出國報告(出國類別：其他(國際會議))

國際資訊安全會議
(RSA Conference 2019)
出國報告

服務機關： 行政院(國土安全辦公室、資通安全處)
國家通訊傳播委員會(基礎設施事務處)

姓名職稱： 黃俊泰 主任
周智禾 科長
余柏賢 設計師
吳銘仁 簡任技正

派赴國家： 美國 (舊金山)

出國期間： 108 年 3 月 4 日至 108 年 3 月 8 日

報告日期： 108 年 5 月 16 日

摘要

本次參加 RSA Conference 2019 會議，除了瞭解到國際上最重要的資安議題及攻擊趨勢，也藉由與不同國家廠商的資安人員交流，以瞭解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，其扮演著整合的角色，讓國際間各不同領域之資安專業人才齊聚一堂，共同探討網路安全問題以及新興科技。

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、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、國土安全部的網路與基礎設施安全局局長都親自出席擔任講座。

RSA Conference 2019 會議於本(108)年 3 月 4 日至 3 月 8 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，物聯網、工業控制系統安全及行動裝置駭侵技術的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會議行程，除邀請美國政府機構國家科學技術研究院(NIST)、北加州地區情報中心(NCRIC)、舊金山市警局官員於聯邦商務部舊金山代表處會談外，另亦安排民間 F5 等公司與我國與會人員交流，分享美國資通技術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(3 月 4 日至 3 月 8 日)的 RSA Conference 2019 會議，在會議中觀摩及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漏洞攻擊手法、資安技術及各種不同領域的新興議題與挑戰，其中包含了雲端服務、行動裝置的安全性、物聯網、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。

本次參加 RSA Conference 2019 會議的目的包括：

一、觀摩美國政府國土安全與資安政策與措施

美國國土安全部、聯邦調查局、國安局、商務部均積極參與 RSA 大會，辦理專題演講、小組討論會及擺設攤位，藉機說明美國面臨的資安風險與威脅，宣導相關政策與措施，是近距離觀察美國政府對國土安全與資安所採取的政策與措施的最佳機會，有許多值得借鏡的地方。

二、掌握最新的資安動態

藉由 RSA 專題演講、小組討論會，瞭解最新資安動態、產業脈動、攻擊手法及偵測分析技術，並瞭解於 RSA Conference 2019 會議參展的各家資安廠商所提供的服務及技術亮點，以此強化本身資安知識。

三、瞭解最新資安研究成果

掌握國際間各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研究成果，如透過某些工具或架構可更迅速、準確識別組織中的弱點，並更有效的改善或防止弱點遭駭客利用，又或是透過現有工具進行反偵查任務，以保護組織本身資訊安全。

四、與美國官員互動，建立交流管道

美國在臺協會(AIT)馬奎立商務官及陳玫芳商務經理，另協助於同期間安排參訪拜會活動，包括 NIST-SCADA 資安規範分享(3/5)、太平洋瓦斯及電力公司(PG&E)-如何因應關鍵基礎建設中新世代威脅分享(3/6)、美國 F5 公司-加密流量解析及安全控管聯防機制研討會(3/7)及與 NCRIC 官員訪談-關鍵基礎設施合作及資訊分享機制(3/8)。

貳、活動紀要

一、概述

(一)會議活動情形

RSA Conference 2019 會議於本年 3 月 4 日至 3 月 8 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：

- ✓ 計有 42,500 名與會者，31 場主題演講、621 場小組討論會、740 名講者、700 家參展商。(相關議程請參閱附件及 RSA 網站)
- ✓ 創新沙盒比賽：最具創新性的創業公司 Axonius 獲首獎。
- ✓ 第 28 屆年度 RSA 會議。
- ✓ 數學領域傑出獎頒獎：獲獎者 Tal Rabin, manager of cryptographic research, Thomas J. Watson Research Center。
- ✓ CISO 新手訓練營：一天半，促進高級安全領導人之間的對話。
- ✓ RSAC 學院：兩天，為大學生和畢業生探索職業選擇，並媒合工作機會。
- ✓ 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 2019 會議-3 月 4 日(一)議程

MONDAY EVENTS & ACTIVITIES

MONDAY

8:30 AM – 5:40 PM — **SEMINARS – FULL CONFERENCE & DISCOVER PASS HOLDERS ONLY**
See following pages for details and room locations.

8:00 AM – 5:00 PM — **SEMINARS – OPEN TO ALL BADGE TYPES**
See following pages for details and room locations.

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

11:00 AM – 12:00 PM — **TWITTER CHAT**
Sponsored by: National Cybersecurity Alliance
Building a Better Today for a More Secure Tomorrow
Follow us on Twitter and use *#ChatSTC* and *#RSAC* to join!

1:30 PM – 4:30 PM — **RSAC INNOVATION SANDBOX CONTEST**
Marriott Yerba Buena
Exclusive RSAC Innovation Sandbox Media Sponsor: WSJ PRO CYBERSECURITY
The RSAC Innovation Sandbox Contest has crowned innovative companies who build cutting-edge technologies to minimize infosec risk for the past 14 years. Witness the 2019 Top 10 Finalists battle it out for the coveted title of "Most Innovative Startup." See page 18 for a detailed agenda.

4:00 PM – 5:00 PM — **FIRST-TIMERS ORIENTATION & NETWORKING RECEPTION**
Marriott Golden Gate A
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.

4:30 PM – 6:00 PM — **RSAC WOMEN'S LEADERSHIP CELEBRATION RECEPTION**
Moscone South 303
Join us in celebrating the contributions and rich history of women in science and technology. Hosted with our planning partners: Women's Society of Cyberjutsu, Executive Women's Forum on Information Security, Risk Management and Privacy (EWF), The Diana Initiative, Women in Security and Privacy (WISP) and Women in CyberSecurity (WiCyS). All RSA Conference attendees are welcome to attend.

5:00 PM – 7:00 PM — **RSAC SECURITY OPERATIONS CENTER**
Moscone South Lower Level
Sponsored by: cisco RSA
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.

5:00 PM – 7:00 PM — **WELCOME RECEPTION**
Expos
Join your peers in the Expo while kicking off RSA Conference in style at the Welcome Reception. Enjoy drinks and light fare from 5 – 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.

圖 1　RSA Conference 2019 會議議程(一)

2. RSA Conference 2019 會議-3 月 5 日(二)議程

TUESDAY EVENTS & ACTIVITIES

TUESDAY

6:30 AM – 8:00 AM | Moscone West Level 2
CONTINENTAL BREAKFAST*
Full Conference Pass holders, grab breakfast and then head directly to your chosen keynote viewing location.

KEYNOTES**
Keynote abstracts can be found on pages 30 – 31.

8:00 AM | West Stage Keynotes
Opening

8:10 AM | West Stage Keynotes
The Trust Landscape
***Rohit Ghai**, President, RSA; **Niloofar Razi Howe**, Cybersecurity Strategist and Entrepreneur*

8:35 AM | West Stage Keynotes
Lightning in a Bottle, or Burning Down the House?
***Dr. Celeste Fralick**, Chief Data Scientist, McAfee, LLC; **Steve Grobman**, Senior Vice President and Chief Technology Officer, McAfee, LLC*

8:55 AM | West Street Level
Rise of the Machines: Staying Ahead of the Next Threat
***Liz Centoni**, Senior Vice President | General Manager Cisco IoT, Cisco; **Matt Watchinski**, Vice President, Global Threat Intelligence Group, Talos, Cisco*

9:20 AM | West Street Level
The Cryptographers' Panel
*MODERATOR: **Zulfikar Ramzan, Ph.D.**, Chief Technology Officer, RSA*
*PANELISTS: **Whitfield Diffie**, Cryptographer and Security Expert, Cryptomathic; **Shafi Goldwasser**, Director, Simons Institute for the Theory of Computing; **Ronald Rivest**, Professor, Massachusetts Institute of Technology; **Adi Shamir**, Borman Professor of Computer Science, The Weizmann Institute, Israel*

10:05 AM | West Street Level
The FBI: At the Heart of Combating Cyberthreats
***Susan Hennessey**, Senior Fellow, Governance Studies, The Brookings Institution and Executive Editor, Lawfare; **Christopher A. Wray**, Director, Federal Bureau of Investigation*

11:00 AM | South Esplanade
Top 10 Ways to Make Hackers Excited: About the Shortcuts Not Worth Taking
***Paula Januszkiewicz**, Chief Executive Officer, CQURE*

1:00 PM | South Esplanade
A Cloud Security Architecture Workshop
***Dave Shackleford**, Sr. Instructor, SANS Institute*

2:20 PM | South Esplanade
Security at 36,000 Feet!
***Emily Heath**, Vice President and Chief Information Officer, United Airlines*

3:40 PM | South Esplanade
Lessons Learned from 30+ Years of Security Awareness Efforts
***Ira Winkler**, President, Secure Mentem*

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

10:00 AM – 6:00 PM | Moscone South Lower Level
RSAC SECURITY OPERATIONS CENTER
Sponsored by: cisco RSA
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.

10:00 AM – 6:00 PM | Moscone North & South Lower Level
EXPO
The RSA Conference Expo will give you the opportunity to interact with an impressive breadth of information security exhibitors and sponsors.

10:20 AM – 5:30 PM | Moscone North & South Lower Level
EXPO BRIEFING CENTER
See following pages for abstracts and a complete schedule on pages 115 – 118.

11:00 AM – 2:00 PM | Howard Street, Mission Street
STREET EATS
With options for all tastes, stop by any of our food trucks on Mission Street or Howard Street. Available to all pass types and both cash and credit cards are accepted.

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

44

= Top-rated speaker.

圖 2　RSA Conference 2019 會議議程(二)

TUESDAY EVENTS & ACTIVITIES

Hours Vary by Location

LAW TRACK SESSIONS*

Marriott Nob Hill A, 11:00 AM – 4:30 PM; Moscone South 201, 5:00 PM – 5:50 PM

See detailed information on following pages for descriptions.

2:20 PM – 4:20 PM

Moscone West 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 Lab on your schedule, so pick carefully from our 20 great offerings. ***Note: Press is not permitted in Lab sessions.***

4:00 PM – 6:30 PM

Marriott RSAC Sandbox

RSAC CYBREW CAFÉ

The RSAC Cybrew Café, our full-service coffee bar, will be serving your favorite beverages.

4:00 PM – 4:45 PM

Marriott Yerba Buena 8

RSAC LAUNCH PAD***

RSAC Launch Pad is designed to give new talent a platform to share their brilliant industry solutions. Watch three selected participants give a 10-minute pitch on their groundbreaking products to a panel of leading security venture capitalists. And see who walks away with investments that could take their company to the next level.

4:45 PM – 6:30 PM

Marriott Yerba Buena 8

RSAC SANDBOX***

The RSA Conference Sandbox is full of hands-on interactive experiences to test your infosec skills.

Exclusive RSAC Sandbox Media Sponsor:

4:45 PM – 6:30 PM

Marriott Yerba Buena 9

RSAC EARLY STAGE EXPO***

The RSAC Early Stage Expo is the perfect megaphone for emerging infosec startups. Located in the Marriott Marquis, meet over 50 of the industry's most promising newcomers and learn about their innovative products and solutions.

Exclusive RSAC Early Stage Expo Media Sponsor:

crunchbase

4:45 PM – 6:30 PM

Marriott RSAC Sandbox & RSAC Early Stage Expo

CYBEER OPS NETWORKING RECEPTION & INTERNATIONAL MEET-UP ***

Delight in local California craft beers and non-alcoholic drinks as you mingle with peers and RSAC friends from around the world. CyBEER Ops opens RSAC Sandbox, where you can check out up and coming startups and the RSAC IoT Village, ICS Village and Wireless Village Sandboxes.

** Event is free for Full Conference and Tuesday Full Conference One-Day Pass holders age 21 and over as well as Press. All other badge holders can purchase tickets through registration for a fee of $25. Event access is limited and is on a first come, first served basis.*

6:00 PM – 9:00 PM

Marriott SoMa

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 Internet Society/Online Trust Alliance and the Cyber Threat Alliance (CTA) invite you to join us for the ninth 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 – 9:30 PM

Moscone West Level 2

RSAC AFTER HOURS: GAME NIGHT**

As a cybersecurity all-star, you'll enter RSAC After Hours: Game Night with VIP treatment. Then it's off to the races. In the Full Court, you'll go head to head with other industry players in our arcade and game hall. Then take a load off in the sports lounge and bar, complete with a live DJ and tailgate-themed refreshments. And at 7:30 PM, the night really gets going as the Celtics face off against the Warriors—live and on the big screen.

Open to Full Conference and Discover Pass holders. Choose one of the RSAC After Hours events on Tuesday, Wednesday or Thursday nights of Conference. Space is limited so make sure to reserve a seat.

= Networking event.

