RSA Conference 2020研習紀要

蘇柏鳴 / 金融聯合徵信中心 資安部

RSA Conference是成立於1991年的IT安全會議，一開始只是一個小型密碼學會議，至今已經發展每年四萬多人參與的大型國際會議，可以稱得上是全球最大的資安產業聚會，不論從與會的人數、展覽場的攤位數，幾乎每一年都是打破前一年的紀錄創造歷史新高。

本文係筆者出席RSA Conference 2020之後，篩選較為重要的4個會議內容與讀者分享，包括：1. RSAC Innovation Sandbox Contest、2. New Paradigms for the Next Era of Security、3. Cyber Defense Matrix Learning Lab、4. The Five Most Dangerous New Attack Techniques and How to Counter Them。其中，RSAC新創沙盒競賽，提供未來資訊安全趨勢走向，藉由入選決賽的參賽公司之服務類型，讓與會者對於未來新型態服務趨勢有個方向；Sounil Yu提出D.I.E.的觀念，來引領思考目前C.I.A觀念，是否在未來典範移轉中會漸漸不適用；另外經由Lab討論的方式來讓參加會議的人，可以更了解Cyber Defense Matrix，並且透過方法論檢視資訊安全是否重複投資，或有哪個區塊尚未補足；最後提到DNS這個服務近30年的模式，遇到了哪些資訊安全上的問題。

一、研習目的

隨著資訊科技的快速發展，便利人們的生活，行動裝置的盛行、雲端服務的普遍、IoT的發展、系統架構的變革（Docker興起）等等，都是近年來資訊快速發展下的產物，導致資訊架構的多元及複雜快速提高，所以當資安防護思維跟不上現實資訊發展速度，就會導致資訊安全作為的實際效果不彰。

舉例來說，近年重大資安事件有：2016年第一銀ATM遭駭事件、2017年遠東銀行SWIFT遭駭事件 、2017券商集體遭DDoS攻擊勒索事件、銓敘部59萬筆文官個資外洩，以及2018年台積電生產線因病毒攻擊停擺事件等，都發生在相對有能力導入資安防護的大企業及政府相關機構上，雖然事件層出不窮，而各個組織也逐漸投入大量人力跟資金至資安防護上，但是目前看來，資安防護速度與駭客攻擊能力手法的競賽中，仍是趨於下風，而聯徵中心收集全台灣人民的信用資料，身為穩定金融責任的重要基石之一，保護好民眾資料並安全的提供徵信給金融機構，就是聯徵中心重要的使命；藉由此次參加全球目前最多人參加的資安盛會RSA Conference 2020，與全世界的資安好手交流，並瞭解目前資安領域最新的資安防護思維，進而提升聯徵中心資安防護能量。

二、研習紀要

（一）RSAC Innovation Sandbox Contest

1. 內容摘要

每年RSA Conference舉辦的創新沙盒（Innovation Sandbox Contest）競賽活動是RSA大會熱門的重頭戲之一，今年已邁入第15年，競賽中創新的題材都是全球網路安全產業中，技術與應用創新的風向指標，可以藉由觀察入圍最後決賽的新創公司的研發方向，來瞭解目前國際上目前資安技術趨勢展的走向。

今年參加團隊共10隊（表1），每個團隊共有3分鐘介紹自己公司服務的內容，最後再由評審提出問題；競賽結果由來自總部在矽谷的SECURITI.ai公司獲得優勝。他們利用AI技術與自動化在不同系統中挖掘並處理結構化及非結構化系統資料，快速檢視組織的隱私狀況與合規風險，幫助組織因應相關法遵面的需求，產品還提供介面讓使用使可以用直覺的語意方式（NLP，Natural Language Processing自然語言處理）來查詢統整的資料。

表 1 RSAC Innovation Sandbox Contest **團隊名單**

	公司名稱	國籍	服務類型
1	AppOmni	美國	SaaS Security
2	BluBracket	美國	DevSecOps安全開發
3	Elevate Security	美國	資安意識培訓
4	ForAllSecure	美國	DevSecOps安全開發
5	INKY Technology	美國	郵件安全
6	Obsidian Security	美國	SaaS Security
7	SECURITI.ai	美國	隱私保護
8	Sqreen	法國	應用程式安全
9	Tala Security	美國	網站安全
10	Vulcan Cyber	以色列	弱點管理

