出國報告（出國類別：其他）

出席2017年物聯網資訊安全高峰會出國報告

服務機關：國家通訊傳播委員會
姓名職稱：陳科長坤中
洪技正嘉璟
派赴國家：美國
出國期間：**106**年**10**月**21**日至**10**月**27**日
報告日期：**106**年**12**月**26**日

摘要

物聯網快速崛起並被運用於多元領域，為產業及社會帶來了便利性及創新應用，但伴隨而來的是新的資訊安全挑戰，如何強化物聯網資安防護已成為各國政府日益重視之課題。

為瞭解物聯網資安威脅趨勢及國際間物聯網資安檢測標準發展情形，國家通訊傳播委員會（以下簡稱本會）積極參與物聯網及資安相關國際會議，「物聯網資訊安全高峰會（IoT Security Summit）」是全球大型的物聯網資訊安全會議，2017 年 10 月 23 日至 24 日於美國紐約舉辦的第 3 屆會議探討的議題相當廣泛，包括物聯網互通性及資安標準、物聯網基礎設施保護、消費性及工業物聯網防護、5G 物聯網應用及運用人工智慧等新興技術保護物聯網服務等議題，相關主題深具前瞻性，可作為本會未來研訂相關物聯網資安檢測指引及政策之參考。

本次會議主要聚焦於物聯網安全技術及隱私保護的討論，讓物聯網製造商、服務提供者、安全解決方案提供者、政府機關、標準制定機構等在開放的氛圍中進行交流與溝通，提供與會者學習及經驗分享的機會。

目　錄

壹、前言

依ITU-R於2015年7月發布之2020至2030年國際行動通信流量預估，物聯網裝置於2020年將達到70億台、2030年更會高達970億台，年均複合增長率達30.1％。這些裝置將廣泛應用於智慧電表、智慧物流、遠距醫療、車聯網、環境監測等多元領域，由連網裝置蒐集、取得之數據可在分析後持續運用在不同的情境中，將大幅改變產業及社會之型態。

物聯網裝置帶來了便利性與創新應用，但伴隨而來的是新的資訊安全挑戰，據市調公司Gartner預測，至2020年企業所遭受的攻擊中將有25%以上與物聯網相關，而物聯網裝置具備之上網能力及所蒐集的資訊（包含個人隱私、企業機密等）更為駭客所覬覦，一旦遭受駭客攻擊將造成巨大的威脅。

物聯網時代與網路匯流已是不可免之趨勢，也隨之衍生諸多資安風險。如何強化物聯網設備資安防護並防範駭客進行網路犯罪及恐怖攻擊，已成為各國政府必須嚴肅面對之課題。因此，通傳會積極參與物聯網及資安相關國際會議，以深入瞭解物聯網資安威脅相關趨勢、國際間物聯網資安檢測標準發展情形及各國推動物聯網商品資安檢測優先順序，並作為未來研訂相關物聯網資安檢測指引及政策之參考。

圖表1：2017 IoT Security Summit關鍵議題

資料來源：大會網站

物聯網資訊安全高峰會（IoT Security Summit）是全球大型的物聯網資訊安全會議，該會議結合研討會及展覽性質，探討議題相當廣泛，包括物聯網互通性及資安標準、物聯網基礎設施保護、消費性及工業物聯網防護、5G物聯網應用及運用人工智慧等新興技術保護物聯網服務等議題，藉由汲取最新的物聯網資安技術趨勢，研擬尋求務實解決方案。

今年在美國紐約舉辦的是第3屆的物聯網資訊安全高峰會，並與區塊鏈（Blockchain 360）及雲端安全高峰會（Cloud Security Summit）共同進行。本次會議的第一天主要聚焦於物聯網安全技術，第二天的會議則是針對隱私保護的討論，將物聯網製造商、服務提供者、安全解決方案提供者、政府機關、標準制定機構等聚集在一起，在開放的氛圍中進行討論與溝通，提供參與者學習與經驗分享的機會。

圖表2：2017 IoT Security Summit參與單位

資料來源：大會網站

貳、行程安排

一、出國時間：2017 年 10 月 21 日至 10 月 27 日

二、地點：美國紐約

三、本會出席人員：

（一）基礎設施事務處陳科長坤中

（二）基礎設施事務處洪技正嘉璟

四、時間安排

日期	行程
10/21 (六)	臺北－舊金山－紐約
10/22 (日)	抵達紐約，準備會議資料
10/23 (一)	物聯網資訊安全高峰會 第一日
10/24 (二)	物聯網資訊安全高峰會 第二日
10/25 (三)	整理會議資料及私人行程
10/26 (四)	紐約－臺北
10/27 (五)	抵達臺北

參、2017 年美國紐約物聯網資訊安全高峰會

一、會議時間：2017 年 10 月 23 日至 10 月 24 日

二、會議地點：紐約時代廣場洲際酒店（InterContinental Times Square）

圖表3：2017年物聯網資訊安全高峰會

資料來源：IoT Security Summit網頁

圖表4：物聯網資訊安全高峰會會場

三、會議議程：

（一）第一日（10 月 23 日星期一）

共享主題演講 （Shared Keynotes）	
8:50	歡迎致詞 Opening Remarks
9:00	下世代網路安全及物聯網的興起 The next generation of cyber security and the Rise of IoT 主講人：Juniper Networks安全技術與策略長(Security CTSO) **Kevin Walker**
9:20	雲端安全 Secure Cloud 主講人：Wellmark Blue Cross Blue Shield資安長（CISO） **Thien La**
9:40	建構值得信賴的物聯網系統 Building Trustworthy IoT Systems 主講人：Microsoft Azure物聯網安全長（CISO） **Dr. Arjmand Samuel**
10:00	從惡意安全破壞中學習 Learning from Infamous Security Breaches 主持人：The Coca-Cola Company隱私長**Katherine Fithen** 與談人：Fortune500 Media Company首席安全工程師**Arun Hegde** Wellmark Blue Cross Blue Shield資安長（CISO） **Thien La** PricewaterhouseCoopers資安總監**Weifeng Li** ➢回顧產業間近期的大規模企業攻擊行為 ➢惡意行為者可以利用哪些漏洞 ➢我們如何更好地因應，並使企業促進安全供應商合作
10:40	休息時間
物聯網安全技術討論 （IoT Security Technical Discussion）	
11:30	來自物聯網殭屍網路的威脅逐漸演進，如何保護物聯網裝置免受攻擊 Evolving Threats from IoT Botnets : A Closer Look at Defending IoT Devices Against Attacks 主講人：Allegro Software行銷副總裁**Loren Shade** ➢「無安全防護（Unsecure）」的完美風暴 ➢了解物聯網設備如何武器化 ➢物聯網殭屍網路「租用」市場 ➢物聯網防禦－降低風險

11:50	使用案例：數據及裝置如何保護產業－支付、運輸、媒體 Use cases: How are data and devices secured across industries- Payments, Transportation, Media 主持人：Lux Research高級分析師**Shriram Ramanathan** 與談人：UPS首席安全工程師**Vijay Vedanabhatla** Fortune500 Media Company首席安全工程師**Arun Hegde** MasterCard資深總監**Mandar Kawle** Coalfire總監暨網路風險顧問**Abel Sussman** GreatBay Software總工程師**Seth Jeacopello** ➢如何建立一個確保物聯網安全措施的發展計畫 ➢建構行動支付基礎設施安全的重要性 ➢運輸業面臨的主要漏洞，及領導者如何處理這些問題
12:30	管理電腦安全 Managing Computer Security 主講人：Verizon高級安全工程師**Marvin Stein** ➢對組織有效的資訊安全計畫 ➢意識到 IT 安全需求的重要性、了解網路安全漏洞及矯正措施 ➢如何識別及管理組織可能面臨的資安風險 ➢數據如何受到攻擊、資安漏洞可能會造成的損失、保護運作的實際措施、如何利用資安供應商及顧問、依據需求評估工具及技術
13:30	保護未來智慧建築的安全 Securing Smart Buildings of the Future 主講人：Johnson Controls全球產品安全技術服務總監 **William Fitzgerald**
13:50	免疫系統方法：運用人工智慧保護物聯網裝置 An Immune System Approach: AI Cyber Defense for IoT Devices 主講人：Darktrace網路智慧與分析總監**Justin Fier** ➢了解威脅如何瞄準網路內的物聯網裝置，及企業如何運用免疫系統防禦措施在威脅提升前識別威脅。 ➢機器學習及數學如何自動化偵測雲端的威脅 ➢實際及虛擬環境 100%網路可視性的重要性 ➢智慧優先順序及可視化可有助於更好的資源分配及快速減輕威脅 ➢企業免疫系統技術偵測威脅之實際案例
14:10	所有工作都與安全相關：儲備工作能量以阻止及處理資安挑戰 All jobs are security jobs: Preparing the workforce to prevent and handle IT

	security challenges before they happen 主持人：Lux Research高級分析師**Shriram Ramanathan** 與談人：Verizon高級安全工程師**Marvin Stein** Praetorian行銷副總裁及物聯網業務負責人**Paul Jauregui** Applied Technology Solutions技術長**Nikhil Kumar** ➢安全必須是所有技術培訓的重要部分 ➢高階主管應策略性思考治理、風險及承諾
14:50	休息時間
15:50	資源受限物聯網裝置之安全性 Trust in Resource Constrained IoT 主講人：美國國防部資訊保護研究物聯網組長**Paul Philip** ➢提升安全性將為資源有限的物聯網帶來巨大的回報。 ➢在晶片、終端設備及系統層級灌輸信任和保證以減輕各種漏洞的影響。
16:10	物聯網／智慧及安全城市與社區的挑戰：網路安全對話 IoT/Smart and Secure Cities & Communities Challenge: Cyber Security Conversation 主講人：DHS Science & Technology網路安全處副處長 **Scott Tousley**
16:30	尋求跨物聯網層面的安全解決方案廠商的合作及互通 Seeking collaboration and interoperability among security vendors across the IoT stack 主持人：Lux Research高級分析師**Shriram Ramanathan** 與談人：Sigma Designs技術服務經理**Mariusz Malkowski** Juniper Networks安全網路產品管理總監**Srini Nimmagadda** Vaxxin總裁**Nick Yuran** Citrusbyte執行長**Brady Brim-DeForest** ➢建立物聯網解決方案互通性的標準 ➢保持工業及消費者物聯網企業的要求在最前線 ➢投資銀行及安全併購公司如何構建未來最強大的安全廠商