** Open to Full Conference Pass holders only.*
*** Open to Full Conference and Discover Pass holders only.*
**** Open to Full Conference Pass holders, Press and CyBEER Ops ticket holders only.*

TUESDAY

45

圖 2　RSA Conference 2019 會議議程(二)

3. RSA Conference 2019 會議-3 月 6 日(三)議程

WEDNESDAY EVENTS & ACTIVITIES

6:00 AM – 7:00 AM | Moscone West Level 2 Alcove
POWER PAUSE— MINDFULNESS & MOVEMENT*
This yoga class and meditation session is designed for all levels from beginners to advanced practitioners.

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

7:00 AM – 7:50 AM & 12:40 PM – 1:30 PM | Moscone West Level 3
BIRDS OF A FEATHER*
Grab your breakfast or lunch and bring it to the discussion rooms. Some topics are pre-defined and led by speakers, others will develop organically; by design, this is loosely structured to give you an opportunity to network and set the agenda for discussions of interest to you. ***Note: Press is not permitted in Birds of a Feather sessions.***

7:00 AM – 8:00 AM | Moscone West Level 2 Alcove
FIRST-TIMERS MEET-UP*
Enjoy this time to regroup, share takeaways and, of course, caffeinate.

KEYNOTES
Keynote abstracts can be found on pages 32 – 33.

8:00 AM – 8:50 AM | South Esplanade
Hacking Exposed: LIVE—Bypassing NextGen
***Stuart McClure**, Chairman and Chief Executive Officer, Cylance Inc.; **Brian Robison**, Chief Evangelist, Cylance Inc.*

9:20 AM – 10:10 AM | South Esplanade
The Role of Security Technologists in Public Policy
***Bruce Schneier**, Fellow and Lecturer, Harvard Kennedy School*

10:30 AM – 10:55 AM | West Street Level
The Power of People: Amplifying Our Human Capacity through Technology and Community
***Ann Johnson**, Corporate Vice President, Cybersecurity Solutions Group, Microsoft*

10:55 AM – 11:15 AM | West Street Level
Palo Alto Networks and Arista Networks CEOs Reveal Secrets to a Successful Cloud Journey
***Nikesh Arora**, Chief Executive Officer and Chairman, Palo Alto Networks; **Jayshree Ullal**, President and Chief Executive Officer, Arista Networks*

11:15 AM – 11:55 AM | West Street Level
Weaponization of the Internet
MODERATOR: ***Ted Schlein**, General Partner, Kleiner Perkins*
PANELISTS: ***Nathaniel Gleicher**, Head of Cyber Security, Facebook; **Del Harvey**, Vice President, Trust and Safety, Twitter; **Robert Joyce**, Senior Advisor, National Security Agency; **Peter Warren Singer**, Strategist, New America*

1:30 PM – 2:20 PM | South Esplanade
Strategic Competition—The Rise of Persistent Presence and Innovation
***Olivia Gazis**, Intelligence and National Security Reporter, CBS News; **General Paul Nakasone**, United States Army, Commander, United States Cyber Command, Director, National Security Agency, Chief, Central Security Service*

2:50 PM – 3:40 PM | South Esplanade
From Dystopia to Opportunity: Stories from the Future of Cybersecurity
***Dr. Amit Elazari Bar On**, Director, Global Cybersecurity Policy, Intel Corporation, and Lecturer, UC Berkeley School of Information (MICS); **Keren Elazari**, Analyst & Researcher, K3r3n3.com*

4:00 PM – 4:25 PM | West Street Level
A View from the Front Lines of Cybersecurity
***Sandra Joyce**, Senior Vice President, Global Intelligence, FireEye; **Kevin Mandia**, Chief Executive Officer, FireEye*

4:25 PM – 4:50 PM | West Street Level
A Conversation with Donna Brazile and Mary Matalin
***Donna Brazile**, Veteran Democratic Political Strategist, Adjunct Professor, Author and Syndicated Columnist; **Mary Matalin**, Celebrated Conservative Voice and Former Presidential Advisor*

4:50 PM – 5:15 PM | West Street Level
How Technology and Innovative Approaches Can Transform Your Organization
***Megan Smith**, Chief Executive Officer, shift7, Third Chief Technology Officer of the United States (2014 – 2017)*

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

8:00 AM – 12:50 PM & 1:30 PM – 5:00 PM | Marriott Nob Hill A
LAW TRACK SESSIONS*
See detailed information on following pages for descriptions.

8:00 AM – 11:20 AM & 1:30 PM – 4:30 PM | Moscone West 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 Lab on your schedule, so pick carefully from our 20 great offerings. ***Note: Press is not permitted in Lab sessions.***

WEDNESDAY

= Top-rated speaker.

圖 3　RSA Conference 2019 會議議程(三)

WEDNESDAY EVENTS & ACTIVITIES

8:00 AM – 4:00 PM | Marriott Yerba Buena 8

RSAC SANDBOX

The RSA Conference Sandbox is full of hands-on interactive experiences to test your infosec skills.

Exclusive RSAC Sandbox Media Sponsor:

8:00 AM – 4:00 PM | Marriott, RSAC Sandbox

RSAC CYBREW CAFÉ

A full-service coffee bar.

8:00 AM – 4:00 PM | Marriott Yerba Buena 9

RSAC EARLY STAGE EXPO

The RSAC Early Stage Expo is the perfect megaphone for emerging infosec startups. Meet over 50 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 180 – 185).

Exclusive RSAC Early Stage Expo Media Sponsor:

orunohbase

8:00 AM – 5:00 PM | Moscone West Street Level

BROADCAST ALLEY

Watch top security publications shoot live and record exclusive interviews.

9:20 AM – 12:50 PM & 1:30 PM – 5:00 PM | Moscone South Level 3

PEER2PEER SESSIONS*

P2P sessions enable groups of no more than 30 people that share a common interest to come together and productively explore a specific security topic, facilitated by an experienced practitioner. ***Note: Press is not allowed in Peer2Peer sessions.***

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 2019 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 following pages for abstracts and a complete schedule on pages 115–118.

11:00 AM – 2:00 PM | Howard Street, Mission Street

STREET EATS

With options for all tastes, Street Eats is the easy way to fuel up between sessions or get energized before your next keynote. Stop by any of our food trucks on Mission Street or Howard Street.

11:30 AM – 1:00 PM | Marriott Golden Gate B

EXECUTIVE WOMEN'S FORUM MEET & GREET AT RSA CONFERENCE 2019

The Executive Women's Forum and Accenture are hosting a Meet & Greet for all the amazing women attending RSA Conference 2019. 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. We look forward to meeting you!

**** All attendees will need an RSA Conference badge to access the Golden Gate level at the Marriott Marquis.***

2:00 PM – 3:00 PM | Moscone West Level 2

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 2019!

4:30 PM – 6:00 PM | Moscone North & South Lower Levels

EXPO PUB CRAWL

Enjoy your choice of complimentary beer, wine and non-alcoholic beverages as you visit sponsoring companies' booths to learn about their latest products, services and innovations. Located at select sponsor booths within both halls.

6:30 PM – 8:00 PM | Marriott Golden Gate B

RSAC AFTER HOURS: WHISKEY & WINE TASTING**

Kick off the night with a walk through the "underground cellar." Then, gather in the lounge to sip on an assortment of wines and whiskeys expertly selected from local vineyards and distilleries while soaking up the jazzy sounds of our live band. And keep the night going in our group tasting area, where you can mingle with other cybersecurity connoisseurs and raise a glass to another great year at RSA Conference.

Open to Full Conference and Discover Pass holders. Choose one of the RSAC After Hours events on Tuesday, Wednesday or Thursday nights of Conference. Space is limited so make sure to reserve a seat.

= Networking event. * Open to Full Conference Registrants only. ** Open to Full Conference and Discover Pass Registrants only.

圖 3　RSA Conference 2019 會議議程(三)

4. RSA Conference 2019 會議-3 月 7 日(四)議程

THURSDAY EVENTS & ACTIVITIES

6:00 AM – 7:00 AM
Moscone West Level 2 Alcove

POWER PAUSE—MINDFULNESS & MOVEMENT*

This yoga class and meditation session is designed for all levels from beginners to advanced practitioners.

7:00 AM – 8:00 AM
Various Locations

CONTINENTAL BREAKFAST*

Full Conference Pass holders, head directly to your chosen morning session. Breakfast is available in Moscone West Levels 2 & 3 and Moscone South Levels 2 & 3.

7:00 AM – 7:50 AM & 12:40 PM – 1:30 PM
Moscone West Level 3

BIRDS OF A FEATHER*

Grab your breakfast or lunch and bring it to the discussion rooms. Some topics are pre-defined and led by speakers, others will develop organically; by design, this is loosely structured to give you an opportunity to network and set the agenda for discussions of interest to you. ***Note: Press is not permitted in Birds of a Feather sessions.***

7:00 AM – 8:00 AM
Moscone West Level 2 Alcove

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.

KEYNOTES

Keynote abstracts can be found on pages 34 – 35.

8:00 AM – 8:50 AM
South Esplanade

Stress, Burnout and You: Fireside Chat with Dr. Christina Maslach
***Josh Corman**, Chief Security Officer, PTC; **Christina Maslach**, Professor of Psychology, Emerita, University of California, Berkeley*

9:20 AM – 10:10 AM
South Esplanade

Hacking Exposed: Hacking Macs
***Dmitri Alperovitch**, Co-Founder & Chief Technology Officer, CrowdStrike; **George Kurtz**, Chief Executive Officer, CrowdStrike*

10:30 AM – 10:55 AM
West Street Level

Stop Worrying about the Right Things
***Mary O'Brien**, General Manager, IBM Security; **Caleb Barlow**, Vice President, IBM Security, X-Force Threat Intelligence*

10:55 AM – 11:40 AM
West Street Level

The Five Most Dangerous New Attack Techniques and How to Counter Them
MODERATOR: ***Alan Paller**, Research Director and Founder, SANS Institute*
PANELISTS: ***Heather Mahalik**, Director of Forensics Engineering, ManTech, and Mobile Forensics Course Director, SANS Institute; **Ed Skoudis**, Instructor, SANS Institute; **Johannes Ullrich**, Dean of Research, SANS Technology Institute*

2:50 PM – 3:40 PM
South Esplanade

The Future of Data Protection: Adapting to the Privacy Imperative
MODERATOR: ***J. Trevor Hughes**, President & Chief Executive Officer, IAPP*
PANELISTS: ***Kalinda Raina**, Senior Director, Head of Global Privacy, LinkedIn; **Ruby Zefo**, Chief Privacy Officer, Uber*

4:00 PM – 4:25 PM
West Street Level

Three Things the Security Industry Isn't Talking About (but Should Be)
***Pat Gelsinger**, Chief Executive Officer, VMware; **Shannon Lietz**, Director, Intuit*

4:25 PM – 4:45 PM
West Street Level

Tales of a Teenage Security Supergirl
***Kyla Guru**, Founder and Chief Executive Officer, Bits N' Bytes Cybersecurity Education*

4:45 PM – 5:30 PM
West Street Level

Connecting the Dots for the Future
***John T. Chambers**, Founder and Chief Executive Officer, JC2 Ventures, Former Chairman and Chief Executive Officer, Cisco; **Diane Brady**, Award-Winning Writer, Author and Consultant*

8:00 AM – 10:10 AM & 1:30 PM – 3:40 PM
Various Locations

TRACK SESSIONS

See detailed information on following pages for descriptions and badge access.

8:00 AM – 11:20 AM & 1:30 PM – 4:30 PM
Moscone West 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 Lab on your schedule, so pick carefully from our 20 great offerings. ***Note: Press is not permitted in Lab sessions.***

THURSDAY

= Top-rated speaker.

圖 4　RSA Conference 2019 會議議程(四)

THURSDAY EVENTS & ACTIVITIES

8:00 AM – 3:30 PM
Marriott Yerba Buena 8

RSAC SANDBOX

The RSA Conference Sandbox is full of hands-on interactive experiences to test your infosec skills.

RSAC Early Stage Expo Exclusive Media Sponsor:

8:00 AM – 3:00 PM
Marriott, RSAC Sandbox

RSAC CYBREW CAFÉ

A full-service coffee bar.

8:00 AM – 3:00 PM
Marriott Yerba Buena 9

RSAC EARLY STAGE EXPO

The RSAC Early Stage Expo is the perfect megaphone for emerging infosec startups. Meet over 50 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 180 – 185).

RSAC Early Stage Expo Exclusive Media Sponsor:

8:00 AM – 5:00 PM
Moscone West Street Level

BROADCAST ALLEY

Watch top security publications shoot live and record exclusive interviews.

9:20 AM – 5:00 PM
South 301

BRIDGING THE GAP: CYBERSECURITY + PUBLIC INTEREST TECH*

See following pages for descriptions.

9:20 AM – 12:50 PM
& 1:30 PM – 5:00 PM
Moscone South Level 3

PEER2PEER SESSIONS*

P2P sessions enable groups of no more than 30 people that share a common interest to come together and productively explore a specific security topic, facilitated by an experienced practitioner. ***Note: Press is not allowed in Peer2Peer 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:

10:00 AM – 3:00 PM
Moscone North & South Lower Levels

EXPO

Come see how RSA Conference 2019 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 following pages for abstracts and a complete schedule on pages 115–118.