圖 1 SAC Innovation Sandbox Contest

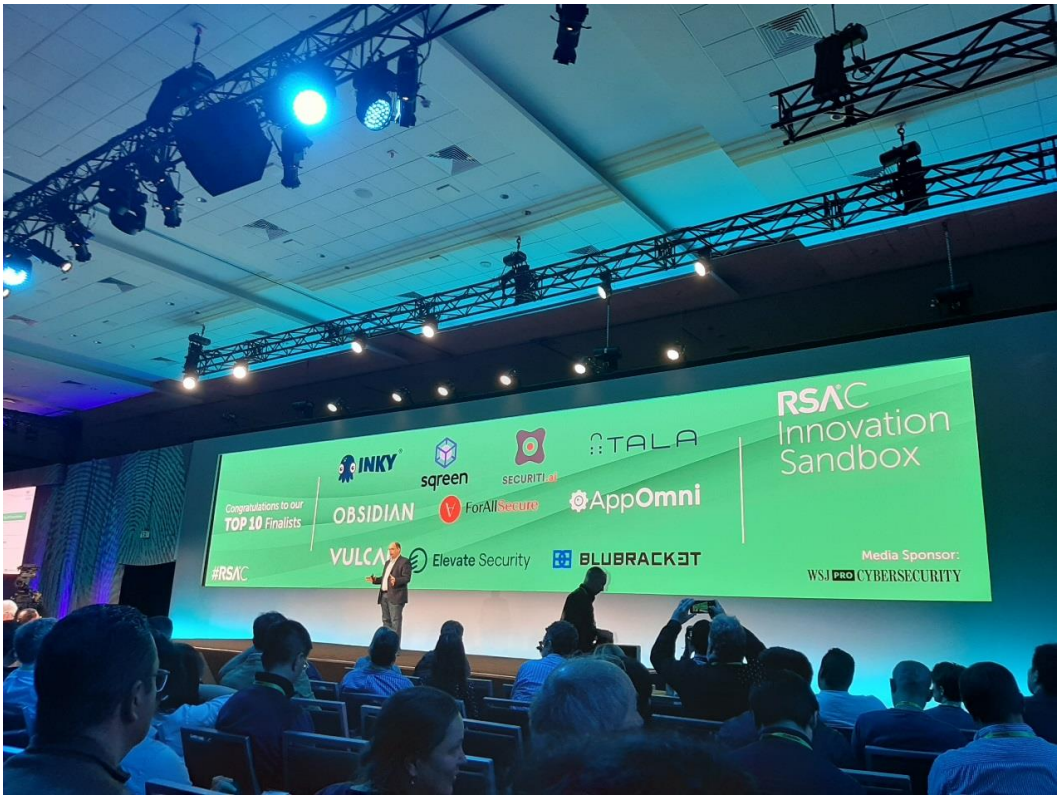
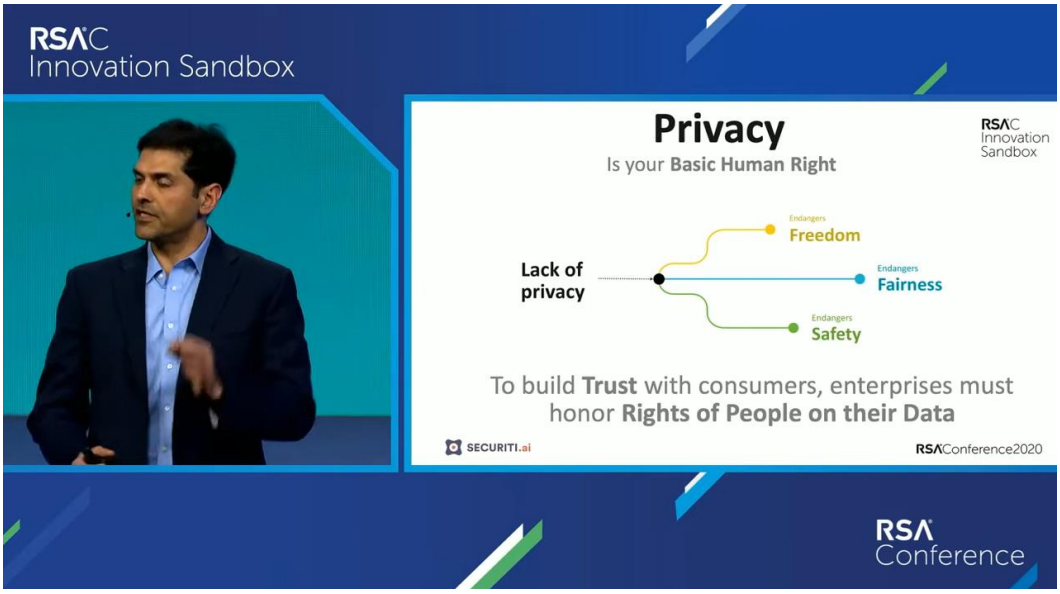