（二）第二日（11 月 30 日星期三）

共享主題演講 （Shared Keynotes）	
8:50	歡迎致詞 Opening Remarks
9:00	網路空間的冷戰逐漸加溫

	The Cold War in the Cyberspace is Getting Hotter 主講人：北大西洋公約組織（NATO）網路中心代表 **Kenneth Geers** ➢區塊鏈及數位身份有潛力將超過 30 億非銀行用戶帶入世界經濟中 ➢我們應該如何負責地處理這個劇烈的變革
9:20	物聯網安全由邊緣開始：從邊緣到雲端的最佳安全措施 IoT Security Begins at the Edge: Security best practices from the edge to the cloud 主講人：VMware物聯網研發總監 **Salim AbiEzzi**
9:40	從人類發展的角度看區塊鏈 Blockchain from the perspective of human development 主講人：聯合國合作及創新首席分析師**Lambert Hogenhout**
10:00	全端安全包－物聯網及雲端安全＋區塊鏈＋隱私及身分 The Full Stack Security Package – IoT & Cloud Security + Blockchain + Privacy and Identity 與談人：Cooley合夥人**Andy Roth** Pricewaterhouse Coopers董事總經理**Radoslav Bakalov** OneWorldIdentity創辦人**Cameron D'Ambrosi** ➢新興技術區塊鏈將如何影響安全環境 ➢數位身分對世界經濟的意義 ➢目前的雲端運算及物聯網安全廠商如何利用區塊鏈來提高安全性 ➢區塊鏈面臨的安全挑戰，及安全工程師如何解決這些問題
10:40	裝置、網路及使用者的物聯網安全 IoT Security for devices, networks and people 主講人：SurePassID業務開發副總裁**Kevin Raineri**
10:50	創造一個不可駭入的物聯網平臺 Creating an Unhackable Platform for IoT 主講人：BlastWave共同創辦人**Blaine Garst**及**Tom Sego**
物聯網隱私保護 （IoT Security Track–Privacy Focus）	
11:10	聯網家庭是傻瓜的天堂？ Connected Home A Fool's Paradise? 主講人：Dojo by Bullguard執行長**Yossi Atias**
11:30	安全的物聯網 The Internet of Trusted Things 主講人：Mocana執行長**Bill Diotte**

11:50	使用案例：允許那些人擁有數位身分？ Use cases: Permissioning: Who Owns Identity in the era of Digital Identity? 主持人：151 Advisors合夥人**Steve Brumer** 與談人：NATO網路中心代表 **Kenneth Geers** Cyber Science Institute常務董事**Robert Katz** Zingbox創辦人**May Wang** ➢一旦數位身份被大量採用，如何進行個人資料的管理 ➢數位身份的法律疑慮為何？新模式可能存在那些風險？
12:30	白帽駭客展示 White Hacking Demo 主講人：Independent Security Evaluators安全工程師**Josh Domangue** Independent Security Evaluators業務分析師**Kevin Thomas** ➢針對生醫裝置（如患者監護儀器）的展示 ➢介紹漏洞可能產生之護理及安全性影響，及補救這些裝置的可行方法
13:30	在現今的安全環境下所面對之身分及接取管理挑戰 Countering The Challenges In Identity And Access Management Within Today's Security Landscape 主講人：CVS Health & Infragard資訊安全營運 **Kathy Braun**
13:50	安全性設計 Security By Design 主講人：Intertek物聯網計畫經理**Delmar Howard** ➢威脅環境及目前的風險、物聯網的設計 ➢新興行業法規的影響
14:10	當企業安全變成國家安全議題 When enterprise security becomes national security question 主持人：151 Advisors合夥人**Steve Brumer** 與談人：Leidos首席網路安全策略師**Gib Sorebo** Guardknox執行長**Moshe Shlisel** Cyber Science Institute執行董事**Robert Katz**
14:50	醫療照護所使用的信任物聯網 The Internet of Medical Things Used in Healthcare 主講人：Zingbox創辦人**May Wang** ➢提升安全性將為資源有限的物聯網帶來巨大的回報。 ➢在晶片、終端設備及系統層級灌輸信任和保證以減輕各種漏洞的影響。

四、會議重點：

（一）第一日（10 月 23 日，星期一）

(1)下世代網路安全及物聯網的興起－Juniper Networks

隨著資通訊科技的演進，物聯網、IPv6及5G快速發展，未來可能所有的物品都有一個IP位址，這些數量龐大的IP位址及具有計算能力的連網裝置卻可能引發管理上的災難。近年來Mirai、WannaCry等惡意軟體造成的安全性威脅不斷增加，裝置迫使業者重新思考網路安全問題，促使網路安全議題邁向下個世代。

這些網路攻擊事件並非新鮮事，但我們卻很容易忽略，其中很大一部分源自於多年來一直存在的常見問題，但隨著物聯網裝置預估將在3年內達到200億台，經由這些數量龐大的裝置發動網路攻擊，將有可能破壞任何的基礎設施。

另外，大多數的物聯網裝置皆具有感測器，例如電視機上的麥克風、手錶上的心律監測，相較於把IoT用於大規模的殭屍網路攻擊，駭客可能對這些感測器所蒐集的資料更感興趣。

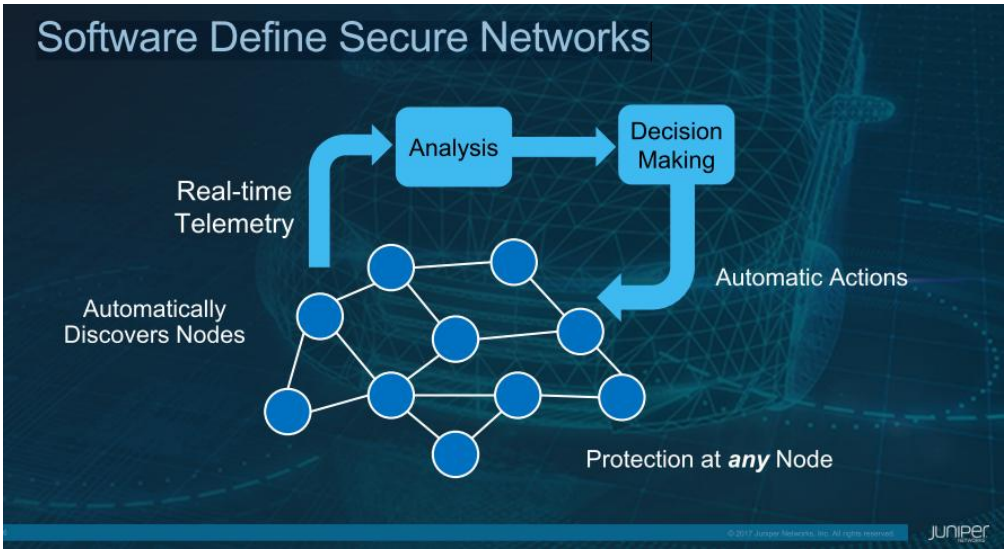
根據最近的一項調查顯示，超過四分之三的組織可能在未來兩年內發生物聯網數據洩露，並造成嚴重的破壞性後果，但卻不一定是因為這些組織缺乏技術性的防禦。

在物聯網時代，網路分割（network segregation）、流量調控（traffic shaping）、阻斷惡意中繼站（CnC blocking）等過去長期建立的網路安全措施仍然可以達到一定的防禦效果。但伴隨物聯網裝置的爆炸式增長，傳統的安全方式已不足夠，下世代的資安防禦必須由目標驅動決策（intent-driven decisions），並增加網路本身的威脅檢測能力，俾在無人監控下更好地偵測及抑制威脅。

Juniper Networks的下世代網路安全包含以下五個技術：遙測及威脅情報（telemetry & threat intel）、自動化（automation）、宣示目標（declarative

intent）、制定決策（decision making）、地區及全球性視野（local vs. global views），藉由及時遙測、大數據分析、機器學習及自動化的方式偵測網路威脅，透過自主分析、發現、配置及修正，達到軟體定義安全網路（software-defined secure networks）的目標。

圖表5：Juniper Networks提出的軟體定義安全網路



資料來源：講者簡報

「分享」是物聯網的一個重要觀念，因此應該將物聯網的資安防護重點放在發生率極高的跨產業共同性問題，如風險管理及網路防禦等，雖然每個行業都有其特定的法律或監管要求，但這也是一個產業間相互學習的機會。

(2)雲端安全－Wellmark

近年來雲端概念逐漸成形，過往的商業模式已大幅翻轉，雲端服務供應商已幫使用者解決許多棘手問題，例如機房建置、資安考量等，使得一間公司開始營運及提供消費者服務所需準備的時間從幾年、幾月縮減至幾週。但是，隨著雲端上的服務不斷推陳出新，雲端的安全性也越來越不容易達成。

透過最近發生的案例，我們可以發現網路安全有以下幾個趨勢。（1）首先，勒索軟體開始橫行，透過簡單、有效的引爆，讓受害者支付贖金，

近期甚至開始出現勒索病毒服務（Ransomware as a Service, RaaS）；（2）新型裝置的攻擊案例亦逐漸提升，2017年開始已有許多聯網醫療裝置受到駭客的攻擊，使得美國食品藥品監督管理局（Food and Drug Administration, FDA）在今年8月召回了6種容易受到攻擊的心律調節器，影響多達46.5萬名患者；（3）社交媒體盛行引發的網路釣魚事件層出不窮，駭客甚至開始利用自然災害進行詐騙募款，今年夏天造成巨大破壞的哈維颶風就吸引許多駭客透過電子郵件及社交網路發送釣魚訊息將善意捐款人引入陷阱；（4）駭客會尋找雲端服務供應鏈中最薄弱的環節，而近期幾個醫療資料洩露的案例皆是源自於第三方供應商的違規。

雖然網路安全是一個日益重要的議題，但對企業來說更重要的是客戶及服務，Wellmark公司認為，雲端服務是一個加強安全控制及公司整體彈性的機會，因此利用雲端服務供應商讓企業更加安全將是一個必然的趨勢。採用安全的雲端技術可以提升數據的可視性、增加對數據的控制能力，確保數據在傳輸及閒置時（idle）均完全加密，自動監控合規性（是否符合產業安全標準、相關法規），並且基於雲端架構的彈性達成業務連續性。