11:00 AM – 2:00 PM
Howard Street, Mission Street

STREET EATS

With options for all tastes, Street Eats is the easy way to fuel up between sessions or get energized before your next keynote. Stop by any of our food trucks on Mission Street or Howard Street.

6:30 PM – 8:30 PM
Moscone South Esplanade, South Stage

RSAC AFTER HOURS: COMEDY NIGHT

You're good for a network backup. How about a laugh? Get your fill at RSAC After Hours: Comedy Club. Stroll in and strike a pose on the red carpet before taking your seat in the front row of our very own comedy club. Serving up bottomless laughs—plus delicious food and cocktails—some of the funniest comedy acts around will take the stage, adding some good humor to a busy week. Now, who said cybersecurity professionals were all business?

Open to Full Conference and Discover Pass holders. Choose one of the RSAC After Hours events on Tuesday, Wednesday or Thursday nights of Conference. Space is limited so make sure to reserve a seat.

THURSDAY

= Networking event. * Open to Full Conference Registrants only. ** Open to Full Conference and Discover Pass Registrants only.

83

圖 4　RSA Conference 2019 會議議程(四)

5. RSA Conference 2019 會議-3 月 8 日(五)議程

FRIDAY EVENTS & ACTIVITIES

7:30 AM – 8:30 AM — **CONTINENTAL BREAKFAST***
Various Locations
Full Conference Pass holders, head directly to your chosen morning session. Breakfast is available in Moscone West Levels 2 & 3 and Moscone South Levels 2 & 3.

8:00 AM – 1:00 PM — **BROADCAST ALLEY**
Moscone West Street Level
Watch top security publications shoot live and record exclusive interviews.

KEYNOTES
Keynote abstracts can be found on page 36.

8:30 AM – 9:20 AM — **In the Wake of an Attack: Thoughts from a Seasoned CISO**
South Esplanade
***Bob Lord**, Chief Security Officer, DNC;* ***Dr. Hugh Thompson**, RSA Conference Program Chair, RSA Conference*

9:50 AM – 10:40 AM — **(Girl) Scouting for Talent: The Solution in the Next Generation**
South Esplanade
***Sylvia Acevedo**, Chief Executive Officer, Girl Scouts of the USA*

11:10 AM – 12:00 PM — **Engineering Trust and Security in the Cloud Era, Based on Early Lessons**
South Esplanade
***Quentin Hardy**, Head of Editorial, Google Cloud;* ***Suzanne Frey**, Vice President, Engineering, Google Cloud;* ***Amin Vahdat**, Google Fellow and Networking Technical Lead, Google*

8:30 AM – 12:00 PM — **TRACK SESSIONS***
Locations Vary
See detailed information on following pages for descriptions.

9:30 AM – 11:30 AM — **JOB SEARCH 2019: INTERVIEW SKILLS & RESUME REVIEW WORKSHOP***
Moscone West 3022
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.

12:30 PM – 1:15 PM — **CONFERENCE CLOSING**
Moscone West Street Level
***Tina Fey**, Writer, Actress, and Producer;* ***Dr. Hugh Thompson**, RSA Conference Program Chair, RSA Conference*

= Top-rated speaker *Open to Full Conference Registrants only

圖 5　RSA Conference 2019 會議議程(五)

二、 參加資安相關演講與小組討論會

(一)駭侵多因子認證的 12 種方法(12 Ways to Hack MFA)

目前多因子認證(Multi-Factor Authentication,MFA)已被廣泛應用在各式各樣服務中，例如登入網路銀行或 Gmail，除一般帳號密碼外，系統會另外傳送一組認證碼到使用者手機，用以確認使用者身份，本場演講首先介紹 MFA 的種類，常見用以認證使用者身份的方式可分為下列 3 種：

1.Something you know：使用者所知道的特定資訊，如密碼(Password)、個人識別碼(PIN)、手機圖形解鎖(Connect the dots)等。

2.Something you have：使用者所持有的特定裝置，如 USB token、智慧卡(Smart card)、無線射頻辨識(RFID)裝置等。

3.Something you are：使用者所擁有的特定特徵，如生物特徵(Biometrics)、指紋(fingerprints)、視網膜掃描(retina scan)等。

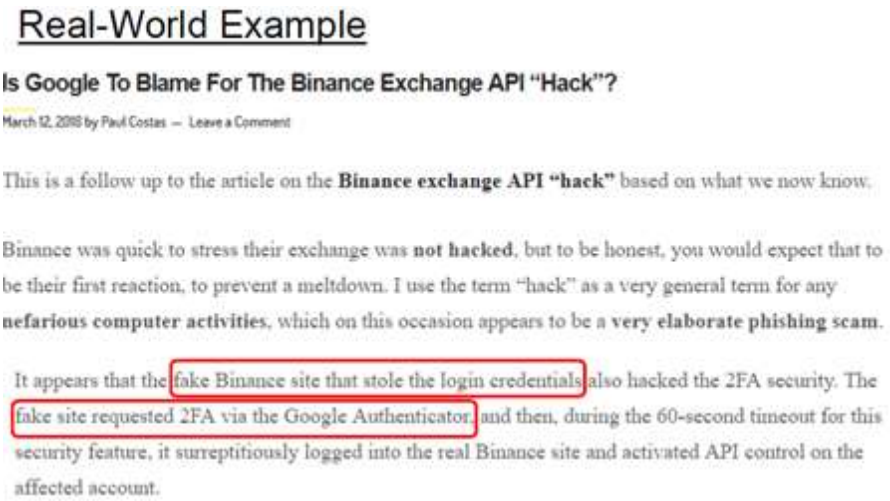
另，亦有將使用者地理位置或行為做為身份認證之用，使用以上其中一種方式稱為 Single Factor (1FA)，使用兩種方式稱為 Two Factor (2FA)，使用兩至三種方式則稱為 Multi Factor (MFA)；在實作 MFA 時，如果 Factor 採同相關管道傳遞撐為 In-Band，若不同則稱為 Out-of-Band；此外，認證方式又可分單向或雙向，顧名思義，單向表示僅認證伺服器端或客戶端的身份，雙向表示採更複雜的方式來交互認證伺服器端及客戶端的身份，主要目的係為了安全性。一般來說，使用 MFA 會比 1FA 來的安全，但是這並不表示 MFA 牢不可破。

認證(Authentication)係指使用一個或多個 factor 來確認使用者的身份，而授權(Authorization)則指的是確認經過認證後的使用者能存取哪些資源，目前最大的問題是認證及授權為完全不同的程序，例如您現在使用生物特徵或智慧卡登入 Windows 系統後，系統會使用 LM、NTLM 或 Kerberos 這一類的文字類型 cookie 來作為您的授權控制，許多攻擊者即是利用這一點來駭侵 MFA，以下簡單介紹 12 種駭侵 MFA 的手法：

1.General：駭侵 MFA 一般常使用手法為社交工程(Social Engineering)及技術攻擊

(Technical Attack)。

2.Network Session Hijacking：通常需要中間人(Man-in-the-Middle)攻擊者，攻擊者在合法的傳送者及接收者間攔截通訊內容，主要係為了竊取成功認證後的合法存取 token(在網站中為文字檔案類型的 cookie)；另一種 Network Session Hijacking Proxy Theft 指的是駭客架設與真實網站一樣的釣魚網站，想辦法誘騙使用者連線並輸入 MFA 相關資料，嗣後攻擊者再至真實網站偽冒該使用者登入，相關真實案例如圖 6 及圖 7。



Real-World Example

Is Google To Blame For The Binance Exchange API "Hack"?

March 12, 2018 by Paul Costas — Leave a Comment

This is a follow up to the article on the **Binance exchange API "hack"** based on what we now know.

Binance was quick to stress their exchange was **not hacked**, but to be honest, you would expect that to be their first reaction, to prevent a meltdown. I use the term "hack" as a very general term for any **nefarious computer activities**, which on this occasion appears to be a **very elaborate phishing scam**.

It appears that the fake Binance site that stole the login credentials also hacked the 2FA security. The fake site requested 2FA via the Google Authenticator, and then, during the 60-second timeout for this security feature, it surreptitiously logged into the real Binance site and activated API control on the affected account.

圖 6：Network Session Hijacking 真實案例 1

圖 7：Network Session Hijacking 真實案例 2

3.Endpoint Attacks：Man-in-the-Endpoint 攻擊指的是當使用者的電腦一旦被入侵，那麼任何的 MFA 都會失效，因當使用者成功登入系統後，攻擊者就可以執行任何他們想做的事，例如開啟一個隱藏瀏覽器、竊取 session cookie、植入後門程式等。

4.Subject Hijack：大部分的 MFA token 或產品會綁定特定用戶，如果攻擊者能使用與受害者一樣的用戶名稱(namespace)，就有可能竊取用戶的認證資料，講者也以微軟 Smartcard Identifier Hijacking 做為實例展示該手法，並說明針對關鍵屬性應定期檢視並給予最小權限，當這類屬性有異動時，應有稽核或告警機制。

5.SIM Swapping：多數的手機將門號及用戶資訊儲存在 SIM(Subscriber Identity Module)卡中，當您從舊的手機將 SIM 卡移除並安裝至另一部新的手機中，那理所當然新手機就使用 SIM 卡的門號；然而許多 MFA 係使用簡訊服務(Short Message Service, SMS)將認證碼傳至使用者的手機，也就是說 SIM Swapping 攻擊可以使得駭客取得透過 SMS 所傳的認證碼，而 NIST SP 800-63 亦建議不要使用 SMS 來傳送認證碼，SIM Swapping 多採社交工程方式達成，常見手法如下(真實案例如圖 8 所示)：

- ✓從電信公司、電話客服、釣魚信件或社群網站取得用戶相關資料
- ✓偽冒用戶向電信公司謊稱 SIM 卡遺失或毀損，申請補發新卡
- ✓使用前面所取得的用戶資訊，用以啟用新的 SIM 卡
- ✓當電信公司要求更多其他資訊時(如詢問您畢業國小、有幾張附卡、電信費透過何種方式繳交等)，攻擊者通常會在先前的資訊蒐集階段取得
- ✓一旦正式啟用 SIM 卡，也就代表攻擊者正式控制這個手機門號

圖 8：SIM Swapping 真實案例

6.Duplicate Code Generator：多數用於 MFA 的代碼產生器，通常會使用內建的亂數種子(Seed)或共享秘密(Shared Secret)值，作為後續產生亂數的起始值，這也就是一般所熟知號稱不會有重複值的一次性密碼(One time password, OTP)；許

多 OTP 會使用當下的日期及時間，用以增加其所產生代碼的亂度，此亦稱為 Time-based OTP。前面所提 Shared Secret 僅會存在後端認證伺服器的資料庫以及用戶的 OTP 裝置中，一旦攻擊者取得這類資訊及運算演算法，即有可能進一步產生出合法的認證碼，例如使用 Cain & Abel 工具計算出 RSA SecureID Token 所產生的亂數(如圖 9 所示)。

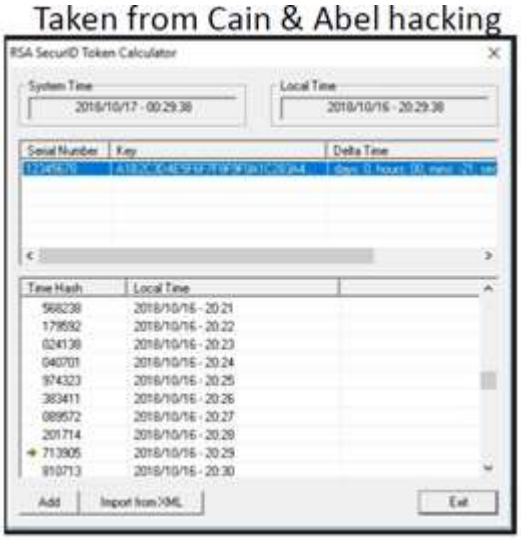


圖 9：Duplicate Code Generator 真實案例

7.Not Required/Downgrade Attacks：假如網站或系統仍允許用戶使用 1FA，那這個系統就不是真正的 MFA，如果您系統的 MFA 是使用非 MFA 程式碼，當該程式碼被竊取，攻擊者則可能使用非 MFA 方式進行存取。

8.Not Required/Recovery Attacks：所有登入復原方式遠比 MFA 的安全性來得更低，例如網站上提供「忘記密碼」的功能協助使用者重設密碼，攻擊者可能可以輸入假的手機號碼以取得重設密碼所需的認證資訊，相關案例如圖 10 所示。