圖 2 獲得優勝的 SECURITI.ai 公司



2. 心得

這個競賽非常精采，從SECURITI.ai獲獎可以瞭解到，目前對於隱私跟法律遵循這領域將是之後資安發展之重點，並且利用AI與高度自動化收集並分析各式類型資料，大大利用AI來處理以前認為廢時的資料統整流程。而與SaaS Security 相關的有兩家（AppOmni跟Obsidian Security），反映了目前Cloud的使用普及，所以對於Cloud平台上的安全控管已是非常重要的的議題。

此外令筆者最有感的就是提出弱點管理的Vulcan Cyber公司，其實駭客攻擊（尤其APT）通常是利用系統內的弱點來慢慢攻克系統主機，再藉由擴權跟橫向移動來慢慢滲透整個網路；就像是一個人的身體如果各個器官都很健康，病菌侵入時就不容易造成身體崩潰，而一個高度資訊化的組織內部，都會擁有可觀數量的系統，摒除Zero Day攻擊不談，光是既有弱點掃描後的管理就是非常棘手的問題，如何在有限人力及資源下，判斷修補策略也將是未來各組織要面對的。

（二）New Paradigms for the Next Era of Security

講者：Sounil Yu（作家、前美國銀行首席安全科學家）

1. 內容摘要

只要是資安領域的人對於C.I.A.絕對不陌生，Sounil Yu覺得是該思考新世代的資安觀念來取代C.I.A，他認為現今2020's應該思考的是如何在資安事件發生後能快速恢復，面對攻擊及威脅資安技術並不萬能的，百密總有一疏，再怎麼防堵資安風險也不可能永遠消失。

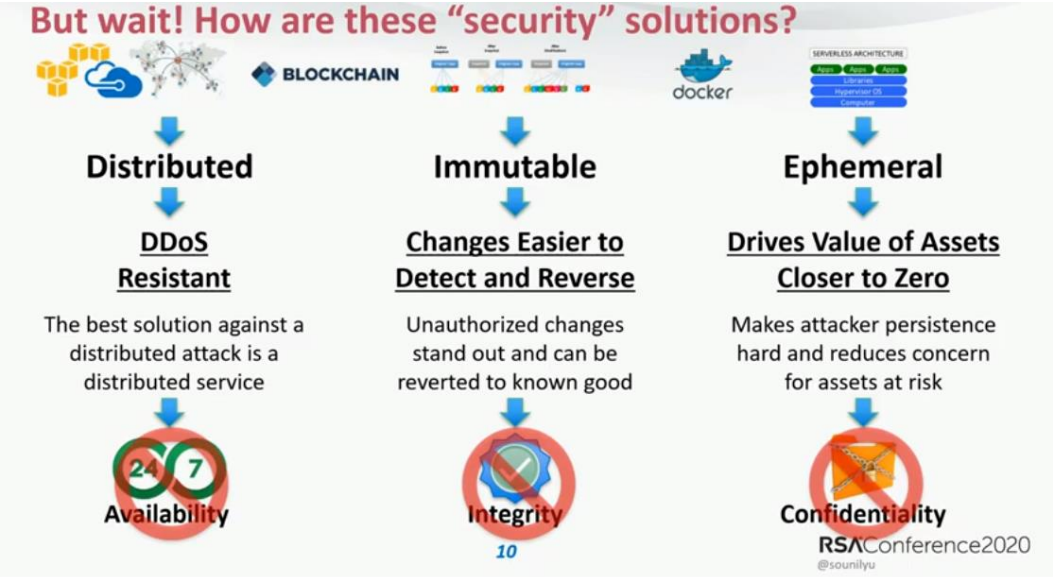
他提出D.I.E.，分散式（Distributed）、不可竄改（Immutable）跟暫時性（Ephemeral），而圖3說明了現在目前的資訊技術與D.I.E.概念的對應：