另外，雲端服務提供者及雲端服務使用者各有其管理及保護服務之責任，也就是責任共享（shared responsibility）的概念，很多資安問題其實是源自於使用者資安意識不足，或錯誤設定所造成，因此如何確保雙方皆盡其責亦是確保雲端安全的關鍵所在。

(3)建構值得信賴的物聯網系統－Microsoft

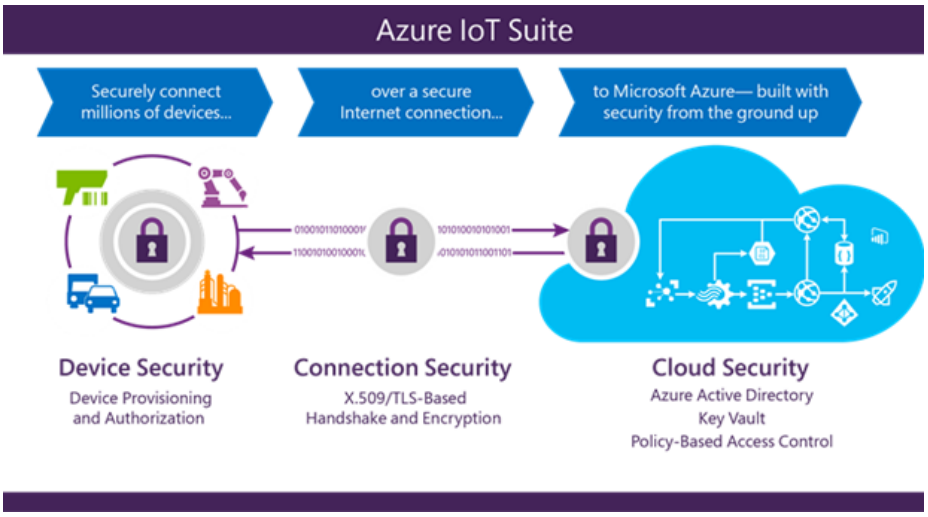
為掌握快速成長的物聯網商機，近年來各企業均致力於開發聯網網裝置及發展創新應用服務，然而，物聯網所牽涉的技術繁雜，不論是建置或規模擴增都曠日費時，因此Microsoft近年來持續發展物聯網裝置至雲端的安全解決方案，協助企業將物聯網簡單、快速地運用於各類型的產業中。

Microsoft開發的Azure IoT Suite包含Azure IoT Hub、Azure Stream Analytics、Azure Time Series Insights及Azure Machine Learning等多種功能，

可以連接、監視並管理龐大數量的物聯網裝置，即時整理、分析所需的資料並轉換成有用的資訊。這一套解決方案可大幅減少企業佈建物聯網所需時間及成本，並且藉由機器學習、大數據分析等新興技術，將及時蒐集的數據轉換成進一步的商機。

伴隨物聯網而來的是新型態的安全、隱私及合規性（compliance）挑戰。端點到端點的物聯網安全包含裝置安全（device security）、連接安全（connection security）及雲端安全（cloud security）等三個部分，首先必須確保物聯網裝置的安全配置及身分認證，再來是使裝置透過可信賴的安全協議（如HTTPS、AMQP、MQTT）連接至雲端，最後則是確保在雲端處理及儲存數據時的安全性。

圖表6：從端點開始保護物聯網



資料來源：講者簡報；Microsoft Azure網頁

提供物聯網服務前，企業應明確了解其物聯網基礎設施可能面臨的威脅，經檢視這些威脅的後果後，仔細評估安全策略，並尋找平臺及其他企業共同合作，以執行物聯網的安全性策略。這需要硬體製造商、物聯網開發者、物聯網部屬者及物聯網營運商等多方緊密合作。透過在製造時加入安全考量、規畫安全更新措施、審慎地使用開源軟體（open source software）、確保身分認證金鑰安全、使系統保持在最新更新版本、經常性稽核、

防禦惡意行為等措施，逐步在每個層面注入安全性防護，以確保物聯網基礎架構的安全性。

保障物聯網的安全性是一個巨大的挑戰，除了利益相關者的優先考量因素不盡相同外，物聯網架構中採用許多不同的通信協議及控制系統也導致整合上的困難，最重要的是截至目前為止的安全標準大多是從資訊業（IT）標準演變而來，缺乏統一的物聯網安全標準，這些都是未來物聯網安全發展所面臨的困境。

(4)討論：從惡意安全破壞中學習

- 資安聯防機制

資通訊科技日新月異，面對層出不窮的資安威脅及駭客攻擊，雖然各企業及組織均有個自資安防護機制，但因商業、合規性考量導致單位間投入資安防護的資源差異極大，造成防護效能參差不齊。因此，各產業、領域應建立完整的資安聯防機制，透過資安監控中心（SOC）、電腦緊急應變中心（CERT）及資安資訊分享與分析中心（ISAC）協同合作，及時偵測網路中的異常行為及潛在威脅，主動彙集資安訊息、資安預警、入侵事件等訊息，並進行跨組織之資安威脅與情報分享。

過去常見的防火牆、防毒軟體的防護與警示功能，已不足夠因應不斷演化的網路安全事件挑戰，唯有藉由有SOC事前監控、CERT事中通報及ISAC事後分享，才能增進資安應變的防禦能力，擁有更堅固的防護體系，，以期降低資安風險或漏洞所造成的損害。

- 資安領域之合規性及政府決策

雲端服務的涵蓋範圍非常廣泛，透過跨領域服務的融合已帶來更多創新、便利的應用，也反應出傳統垂直式的管制模式已逐漸無法滿足匯流時代的需求。舉例來說，連網車輛的相關問題時可能同時與交通運輸部門、通訊傳播監理機關及個資保護機構相關聯，也就是說必須要同時符合很多不同政府單位的法規，而這些法規針對資訊安全保護可能有不同程度的

規定；另外，雲端運算的資料可能分別儲存於不同地區及國家，而不同區域的法規要求也不盡相同，這些因素都導致雲端服務合規性的困境。因此，各國政府應謹慎處理合規性與法規衝突議題，以免扼殺新興技術、產業的發展機會。

另一方面，面對不斷演進的駭客攻擊，政府單位也應主動防禦，降低網路威脅可能造成的嚴重後果。近期，美國國土安全部公開宣布禁止聯邦機構使用知名防毒軟體卡巴斯基（Kaspersky）、中國大陸的網路安全法要求關鍵資訊基礎設施運營者所蒐集之個人資料及重要商業數據必須儲存於中國大陸境內，這些行動正是各國政府基於國家機密資訊、民眾隱私安全風險所做出的防禦性決定。

- 資訊網路保險（Cyber Insurance）的重要性

愈來愈多服務及資源建構在雲端系統，產業技術轉型的同時也帶來了新的資訊安全風險，因此資訊網路保險的重要性就好比金融保險一般，尤其小型企業常因資金因素，無法進行完整的防禦工作，反而更容易受到駭客攻擊。保險公司亦觀察到資安市場，並開始提供網路保險方案，除像理賠企業因資安事件造成的損失外，亦協助客戶評估系統，尋找潛在的安全漏洞，確保問題不會再次發生。

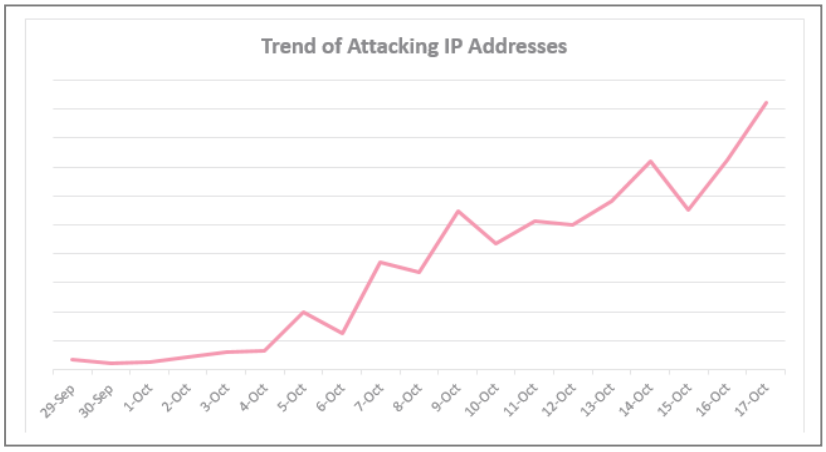
(5)來自物聯網殭屍網路的威脅逐漸演進，如何保護物聯網裝置免受攻擊－Allegro Software

隨著物聯網裝置大量的佈署、越來越多的服務依賴雲端資源、線上駭客團體成熟茁壯，物聯網資安議題更顯重要，但物聯網裝置製造商、物聯網服務提供者及使用者卻仍未建立完善的安全性意識，導致物聯網殭屍網路風暴即將成形。

已經有多個殭屍網路正在快速地發展並吸收物聯網裝置作為DDoS攻擊的工具，即物聯網裝置逐漸「武器化（weaponization）」。根據Check Point Software的報告，由於編碼重複使用導致軟體、硬體漏洞（如CVE-2017-8225

漏洞）出現在大量的IP Camera，這些漏洞造成裝置被惡意程式感染，而受感染的裝置可能再傳播惡意程式至其他類似設備中。據估計，全球已有超過一百萬的機構受到影響，而且數量還在不斷增加中。

圖表7：IP位址攻擊趨勢



資料來源：講者簡報；Check Point網頁

物聯網的安全性包含物聯網裝置/技術使用者及物聯網裝置製造商兩個面向。

在物聯網裝置/技術使用者中，最重要的部分是系統整合商，他們必須明確的知道系統中連網裝置的數量、型態、位置，以及這些裝置所蒐集的資訊如何傳輸及儲存，並採取網路分割等方式降低系統風險，同時亦應建立事件應變計畫（Incidence Response Plan, IRP），規劃緊急事件處理流程與步驟，以降低事件發生時的損害。

針對物聯網裝置製造商，Allegro Software則建議在產品內建「主動式（proactive）」的安全性功能，以硬體信任根（root of trust）、安全的參數與金鑰儲存、安全的裝置更新、營運數據安全性、存取控制與金鑰管理、監控及矯正、經認證的加密方式等七個主動式要素，提升物聯網裝置的安全性。