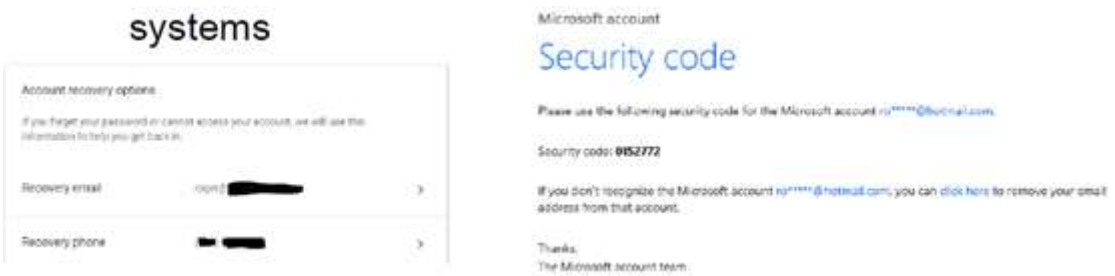


圖 10：Not Required/Recovery Attacks 真實案例

9.Not Required/Recovery Questions：最不安全的復原方式為安全提問(Security

Questions，如圖 11)，也就是在用戶註冊時，系統要求用戶選擇幾個問題(如您出生地的郵遞區號、您最要好朋友的姓氏等)並輸入答案，以作為後續復原(如重設密碼)時認證之用，然而這類資訊取得實際上並不困難，根據統計，有20%的安全提問能在一開始就被猜對，40%的用戶根本忘記當初所輸入的答案，有 16%的答案能在用戶的社群網站資料中找到。對用戶來說，解決方式為在註冊時，針對安全提問輸入與題目毫無關聯的答案，但您必須把這些答案另外存在其他地方，因為您會忘記。

圖 11：安全提問範例

10.SMS Rogue Recovery：攻擊者首先強制讓用戶的電子郵件進入 SMS 簡訊回復狀態(如多次輸入錯誤密碼)，接著偽冒電子郵件管理者，傳送簡訊至用戶的手機，說明其 email 已被駭侵，為安全起見，請用戶回傳認證碼，嗣後，攻擊者使用這組認證碼登入用戶的電子郵件。講者也提到許多防護的方式，主要為提醒用戶應提升警覺。

11.Social Engineer Tech Support：真實案例顯示，就算用戶使用 MFA 登入網站或系統，攻擊者仍可透過社交工程方式取消 MFA 或重設密碼，著名的案例為 DEFCON 的影片「This is how hackers hack you using simple social engineering」(網址 https://www.youtube.com/watch?v=lc7scxvKQOo)，攻擊者偽冒成用戶(Roose)的妻子，撥電話至客服中心，並播放嬰兒哭泣的聲音，營造出來電者既心煩又忙碌的氛圍，最後僅花了 30 秒就取得 Roose 的電子郵件信箱名稱及手機認證碼，甚至進一步請客服人員修改 Roose 的信箱密碼，讓在場的 Roose 相當驚訝。

12.Buggy MFA：如果所使用的 MFA 相關模組存在漏洞，可能會影響廣大的用戶，例如 106 年 10 月媒體揭露德國半導體業者英飛凌(Infineon)所生產的可信賴平台模組(Trusted Platform Module, TPM)含有安全漏洞，如果私鑰長度小於 2048 位元的話，將允許駭客計算出私鑰，並用來執行各種攻擊，間接導致影響數以百萬的用戶。

(二)日本強化物聯網的新資安策略(Japan's new cybersecurity strategy to close an IoT gap)

日本在 2013 年被選為 2020 年夏季奧運及殘障奧運主辦國家，為此，除強化實體安全外，亦積極推動網際網路及物聯網(IoT)的安全；在日本物聯網的應用包括：

1.製造業：用以增進生產力及效率，包括監看產品包裝過程、監測有無異常狀況發生、提醒操作人員相關作業程序。

2.零售業及物流業：用以降低人力，如 2018 年開設第一家無人便利商店，以及利用 AI 及 IoT 等技術降低物流業 50%的運送車次並減少 35%的工時。

3.農業：與 1985 年相比，減少 60%的人力，並在 2018 年開始使用智慧型牽引機。

為了加速 IoT 安全的發展，於 2015 年由政府、企業及學術單位成立 IoT Acceleration Consortium，在透過公私協同合作為 IoT 創造一個吸引未來投資的充足環境，期望結合政府，企業和學術單位的優勢，並建立一個用於開發及展示與物聯網推廣相關的技術，以及創造和促進新的商業模式；並在 2016 年發布物聯網安全指引(IoT Security Guidelines)，旨在為各行各業物聯網裝置、系統和服務的提供商和用戶提出基本戰略，以適當及基於風險的網路安全措施，認識物聯網的新風險，包括網路攻擊，將對其產生不利影響，期藉由該指引促進物聯網裝置、系統和服務的提供商和用戶識別他們的角色，並解決物聯網安全問題。

從圖 12 及圖 13 中，可以看出來日本企業對資安的重視度不及歐美，爰此，日本積極從各種不同面向強化資安：

1.在 2018 年提出發展資安策略，主要融合實體及網路安全、減緩殭屍網路

(botnet)、培育多面向資安人才。

2.在 2018 至 2021 年推動租稅減免措施，鼓勵 IoT 業者投資資安防護項目，可獲得 3%的公司所得稅減免，以及特別折舊達 30%。

3.由政府提供實驗場域，由總務省(Ministry of Internal Affairs & Communications)、ICT-ISAC 及橫濱大學(Yokohama National University)共同合作，在 2018 年協助發現 150 個有弱點的 IoT 裝置。

4.於 2018 年進行修法，讓總務省下的情報通信研究機構(National Institute of Information & Communications Technology, NICT)可以掃描網路上是否存在預設密碼的 IoT 裝置，並與 ISP 業者分享資安威脅情資。

5.在 2018 年修改電信事業法(Telecommunication Business Act)，讓 NICT 透過 ICT-ISAC 與 ISP 業者分享資安威脅情資，ISP 業者可以通知用戶其 IoT 裝置遭感染，並封鎖相關分散式阻斷服務(Distributed Denial-of-Service, DDoS)攻擊。

圖 12：Cybersecurity & risk management in Japan

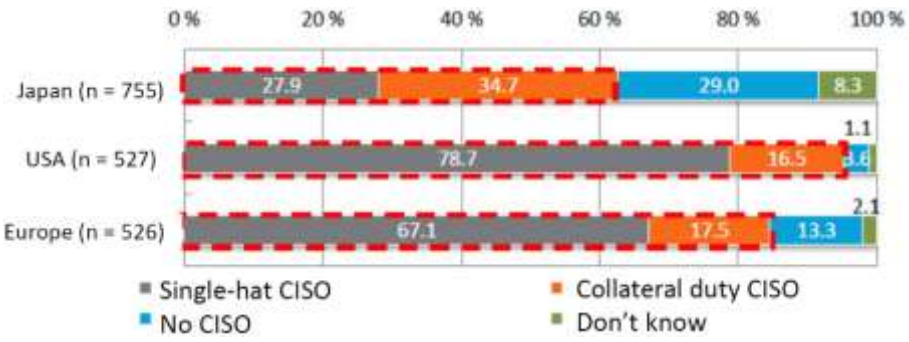


圖 13：CISOs in Japan, USA, and Europe

而在減緩 botnet 部分，過去日本與 ISP 業者於 2006 至 2011 年間合作執行 Cyber

Clean Center (CCC)的機制，並於 2013 至 2018 年間合作執行 Advanced Cyber Threats response InitiatiVE (Active)的專案，主要係向 Internet 用戶發送警告，以防止惡意軟體感染，並協助刪除惡意軟體，鼓勵用戶採取相對應的自主防護措施，期以減少日本惡意軟體感染的數量，進而營造高安全的網際網路環境。但是實務上面臨很多瓶頸，除了增加 ISP 的成本外，針對所發現惡意軟體研發出的病毒碼或防護措施，如何有效的讓用戶落實執行，甚至用戶會進一步質疑 ISP 是否違法監控他們的通訊內容。

為了持續強化日本整體資安防護能量，未來日本將導入更多的 IoT 及 AI 到農業及居家服務等各種行業上，培育更多 IoT 資安專家；為了讓大家更了解日本資安推動的相關策略，講者建議大家可參考 CSDE (Council to Secure the Digital Economy)所出版的 2018 International Anti-Botnet Guide，各國也可透過各種管道與日本建立資安實質合作，特別是針對認證、教育訓練及人才培育等項。

(三)**ATT&CK**

本次演講有許多場次聚焦在 ATT&CK，包括下列 5 個：

1. ATT&CK in Practice: A Primer to Improve Your Cyber-Defense
2. Fine-Tuning Your Cyber-Defense Technologies with the ATT&CK Framework
3. How to Evolve Threat Hunting by Using the MITRE ATT&CK Framework
4. Lessons from Applying MITRE ATT&CK in the Wild
5. Making MITRE ATT&CK™ Work for You: Sharing Best Practices for Success

首先簡單背景說明，MITRE 成立於 1958 年，理念為與政府機關或民間企業合作，透過運用系統工程與先進技術，協助解決國家層級的重要問題，促進世界的安全；由於 MITRE 為非營利機構，不具商業利益衝突問題，因此政府及其他合作單位願意提供機敏訊息；目前 MITRE 主要任務包含營運 7 個 FFRDCs (Federally Funded Research and Development Centers)如下表 1，為聯邦政府提供工程與技術指導，持續研發與精進 4 大領域核心能力。

表 1：MITRE 營運之 7 個 FFRDCs

FFRDC 名稱	成立時間
國家安全工程中心(NSEC)	1958 年
先進航空系統發展中心(CAASD)	1990 年
企業現代化中心(CEM)	1998 年
國土安全系統工程與發展研究所(HSSEDI)	2009 年
司法機構工程與現代化中心(JEMC)	2010 年
現代化醫療 CMS 聯盟(CAMH)	2012 年
國家網路安全研究與發展中心(NCF)	2014 年

ATT&CK(Adversarial Tactics, Techniques and Common Knowledge)為 MITRE 所提出的資安框架，主要係描述攻擊者行為的知識庫，其特性為用以描述真實攻擊事件、免費使用、使用 STIX 通用語言、有相關工具可導入使用；ATT&CK 可分為 Enterprise、PRE 及 Mobile 三種，相對應於網路攻擊狙殺鍊(Cyber Kill Chain)，PRE-ATT&CK 用在描述探測目標可能存在的弱點、研發入侵工具及傳遞入侵工具等前 3 個階段，Enterprise-ATT&CK 則是用來描述執行弱點攻擊、安裝後門程式、竊取資料及持續存在目標環境中等後 4 個階段，而 Mobile-ATT&CK 顧名思義是用來描述針對手機的攻擊行為。

MITRE 提出的 ATT&CK 係將駭客入侵細分為 11 個策略階段，包括入侵初期、執行、權限提升、防禦逃避、憑證存取、發現、橫向移動、收集、滲透、指揮與控制，並彙整每個階段的攻擊手法及工具成為一個知識庫，主要係為了描述攻擊者行為。以圖 14 為例，ATT&CK 使用 Group、Software、Technique 及 Tactic 等物件，其中關係為 Group 使用哪些 Software 實現哪些 Technique，以達成哪些 Tactic。

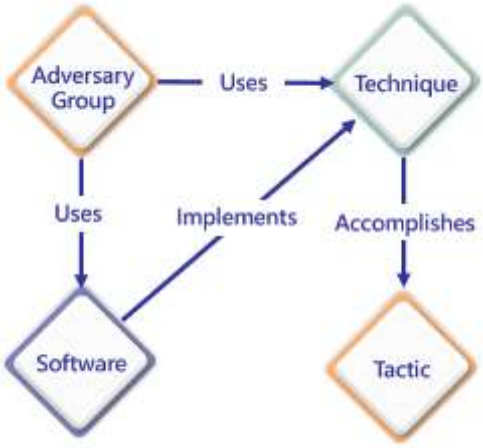


圖 14：ATT&CK 物件間的關係

在 ATT&CK in Practice: A Primer to Improve Your Cyber-Defense 演講中，講者以風

險管理的角度(如圖 15 所示)，說明應先識別出哪些是關鍵資產，誰對這些資產有興趣，以及其原因為何；再來要了解敵人的行為，包括他們的興趣為何，他們會使用哪些技術及軟體，他們對您的資產所帶來的威脅為何；最後，使用戰術、技術、流程(Tactics, Techniques and Procedures, TTPs)及入侵指標(Indicators of Compromise, IOC)補強資安防護措施，投資適當資源於資安防護、偵測及回應等機制上。

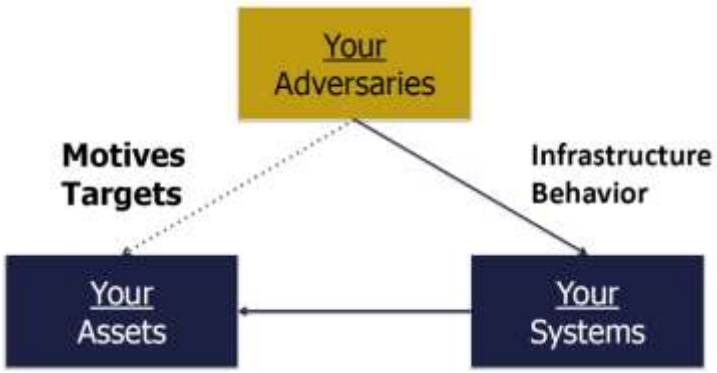


圖 15：識別威脅以改善防護措施

講者也特別調查組織是否採用 MITRE ATT&CK 架構，結果顯示 30.36%的組織已使用 MITRE ATT&CK 架構，惟超過半數並沒有使用(如圖 16 所示)；同時也調查使用者認為 ATT&CK 對哪些領域最有幫助，結果顯示對於偵查方面最有幫助(如圖 17 所示)；最後，亦調查 MITRE ATT&CK 能在哪方面提供實務面上的幫助，結果顯示在教育訓練上最有幫助(如圖 18 所示)。