（1）分散式：內容傳遞網路（Content Delivery Network）、雲端服務及區塊鏈。

（2）不可竄改：寫入時複製技術（Copy on Write）。

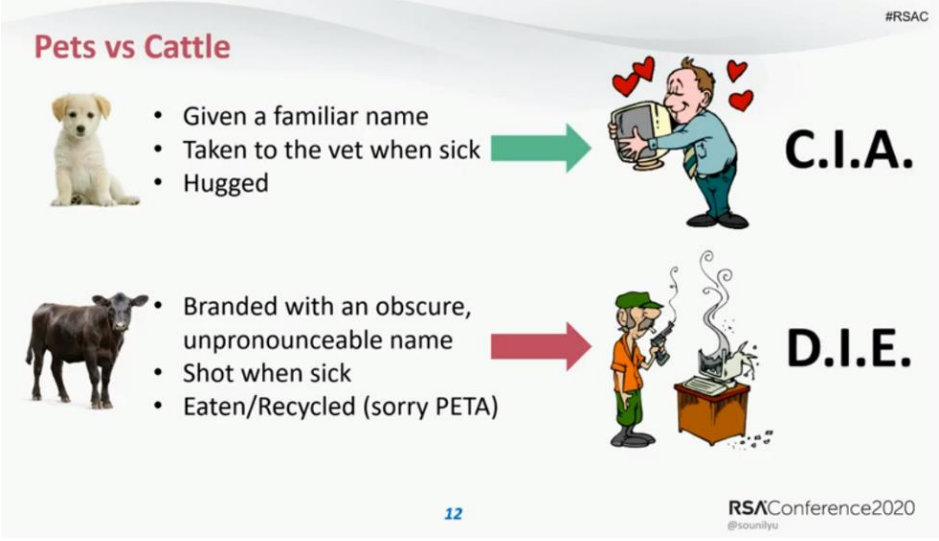
（3）暫時性：Docker及無伺服器架構（Serverless Architecture）。

圖 3 D.I.E. 概念



另外也提到，組織基本上都需要在講求穩定性的資訊長（CIO）跟講求安全性的資安長（CISO）兩者的訴求之間取得平衡。平衡的點偏向哪邊，最後將影響到整體組織資訊資安的施行方向；而傳統的C.I.A.的觀念則是CISO派的核心教條，基於目前的法規限制，我們不可能完全將C.I.A.丟棄，完全走向D.I.E.，講者提出一個有趣的觀點，他覺得應該將組織內的系統／資產分成Pat（寵物）跟Cattle（家禽），Pat有名字，且你會細心的照顧他，而Cattle數量較多偏向功能性但取代性高，所以講者建議要將系統區分成重要跟不那麼重要兩部分，而重要的系統就要跟照顧寵物一樣，用C.I.A.概念管理，而Cattle屬性的系統則用D.I.E.概念管理。

圖 4 Pets vs Cattle



2. 心得

典範轉移（Paradigm Shift）帶來的衝擊都是破壞性的，舊的產品或方法只要發生典範轉移，舊的運行方式就會快速被淘汰。Smart Phone推出後，傳統手機快速消失，如曾經的手機霸主Nokia，也無法扭轉在手機領域被淘汰的命運；科技發展如此快速，目前來說，像是Docker技術的發展，對於系統架構也會產生根本性的衝擊，而資安管理的思維，也必須隨著有所進化，不合時宜的資安防禦概念，也是很大的風險。

（三）Cyber Defense Matrix Learning Lab

講者：Sounil Yu（作家、前美國銀行首席安全科學家）

1. 內容摘要

講者提到網絡安全供應商市場上的產品琳瑯滿目，每次參與大型資安會議時都可以看到一攤一攤的廠商，供應商每個講得口沫橫飛，一堆新穎炫麗的技術名詞，由於資訊安全需求沒有使用一致的術語來描述內容，因此許多供應商產品的實際用途我們無法瞭解。Cyber Defense Matrix通過邏輯結構幫助我們了解我們需要組織的內容，以便在進入資安供應商市場時，我們可以快速識別出哪些產品可以解決哪些問題，並可以獲知產品的核心功能是什麼。

