願性方式辦理，NIST 參考國際資安相關標準、政府指導方針及企業最佳作法等後，提出此框架修正建議，以提供政府、關鍵基礎設施提供者及企業等機關(構)資安推動參考。各參考機關得以該框架之網路安全生命週期的風險管理，檢視其組織安全現況、風險評鑑、資安政策目標、優先防護順序

之實施計畫及安全成熟度評估等措施實施，以持續強化其網路安全。

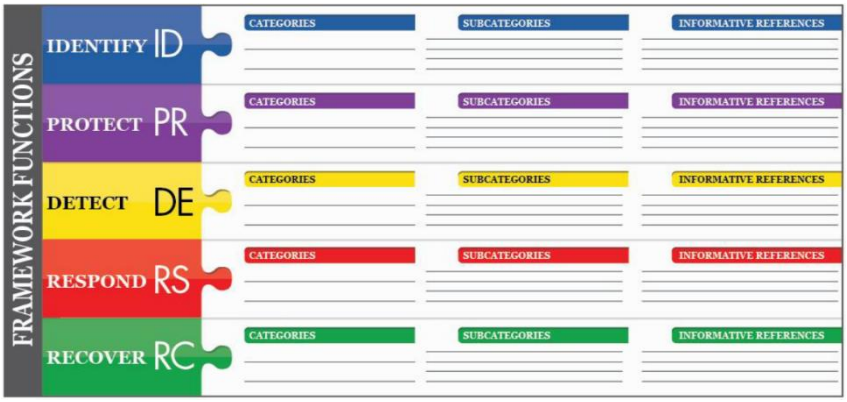

圖 7：NIST CSF 的 5 大功能示意圖

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

圖 8：NIST CSF 23 項類別

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

圖 9：NIST CSF 識別之子類別示意圖

(二) NIST 的隱私保護框架

講者 Katie Boecki 女士以簡報介紹 NIST 於 109 年 1 月 16 日發布「隱私框架 1.0 版」（NIST Privacy Framework Version 1.0），為促進資料的有效利用並兼顧對隱私權的保障，以風險管理（risk management）的概念為基礎，建構企業組織隱私管理框架。本隱私框架依循 NIST 於 107 年所提出的「健全關鍵基礎設施資安框架 1.1 版」（Framework for Improving Critical Infrastructure Cybersecurity Version 1.1）架構，框架由框架核心（Core）、狀態評估（Profile）與實施層級（Implementation Tier）等組成(詳

圖 10)，以利參考之組織能夠同時導入隱私與資安兩種框架。由隱私框架核心所建構的風險管理機制，透過狀態評估來判斷當前與設定目標的實施層級，進而完成組織在隱私保護上的具體流程與資源配置。

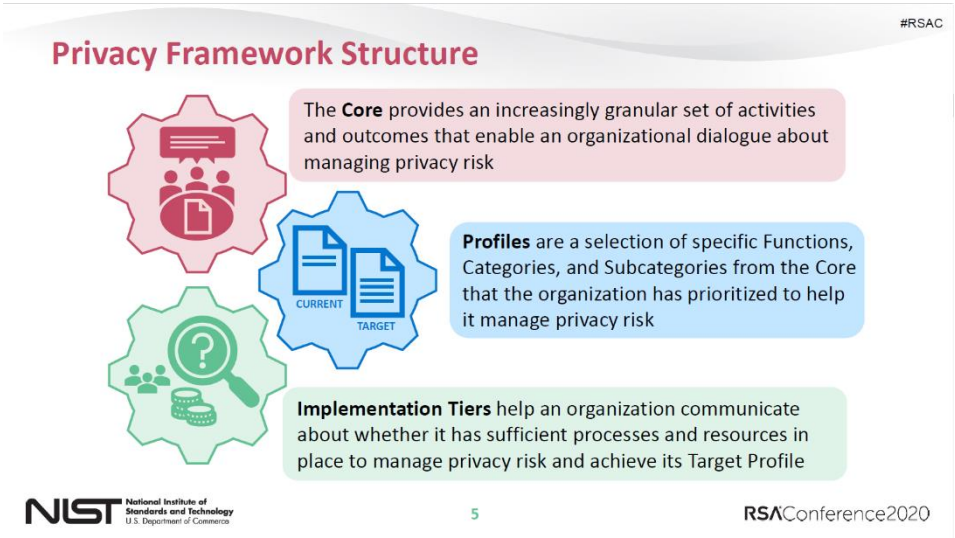

圖 10：NIST 隱私框架示意圖

NIST 基於透明、共識、兼顧公私利害關係人的程序訂定本隱私框架，用以促進開發者導入隱私設計思維（privacy by design），以及協助組織保護個人隱私，其目標包含產品或服務設計的倫理決策（ethical decision-making）及最小化隱私侵害以建立客戶信任；在當前與未來的產品或服務中，因應持續變化的技術與政策環境遵守對隱私保護義務；以及促進個人、企業夥伴、稽核者（assessor）與監管者（regulator）在隱私權保護實踐上的溝通與合作(圖 11)。