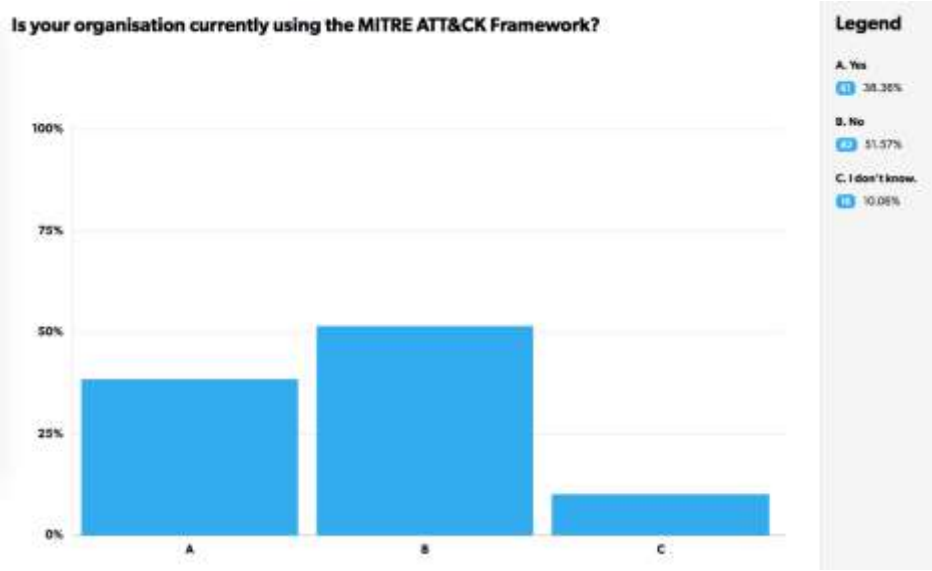


圖 16：組織是否採用 MITRE ATT&CK 架構之調查結果

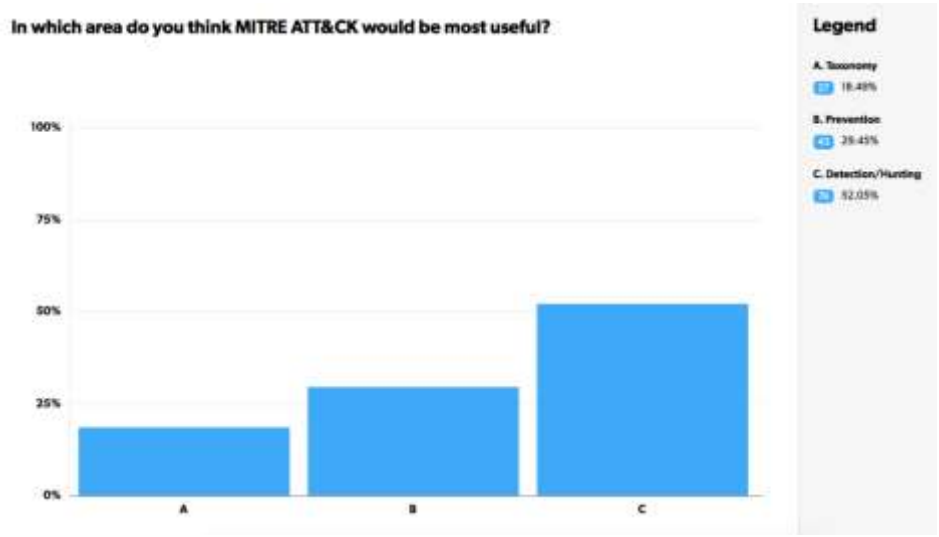


圖 17：ATT&CK 對哪些領域最有幫助之調查結果

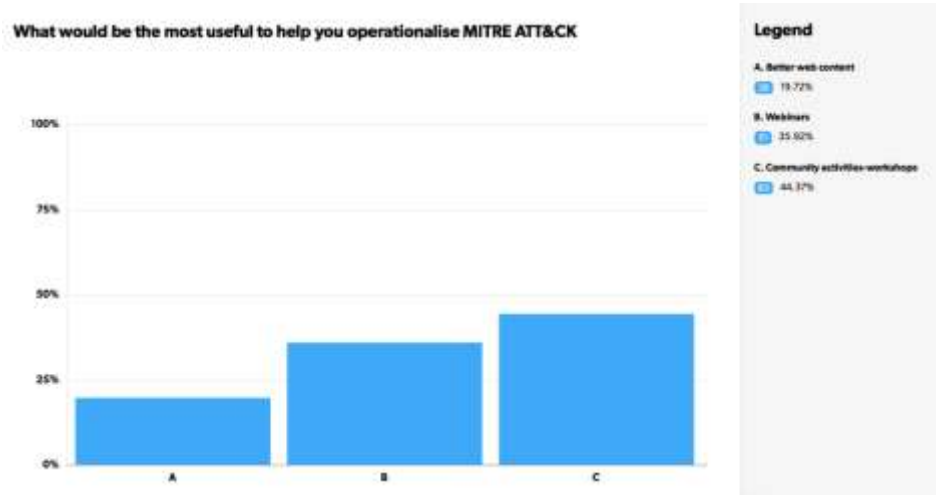


圖 18：ATT&CK 能在哪方面提供實務面上的幫助之調查結果

同時，亦介紹一些 MITRE ATT&CK 控制測試工具，包括：

1. MITRE Caldera：Caldera 是一個自動化的對手模擬系統，其平台設計為利用計畫系統和基於對抗戰術、戰略和流程的系統，預先配置對手行為模型，以在作戰期間生成計畫；Caldera 對於識別新的資料來源和基於行為入侵偵測分析、測試防禦的改善非常有用。(link: https://github.com/mitre/caldera)

2. Endgame RTA：由 python 腳本編寫，這些腳本生成了 50 多種不同 ATT&CK 策略，以及一個編譯後的二進位應用程序，可以根據需要執行的檔案，類比相關的程式注入行為，允許藍隊測試他們的檢測能力，以抵禦惡意攻擊。(link:

https://github.com/endgameinc/RTA)

3. Red Canary Atomic Red Team：為一個簡單的測試資料庫，每個安全團隊都可以執行這些測試來了解控制能力是否符合標準，並可透過此工具每五分鐘內進行一次測試，以得知自身盲點。(link: https://github.com/redcanaryco/atomic-red-team)

4. Uber Metta：是一種資訊安全準備工具，可用以執行任何網路的偵測及控制。(link: https://github.com/uber-common/metta)

(四)網路風險管理：減少網路曝光的新方法(Cyber Risk Management：New Approaches For Reducing Your Cyber Exposure)

本次會議客觀地描述如何確認組織中各種網路風險的優先等級，並提供衡量的前述風險的基準，以幫助組織進行決策，講者 Kevin Flynn 為 Tenable(Cyber Exposure)公司的高級產品行銷經理。

講者主要先說明現今基礎設施(IT)、雲端(Cloud)及物聯網(IoT)於網際網路上可能產生的弱點 (詳見圖 19)，並指出組織對於前述設施應逐一提出下列 4 個關鍵問題：

- ✓Where are we exposed？
- ✓Where should we prioritize based on risk？
- ✓How are we reducing exposure over time？
- ✓How do we compare？

並指出資安團隊在面對問題時，如果以手動方式逐一找出風險及漏洞、確訂優先等級及集中修復，將耗費大量的時間在找出問題，因此組織需要將原始漏洞和威脅情資數據轉換為商業洞察，以幫助資安團隊根據業務風險和威脅情資確定優先等級並集中修復。

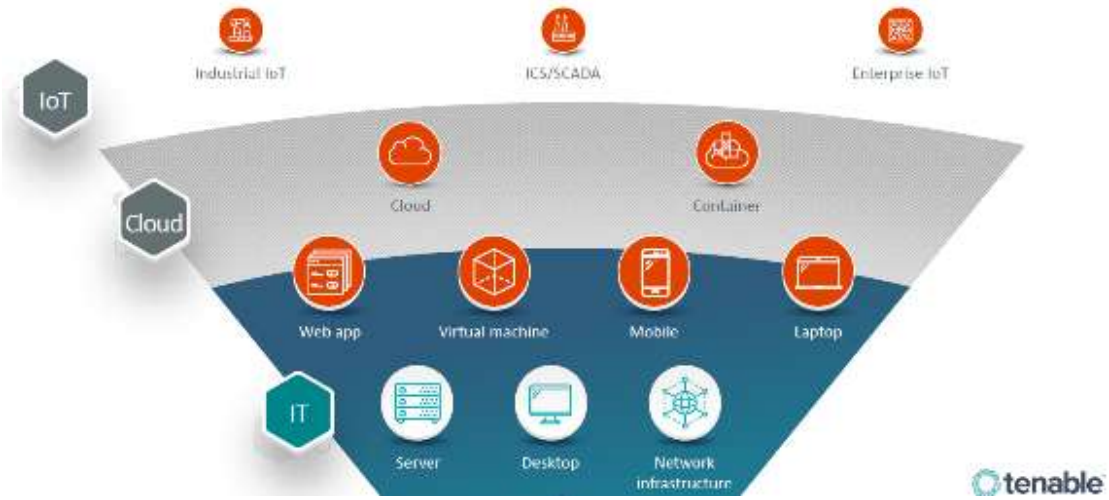


圖 19　The Cyber Exposure Gap

接著說明共通性漏洞評鑑系統(Common Vulnerability Scoring System,CVSS) 是一套公開的評鑑標準，經常被用來評比企業資訊科技系統的安全性，並受到 eBay、賽門鐵克(Symantec)、思科(Cisco)、甲古文(Oracle)等眾多軟體廠商支援。CVSS 是運用數學方程式，配合基本矩陣群(Base metric group)、暫時矩陣群(Temporal metric group)及環境矩陣群(Environmental metric group)等 3 個群組來判斷某特定網路的安全性是否存在弱點，讓組織能識別漏洞的嚴重程度。

最後，提到了 Tenable 公司的產品，如 Predictive Prioritization 將 Tenable 收集的漏洞數據與第三方漏洞和威脅數據相結合，並與 Tenable Research 開發的高級數據科學算法一起進行分析，並通知漏洞優先級(VPR)及分析結果(詳見圖 20)。

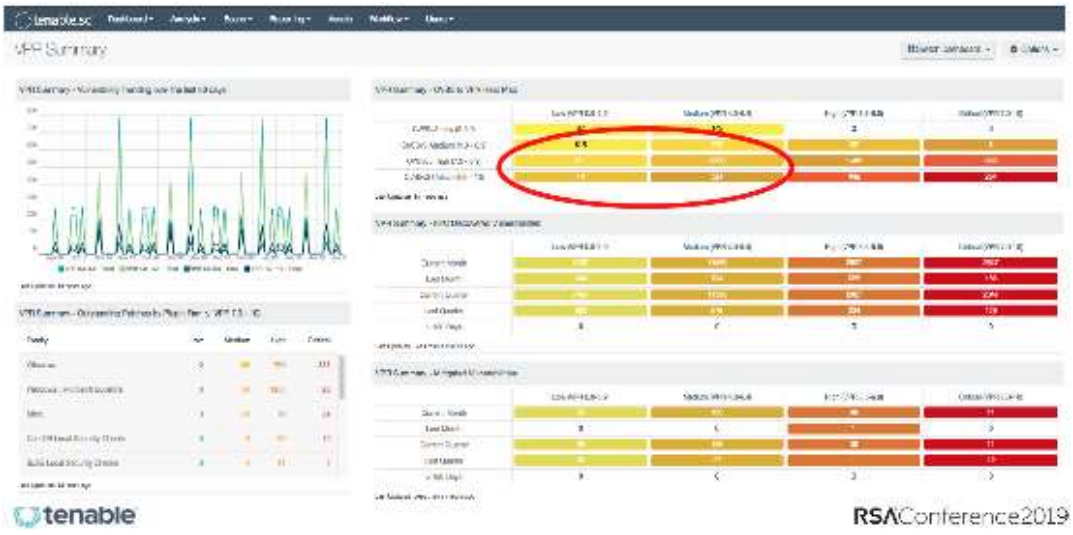


圖 20　CVSS TO VPR：MORE LOW/MEDIUM-FEWER HIGH/CRITICAL

(五)面對未來的網路安全戰略(Future-Proof Cyber security Strategy)

本次會議內容主要透過現實生活中的例子讓聽眾瞭解各種快速發展的網路安全工具的優勢和挑戰，以制定面向未來的網路安全戰略，講者 Timothy Lee 為洛杉磯市的首席資訊安全官。