這個矩陣還有一個更重要的部分，在網格的底部，展示了一個連續體，該連續體描述了我們在通過NIST網絡安全框架的五個操作功能前進時對技術、人員和流程的依賴程度，技術在Identify和Protect方面起著更大的作用。隨著轉向」「Detect」、「Respond」和「Recover」，我們對技術的依賴性逐漸降低，而對人的依賴性也在增長；在所有五個操作功能中，對Process的依賴程度始終保持一致，這個連續體有助於我們了解在嘗試解決資訊安全挑戰時，在人員、過程和技術方面可能存在的不平衡之處。

圖 5 Cyber Defense Matrix

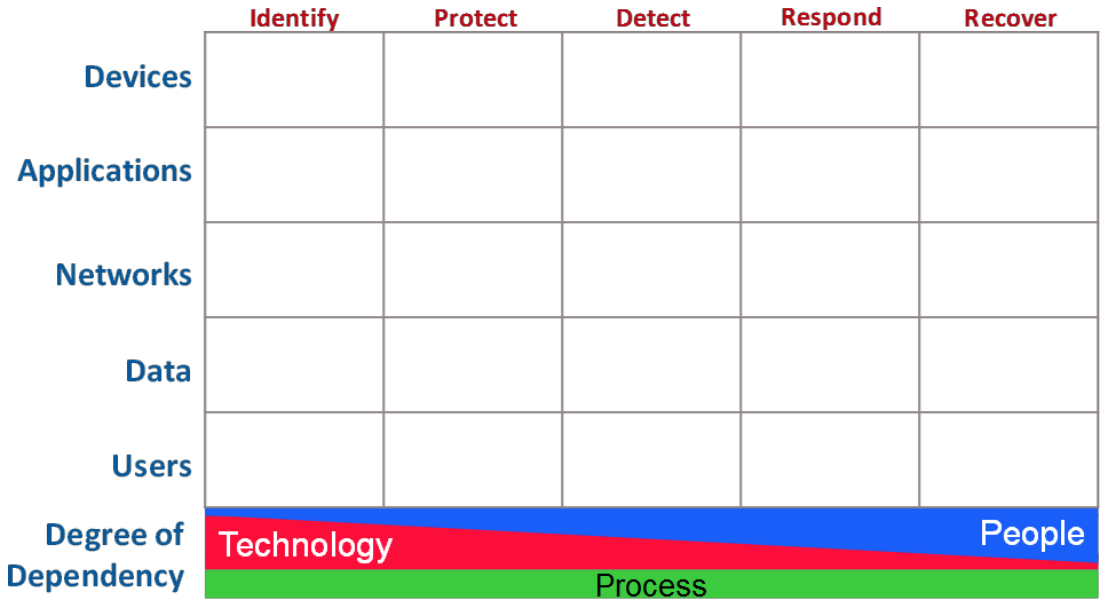
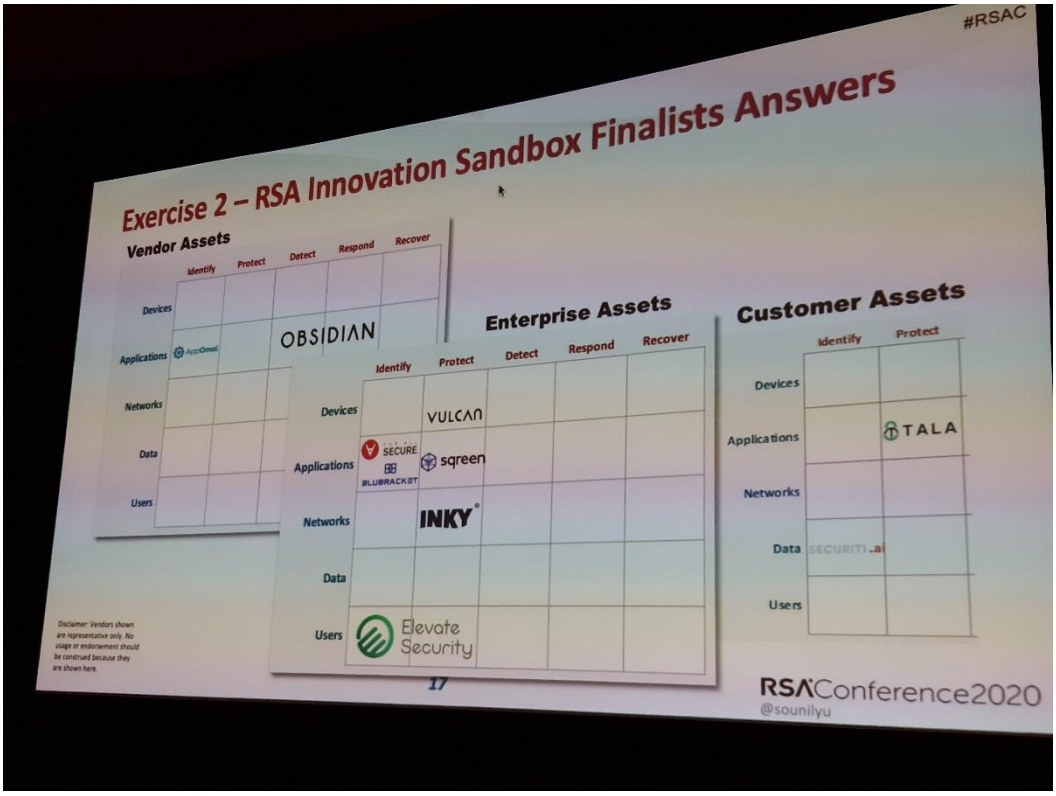