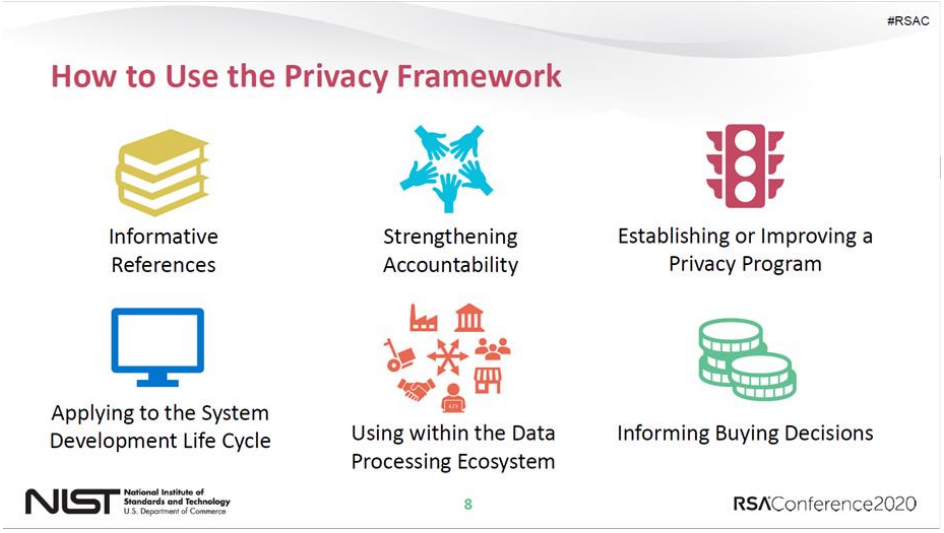

圖 11：NIST 隱私框架應用示意圖

NIST 表示本隱私框架不具備法律效果，僅是 NIST 協助企業於數位環境下導入隱私管理制度的參考工具，企業或組織可基於本隱私框架靈活應用於多樣化的隱私需求，並掌握其產品或服務所含隱私侵害風險，及識別隱私相關法律規範，包含加州消費者隱私法（California Consumer Privacy Act）與歐盟資料保護一般規則（General Data Protection Regulation, GDPR）等，以便可提出更具創新性與有效性的解決方案，及有效因應 AI 與物聯網技術的市場發展趨勢。

三、參加資安相關演講與小組討論會

本次 RSA 會議共邀請 700 多位講者參與數百場次主題式演講、相似議題會議、教學課程、研討會及個案探討等型式活動，報告人本次參與會議著重在 5G、IoT 等資安領域發展會議之觀察。

(一) 以威脅建模探討 5G 資安

5G 行動寬頻技術具有高頻寬(20Gbps)、低延遲(<=1ms)及可巨量裝置(每平方公里可容納 1 百萬裝置)連接的優勢(圖 12)。但在 5G 網路新技術組件及其提供新服務模式中，其新架構的網路切片(Network Slicing)、軟體定義網路(Software-Defined Networking, SDN)及邊界多重接取運算(Multi-access Edge Computing, MEC)等功能(圖 13)，若未做好資安管控將為 5G 網路引入更多資安風險，阻礙新網路架構優勢所提供創新服務的發展。講者於會議中更進一步以世界銀行集團開發的威脅模型為例，全面分析 5G 生態系統中的風險(圖 14)，並討論可緩解威脅的措施(圖 15)。