講者先引用「Richard P. Rumelt (2012)・Good Strategy / Bad Strategy: The Difference and Why It Matters・United Kingdom：Profile Books」一書，說明好的策略幾乎永遠看起來極度簡單明顯，不需要一份厚厚的 PowerPoint 投影片來解釋，並提出一個好的網路安全戰略須具備識別關鍵挑戰、框架、協調行動及監控與適應等四個因子(詳見圖 21)。

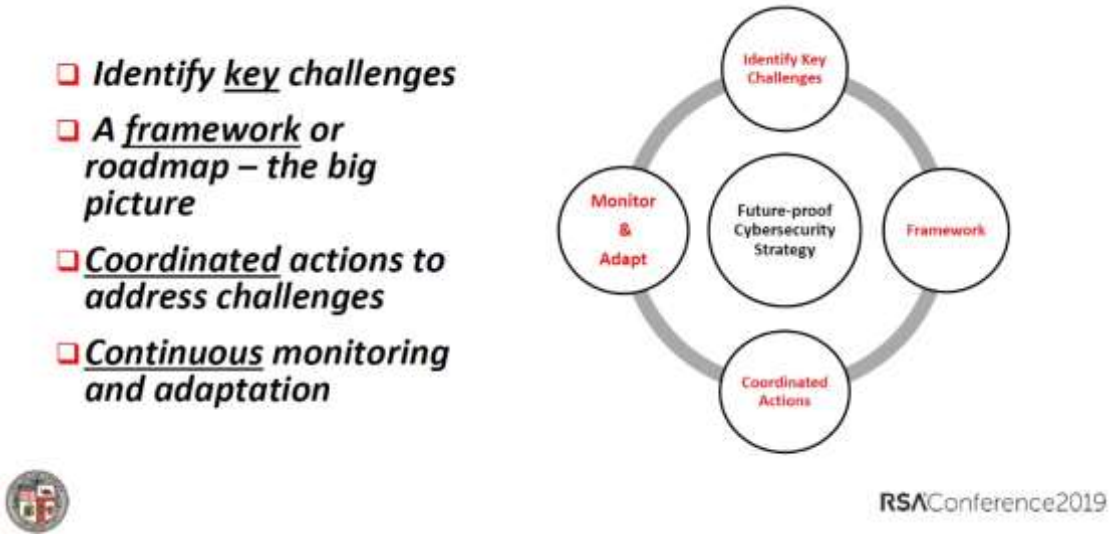


圖 21　What is good(future-proof) cybersecurity strategy？

接著說明面對未來的網路安全戰略時，應考量 5 個關鍵的網路安全挑戰、1 個框架及 3 個必備條件，如下：

1. 關鍵的網路安全挑戰：人類(仍)是網路安全中最薄弱的環節、不斷變化的威脅形勢、攻擊面向越來越廣泛、巨量資料、商業模式與網路安全的取捨。
2. 框架：網路安全框架(Cybersecurity Framework,CSF)。(詳見圖 22)
3. 必備條件：保護人類錯誤的行為、以情資為驅動的防禦及團隊合作。

圖 22　網路安全框架(Cybersecurity Framework,CSF)

三、參加國土安全相關演講與小組討論會

(一)國土安全部(DHS)著重關鍵基礎設施風險管理與創新運用

美國國土安全部參與或舉辦下列活動：關鍵基礎設施的風險管理、人臉辨識提升入出境管理效率、鼓勵民間的國土安全創新與運用、推動對安全物聯網產品和服務的需求、區塊鏈的身分管理、網路安全事件的快速應變及復原措施、以及如何結合國際力量支援關鍵功能的網路安全。本訪問團參加的活動如下：

1.國家關鍵基礎設施的風險管理(Risks and Results: Counter-Risks to the Nation’s Critical Infrastructure)

由國土安全部網路與基礎設施安全局(CISA)局長 Christopher Krebs 與奧本大學 McCrary 網路和關鍵基礎設施的安全研究所主任 Frank Cilluffo 對談，K 局長簡介 CISA 為保護美國關鍵基礎設施，透過轄下國家風險管理中心(NRMC)，致力於識別和解決國家關鍵基礎設施面臨的最重大風險，並與 24/7 運營中心、CISA 的國家網路安全和通信整合中心(NCCIC)和國家基礎設施協調中心(NICC)合作，藉提供戰略性的分析填補關鍵的風險管理差距，在聯邦政府和私部門合作夥伴中創建跨領域風險管理方法，主要透過過三方面的運作：(1)確定戰略風險並確定其優先級，(2)整合政府和各行業的風險管理活動，以及(3)同步推動風險管理活動。

K 局長認為 CISA 處於網路安全威脅的最前沿，因此了解風險趨勢，可以幫助私部門提高網路態勢感知能力並降低風險；主張主要的風險來自：俄國、中國、伊

朗和朝鮮；其主要關注點是供應鏈風險；由 NRMC 主導，與公私合作夥伴組成資通訊(ICT)供應鏈風險管理工作小組，作為聯邦協調中心，審查和製定共識性建議，以識別和管理全球 ICT 供應鏈的風險。例如 2018 年，美國政府禁止俄羅斯卡巴斯基實驗室的技術，現在它主要關注華為和 5G，擔心來自外國供應商的技術設備可能被用於惡意目的；另一個重點領域是外國 VPN 應用程式，特別是來自 Dolphin，Opera 和 Yandex 的中國應用程式。

此外，NRMC還與金融、通信電子、財政部和能源部的高級政府代表組成工小作組，直接收集情報、分析系統性風險，建立跨部門風險管理手冊。

K 局長還舉出「集體網路防禦」的重要性，因為民間業者無法獨自對抗網路戰，主張多個利益相關者可以合作獲得正在發生的資訊 – 快速識別特定的威脅、戰術、技術、漏洞，以獲得最大的效果，因此，透過集體網路防禦，CISA 正在強化其自動指標共享(AIS)計畫，以包含更多背景和特異性，俾為私部門提供更多加值的威脅情報。

選舉安全是 CISA 促進集體防禦的另一個領域，CISA 在短短九個月的時間內，促進選舉基礎設施部屬入侵檢測和預防感應器，現在這些感應器覆蓋了 90%的選舉基礎設施，高於 2016 年的 32%。

根據 CISA 的重點，私部門組織可以採取三項關鍵措施來改善其網路運營：

(1)增加對供應鏈和第三方風險的關注，包括技術平台以及與業務相關的各種第三方實體的相關風險。

(2)重新審視，並採取有關減少攻擊面的一些基礎措施。例如，如果業務上與俄國無關，則不應在網路上允許來自俄國的流量。

(3)擴大威脅情報的資訊共享，以便從集體防禦中受益。例如將威脅情報加入 DHS 的 AIS 計畫，在共享社區(資訊共享和分析中心和組織)與行業同行共享威脅資訊。

2.人臉辨識提升入出境管理反恐效率(Use of Facial Recognition to Combat Terrorism)

由國土安全部代理首席隱私官 Jonathan Cantor 主持，介紹美國海關與邊境保護局(CBP)開發的雲端臉孔生物識別匹配服務平台，可在任何須要出示旅行證件的地方，提供自動身份驗證程序來取代手動檢查紙本旅行證件，該服務平台不須要按指紋及核對的程序，因此可達到安全和快速的身份驗證，目前已在亞特蘭大等機場實施，證實可以縮短旅客通關時間。

該平台使用 APIS 數據，CBP 為所有出發和到達的美國航班的乘客拍攝臨時的照片，並產生唯一標識符號(UID)，透過 CBP 為航空公司和機場提供網路服務和閘道，以及應用程式介面(API)提交旅行者照片和 UID，在雲端進行匹配服務：

(1)驗證 - 驗證安全憑證並授予對系統的存取權限

(2)識別 - 從航空公司的系統接收照片並予以識別

(3)回應 - 在兩秒或更短的時間內回應匹配結果

與會者極關心隱私的保護，CBP 代表解釋該平台使用雲端安全機制，只有照片，並無旅行者的個人識別資訊存儲在雲中。用於匹配的照片會立即轉換為無法恢復到原始狀態的格式。一旦旅行者的身份得到確認，旅行者的照片將在 14 天后後刪除。相關保護隱私和保護旅行者數據的做法，可以參考 CBP 已向公眾發布許多隱私影響評估，說明如何擷取、存儲、傳輸數據以及保存數據的時間。同時 CBP 也加強宣導，解釋臉孔識別過程和替代檢查程序。

3.鼓勵民間的國土安全創新與運用(Dancing with Elephants: Bridging the Government Innovation Gap)

由國土安全部科學技術局(S&T)技術總監 Anil John 主講，探討科技管理局在 2015 年推出的矽谷創新計畫(SVIP)，如何透過新的融資模式和靈活的合約流程，向新創公司尋求商業技術的共同投資機會，目的在於與新創業界保持同步，共同尋找尖端解決方案，開拓強化國家安全的新技術，以解決國土安全部和國土安全企業面臨的最棘手問題，並重塑政府，縮短政府創新差距。

該計畫通過簡化的應用程序和投資流程，利用創新其他交易徵集，尋求解決方案，雖位於加利福尼亞州矽谷，卻是尋求美國和世界各地(目前有英國、以色列)的新創公司的合作，利用其商業研發環境與技術應用，共同投資並加速技術向市場過渡，實施以來，已有不少公司將其技術移轉為美國國土安全部業務上的應用系統，例如 Tamr 公司的加強全球旅行者評估系統(GTAS)、Echodyne Corp.的超材料電子掃描陣列(MESA)雷達系統、DataRobot 應用於 GTAS 的自動化機器學習(AML)，可加快預測模型的開發等。目前還有許多合作案正在進行，開發領域涵蓋物聯網安全、身份保證和反欺騙功能、K9 的穿戴監測系統、小型無人機的偵監控制系統、金融服務網路安全主動防禦系統、邊境管理系統等。

(二)國家安全局(NSA)分析主要對手，推行持久戰之戰略

美國國安局關心對手(尤指俄國、中國、伊朗、北韓)在複雜度、強度、數量和發展速度不斷強化的情況下，已危及國家安全利益和經濟福祉，除了公開該局開發的 GHIDRA 軟體逆向工程平台，幫助漏洞獵手、學生和其他安全專家分析惡意軟體和其他惡意程式外，由國安局局長兼網路司令部司令 Paul Nakasone(中曾根)將軍，與哥倫比亞廣播公司新聞部情報和國家安全記者 Olivia Gazis 對談，主題為 Strategic Competition: The Rise of Persistent Presence and Innovation，探討美國面臨的主要威脅：

1.破壞性的網路攻擊

2.網路間諜竊取智慧財產權

3.破壞美國選舉的民主進程

中曾根局長認為美國網路司令部儘管具有網路安全的快速打擊能量和能力，國安局具有密碼分析、決策研判、大數據研析的優勢，但對手正不斷改進他們的技術，擅長加密通信手法，部署更複雜的戰術，不斷威脅美國的國家安全，因此必須充分了解這些對手，加強公、私部門的情資交換，人才培育，鞏固伙伴關係，並保持警惕。尤其網路攻擊活動日趨熾烈，安全上需要專業人才和投資，惟有透過整體國家的行動才能實現，因此必須就現有法律程序進行公開討論，確保國民的健康和安全與個人的隱私平衡。談話重點如下：

1. 俄國干預 2016 年總統大選之後，網路司令部和國安局與其他政府機構密切合作，包括國土安全部(DHS)，聯邦調查局(FBI)和國家情報總監辦公室(ODNI)對於外國試圖破壞選舉進程或以其他方式影響美國政治言論的情資，強化其蒐集與分享機制，甚至曾在 2018 年期中選舉時曾截斷俄國的巨魔農場的接取，預計在 2020 年總統選舉需要進行更緊密的協調合作，因為對手不斷改進其現有戰術或開發新戰術，而且即使美國採取更加協調的策略來反擊，外國對手的假訊息攻擊力道也不大可能減弱，所以這將是「持久戰」，必須確保充分的情資分享，要求社群媒體適時關閉假帳號。

2.關於國安局蒐集電話紀錄以識別可疑的恐怖分子的授權，將在今年到期(指愛國者法第 215 條)，該局可能不再延長，將與政府和國會密切合作，就是否應該重新授權提出建議。

3.中國利用其經濟實力，已能發展自己的定位，而且在人工智慧、機器學習、量子計算方面投入巨大資源，與美國正處於激烈競爭時期。而隨著全球各國準備建設 5G 無線服務，中國電信巨頭華為的風險特別引起關注，尤其華為與中國政府之間的直接聯繫應持謹慎態度，因此希望盟友，尤其所謂的「五眼」情報共享聯盟，不應因為容許華為產品而形成破口，而傷害聯盟，將持續與五眼夥伴就挑戰和風險進行對話。