圖 6 將 RSAC Innovation Sandbox Contest 廠商納入 Cyber Defense Matrix



2. 心得

這個矩陣表可以幫助我們了解目前已購買的資訊產品，在矩陣的哪個位置，並且幫助瞭解目前所導入的防護是否有重複投資，也可以從最後矩陣表中知道橫軸「Identify」、「Protect」、「Detect」、「Respond」和「Recover」，與縱軸「Devices」、「Applications」、「Networks」、「Data」和「Users」的關係，從中知道整體防護缺乏或者需要加強的部分，對於整體資安綜合防護提供一個很好的評估整理方法，可將目前防護產品對應其中，提供決策者更直觀更有效的資安產品投資決策依據。

（四）The Five Most Dangerous New Attack Techniques and How to Counter Them

講者：Ed Skoudis、Heather Mahalik、Johannes Ullrich

1. 內容摘要

講者Ed Skoudis提出在他的研究案例中，發現許許多多被駭客用來當作攻擊的媒介，而這些技術也用在滲透測試及紅隊攻擊，在這場會議中他舉出了兩個，manipulation of the domain name system（網域名稱的操縱）跟Domain Fronting。

(1) manipulation of the domain name system：
透過被洩漏出來的帳號密碼登入DNS提供商及名稱註冊商內，操縱DNS的MX紀錄，誤導原本指向為不該指向的位置；舉例來說，會讓發往組織的Email實際上被重新定向到惡意郵件伺服器，以便通過這種攔截Email方式，更甚者申請TLS證書，證明為Domain的擁有者，給這樣的行為給一個貼切的名稱，DN espionage，如何防禦這種攻擊：