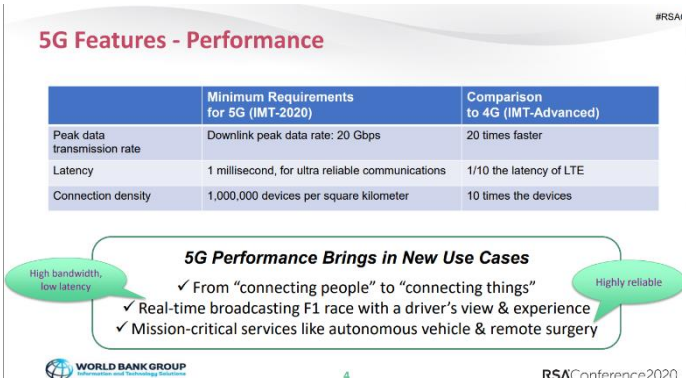

圖 12：5G 系統效能示意圖

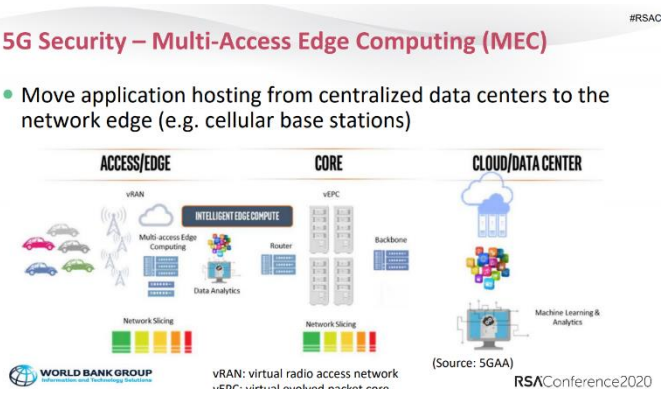

圖 13：邊界多重接取運算示意圖

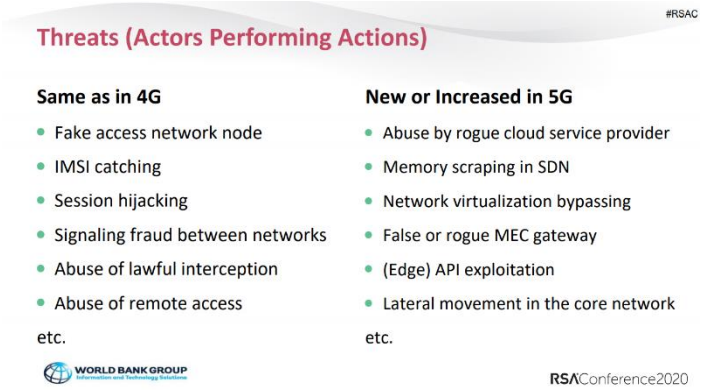

圖 14：5G 新增威脅種類

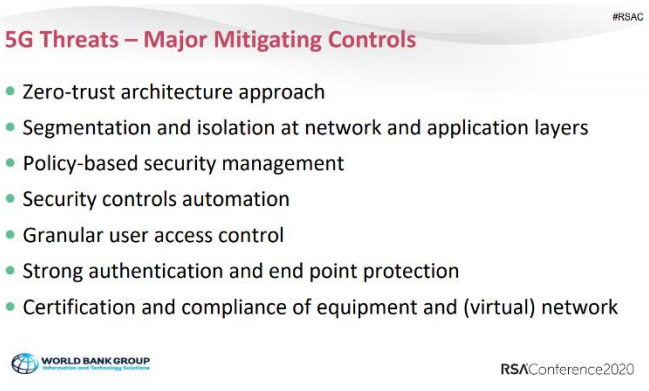

圖 15：降低 5G 資安威脅的控制措施

(二) 5G 信任模型：針對 CSP 的建議和最佳實踐

演講從 5G 系統的安全性和信任模型切入，探討為什麼 5G 系統安全性需要具備靈活性？ 5G 的新安全範例和方法是什麼，它們與 4G 有何不同？ 在 5G 安全中如何利用 AI 等最新技術？整合業務流程和自動化的最佳實踐和建議是什麼？有什麼標準？等議題，以提供 5G 系統服務業者(Communicaitons Service Providers, CSPs)有效建立 5G 資安防護。

講者認為 5G 已從傳統 4G 提供用戶行動服務，走向更多元的服務型態及更不同價值鏈之服務，如大量 M2M、IoT 及雲端等服務。另外以往行動通訊系統隨著新技術引進不斷提升網路安全之機制，例如 4G 比 3G 更好,3G 又比 2G 更好的資安機制，因 5G 網路開放架構與 4G 網路封閉架構的重大差異，如 SDN、Slicing serive 及 MEC 等許多 IT 技術溶入通訊網路中，使該網路提供者(CSP)將面對更多的資安風險需要被考慮及面對。講者以圖示向與會者說明 5G 網路之資安需求將隨不同服務而有不同等級的變化(圖 16)，且 5G 通訊系統從初期與 4G 溶合之 NSA(Non-StandAlone)架構發展至走向純 5G SA(StandAlone)網路架構時，其面對各網路區塊之資安需求亦有所不同，如 3GPP(3^{rd} Generation Partnership Project)標準所述的 4G 及 5G 資安差異圖 17。講者表示為確保 CSP 業者提供安全的 5G 網路服務，建議各國監理者應考量對 5G 加強資安領域的監理，並可採全球一致且廣泛之資安標準及框架準則。講者並以 108 年 5 月 3 日全球 30 餘國政府代表於捷克布拉格所舉辦的 5G 資安會議為例，說明該會議共同倡議的 5G 資安建議，並分享給與會者參考(圖 18)。另講者建議 CSP 業者應就 5G 端對端服務所涉及網路