4. 雖然川普總統表示伊拉克和敘利亞的伊斯蘭國已被「摧毀」，其領土幾乎 100%被收復，而中曾根局長率領的聯合特遣部隊對伊斯蘭國進行攻擊性網路行動，以破壞其招募工作和網路宣傳，已使得 ISIS 在這方面的能力顯著下降，但對於伊斯蘭國勢力的逃竄與擴散，仍須保持警戒，這也是「持久的交戰」策略中的一部分。

5.北韓有能力和意圖在網路空間進行破壞性打擊，正處心積慮攻擊美國的企業和政府機構，且不斷提升能力，意圖在網路空間持續進行破壞性攻擊。但美國對於北韓的網路攻擊行為模式之理解，與日俱增。

6. 有關俄國政府可能會尋求建立一個「網際網路主權」，使莫斯科能夠在內部控制資訊流，免受外國的干擾之報告，中曾根局長認為專制模式不太可能成功，

並舉伊朗為例，主張極端主義模式無法獲得大量數據，不利於公民的資訊交流，無法被全世界接受。

7.在過去一年當中，美國網路安全的主要變化是，修訂國家網路空間戰略，涵蓋了網路司令部如何在政府部門防禦中運作，並且在 2019 年國防授權法案，明確規定將網路空間的經營納為傳統軍事活動之一環，鼓勵國防部資訊網路部門與國土安全部以及其他部門密切合作。因此對行政部門、立法部門已經做出了承諾，以確保能迅速因應網路攻擊事件。

8. 中曾根局長對於該局稍早宣布開放的 GHIDRA 軟體逆向工程平台獲得正面迴響表示欣慰，該平台使用 Java 開發，無需特定的安裝方法，可幫助漏洞獵手、學生和其他安全專家分析惡意軟體和其他惡意程式，挖掘其源碼，進一步檢測病毒威脅或潛在的錯誤。其交互式GUI功能可以在交互模式和自動模式下運作，方便逆向工程師能夠在各種作業系統上操作，包括 Windows，Mac OS 和 LINUX，並支援各種處理器指令集。GHIDRA 平台整合高端商業工具所需的所有功能，免費公開下載，網址為 https://ghidra-sre.org/。

(三)聯邦調查局(FBI)強化技術和夥伴關係以剷除網路罪犯

聯邦調查局參與或舉辦的活動以打擊網路威脅與犯罪為主，介紹網路違法行為中，執法人員和律師的應處之道、監督與保護特權用戶 IP、物聯網犯罪之調查與物聯網犯罪分級，其中比較重要的專題座談是聯邦調查局局長 Christopher Wray 與布魯金斯學會治理研究高級研究員 Susan Hennessey 對話，主題為：The FBI: At the Heart of Combating Cyberthreats，討論聯邦調查局作為美國國內執法和情報機構的獨特地位，如何利用全方位的專業知識，技術和夥伴關係來剷除網路罪犯，成為打擊公民犯罪和國家安全網路威脅的核心。

W 局長認為，今天的網路威脅不是任何一個政府機構可以單獨解決，而且也沒有任何機構具備像 FBI 一樣的範圍和規模、經驗、設備。所以 FBI 與公部門如國家安全局、國土安全部等密切合作外，與私部門合作夥伴關係亦非常重要，特別是在網路領域，現實是，如果沒有私部門的合作，FBI 很多任務無法達成，而反之亦然。由於 FBI 擁有精銳的快速部署部隊和網路行動小組，與其他聯邦，州和地方執法

機構的網路任務小組一起協調應變，在全球 60 多個國家派駐 FBI 經過特殊網路安全培訓的法律專員，因此關鍵在於私部門能否事先開始與當地辦事處建立關係。

H 研究員詢及俄國干擾美國選舉，中國偷竊技術問題的看法，W 局長答覆 FBI 會獨立地探究事實，無論攻擊者躲在哪裡，由誰領導，只要發現有人犯下聯邦罪，危及美國人或美國企業時，FBI 會持續追蹤處置，不會在乎外國政府對此有什麼看法。

H 研究員也關心 FBI 招募特工和專業人員的情形，W 局長表示過去一年來，FBI 成功招聘計算機科學家、數據分析師和工程師，特工和實習生的錄取比率在 5%到 6%之間，比大多數常春藤聯盟學校更具挑戰性，歡迎有志於打擊網路駭客，保障美國的安全、商業公司的穩定、公民福祉的人加入 FBI 行列。

(四)國家標準暨技術研究院(NIST)推廣網路安全與保護隱私框架

國家標準暨技術研究院(National Institute of Standards and Technology，NIST)參與或舉辦的活動主要在推廣其網路安全框架(參閱三、會外參訪活動之(三))、隱私框架，並關注勒索軟體和關鍵事件的數據完整性保護和應變、推動區塊鏈技術與供應鏈風險管理、零信任網路、網路安全漏洞的消除等。其中有關隱私框架部分，由 NIST 應用網路安全部門負責人 Kevin Stine 與美國國家標準與技術研究院高級隱私政策顧問 Naomi Lefkovitz 對談，主題為：The NIST Privacy Framework: What It Is and What It Means for You，介紹物聯網和人工智慧等尖端技術發展後，如何保護個人隱私，說明該研究院(NIST)正在與私營和公共部門利益相關者合作開發一個自願隱私框架，以幫助組織更好地識別、評估；管理和傳播隱私風險，促進保護個人隱私的創新方法的發展，並增加對產品和服務的信任。

雖然良好的網路安全制度可以保護人們的資訊來幫助管理隱私風險，但隱私風險也可能來自組織為滿足其使命或業務目標而收集、存儲、使用和共享資訊。NIST 認為，必須要有更多工具來解決全方位的隱私風險，以支援隱私保護的實施。

此自願框架為各種組織制訂各種隱私及其保護方法，以更好地識別、評估、管理和溝通隱私風險，使個人能夠更有信心和信任地享受創新技術帶來的好處。認為應與現有的國內和國際法律和監管制度兼容，以方便組織廣泛採用。

由於開發此框架攸關關鍵基礎設施網路安全，必須採取開放、透明和協作的方法，因此 NIST 積極與行業、民間社會團體、學術機構、聯邦機構、州、地方、地區、部落和外國政府、標準制定組織等合作，藉一系列研討會廣泛宣傳。

與此同時，為與商務部國家電信和資訊管理局(NTIA)正在製定的隱私原則有所區隔，NIST 框架專注於進一步發展美國國內政策，俾成為企業級隱私風險管理工具，可以兼容並支持組織在適用的國內和國際法律或監管制度下運營的能力。

NIST 隱私框架旨在適應許多不同的組織、技術、生命週期階段、部門，也可以擴展到各種規模的組織，無論是公共的還是私人的、任何部門、以及在國內或跨境運營。

與會者詢問該框架是否有行政命令或政府程序來推動這項工作？NIST 代表回答此隱私框架為自願性質，該機關只是憑藉改進關鍵基礎設施網路安全框架方面的經驗，以及廣泛的隱私專業知識，領導隱私框架的開發。此框架預定於 2019 年末發布。

四、會外參訪活動

(一)拜會北加州地區情報中心(Northern California Regional Intelligence Center)

北加州地區情報中心(Northern California Regional Intelligence Center, NCRIC)為一政府的計畫，於 2007 年由北加州高強度藥物販運區(Northern California High Intensity Drug Trafficking Area, NC HIDTA)執行委員整合地區調查支援中心(Investigative Support Center，ISC)、北加州地區威脅評估中心(Northern California Regional Threat Assessment Center，NCRTA)和恐怖主義預警組織(Terrorism Early Warning Groups, TEWGs)的人員、情報和調查資源而成，期藉由犯罪威脅、提升訊息分享機制及情報分析的訓練，建立動態安全防禦體系，以強化區域安全；該中心由聯邦、州和地方執法單位、消防和公共衛生機構指派的 70 多位情報官員、情報分析師、關鍵基礎設施專家、調查人員和私部門對外聯絡官員等組成工作團隊，目前該中心為國家整合中心企業(National Fusion Center Enterprise)、國家威脅評估系統(State Threat Assessment System, STAS)、美國國土安全部指定的整合中心(Fusion Center)成員之一。

NCRIC 為公共安全提供國土安全課程培訓，受訓單位包含政府部門和私營組織。課程內容包含提供分析資料以識別地區的重大刑事和國土安全威脅、使用前端科技整理和分析犯罪數據、可疑活動通報、區域風險/脆弱性數據和刑事情報；以及開發和傳播與恐怖主義、關鍵基礎設施、重大行動有關的戰術和戰略評估事件、重大刑事威脅和重大犯罪調查。另針對關鍵基礎設施防護，除了與區域相關單位實質合作外，NCRIC 協助成員關於恐怖攻擊事件的應變處置作為，以藉由提高警覺和降低其他風險來保護關鍵基礎設施。實現方式如下：

- ✓ 收集威脅與情資等相關數據，進行風險分析
- ✓ 提供諮詢服務、威脅情資分享
- ✓ 強化訊息共享環境
- ✓ 提供國家整合中心情報資源

本次赴美國參加 RSA 會議期間，安排於 3 月 8 日上午與 NCRIC 的 Sena 主任及 Mahoney 副主任訪談，期間談到 NCRIC 主責為犯罪與威脅的情資交流，透過收集線索、分析可疑活動通報(Suspicious Activity Reporting, SAR)及犯罪訊息，輔以提供協同部門之培訓課程、技術資源，以促進北加州執法單位、政府、私部門間和公共部門關鍵基礎設施的合作，提升區域間的緊急應變能力。

另，美國國土安全部、聯邦調查局以及州和地區執法合作單位共同合作提出全國可疑活動通報倡議(Nationwide SAR Initiative, NSI)，為執法部門提供了另一種工具，透過建立蒐集、記錄、處理、分析和共享訊息的能力，幫助預防恐怖主義和其他相關犯罪活動；該倡議提供多重面向策略，旨在提高州、區域執法專業人員識別、報告、評估和情資分享相關知識以有效防阻恐怖主義攻擊，並提高全國防禦能力，並針對不同職責人員分成三個培訓計畫：

- ✓ 分析/調查人員培訓：此類培訓重點是分析/調查人員對 SAR 的情資評估，以識別與恐怖主義有關的事件關聯指標，並根據背景知識、經驗和現有訊息的整合驗證，評估是否與恐怖主義有潛在關聯並符合提交標準，培訓以 8 小時的研討會形式進行。
- ✓ 主管人員培訓：確保 SAR 流程正確，並具有執行、政策制定的能力。
- ✓ 一線執法人員培訓：透過平時的訓練，使人員觀察敏銳，回報可疑的行為或活動。

本次討論囿於時程關係，僅安排 1 小時拜會行程，為進一步深入了解該中心推動情資之通報、處理及分享等實務作法，會後以電子郵件連繫 Sena 主任表達希望於本年 7 月另安排討論會議，期深入交流相關經驗，已初步獲得允諾。

(二)與美國國家標準暨技術研究院(NIST)代表會談

NIST 前身為國家標準局(NBS，1901 年~1988 年)，目前屬於美國商務部之一個機構。該院研究量測範圍可從小至奈米等級，到大至摩天大樓的防震與全球通訊網路的規模。該機構藉由提高測量科學、標準及技術等，以促進美國的創新和產業競爭力，並強化經濟安全及改善生活品質。

NIST 電腦安全部門主管 Mr. Scholl 及資訊技術實驗室資深政策顧問 Mr. Sedgewick，首先介紹 NIST 在電腦及 IoT 領域的資安規範措施，及與企業、政府等單位在資安領域的合作情況，並表示近期更著重在企業網域資安分類、當前資安議題、資安架構等研究。另就與會者詢問問題，分享說明機構在標準、指引等特定代碼意義，NIST 800 代碼屬於資通領域涉及硬體架構的探討，NIST 1800 代碼則著重在軟體特定議題的網安實踐指引探討。

以 1800-14 標準草案為例，該草案係針對業者間建構網路互連使用的邊界閘道路由器之互連協定(Board Gateway Protocol, BGP)，訂定更嚴謹的認證及相互確認程序，希望藉由使用公開金鑰資源基礎(Resource Public Key Infrastructure, RPKI)提供可信賴路由來源(Route Origin Validation, ROV)平臺機制(詳見圖 23)，草案並舉例說明一個安全平台，經由使用 RPKI 方式提供路由來源驗證(ROV)以減輕與路由劫持相關的一些錯誤配置和惡意攻擊(例如，拒絕訪問網際互聯網服務、網際互連流量被繞道經攻擊端點的竊聽、錯誤的將互聯網網路流量導入惡意終點、破壞網際互聯協議(IP)地址的信譽和過濾系統，以及導致網際互聯網中的路由不穩定等)，使達到提高網域間路由流量交換的安全性。

NIST 代表表示，該草案於 2018 年 8 月公布草案後，意見徵詢期間共收到 15 份意見書，NIST 將針對意見書逐一研究及回應，必要時，將再修正草案後進行第二次意見徵詢。此外其定訂的指引規範，對企業並無強制遵守的規定，僅係提供產業界及政府等機構應用參考。原則上，政府部門對於 NIST 標準的應用，會依據與聯邦政府簽約的業者，依契約要求業者提供服務時，應符合 NIST 相關標準。