最後，製造商亦應經常檢視物聯網產品的生命週期，並加強物聯網裝置的遠端更新功能，以適時進行大規模、多樣化、針對性的軟體更新服務，保障所有的裝置都可以維持在最新狀態。

(6)討論：數據及裝置如何保護產業

- 持續進行軟、硬體修補

過去的網路安全防禦較著重於雲端服務、數據中心等網路基礎建設的保護，因此其資訊安全成熟度也較相對高，伴隨大量的物聯網裝置佈署於各個領域，駭客開始將攻擊的重心轉向這些不一定具備安全性功能的連網裝置，如何將過去網路安全防禦的經驗轉移是一個重要的課題。

資安防禦的思維應以整體架構進行全面考量，獨立運作時很安全的組成元件，整合在一起時卻可能產生很多漏洞，另外，系統、裝置設計時應納入安全性考量，其中最重要的一個部分是確保軟、硬體設備可以持續接受修補（patch）更新，使作業系統或應用軟體隨時保持在最新版本狀態，確保所有資安漏洞皆可以被修補，縮短資安漏洞的空窗期，以降低遭受攻擊的可能性。

- 新興技術輔助資安檢測

科技不斷進步，駭客攻擊的手法也持續翻新，過去使用防毒軟體更新病毒碼的方法，已經不足以因應駭客的攻擊。面對數百萬的惡意軟體唯有導入人工智慧、機器學習等技術，取代傳統耗時的人工威脅分析資訊，才可達到多層次的防護功能。

機器首先大量分析網路流量的特徵，經由比對過去資安事件的資料，或即時判讀網路流量中的異常、惡意行為並提出警告，以及協助進行事件後的調查工作。透過這些創新技術的輔助，網路安全產品可以更有效地封鎖威脅，節省資安團隊所需的人力資源，讓人力可以專注於更具挑戰性的工作。

(7)管理電腦安全－Virtustream

美國國家標準技術研究所（NIST）將物聯網視為科技的進化而不是革命，但因為不同類型的系統可能有不同類型的風險需要考慮，所以識別、減輕安全與隱私風險不可能有一個通用性（one size fits all）的方法。因此

，物聯網系統亦引入了新的風險考量因素，劫持通訊通道、修改設備的訊號、竄改感測器的數據等都是可能發生的新興風險。其後果可能只是蒐集到錯誤、不良的數據，也有可能導致嚴重的實體損害，因此我們應意識到資訊安全的重要性，並了解資安漏洞及相關補救方法。

根據NIST的定義，資訊安全係指保護資訊及資訊系統免於遭受未經授權的訪問、使用、揭露，破壞，修改或破壞，以保障資訊的機密性（confidentiality）、完整性（integrity）及可用性（availability）。依據美國聯邦調查局（FBI）發布的2016年網際網路犯罪報告（2016 IC3 Annual Report），去年最受駭客青睞的網路犯罪類型包括變臉詐騙（BEC）、勒索軟體（Ramsomware）及技術支援詐騙（Tech Support Fraud）。報告同時指出，雖然預估只有15%的受害者向執法單位舉報，但這些投訴案件的總損失已高達13.3億美金。因此，評估被駭客攻擊可能造成的潛在損失（包含資訊重建、商業信譽等），並進行適當的資訊安全防護投資實有必要。

資訊安全風險的評估包括識別資安威脅、漏洞及風險等三個部分。資安威脅非常多元化，包括電子郵件詐騙、被惡意程式感染的網站、身分竊取等；資安漏洞則代表容易受到威脅的部分，例如未授權的軟體、缺少完備的程序、不合宜的政策等；資安風險則是漏洞受到威脅後產生的結果，可能是輕微的數據受損，也有可能導致客戶流失及法律訴訟。我們必須了解風險無法完全排除，僅可透過各種控制方式降低發生的可能性，但是標的物如果對資安風險的容忍度很低，或是努力排除後仍然無法有效降低風險，則企業可以考慮透過商業網路保險（commercial cyber insurance）的方式將風險進行分攤。

NIST也提出許多針對使用者的資訊安全性最佳實踐措施，包括不要從未知的來源下載檔案、謹慎開啟電子郵件的附件、加密機敏性數據、經常備份資料（使用雲端備份時應先進行加密）、定期更新惡意程式的檢測工具等。

另一方面，針對物聯網的安全，連網裝置除了要防止硬體被竄改外，提供韌體更新、明確定義數據保護與裝置部屬的程序亦非常重要，而物聯網的網路則應該要採用強而有力的認證與加密機制、安全的協議（protocol），並採用網路分割技術以區分安全區域，同時盡可能縮小連網裝置的頻寬，以避免大量的物聯網裝置成為DDoS攻擊的工具。

(8)保護未來智慧建築的安全－Johnson Controls

物聯網快速崛起，智慧家庭及智慧建築已不再遙不可及，雖然連網裝置將帶來輕鬆、便利的生活，但卻也可能衍伸各式各樣的網路犯罪機會，例如透過監視器偷窺居家或辦公環境、竄改智慧電錶的紀錄、關閉門禁管理系統或氣體感測器、獲取機敏資料的存取權限等，因此隨著智慧建築中連網裝置數的快速增加，資安威脅的風險也日益提升。

為降低智慧建築遭受資安威脅的機率，我們應分別從供應商及使用者兩個面向進行思考。

針對供應商而言，應在設計建築、使用相關物聯網設備時加入安全考量（security by design），相關措施包含產品發展週期、網路安全訓練及意識、原始碼及開源資料庫掃描、漏洞掃描、滲透測試、事件應變處理程序及修補程式更新管理等，供應商應用心設計、橫縱思考，將資安防禦的思維設計於其中以降低資安疏漏導致之危害。

而消費者的部分則著重於安全性管理（secure management），強調使用者資安意識的重要性，相關措施包含變更裝置預設密碼、刪除不必要的服務、限制存取控制的權限、透過安全通訊進行遠端控制、經常進行系統更新、建立應用程式白名單等，確保不會因為使用者管理、操作不當而造成資安風險。

智慧建築貼近人們的生活，帶來許多生活上的便利，但同時也勢必成為駭客重要的攻擊目標，唯有透過供應商在設計時倒入安全性考量及使用者加強安全配置的管理，才可有效控制智慧建築的資安風險。

(9)免疫系統方法：運用人工智慧保護物聯網裝置－Darktrace

為達成自動化及智慧化的目標，近年來越來越多的物聯網裝置被應用在企業、工業及生活環境中，除提高效率、減少資源使用及降低成本外，蒐集的數據經過分析、處理後產生的預測性資訊，亦帶動許多創新服務的發展，並提供人們更便捷的生活。

但是，許多分析報告皆指出物聯網將會成為漏洞的溫床，而傳統特徵碼的防禦工具將無法抵擋這些未來的威脅事件，且物聯網裝置的種類極度多元化，每個類型的裝置都有其獨特地性質，因此Darktrace將人類的免疫系統概念運用到物聯網裝置的資安防禦。每個人體的免疫系統都因個人情況而有所差異，就如同物聯網系統的各式各樣裝置般，Darktrace藉由機器學習的方法，及時自動化地探勘所有連網設備的封包數據，並分析大量數據的關聯性及規律性，建構獨一無二的使用者防護免疫系統，偵測異常行為以達成識別威脅的目的，降低暴露在未知威脅中的風險。

Darktrace的防護免疫系統方法，最重要的部分是識別異常行為，舉例來說，當一個連網魚缸、無線攝影機向外發送大量的數據或是有不尋常的連結時，免疫系統就會識別異常行為，並開始分析該次異常的來源（如連網魚缸、無線攝影機）及駭客攻擊的目標（如竊取企業機敏性資料、使用者帳密），並進行防禦與保護。

(10)討論：所有工作都與安全相關：儲備工作能量以阻止及處理資安挑戰

- 使用者、員工資安意識（user awareness）培養

許多資安問題的源頭是「人」，絕大多數的風險及威脅與使用者的行為息息相關，近年來越來越多組織開始大力呼籲提升使用者資安意識，透過教育訓練讓使用者了解資訊安全威脅對生活、工作可能造成的衝擊與影響，讓他們深切瞭解資訊安全的重要。

資安意識的培養，是一個持續的過程而非一次性事件，安全的文化包含改變使用者操作時的不良存取習慣，如隨意存取電子郵件中的附件、下

載來路不明的軟體，以及建立正確的資安保護措施，包含定期更換密碼、進行資料備份及經常更新設備的軟體與韌體等，藉由這些基本遵循的要領與方向，提升使用者對惡意威脅的警覺性並謹慎地使用網路資源，降低誤觸資安地雷的可能。

- 教育訓練的成本衡量

另一方面，如何衡量教育訓練的成本亦是一個企業經常面臨的問題，也可凸顯企業管理階層與資安團隊思維衝突的所在。討論過程中部分與會者詢問，若考量成本因素，對於短期或約聘員工是否有進行資安教育訓練的必要。講者則回應，教育訓練的確會提高成本，但資安威脅所造成的危害可能造成公司巨大的財務及商譽損失，因此即使只是短期的員工，企業也應該評估這個員工的工作、責任及其可能面對的風險及威脅，並權衡員工訓練的成本及未訓練可能產生的後果，再決定需要進行何種程度的員工安全意識訓練。

(11)資源受限物聯網裝置之安全性－美國國防部

物聯網的安全性逐漸受到重視，美國國防部（Department of Defense, DoD）認為在產品開發的設計階段就應該考量資安議題，並在晶片、連網裝置及系統層級灌輸信任和安全機制，以減輕各種漏洞、威脅的影響。

近年來，DoD及JHU-Applied Physics實驗室，嘗試將可靠的測量及認證（Measurement & Attestation, M＆A）資源引入受限物聯網系統，對個別系統進行完整體性的安全評估。信任框架包含完整性（completeness，足夠的數據量）、新鮮度（freshness，近期的系統狀況）、語義明確性（semantic explicitness，足以做出有效的決定的證據）、真實性（authenticity，確定證據來自被評估的目標）、正確性（correctness，值得信任的數據）、保護（protection，防止數據被破壞）、靈活性（flexibility，支援多種認證協議）、可用性（usability，蒐集的數據經處理可做出有用的決定），該研究論文已被IEEE/ACM及產業會議所接受。