每一區塊部分，訂定相關資安措施(圖 19)。

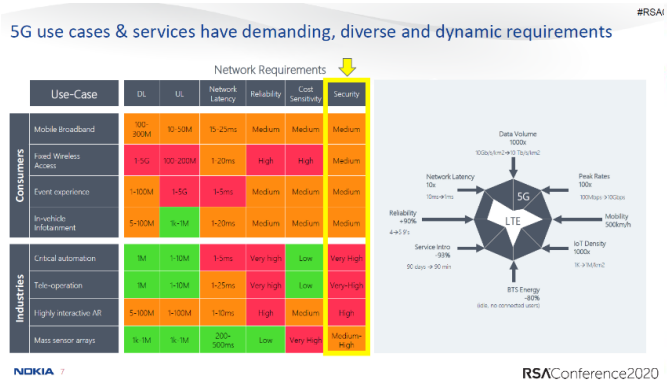

圖 16：不同服務不同資安需求示意圖

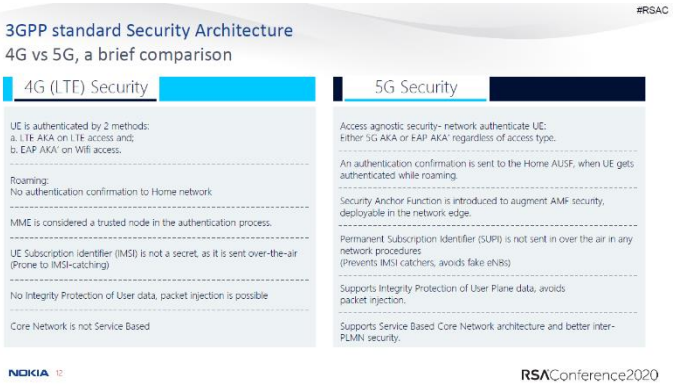

圖 17：3GPP 之 4G 與 5G 資安比較

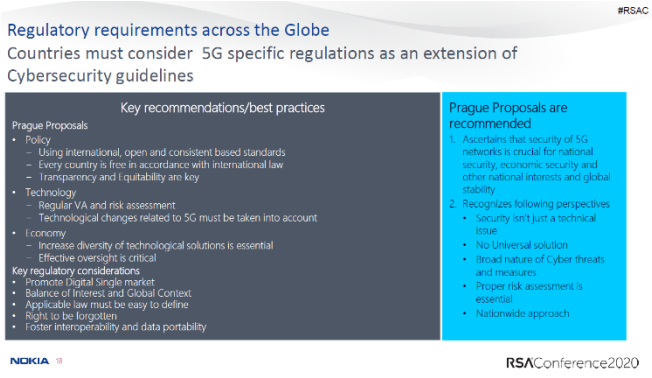

圖 18：布拉格 5G 資安倡議

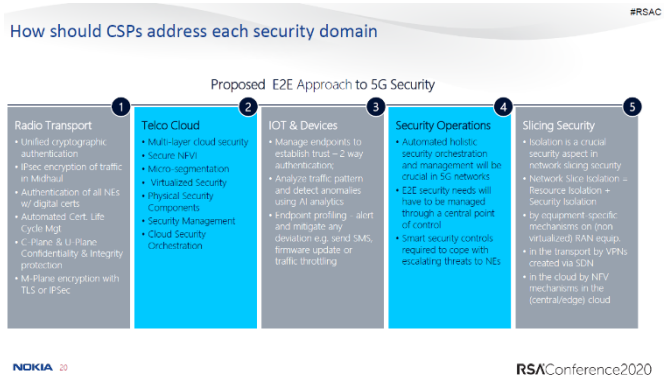

圖 19：CSP 在每一領域之資安課題

(三) 建立全面的 IoT 資安檢測方法

講者於本會議中重點介紹物聯網（IoT）產品生態系統(詳圖 20)，及如何建立有效的資安檢測方法。考量物聯網產品種類繁多，在進行 IoT 產品測試時，需要有明確的測試定義及程序(詳圖 21)。講者並以結構化測試程序，介紹 IoT 產品的測試方法及相關技術，使與會者掌握 IoT 產品資安檢測所面臨的挑戰。

講者表示 IoT 生態系包括內嵌式硬體、應用管理控制、雲端服務的 API 及資料儲存等。在進行 IoT 產品測試時，需先評估產品整體的架構及其可能的資安威脅，以利其資安檢測的建立。每一 IoT 產品的檢測方法主要可分為功能、評估、測試及分析的四個面向，各面向的重點摘要說明如下：

1. 功能面：包括檢測標準的建立及實施，其目標在掌握 IoT 產品的特徵、功能、模組及通訊方式。

2. 評估面：包括開源情資及賣方提供的資料。其開源情資含 FCC ID、使用手冊、電子零件資料表、產品歷史、軟體弱點及電子零件缺失等。
3. 測試面：共可包括雲端及網頁測試、應用管理控制測試、網路測試、內嵌硬體測試、韌體分析測試及無線電測試等。
4. 分析面：則從資安(含機敏性、完整性及可用性)、模組生態系及可建立延伸的測試概念。