＊管理員登入需要雙因子認證，更改DNS基礎結構時至少要有兩步驟驗證，無論是自己的控制的基礎架構或者第三方的基礎架構。

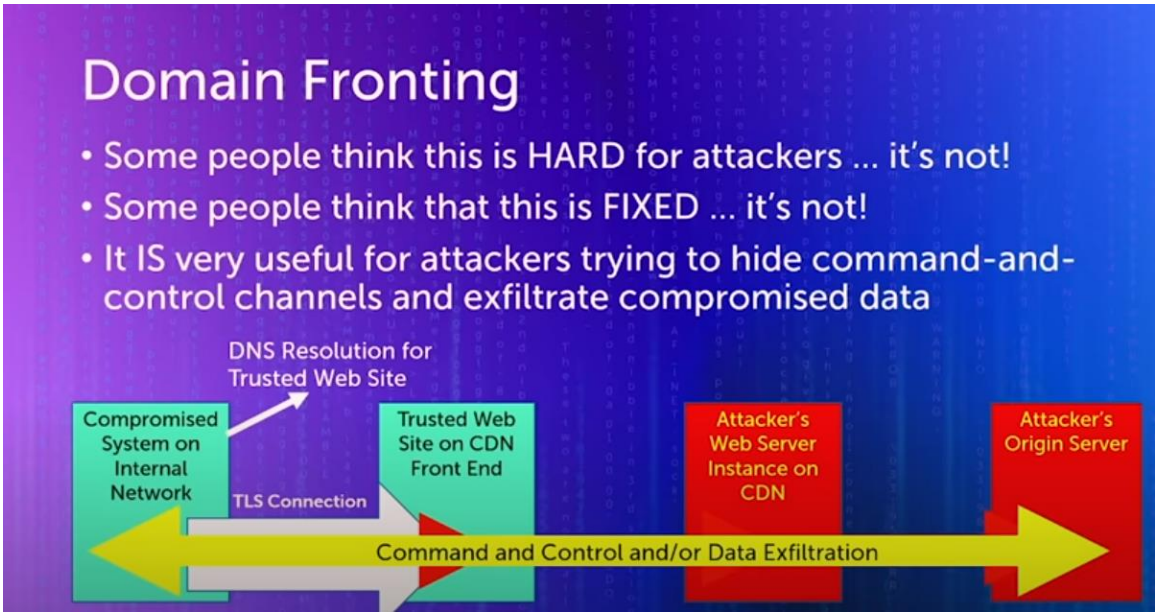
＊DNS SEC 記得Sigh及驗證DNS紀錄。

＊撤銷不良的憑證。

＊監視DNS紀錄，這可以靠一些免費服務，例如一個名為SecurityTrails的安全組織，可以通過API請求，查找與DNS相關聯的任何更改，可以寫些Script程式來追蹤。

(2) Domain Fronting：
其特點在於你真正訪問的變數名稱，並不是你看到的變數名稱，即可以隱藏攻擊者的真實位址，並且此技術能夠讓我們在一些受限制的網路中，依然連接到C2伺服器，其關鍵是在不同的通信層，使用不同的變數名稱，在HTTP（S）請求中，目標變數名稱通常顯示在三個關鍵位置：DNS查詢，TLS（SNI）拓展及HTTP主機Head中，通常這三個地方都會是我們要訪問的變數名稱位址，然而，在Domain Fronting請求中，DNS查詢以及SNI攜帶了一個變數名稱（前域），而在HTTP host頭中攜帶了另一個功能變數名稱（隱蔽的，被禁止訪問的變數名稱）。

圖 7 Domain Fronting



Heather Mahalik提出的是具有目標性的個人攻擊（Target, Individualized Attacks），對於個人在網路上的訊息收集，來逐步入侵使用者使用的相關線上服務，而當你在使用網路上免費的服務時，是否有注意一些隱私設定。舉例來說，有些人會在Facebook公開生日或常用Gmail，這些都是提供攻擊方第一步的攻擊資訊，而當有一個你使用的服務被駭客入侵後，他能擷取更多資訊往下一個服務入侵，結尾講者提到雙因子認證密碼，是可以很有效避免掉被入侵的危機。

第三位講者Johannes Ullrich，他說安全的難題始終是某些安全性與隱私，例如要上網然後連至組織內自己建立的recursive DNS，裡面記錄著所有上網的資訊，因為Recursive DNS會將詢問過的IP資訊儲存至Server上，提高DNS查詢的效率，上面的資訊也能提供當成資訊安全控管的重要資訊；但在與recursive DNS連接時，如果中間有人可以監聽封包，那隱私部分將會暴露，為了解決這個問題，DNS over HTTPS（DoH）是一個好方法，DoH進行安全化的域名解析的方案，其意義在於以加密的HTTPS協定進行DNS解析請求，避免原始DNS協定中，用戶的DNS解析請求被竊聽或者修改的問題（例如中間人攻擊），來達到保護用戶隱私的目的。

2. 心得

講者就DNS衍生出來的問題，即目前使用者網路資訊揭露造成的風險提出見解，其實問題的核心皆在於帳號密碼的保護跟驗證，DNS紀錄修改也必須有帳號密碼，網路上服務透過個人資訊揭露，進行密碼修改也跟密碼有關，最後結論時三位講者一起提到多因子認證是目前防護的最重要關鍵，而密碼被嘗試登入失敗也必須要有警))告通知；最後我個人對於manipulation of the domain name system解決的方法最有感的就是監控，資訊安全防護最重要還是建立在你是不是有發現被攻擊這件事，資訊化的結果就是會有一堆的資訊系統產出，有效監控並對異常快速反應才是目前資安最合適的方針。