另外，為降低物聯網的潛在安全風險，DoD推動的「安全可穿戴驗證裝置（Secure Wearable Authentication Gear, SWAG）」計畫，透過穿戴於用戶手腕上或身體上的感測裝置，及NFC或藍芽等無線通訊，以確認及確保用戶的身分。當感測器發現用戶遠離使用中的設備時，即會立刻將設備的螢幕鎖定，避免資料外洩發生。

DoD亦與許多實驗室與產業團隊合作，推動一系列關於物聯網裝置安全研究工作，如Secure RFID、CubeSat Trust等計畫。

(12)物聯網／智慧及安全城市與社區的挑戰：網路安全對話－CSD 網路安全處

虛實整合系統（Cyber-Physical System, CPS）與物聯網智慧型裝置近年來開始被應用於改善城市及社區服務，除促進經濟成長外，同時大幅提升生活品質。這些龐大數量的CPS及物聯網裝置快速進入市場並逐漸普及，但是卻缺乏備智慧城市/社區長期發展所需的安全架構及考量，因此美國國家標準技術研究所（NIST）與國土安全部（DHS）正密切合作，期打造安全值得信賴的智慧城市。

其中，NIST與國土安全部所擔任的角色略有不同，NIST主導制定的網路安全框架主要是以定義關鍵基礎設施為目標，而國土安全部則是以非管制的觀點切入，並致力於促進政府單位及關鍵基礎設施在短時間內導入資訊長（CIO）及資安長（CISO）的功能。同時，透過NIST正在推動的「全球城市團隊挑戰博覽會（Global City Teams Challenge, GCTC）」計畫，鼓勵參加團隊將網路安全及隱私保護，視為設計及實現智慧城市的優先考量因素。

面對安全性的挑戰，應先了解系統及威脅的環境，並測試、評估風險發生的可能性，再決定應被優先考量的因素及進行風險管理，最後則是持續的分析、學習及改善。

網路安全及隱私對未來的全球經濟及國家安全至關重要，隨著科技演變的速度不斷加快，安全性議題的範圍、複雜性及影響程度也不斷擴大。

智慧城市的環境正是一個公私合作的機會，雙方透過持續的對話共同研發解決方案，以建立足夠安全智慧城市。

(13)討論：尋求跨物聯網層面的安全解決方案廠商的合作及互通

- 物聯網的互通性（interoperability）

物聯網的應用案例數以千計，但是截至目前為止已經開始的實施方案仍不多，「互通性」即是其中一個關鍵因素。

未來，物聯網的觸角將深入民生、汽車、自動化、醫療等各個產業領域，網路中將包含數以億計的連網設備，製造商依據各自商業考量開發出各種裝置，因無法共用標準及解決方案，將使網路處於破碎分裂的危險之中。

互通性就是讓各系統間可以互相溝通、連成一體，讓消費者容易使用，並獲得更好的使用體驗。但同時，互通性代表物聯網裝置間可以相互溝通交換資料，甚至可以遠端執行命令，這些情況都可能伴隨資安議題。

與會者提出，若由單一廠商自行考量互通性的資安問題，可能使該產品的成本大幅提升，因此建議由元件供應商著手，在晶片中加入資安功能，並由所有系統整合商共同負擔該晶片設計的成本，如此才是經濟實惠的方法。

- 物聯網安全標準及業者的責任

隨著越來越多的物聯網資安事件爆發，全球各國、各領域已開始著手推動一套基本的物聯網安全性及隱私保護標準及測試流程。與會者表示，這個框架應該由權威標準制定機構及產業代表共同制定，盡可能簡化測試及驗證的程序，盡可能讓所有供應商容易遵守，同時，也應將產品為符合標準所衍生的成本納入考量。

除此之外，所有廠商皆有責任及義務來管理產品的安全性、隱私保護以及接取控制等事項，例如提供產品韌體修補、提醒客戶更新版本老舊的

設備等。針對產品管理議題，大型企業與小型供應商的處理模式大不相同，許多小型供應商為快速搶佔市場，常常推出許多沒有後續保固、更新服務的產品與服務，而大型企業如Google及Apple相較之下，很重視其產品的資安設計及產品管理程序，甚至可以為了資安因素而延緩產品的上市計畫，這一點值得我們深思。

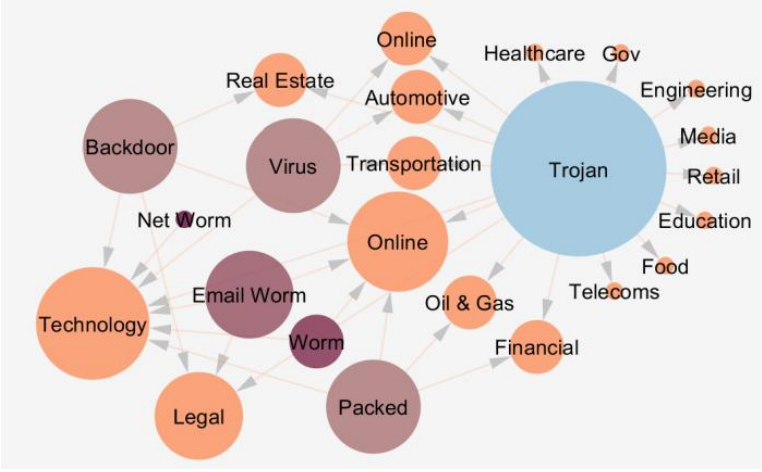
（二）第二日（10 月 24 日，星期二）

(1)網路空間的冷戰逐漸加溫－北大西洋公約組織（NATO）網路中心

北大西洋公約組織（North Atlantic Treaty Organization，NATO，簡稱北約）是歐洲及北美洲國家為實現防衛合作而建立的國際組織，而根據北約近年的觀察，網路攻防已逐漸成為軍事衝突的一部分，為因應與日俱增的網路攻擊行為，北約已宣布將網路視為一種軍事領域，如同陸、海、空同等重要，同時成立網路中心以增加網路戰略的應用，並對網路攻擊進行防禦。

根據講者提供的統計分析資料，可以觀察到各種領域（如科技、能源、金融、運輸）所面對的網路威脅型式（如木馬Torjan、後門backdoor、蠕蟲worm、病毒virus等）並不相同（詳如下圖），因此各產業必須明確了解自身所面臨的威脅，並對症下藥。

圖表8：各領域所面臨之網路威脅



資料來源：講者簡報

近年來，許多國際組織已開始重視網路安全議題。如北約已將網路升級為第四類軍事領域，亦即同盟國應共同防禦核心任務並主動分享資安情資，另外，上海合作組織（Shanghai Cooperation Organisation）及歐洲安全與合作組織（Organization for Security and Cooperation in Europe, OSCE）亦開始推動公私合作夥伴合作，及進行資安訊息、意見交流，以共同防禦網路攻擊行為。

(2)物聯網安全由邊緣開始：從邊緣到雲端的最佳安全措施－VMware

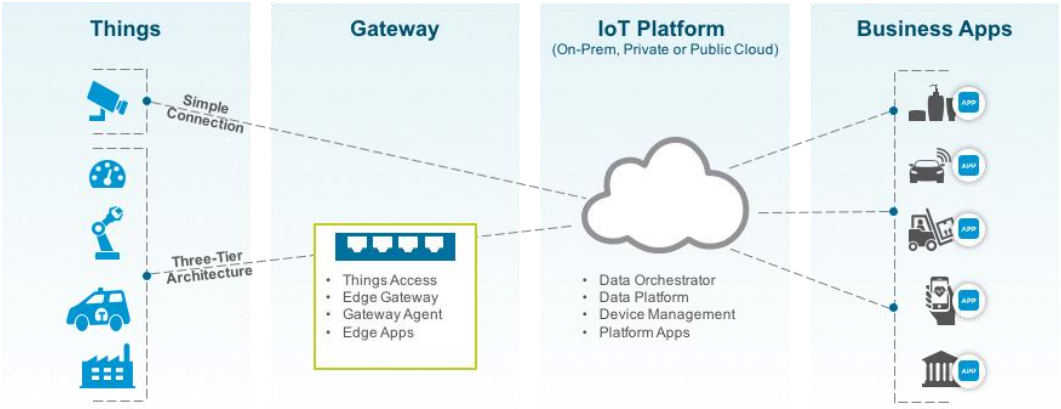
網路攻擊的模式層出不窮，2012年的Heartbleed漏洞讓駭客可以侵入網站的伺服器，全球約66%的網站受到影響；2016年秋天，知名的網路服務Dyn遭受Mirai殭屍網路發動DDoS攻擊，造成大部分美國的網路無法提供服務；今年上半年出現的wannacry勒索軟體，至今已經感染全球超過150個國家的23萬台電腦；而近期爆發的WPA2漏洞－KRACK，造成大量的Wi-Fi網路暴露在威脅環境中。物聯網帶來了龐大商機及便利生活的同時，也迅速擴大了網路攻擊的範圍及層次。

根據2017年RSA會議的統計資訊，高達83%的機構擔心會被物聯網裝置攻擊，63%的組織沒有信心可以完善地追蹤、管理自身網路內的連網裝置，另外，大約只有不到半數（49%）的物聯網裝置可以修改預設的帳號密碼。物聯網的崛起造成網路安全難以防禦，主要原因是數量龐大、複雜性及異質性（heterogeneity），可能發生的攻擊模式也更多樣化，只要透過雲端下達惡意的指令，連網裝置就可能遭到破壞或竊聽，並傳輸錯誤的數據回復雲端。

因此，美國聯邦政府亦提出一些管制的措施，舉例來說，聯邦機關使用的物聯網裝置的軟體必須可以被修補（patchable），亦不得將密碼硬式編碼（hard-coded password），並採取相關的安全方法（如閘道）隔絕不安全的裝置，確保內部網路的安全性。