講者表示要進行 IoT 產品檢測，需要建立檢測實驗室及相關檢測技術。其基本的檢測技術包括孰悉行動裝置作業系統(如 Android、iOS)、網頁服務及 API、網路與無線 WiFi 的檢測技術，並應有持續不斷的學習態度(詳圖 22)。另外，檢測實驗室應包括快閃記憶體讀取機、焊接器材、電路分析工具、放大鏡、手工具及充裕的預算等器材及資金(詳圖 23)。

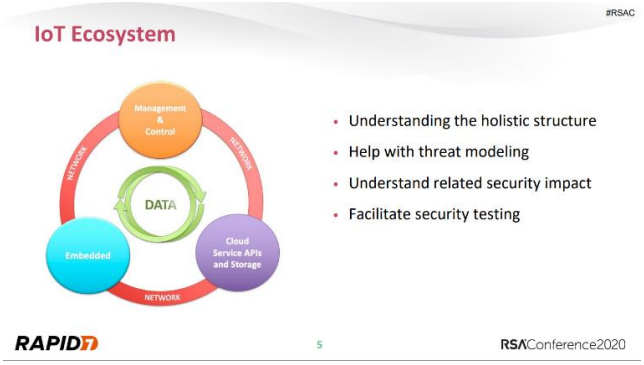

圖 20：IoT 生態系示意圖

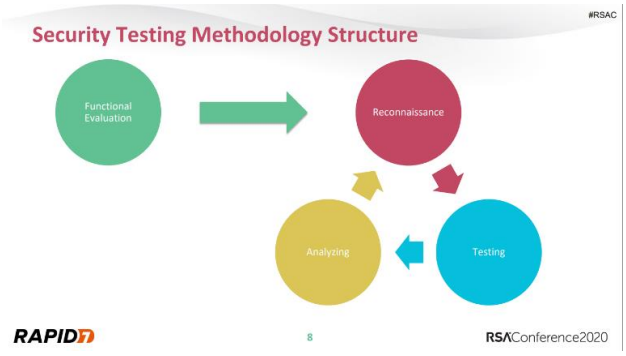

圖 21：資安檢測架構示意圖

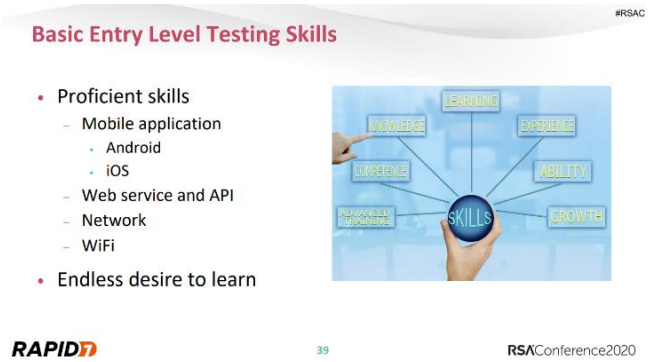

圖 22：檢測技術示意圖

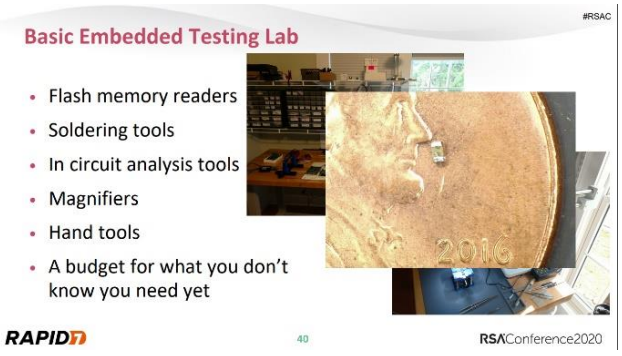

圖 23：檢測實驗室基本配備示意圖

(四) **物聯網存取管理-使用 MUD 協定**

本會議採專家座談方式舉行，會議邀請 NIST、有線電視實驗室、大學教授及企業家等公、私部門代表分享及探討各領域在 IoT 的使用情況，以蒐集及歸納 IoT 產品最佳的資安措施。會議並以跨領域合作模式，探討產品製造商使用說明規範（MUD,RFC 8520）的概念，以驗證對 IoT 設備存取管理的實施。

主持人以烤箱及印表機連線的資安威脅說明當前 IoT 產品發展趨勢，並就與會者對 IoT 的資安認知進行口頭問卷調查，以驗證說明一般使用者無法有效掌握 IoT 產品的資安威脅。因此 IoT 的資安標準就需要有公權力的介入，其中 NIST 最具重要角色。NIST 代表表示其機構任務之一，就是在確保資訊關鍵基礎設施的安全，並舉例說明其在 IoT 資安領域已發布 NISTIR 8228、8259 及 NIST SPECIAL PUBLICATION 1800-15A,B,C 等標準及文件(詳圖 24 及 25)，以提供 IoT 產品製造商、IoT 資安管理者建立 IoT 資安防護措施，降低 IoT 使用者在網路上使用其 IoT 設施被駭風險。另與談者從經濟發展議題探討，說明其研究發現當產品製造商提供消費者更完整的 IoT 資安風險資訊時，一般消費者願意付更多錢買具相同使用功能但更具有資安保障的產品。