三、心得及建議

RSA是一個IT資安頗具盛名的大會，從小型的會議逐漸受到眾人矚目，每年參加人數更是超過數萬人，參展廠商超過500家，大會上的博覽會是業界領先的公司在此展示最先進的產品和解決方案，以幫助客戶保護組織的安全，在展區特別吸引我注意的是早期博覽會（Early Stage Expo），這是一個新創舞台，裡面聚集了51家的資安新創廠商，這些新創在此展示他們的資安新興應用與產品，主要分成五大類：

1. 雲端資安解決方案（Cloud Security）

2. 企業與應用解決方案（Enterprise Security）

(1) 電子郵件防護（email protect）

(2) 資料保護（data protect）

(3) 身分確認與存取管理（Identity and Access Management ，IAM）

(4) 應用層保護（Application protect）

(5) 監控與日誌分析（Monitor and Log Analyzer）

(6) 網絡安全（Network Security)

3. 端點保護（End-point Protection）

4. 弱點探析與風險評估（Vulnerability and Risk Assessment）

5. 資安部署與維運（DevOps Security）

今年RSA新創發展的主軸，還是在於企業與雲端的資安偵測與防護的解決方案，包含企業內主機設備防護、網路防護、電子郵件防護、身分確認與存取管理，雲服務的防護以及跨雲服務間資料傳遞加密保護等等。另一個需求上升的趨勢則是佈署與維運部分，伴隨開源觀念的普及，跨團隊開發、佈署、錯誤修正、維運的難度大增，因此如何利用自動化、智能化的工具來輔助開發部署流程，讓整體程序更節省人力、更安全的概念受到關注。

除了廠商參展外，有關各種面向的資安議題的討論更是多達數百場，今年RSA主題是Human Element（人性元素），人工智慧、5G網路、物聯網與雲端架構，這些當前最受關注的技術讓資訊科技與人之間的距離越來越緊密。然而，儘管技術一直在進步，但人類本身始終沒有變過，科技與生活的緊密連結反倒為駭客提供前所未有的舞台，當民眾沒有足夠的資安意識與習慣，科技的滲透只會放大「人」這個漏洞，所以「好的資安」不再從高深的技術所定義，它也可以是一套從人的角度出發、能夠盡量避免人性漏洞的制度與文化。

關於資安意識，長久以來資安產業都慣於採用恐懼訴求，向大眾灌輸諸如「如果你不做什麼，那麼駭客就會有機會找上門」的觀念。然而，我們可以看到這種行之有年的作法，並無法有效在普遍的資安意識，其原因不在於恐懼訴求本身沒用，而是我們的用法不對。

一般來說，現代人都知道「駭客是真實存在的，而他們的確會造成各種危害」，但他們通常會抱持著逃避的心理，認為那些駭客才不會盯上自己。所以建立大眾資安意識的第一件事，就是讓溝通對象明確知道自己從來就不可能置身事外，讓大家有了危機意識之後，我們就要想辦法讓他們採取實際作為；因為他們多半不具備資安知識，而這樣陌生的感覺會放大他們的恐懼與抗拒心理，因此我們所提供的解決方案不僅要有用，更要越簡單明瞭越好。像是「每半年換一次密碼，而且要兼有英文大小寫、數字與特殊符號」這樣麻煩的要求，一般人看到肯定直接拋在腦後；「採用一個長度超過 15 字元的密碼」則會是更加合理且具可行性的做法，微軟承認，定期使密碼過期是古早且過時的安全作法，效益極低，微軟現在不認為還有必要在安全基準要求中保留這條政策；而在移除密碼有效期限後，企業可以選最適合他們的安全管理措施。

當我們提供了（足夠簡單的）指引與工具，人們才能更有機會落實行動；也因此，我們不能奢望一蹴即成，期待一般人馬上就能學會並執行所有的資安守則。我們需要按照難易程度與重要性，慢慢培養資安習慣，久而久之，我們才有可能逐步拉升大家的資安意識。所以資安產業不能只專注技術上面，需要重新思考什麼叫做好的資安設計，好的設計不是只是展現高深的技術，而是讓高深的技術用簡單的方法表達出來；所以資安產品需要從產品設計到行銷包裝的思維，應該站在一般大眾角度思考，如果不這麼做的話，人始終會是整個資安體系最大的破口，而這個破口永遠不法被彌補起來。