物聯網服務主要由四個元素所構成，也就是連接網路（connect）、資料蒐集（collect）、數據分析（analyze）及後續行動（act），為此VMware提出三階層架構（在物聯網裝置及平臺之間加入閘道進行防護）、修補程式管理（在佈署前規劃修補方式，確保可以透過OTA的方式進行軟體、韌體更新）、最低權限（裝置僅開放給需要的使用者操作）、網路分割（隔離不安全的連網裝置以減少其他網路區域的風險）、點到點信任模型（硬體信任根RoT、傳輸及儲存均加密、多重要素認證等）及主動威脅偵測（持續的安全分析及異常行為偵測）等6種物聯網防禦措施，以確保物聯網系統的安全性。

圖表9：Vmware提出之三階層架構（3-tier architecture）



資料來源：Vmware網站；講者簡報

(3)從人類發展的角度看區塊鏈－聯合國

未免後世再遭現代人類兩度歷經慘不堪言之戰禍，重申對基本人權之信念，以促進更大的社會進步和更好的生活水準，係聯合國成立的宗旨。即隨著世界迅速地變化，世界所面臨的問題也不斷快速地轉變，但聯合國仍然致力保障國際的和平及安全。

近年來，區塊鏈（blockchain）快速崛起，藉由信任機制的導入，進而帶動經濟發展，聯合國也已將該技術運用在保障全球人民的基本人權上。例如，聯合國世界糧食計畫署（World Food Programme, WFP）已透過區塊

鏈技術，將食物券以虛擬貨幣形式發放給約旦的難民，至今為止已達10萬次的交易，並收到約100萬美金的援助，超過1萬名難名受益。

由這個案例可以了解，虛擬貨幣除可提高資金流動的效率與安全性外，亦開始在人道救援上發揮作用，讓救援物資的發放與分配更加公開、透明及公平，並降低詐欺與資料管理誤差的可能性，聯合國未來也將推動更多區塊鏈相關計畫，如難民身分認證管理，以更有效率的方式協助遭受天災、人禍的區域。

講者也提到，區塊鏈的發展讓政府在某些需要公開、透明與認證的角色上逐漸式微（如各國政府無法控制虛擬貨幣的匯率），而比特幣（bitcoin）等「匿名制」的區塊鏈技術卻也帶來了許多新的犯罪機會，因此各國政府仍須考量對區塊鏈進行適度的監管，在促進新興技術發展的同時降低風險發生的可能。

(4)討論：物聯網及雲端安全＋區塊鏈＋隱私及身分

- **物聯網 vs. 區塊鏈**

物聯網、雲端與區塊鏈從技術本質上來看並不相同，但三者間卻有很強的連結。回顧資訊科技發展史，早期企業集中管理及營運各自的機房；網際網路興起後，這些資訊、資源逐漸轉移到雲端；為了資訊安全，未來將會大量採用區塊鏈的方式進行加密，這就是IT的趨勢。

區塊鏈是一串使用密碼學方法相關聯產生的數據塊，從一開始的金融交易，逐漸延伸到需要中間人作保證的項目，若將區塊鏈運用於物聯網系統，可以強化其安全性及可靠性題。區塊鏈可以追蹤數十億相互連接的裝置，其特有的共識機制係透過點對點的方式分別連接，而不是透過中央處理器進行中心驗證，因此可以保證當其中一個個節點出現問題時，不會影響整體網路的安全性；另外，區塊鏈所採用的加密演算法，還可以為用戶個人資料提高更佳的隱私保護效果。

講者提到，雖然目前基礎建設產業（如能源）因為系統過於陳舊，尚無法立刻運用區塊鏈技術，但未來的基礎設施趨勢是讓所有供應商連接到分散式的區塊鏈系統，在區塊鏈上分享資料，並建立與區塊鏈相連接之的經濟行為，以大幅提升基礎建設產業的安全性、靈活度與透明度。

- **區塊鏈 vs. 身分識別**

目前的數位身分太過零散，每個人在不同企業、機構（如商店、銀行）都提供了重複的個人資料，而資料又掌握在互不相通的機構手中，隨著區塊鏈技術的成熟，這些散亂的資訊將可以獲得整合。

舉例來說，現在如果要在便利商店購買含酒精飲料，店員通常會驗證客戶身分證以確認年齡是否合法，但同時，店員也可以從身分證上看到許多其他的個人資訊（如婚姻狀態、居住地址），而在這個情境中如果可以引入區塊鏈技術將大不相同。藉由區塊鏈儲存所有節點的資訊，可以在網際網路的任何地方對身份進行驗證，因此，店員僅需接收他需要了解的資訊，而這個資訊已經由其他可信賴的機構進行驗證，將可大幅降低隱私洩露的風險。

但區塊鏈的解決方法也可能帶來其他的問題，例如所有廠商如何分攤區塊鏈建置、維運的成本，某機構蒐集的個資再被其他機構所使用是否會有法律上的問題，以及如何監督、管理這個共用的區塊鏈系統，這些都是將來必須面對的挑戰。

(5)裝置、網路及使用者的物聯網安全－SurePassID

物聯網快速的崛起及大量的普及，導致物聯網帶來的安全性挑戰更加艱鉅。依據講者的簡報資料，每個小時約有40萬的連網裝置加入網際網路，至2025年連網裝置的總數將達到750億台，但是約有七成的裝置存在弱點，因此近年來各個企業針對物聯網安全技術的投資不斷上升，預估2020年時物聯網資安市場將高達290億美金。

由於物聯網的應用層面非常廣泛，物聯網安全漏洞的破壞性將遠甚於單純網路攻擊所造成的機敏資料洩露，若無法保障裝置的安全，劫持無人駕駛飛機、關閉智慧電網、控制無限醫療設備等情境都可能在未來發生。

因此，物聯網裝置必須在產品規劃初期加入內建安全性設計，為面對錯綜複雜的物聯網系統，SurePassID提出以下幾點方法：（1）地點、人員、應用程式、網路、裝置、機器等具有身分的東西皆須進行管理；（2）透過多因素身份驗證及強大的加密功能，達成無縫、透明、堅固的安全性；（3）確保所有的實體及邏輯連結都是安全的，且可以容易地管理；（4）藉由開放標準、自動化及集中化的方式，將安全性解決方案擴展至所有的連網裝置及連接點。

(6)創造一個不可駭入的物聯網平臺－BlastWave

根據Sapio Research的於今年5月發布的調查報告，87%的IT管理人員認為該組織已大量投入資源於網路安全準備工作，但卻有71%的企業在過去一年中至少出現過一次網路安全性的侵害，其中近八成的受害企業遭受營收損失、營運停擺、客戶及合作夥伴流失等實質性損害。

日本軟體銀行（SoftBank）的執行長孫正義曾預估，未來將有64%的網路犯罪是的目標是物聯網，為達成不可駭入（unhackable）的物聯網，除連網裝置應內嵌具備安全性功能的晶片外，亦可以透過加密功能保障資訊傳輸的安全，並採用新型的命令稿語言（scripting language）撰寫應用程式。另外，提升使用的安全意識，包含修改預設密碼及定期進行軟體/韌體更新，亦是關鍵之一。

(7)連網家庭是傻瓜的天堂？－Dojo by Bullguard

據市場調查機構Gartner的資料顯示，2017年智慧家庭在美國家戶的普及率為32%，約有50億台的消費性連網裝置，而至2020年將有超過五成的智慧家庭，消費性連網裝置的數量將高達130億台。其實智慧家庭就好比

一個小型公司，但是卻沒有足夠的工具、資源及人員保護這些數量越來越龐大的連網裝置。

網路攻擊比防禦更容易！隨著越來越多的駭客工具可以在線上取得，因此駭客可以輕易地進行網路犯罪，並同時攻擊全球數百萬臺的裝置；另一方面，每年約有1.5萬個新發現的資安漏洞，其中九成源自於軟體因素，但是大約只有30%的裝置有進行軟體修補與更新。

家庭、辦公場所中常見的Wi-Fi路由器就是一個容易被駭客盯上的脆弱環節， Netgear、Ubiquity等網通公司的路由器接連被資安研究人員證實存有後門漏洞，即使未經授權也可以隨意存取該路由器。維基解密公布的文件更指出，美國中央情報局CIA開發的攻擊工具Cherry Blossom，可以入侵數十款路由器，經由裝置透過網路升級韌體時植入惡意程式，再透過中間人攻擊以監控使用者或操縱網路流量。

其實並不只有路由器容易受到攻擊，智慧家庭常見的連網電視、IP攝影機、醫療監控裝置等都陸續傳出存在漏洞，而物聯網裝置製造商卻缺乏誘因及能力去保護這些裝置，所以目前市面上絕大部份的裝置都缺乏基本的保護，諸如採用預設密碼、打開不必要的連接埠、未修補的韌體、未經加密的連線等。因此， BullGuard推出Dojo以保障智慧家庭的安全，當Dojo連接到家中的Wi-Fi路由器時，就可以偵測網路中所有的裝置，並充當連網裝置和潛在威脅之間的防火牆。首先，透過機器學習的方式了解所有智慧裝置的習慣，當發現異常行為或威脅時，Dojo可以自動截斷受影響的設備的連接，防止惡意軟體竊取數據或侵入其他設備。

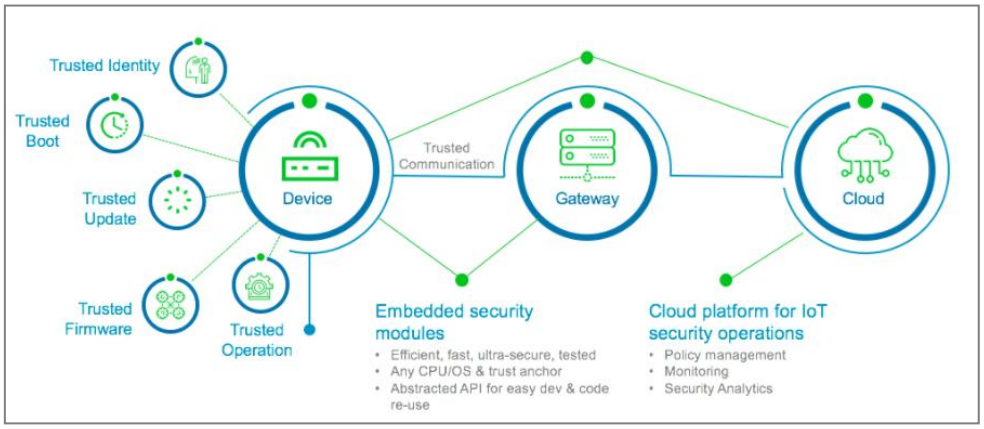
(8)安全的物聯網－Mocana

物聯網帶來龐大的商機並逐漸引領未來的科技潮流，但因為導入資安的投資報酬率低、增加產品製造成本、拉長產品上市時間、必須具備高級資安技能，又物聯網設備資源有限、傳輸網路異質性等原因，所以在大多數製造商的設計思維中，資訊安全不是首要考量因素。