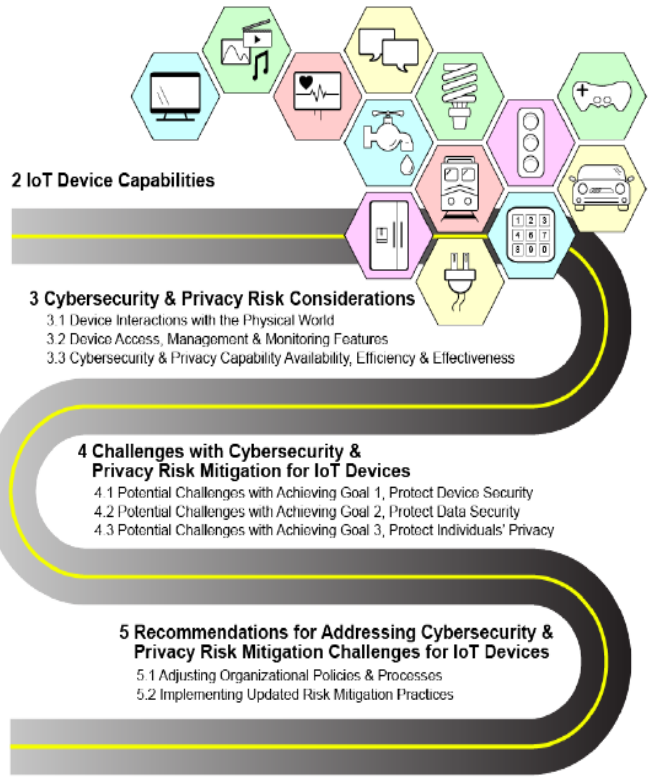

圖 24：NISTIR 8228 標準章節架構

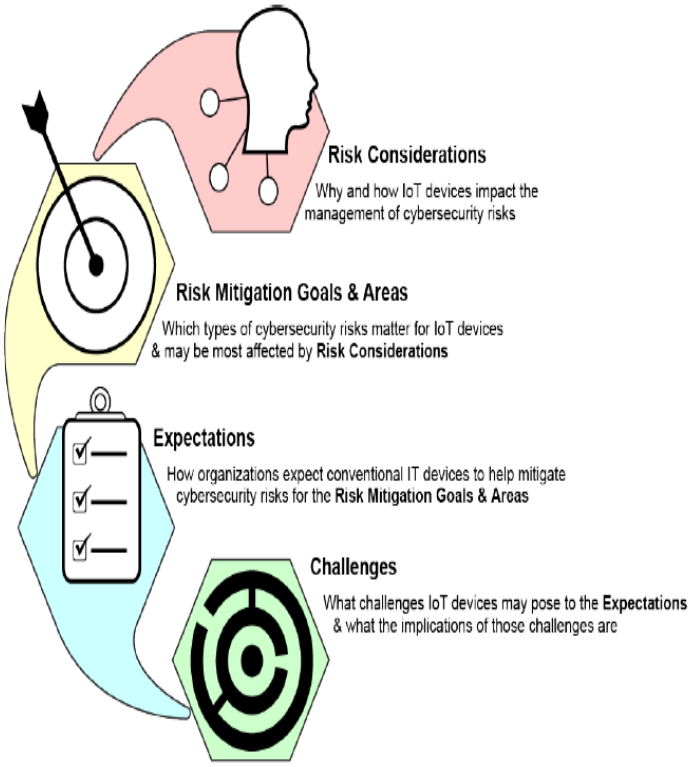

圖 25：NISTIR 829 標準與 8223 的關聯性

註：Internet Engineering Task Force (IETF)於 108 年提出 Request for Comments (RFC) 8520 標準，稱為 MUD（Manufacturer Usage Description），係規範產品功能在網路存取控制的協定。其運作方式是由製造商在產品出廠前，先將產品在 MUD 平台註冊，以建立 SDK 嵌入連結機制。產品一旦連網就會主動與 MUD 控制器平台互動，以確認該產品功能需要的網路接取方式。

四、參訪美商 SPLUNK 公司

美國在臺協會於 28 日上午安排我國參訪團參訪在資安大數據分析領域，具有一定市場規模之美商 SPLUNK 公司，並由該公司宋海燕資深副總裁等人接待(圖 26)及介紹該公司資安產品發展趨勢。