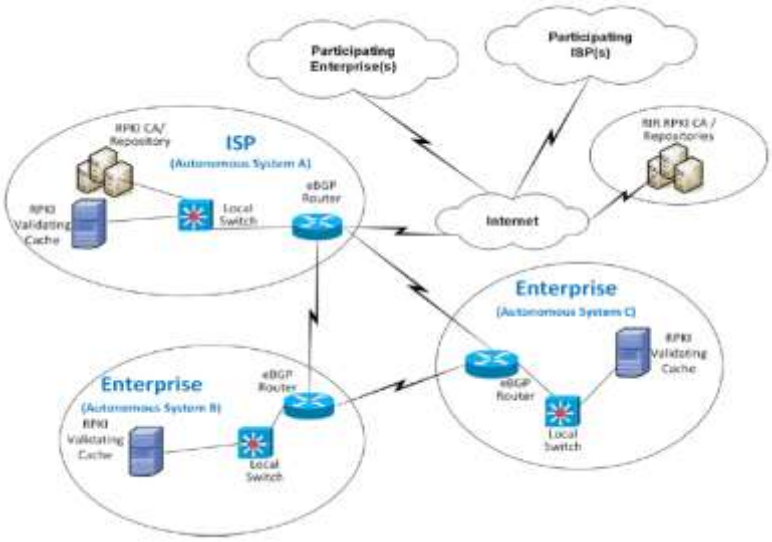


圖 23　ROV 及 RPKI 架構範例說明

(三)與舊金山市警局(SFPD)網路情報與調查主任會談

AIT 商務組專員 Matthew Quigley 安排舊金山市警局網路情報與調查主任 David Chasteen 會談，討論 SFPD 退出聯邦調查局聯合恐怖主義專案小組（Joint Terrorism Task Force , JTTF）之後與聯邦反恐合作關係，以及 SFPD 的國土安全小組的任務及運作情形。C 主任曾於 2003 年於伊拉克擔任第三步兵師化學軍團的上尉，嫻熟生物和化學武器。退伍後曾加入中央情報局（CIA）的國家秘密服務處（National Clandestine Service , NCS），擔任包容性諮詢小組的成員，致力於改善 NCS 的包容性、多樣性和參與度。

有關舊金山市警局退出聯邦調查局的 JTTF，C 主任說明起因在於川普政府的旅行禁令引起爭議，舊金山市公民自由倡導者和穆斯林社區擔心市警局參與聯邦調查局可能違反當地保護移民和宗教少數群體的法律，在他們的壓力下而退出，但市警局為維持情報暢通，仍與 JTTF 透過公務管道保持密切聯繫，所以並未影響情資的交換，只影響來自聯邦政府的資金補助，實際上的運作，仍由市警局在市政

府架構下獨立運作。

至於 SFPD 的國土安全小組(Homeland Security Unit)係於 911 紐約恐攻事件後成立，負責交通系統和關鍵基礎設施的保護，向公民宣導如何準備和應對災難，規劃與執行恐怖主義之打擊行動，因此與地方、州和聯邦執法機構以及其他公共和私人組織保持廣泛聯繫。該小組的特別行動分組特別提供專業知識和設備來支援反恐任務，例如防制爆裂物、偵爆犬、人質談判等，類似我國各地區警察的霹靂小組或除暴特勤隊。

(四)美國業者技術研討會分享

1.F5 公司分享其在 SSL Orchestrator 架構下加密流量安全管理解決方案的探討，由於目前惡意軟體在傳遞過程中，經統計已達 100%加密方式傳遞，比一般應用軟體連線僅 71%加密機制還高，對於偵測及防禦惡意軟體的侵害，已需要即時將傳遞中的每一加密封包先解密檢查是否有異常行為的資源配置。因此，如何以有效率的防禦架構，以達到對每一傳遞中的加密封包進行資安檢視，已是資安防護及電腦資源配置的重要議題。F5 公司介紹其公司目前的產品功能，並簡介其系統運作原理，及如何改善傳統串聯式解、加密流程造成電腦資源耗盡及無法完全檢視每一加密封包內容是否安全的缺點。

該公司表示，其提出的 SSL Orchestrator 5.0 完全動態代理架構之運作架構(詳見圖 24)，具有利用單一解、加密機制，將可整合所有的偵測防禦元件共同運作，經由其代理的統一窗口分別依偵測防禦元件的負載情況，動態分配偵測，以達到每一加密通訊包封皆可進行核對是否有惡意軟體行為，達到資安防護目的。

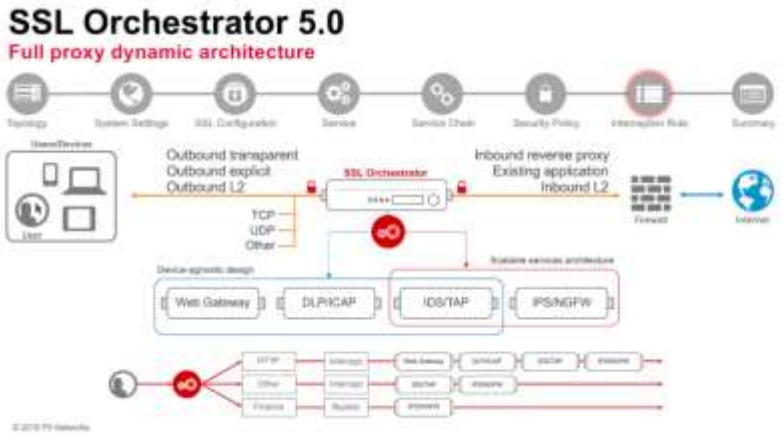


圖 24　F5 公司提出 SSL 加密流量安全管理解決方案

2. Palo Alto 公司與與會者分享如何管理從資訊技術(Information Technology, IT)匯流工控技術(Operation Technology, OT)的網路資安，該公司表示 IT 與 OT 滙流可概念性分為 IT 與 OT 實體隔離之 IT 有資安及 OT 無資安情境；再發展至目前產業界情況為其 IT 與 OT 有相連，且各自皆有其資安措施；未來將發展至 IT 與 OT 的匯流整合式的資安。

該公司表示目前企業在進行其本身 IT 與 OT 融合時，因 OT 領域人員及設施在連網後面臨資安防護措施，與 IT 領域比較皆較不足，各企業皆需面對如何補強因應的課題，該公司認為其可在領域提供相關服務。因此，該公司就其產品特色與與會者進一步分享(詳見圖 25)。

圖 25　Palo Alto 公司提出的網路資安運作平臺架構

參、心得及建議

一、RSA 會議部分

本次參加 RSA Conference 2019 會議發現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、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、國土安全部的網路與基礎設施安全局局長都親自出席擔任講座，而會議中的專題演講與小組討論幾乎大部分主題都在於新興資安議題、創新研究，心得與建議如下：

(一)假訊息納入資安範疇，並鎖定主要對手

美國國家安全局、聯邦調查局、國土安全部的網路與基礎設施安全局局長在談話中，均一致同意美國面臨的風險與威脅之對手來自俄國、中國、伊朗與朝鮮，並將 2020 美國大選的假訊息攻擊、竊取智慧財產權、5G 及新興科技的威脅、網路破壞性的駭客攻擊當作假想敵，公開演講，對於這幾個國家的與會者，毫不避諱，導致展覽會場中，中國的攤位極為冷清，舉辦的小組討論會亦極為低調。對於我國而言，中國亦為資安攻擊的主要來源，需長期防範，但在假訊息方面，雖已引起國人關注，民間亦有自發性成立的事實查核平台，惟仍需要更多的訊息交流，亦可仿效美國的作法：截斷來自外國的巨魔農場的接取，並與社群媒體合作，刪除假帳號。

(二)導入社交工程及攻防技術

1.社交工程防護建議：

必須要認知沒有牢不可破的防護機制、加強對使用者的資安教育訓練、勿點擊來路不明的網址、盡可能透過防護機制阻擋惡意的網址。

2.攻擊技術防護建議：

強制使用 MFA、勿使用 SMS 作為認證管道、建議使用雙向(Mutual)認證、挑選合適的 MFA(能對抗重送攻擊、遵守安全軟體發展生命週期、有帳戶鎖定機制等)、不同 Factor 使用不同的管道、安全提問不要使用正確答案等。

(三)**從新興資安議題驗證我國資安問題**

今年的演講與小組討論會的領域，涉及威脅、加密貨幣攻擊、IoT 安全、勒索軟體、安全基礎架構、隱私等諸多議題，其中包括「訊息戰」，旨在破壞公民對媒體及其資訊消費的信任，利用社交媒體進行影響力宣傳以及人工智慧(AI)和物聯網(IoT)的出現，這些資安的議題非常貼近民眾，且這些問題可能造成的衝擊，相較於傳統的資安問題，將產生更大的風險，針對這類問題的掌握程度及可能影響的層面可能都要投入資源進行研究，例如 107 年度起網路攻防演練納入了工控系統，正可以驗證台灣在這方面是否可能有相關的問題發生。

(四)**探討發掘漏洞之創新方法**

許多講者都是針對系統底層的架構去進行分析與研究，並從中找出各系統實作時的漏洞，或是封閉系統未公開的 API 與資料結構，例如微軟提出的遠端桌面協定，可以讓管理者方便地進行遠端管控，但是微軟是如何實做此協定的？在現在的環境下會暴露哪些風險？暫存資料會遺留在哪裡？是否有可能遭駭客取得？

很多時候我們只會享受某個軟體或某個功能給我們帶來的便利性，但並沒有思考到他背後的實作方式及可能帶來的資安危害。

以往覺得需要利用偵錯和反組譯等困難的技術才能找出原始設計的架構並挖掘漏洞，但其實許多地方都有捷徑可以利用，例如本次會議中有位講者提到他研究 CPU 的漏洞，不過他最後找到 CPU 實作方式並不是透過實驗和測試，而是直接閱讀大量的 CPU 專利文件去找出整個架構的漏洞。

(五)**借鏡資安防護趨勢**

今年的演講與小組討論會中，亦看到幾個幾個資安防護概念逐漸成形，例如系統開發流程導入 DevSecOps，係由 DevOps 衍生而來的新興概念，將開發人員，安全性和操作人員整合在統一的工作流程中；攻防演練中設置紫色團隊，擔任第三方監督及分析紅隊和藍色隊如何運作，促進紅藍兩隊交換意見，相互合作，並談論各種攻擊和防禦；「零信任」假定所有設備和實體都是不值得信任的，除非另有證明等等，均足得關注，並探討運用之可能性或推廣之必要性。

(六)活用 RSA 網路資源

本會議在 5 天內舉行 31 場主題演講、621 場小組討論會，計有 740 名講者，加上 AIT 另外安排參訪活動，實際上無法參與每場演講及討論會，幸好主辦單位於會後向全付費報名者提供重要會議及討論會之紀錄影片與講義，可隨時觀看錯過之演講及討論會，亦可針對機關任務，挑選相關講題，與未能與會之同仁探討國際動態，吸收新知。

二、美國 AIT 安排參訪部分

(一)把握與美國官方互動機會

本次會議承蒙 AIT 商務組協助於 RSA 會議會場外安排與國家標準暨技術研究院、北加州地區情報中心、舊金山市警局官員會談，了解許多無法於網路上獲知的美國政府運作機制，以及美國網路安全與國土安全相關規範之推動情形，並建立聯繫管道，實不可多得的良機，未來可循此模式，於參加國際會議及展覽活動時，儘量安排與官方之接觸，另外 RSA 講者中不乏政府重量級人物，應於會前掌握資訊，請 AIT 安排會談，必要時邀請駐地同仁參與，以確保後續追蹤，擴大外交聯繫管道。

(二)應持續關切國內 IASP 業者 BGP 之正常運作

近幾年美國亞馬遜雲、美國 Level3 配置失誤、Google BGP 設定錯誤及國際金融機構網際互連，分別有發生其 BGP 路由被劫持事件，造成有澳洲、美國等地區服務受影響、美國與全球互連網大規模中斷、日本 NTT 國際網際網路互連產生重大癱瘓、或國際金融交易受影響等情勢。上述各事件，突顯當一網際網路互連業者或交換中心，若有因人員對 BGP 設定不當或不小心重設路由指向時，都可能會造成某網際網路使用者、企業或國家的網際互連產生瞬間的重大危害。因此，美國 NIST 針對如何確保 BGP 有效安全運作，於去年 8 月提出解決方法的指引草案，以降低國家及企業因 BGP 不正確造成的資安風險。該草案未來能否成為業界普遍引用之正式標準指引，值得我國政府及 IASP 業者持續關注，必要時，可做為國內 IASP 業者實施參考，以確保我國國際及國內關鍵基礎設施(CI)的網際互連持續正常運作，並降低 CI 的 BGP 資安風險。

肆、參考資料

[1] USA 2019 | RSA Conference 官方網站,https://www.rsaconference.com/events/us19

[2] NIST SPECIAL PUBLICATION 1800-14，官方網站,https://csrc.nist.gov/publications/detail/sp/1800-14/draft