隨著工業物聯網（IIoT）的發展，工業環境開始借助物聯網及網際網路服務改善生產流程，透過設備間相互溝通、作業環境監控，及時找出異常並加以排除，讓生產流程更具備彈性。不過，未修補的裝置、弱密碼、缺乏多重要素認證等在消費性領域困擾使用者的連網裝置資安問題，如果發生在工業物聯網上將造成更具破壞性的損害，如核能電廠異常中斷或醫療設備被控制。

有鑑於連網裝置開發、佈署之後很難正確、完全地掌握其安全特性，因此，Mocana提出「信任標準化（Standardize on Trust）」的解決方案，即是確保整體物聯網系統皆值得信賴。首先在裝置及其設計流程中建構安全性功能（包含值得信賴的身分認證、韌體、硬體信任根、更新等），再藉由安全的加密傳輸方式連接至閘道及雲端，以實現裝置、閘道至雲端應用信任鏈的可靠性。

圖表10：Mocana提出之信任標準化（Standardize on Trust）



資料來源：Mocana網站；講者簡報

(9)討論：允許那些人擁有數位身分？

講者認為目前身分識別所面臨的挑戰有以下幾點：（1）個人資料的濫用，雖然有法規卻無法有效監管濫用情形；（2）除非市場或消費者強烈認知到個資保護的重要性，否則企業本身沒有動機認真管理客戶的個人資訊；（3）物聯網裝置將大量掌握使用者的機敏資料，而人工智慧技術將

使裝置如同人一般具有對話、執行與決策行為，更擴展了身分識別的範圍及難度。

許多近期爆發的物聯網攻擊事件，起因都是因裝置缺乏身分認證機制，大部分的物聯網裝置因為尺寸太小或是基於生產成本考量，以至於很難包含身分認證功能。如果可以對物聯網設備進行身份驗證，並以加密的方式傳輸物聯網系統及網路間的數據，就可以從源頭保證物聯網的安全性，透過適當的相互身份驗證，有助於確保設備只接受經授權的連接與命令，避免駭客對醫療設備、工業系統與智慧城市進行非法操控。

建立物聯網共通的身分認證標準具有相當大的困難，但是製造商及服務提供者必須了解許多原本運作正常的身分認證機制已無法適用，物聯網系統、裝置如何進行身分認證將是需要重新認真思考的議題。

(10)白帽駭客展示－Independent Security Evaluators

講者使用長達兩年的時間，針對12家醫療機構的醫療數據設備或醫療裝置進行了評估，然後發現目前常用的生理監視器（Patient Monitor）及中央監護系統（CMS）在溝通時並未加密，且兩個設備皆不具備身分認證功能，因此駭客可以利用上述漏洞在遠端輕易發動攻擊，惡意行為諸如置換生理監視器的血型科導致輸血錯誤、置換傳送至護理站CMS的數據導致無法提供病患即時照護等，皆可能危及患者的健康及生命。

研究結果顯示，醫療設備的連網反而使醫療系統更加動蕩，尤其這個行業還未有足夠的安全意識，缺乏行政支持、資安人才不足、對敵人的認知已過時及合規性的錯誤依賴等情況，皆造成醫院的處境、病人的健康更無法受到保護，醫療機構必須了解這些可能發生的情境，並引入適當的安全性措施以保護病患的健康資產。

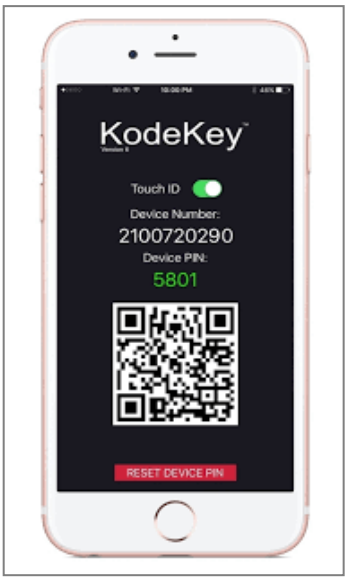
(11)在現今的安全環境下所面對之身分及接取管理挑戰－CVS Health & Infragard

在線上通路稱霸的Amazon，近年嘗試將物聯網、機器學習、雲端計算等新興技術應用於實體零售商店，並於去年底在西雅圖開了第一家智慧超市Amazon Go，消費者進入商店時只要用手機掃描QR Code即可開始購物，而系統藉由感應器、電腦視覺及等技術，可以自動判別消費者拿取的商品，購物結束直接離開商店後，系統會自動從消費者的信用卡或金融帳戶扣款並寄出收據。

由Amazon Go的例子可以發現，「消費者」及「企業」是物聯網服務中兩個主要的角色，因此講者認為要建構安全的物聯網框架，身分及接取管理相當重要。

越來越多的研究指出， 以密碼的方式保護我們的數據及身份並不夠可靠，密碼的管理、保護、記憶的問題逐漸浮現，而駭客有無數方法可以竊取、破壞或重置使用者的密碼，因此，多重要素驗證（Multi-factor Authentication, MFA）被認為是一個取代密碼的方案。伴隨智慧型手機的普及，行動裝置開始變成一個身分認證媒介，電話號碼、個人識別碼（PIN）、生物特徵（指紋）等皆可以當作是多重要素驗證的一環。

圖表11：KodeKey平台之身分認證畫面



資料來源：講者簡報

電子收費道路付費E-Z Pass 、美國政府為社會福利所發行的電子福利轉帳（EBT）及數位錢包等，皆是整合行動裝置與身分認證所推出的服務。舉例來說，波多黎各的一家新創公司推出的KodeKey平台，先透過生物識別技術將使用者與其行動電話號碼進行連接，之後及允許使用者藉由該號碼進行身份驗證，也就是說，當某個已整合KodeKey的服務需要認證使用者的身份時，可以要求使用者在啟用KodeKey的裝置上掃描指紋，該應用程式即可以驗證使用者的身份。

(12)安全性設計－Intertek

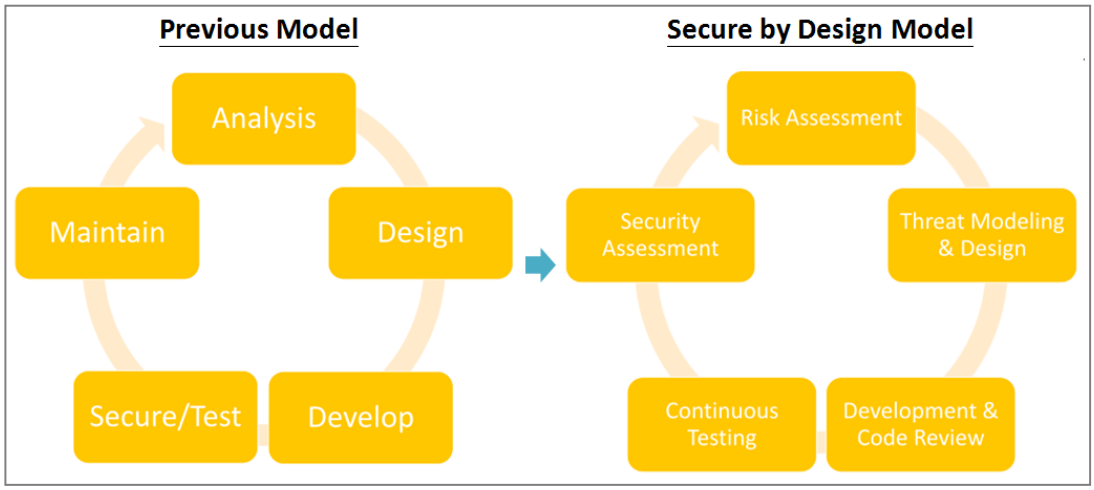
根據IBM的統計數據，在未來的兩年約有四分之一的組織可能受到網路侵害，而每一個網路侵害造成的成本損失約400萬美元。物聯網促使網際網路將人、事、物緊密的連結在一起，每一個新的連接都可能帶來新的風險及攻擊機會，駭客在線上不間斷地掃描漏洞並發起攻擊，一旦系統被入侵，駭客可以取得企業的機敏資料，造成商譽、智慧財產權的損失，導致客戶流失及潛在的訴訟。

2018年5月25日開始實施的歐盟「通用資料保護規則（General Data Protection Regulation, GDPR）」是一個強制性的規定而不是參考性指引，所有提供歐盟民眾使用的服務，或蒐集、處理及利用歐盟民眾的個人資料的企業或組織，都必須遵守GDPR非常嚴格的個資保護規範。這些單位必須設立資料保護長（Data Protection Officer, DPO），定期稽核、更新資料保護政策，一旦發生歐洲民眾個資外洩的情況，該單位必須要在72小時內通報資料保護主管機關（Data Protection Authority, DPA），並可能被判處高額罰款。

為保護使用者的隱私，各企業應更加重視產品的安全性，並在設計時融入安全性考量。既有產品設計模型流程的重點通常是設計部分，安全常常被忽略或僅是測試的一個部分。而講者提出的新模型中，安全是第一考量要素，產品設計的目的是保護產品的安全，並在過程中不斷進行測試及評估，保障所有產品推出前，皆能以嚴謹的設計初步解決產品可能面臨的

各種資安風險。另外，講者也提到設計時應盡可能遵循已建立的設計指南，如OWASP Top 10或NIST安全框架，同時企業應確實瞭解產品所處的環境、調查供應商的資安防護情況，以達成完整的產品安全保護。

圖表12：產品設計模型流程轉變



資料來源：講者簡報

(13)討論：當企業安全變成國家安全議題

講者提出，目前美國約60%至85%的基礎建設（如電網、交通建設）由私人企業所擁有或營運，如同物聯網系統一般，未來這些基礎建設勢必會為了提升效率而相互連結，因此當其中一個環節出現漏洞時，所有的基礎建設都會因為該脆弱點的存在而暴露在風險之中，進而導致國家安全議題。另外，因為基礎建設往往直接關係到民眾的日常生活，即使只是單一公司遭駭客入侵，如電網系統被關閉，也可能產生巨大的動盪而影響國人的信心，間接造成國家安全議題。