圖 26：我國資安參訪團參訪美商 SPLUNK 公司總部合影

(一) 公司簡介

SPLUNK 公司成立於 92 年 10 月，其公司總部設在加州舊金山，全球約有 5,800 員工及取得 371 項專利，108 年全球約有 18,000 客戶及約 18 億美金之營業額。該公司為一大數據分析資安公司，其提供的軟體平台可經由任何時間範圍內處理蒐集自各方之非結構性數據，並可將相關數據整併以提供客戶調查、監視、分析數據及採取行動等功能之整合服務。

(二) 資安產品發展

該公司表示資安市場趨勢已從以往與資料應用相關之資安防護策略，發展至為客戶提供一包括雲端及大數據分析的資安平臺防護策略。因此，該公司將其產品發展定位為資安的神經中樞(如圖 27)，以提供客戶最好的資安防護服務。

該公司並以雲世代的資安為例，分享其為公部門客戶白宮軍事辦公室(WHMO)提供該公司產品後實際增強及解決資安人力需求的問題。該公司表示其產品具有提供蒐集場域中各種感測器和 IT 設備警告訊息、以視圖方式將場域 10 餘個系統日誌資料進行蒐集分析，並就網路端至端的威脅及異常情況主動示警，以利資安分析人員得以及時處置及應變的整合能力。另 SPLUNK 亦提供客戶以網路圖示方式，協助客戶排除營運中 IT 設施的障礙。

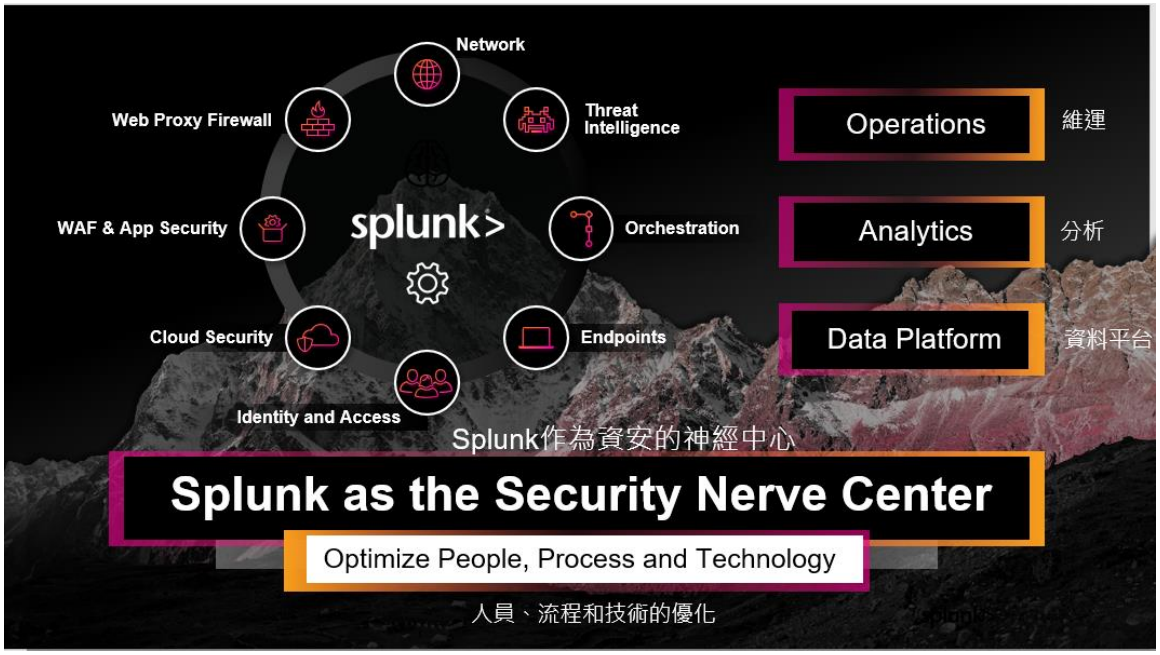

圖 27：SPLUNK 發展資安神經中樞的示意圖

參、心得及建議

一、RSA 會議部分

本次參加 RSA Conference 2020 會議發現美國政府極為重視該會議，國家安全局、聯邦調查局、國土安全部的網路與基礎設施安全局，均在展場處設點舉辦招募、教育及媒合人才等活動。另主辦單位亦盡力提供與會者最佳的會場服務，以維持其為國際資安重要會議活動場域之一的形象。本次會議觀察心得與建議如下：

(一) 建議持續關注國際 5G 系統資安標準發展，督促業者加強資安防護

NCC 已於今(109)年初完成行動寬頻業務 5G 頻率釋出作業，共有 5 家既有行動寬頻業者分別取得 3GHZ 及 28GHz 頻段的不同頻段頻率執照，且已有 5G 頻率得標者表示將於第 3 季規劃提供國人 5G 行動寬頻服務。如本次會議 NOKIA 專家於會中分享 5G 資安的建議，NCC 為確保經營者於 5G 開臺時，即提供消費者安全可靠的行動寬頻通訊環境，於去年年中修法時，即參考 NIST 的 CSF 資安框架、ITU 及 3GPP 的資安規範，除於開放受理申請時，要求申請者應先提出資通安全維護規劃外，業者得標後依規定應提出資通安全維護計畫，並規範業者要符合 17 項資安要求。NCC 為加速得標者完全掌握其提供 5G 網路服務之資安風險，及提早實施相關資安防護控制措施，於今年 1 月中旬發布 5G 系統資安維護計畫框架參考文件，以引導得標者全面評估 5G 系統資安風險，並提出自已的 5G 系統資安維護計畫。NCC 另要求業者需先取得計畫審核通過後才能辦理系統架設，系統完成建設需通過資安審驗後，始具開臺條件。因此，建議業者未來營運 5G 網路提供消費者行動寬頻服務時，除依法規要求落實資安防護外，亦可參考國際 5G 資安標準發展，持續不斷精進 5G 資安防護措施，在制度面完備、管理面到位及技術面齊全下，強化 5G 網路營運韌性，以提供消費者安全且服務不中斷的行動寬頻使用環境。

(二) 建議持續推廣 IoT 資安檢測，降低民眾使用 IoT 產品之資安風險

NCC 為推動連接電信網路之物聯網資安檢測認證標準，自 107 年 6 月起即與經濟部合作共同發布相關資安驗證標章制度，以帶動我國 IoT 產品之資安水準。該計畫推動至去(108)年底已有 8 家取得物聯網資安認可實驗室，並有 9 家 IoT 產

品製造業者之 22 款產品，分別通過不同等級之資安檢測，取得資安合格標章，為消費者提供更有資安保障及完整資安訊息的 IoT 產品。另從本次會議亦可看到專家分享 IoT 產品檢測機制及檢測重點項目與方法，建議我國相關機關(構)可適時就我國 IoT 檢測生態系發展成果，於國際會議與其他國家交流分享，為我國通過 IoT 資安檢測產品，創造更高利基及外銷機會。

二、美國 AIT 安排參訪部分

(一)把握與美國官方及民間資安公司之互動機會

本次會議承蒙 AIT 商務組代表協助，於 RSA 會議期間於會場外另安排與國家標準暨技術研究院及美商 SPLUNK 公司等機關(公司)交流，除可適時掌握美國政府機關推動資安標準及美商公司提供資安產品發展外，亦有利國內相關單位建立跨國可信賴資安聯繫管道。另 NIST 發布的通則性資安框架、IoT 資安規範及個人隱私保護建議等文件，皆具參考價值，值得我國相關機關修訂資安相關規定或標準之參考。

(二) 機關持續強化網路資安防護韌性，確保服務營運不中斷

近期國內接連發生幾件駭客攻擊(如報載 5 月 4 日至 5 日期間中油、台塑、力成業者遭到駭客惡意攻擊，造成重要檔案無法開啟、系統停擺，及被要求交付贖金等情事。)，及竊取敏感資訊(如報載總統府疑遭駭客入侵造成部分資料外洩，刑事局受理總統府報案後處理中)等事件，顯示公、私部門皆有再強化資安防護的成長空間。

以中油為例，因其係屬我國八大國家關鍵基礎設施之一，如何做好資安防護降低駭客惡意攻擊之資安事件，已是迫不及待亟需面對的資安課題。要做好資安防護整備，建議可從組織的資安政策、目標、核心業務、資安人力組織、資安防護範圍、資產盤點、風險評估、控制措施、實施計畫及稽核等面向進行盤點，再從制度面、管理面及技術面等 3 個面向分別交叉檢視，以促使組織的資安內規及法遵更完備，組織的資安人力及運作架構更到位，及資安偵測及防護設施建置更

齊全，並在組織不斷推動 PDCA 活動及稽核程序中，全面提升組織之資安防護等級。另參訪美商 SPLUNK 資安公司，令人印象深刻的是該公司專家以美國公部門 WHMO 為例，分享其協助公部門在技術面建置更齊全的偵測防護措施所產生成本效益及應變成效，值得我國公部門資安防護規劃參考。

肆、參考資料

[1] USA 2020 | RSA Conference：https://www.rsaconference.com/usa

[2] NIST NISTIR 8228：https://csrc.nist.gov/publications/detail/nistir/8228/final

[3] NIST NISTIR 8259(Draft)：https://csrc.nist.gov/publications/detail/nistir/8259/draft

[4] NIST Privacy Framework Version 1.0：
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

[5] NIST SPECIAL PUBLICATION 1800-15A,B,C：
https://www.nccoe.nist.gov/publication/1800-15/VolA/index.html

[6] IETF RFC 8520：https://tools.ietf.org/html/rfc8520