外部攻擊與人為錯誤總是不斷的發生，我們應該藉由過去的損害與經驗，學習、演變成為來的防護能力，因此，建立一個整體機制管理資訊安全事件並進行損失控管勢在必行。但是也有些人質疑，網路攻擊並不是每次都會造成嚴重的後果，建立資安損害管理是否有其必要性。講者提出，在美國每個消防員一年平均只處理一件火災而已，但是消防裝備的投資及

消防員的訓練仍然不間斷，如果消防員的存在是必須的，同理，資安風險管理機制亦必須被建立。

不僅如此，物聯網牽涉的範圍太廣泛，因此還有許多安全性問題需要解決，舉例來說，無人車可以透過無線網路更新韌體，但若客戶未行韌體更新，後續無人車因為漏洞發生車禍時，責任歸屬問題將非常複雜。物聯網所衍伸的問題繁雜，政府及產業需要排定優先順序，逐一擊破。

(14)醫療照護所使用的信任物聯網－Zingbox

資訊技術（IT）安全一直以來都是各個組織策略中很重要的一個部分，在傳統上，IT與能源、交通、醫療等作業技術型（OT）系統是兩個獨立的領域，但近年來為了提升效率，IT和OT逐漸融合。OT系統中加入許多連網裝置，也就是工業物聯網革命的核心，而過去困擾IT產業的資安議題也迅速擴展至其他產業領域。

今年9月，美國國土安全部的工業控制系統網路安全緊急應變小組（ICS-CERT）針對醫院使用的小劑量藥物注射輸液幫浦提出警告，指出該裝置存在一些安全性漏洞，可使攻擊者在遠端進行未經授權的接取，並影響輸液幫浦的運作，也就是說，駭客可以隨意改變患者注射藥物的劑量。

相關資料顯示，自2015年開始，醫療照護是最易受到攻擊的產業，且90%的醫院表示他們在過去兩年中是網路犯罪的目標。現在，醫院中許多的醫療設備透過網際網路進行連接，而防火牆是醫院唯一的防禦工具，機構內部的網路沒有加密，醫院也不了解單位內究竟有多少醫療設備連結到網路，因此，要進行風險評估及網路攻擊防禦非常困難，若X光放射機、輸液幫浦等重要醫療設備遭受攻擊，則可能使病人的健康、安全、隱私暴露在巨大的風險之下。

針對醫療機透面臨的資安困境，ZingBox提出的解決方案主要步驟包含：（1）瞭解身體：由可視性（visibility）開始，識別單位內究竟有多少連網裝置連結，並了解及分析每一個裝置正常的行為與運作模式；（2）維

持健康：持續監控裝置的重要訊號，識別可疑行為，並檢查漏洞及評估潛在風險；（3）運動：主動偵測可疑行為，及進行員工資安意識培訓。另外，透過人工智慧與機器學習等創新技術，可以在幾個小時內自動偵測出特定區域內絕大部分的物聯網設備，並僅需將所有蒐集數據的1%上傳雲端進行分析，即可以快速識別每一個裝置的獨特性（personality），及時監測裝置的流量，判別異常行為，並進行防禦工作。

肆、心得與建議

◆ 物聯網資安，言者諄諄但外界有多少共鳴有待商榷

近年來物聯網服務快速崛起,無線通信應用在感測資訊的傳輸日益普及,萬物聯網不再是夢想，並橫跨智慧運輸、智慧城市、智慧家庭、智慧醫療、環境監測等領域，讓民眾享受科技紅利-智慧與便利的生活。

物聯網服務帶動連網裝置的崛起，根據市調機構Gartner的報告顯示，全球物聯網裝置數量至2020年將高達204億台。但在這亮麗的數字背後，也潛藏著極大的風險。Gartner預估，2020年企業所遭受的資安攻擊，25%以上將與物聯網裝置相關。換言之，在已知萬物即將相連的世代，如果連網裝置在設計、規劃時，並未納入資安考量，只一味追求快速進入市場，搶食物聯網大餅；後端傳輸網路元件（如閘道設備）也持同樣態度；消費者採購物聯網裝置或訂購物聯網服務時僅以價格為考量,那萬物相連屆時可能變成萬物可駭,智慧與鬼魅恐將劃上等號。

美國是一個非常注重消費者權益的國家，因此這次物聯網資安高峰會於美國召開極具意義。與會講者們大談物聯網資安議題的重要性及已有從物聯網終端到雲端的資安防護解決方案，協助企業打造完善的物聯網網路，但可惜的是與會者多為其他場次的講者、資安界及學術界的菁英，部分為電信業者。換言之，與會者多為對物聯網資安之防護有充分共識之人，無須推廣資安防護之重要性即有高度成效。然而物聯網最大的資安隱憂並非企業，而是消費者個人。

2016年10月，知名網域名稱服務公司Dyn攻擊遭受大規模DDoS攻擊，Amazon、Twitter、Netflix等大型網站都因此而中斷。看似與物聯網資安無關的事件，經資安專家調查結果，近24%的攻擊來源為受殭屍網路Mirai控制的路由器、IP攝影機等物聯網裝置。接取物聯網裝置無須使用密碼或弱密碼、資料傳輸沒有加密、產品沒有資安設計等都是資安防護的大忌，但這些都是消費者可以避免的，所以此次高峰會並無類似我國消費者文教基金會或消保官等代表與會甚為可惜。主持人、與談人在台上大聲疾呼物聯網資安的重要性，部分講者更提供智慧家庭變成鬼屋、加護病房生理監視器（監測病人的

生命徵象，包括：心電圖、心跳、血壓、呼吸、血氧濃度等）遭駭引發誤診情事發生的案例，但對位於會場外面熙熙攘攘的紐約客或是遊客能夠產生多少共鳴仍有待商榷。

◆ 物聯網資安防護尚無一致規範

物聯網資安議題非常重要且亟待解決，與會者均有共識，但目前仍是百家爭鳴，各吹各的調，並無一致規範。目前美國商務部下的國家標準技術研究所（National Institute of Standards and Technology）所提NIST SP800系列、GSM協會所提IoT Security Guidelines及OWASP（The Open Web Application Security Project）IoT Security Guidance、UL認證機構之UL 2900系列，較為外界所熟知、接受。

由於國家標準主管機關、產業協會相關資安防護產出均為指引，所以各界解讀不一，造成今日百家爭鳴。國際標準組織內部仍對如何防護物聯網資安爭論不休，暫無相關標準可供外界參考。

◆ 物聯網資安防護之推廣應有優先順序，並由國家標準單位制訂相關標準後，其他政府單位再行引用、推廣至轄管領域

國際電信聯合會（International Telecommunication Union, ITU）在2005年世界資訊社會峰會（World Summit on the Information Society）提出報告「The Internet of Things」，正式預告物聯網時代的來臨。現行大家耳熟能詳且廣泛使用之Wi-Fi、Bluetooth、NFC、RFID等裝置，所採技術也是物聯網無線通訊技術之一。換言之，物聯網早已深入我們的生活，只是我們不自知。在已知的未來，隨著低功率廣域網路（LPWAN）技術及服務的普及，如使用免執照頻段之LoRa、 SigFox及使用行動通信網路頻段的LTE-M1、NB-IoT，物聯網服務勢將橫跨智慧運輸、智慧城市、智慧家庭、智慧醫療、環境監測等領域。但要將物聯網延伸至各個領域，物聯網裝置的價格必須低廉，才有市場競爭力，吸引消費者使用物聯網服務。在此限制下，要求所有物聯網裝置均具資安防護能力，並不可行，且無法引起外界共鳴。對於哪些領域所使用的物聯網裝置應具備資安防護能力，從講者分享內容看來醫療、汽車、國安及攸關

生命財產安全領域等開始較為可行；並由國家標準單位制訂相關標準後，其他政府單位再行引用、推廣至轄管領域。此與行政院資安處為推動物聯網資安檢測，建議由經濟部訂定IoT軟體相關之資安規範，並協助各中央目的事業主管機關將其納入商品檢測之意見一致。

◆ 物聯網資安防護深入人心才能營造一安全的物聯網環境

現行普羅大眾使用的智慧型手機與平板電腦等行動裝置由於輕巧靈活、攜帶方便，並可提供上網、收發電子郵件、文件編輯、簡報瀏覽、存取遠端資料，甚至遠端遙控其他網路設備等功能，除有效提高生產力及工作效率，同時也帶來資安疑慮。雖然資安防護專家大聲疾呼；經濟部工業局也委請第三方推動行動應用App基本資安檢測服務，但智慧型手機經由中間人攻擊或安裝不明、受感染之APP或使用不安全的Wi-Fi被駭仍時有所聞。未來物聯網裝置之硬體規格及功能較智慧型手機更為陽春，使用場域多元又非唾手可得，所面臨的資安挑戰將更為嚴峻。依市調機構Gartner預估，到2018年，50%以上的物聯網設備製造商將無法應對弱認證（weak authentication）威脅；2020年企業所遭受的資安攻擊，25%以上將與物聯網裝置相關。換言之，未來萬物可駭，對於駭客而言，將不再是夢想，而是一蹴可幾。但如果物聯網服務提供者、設備或裝置製造商、消費者具備資安防護意識的話，就可以大幅降低其風險。

為營造一安全的物聯網環境，本會自106年起，已依行政院資通安全處規劃的106年至109年4年期「資安旗艦計畫」，推動「數位匯流/IoT資安威脅防禦機制暨資安實驗室建置與服務」計畫，據以建置IoT資安檢測實驗室及網路實驗平臺，以研析IoT之資安威脅與漏洞，並研訂IoT之資安檢測規範。經由建構資安檢測及驗證體系，協助國內網通廠商研發符合資通安全規範之IoT產品，增加國際市場競爭力。然而現行國際間對於智慧型手機或是物聯網裝置之資安防護均非強制規定，也就是由製造商依其需求，自行決定是否受測。

目前，國際間已有98家物聯網裝置製造商或服務提供者（如intel、SAMSUNG、PHILIPS、vodafone、UL、dyson等）自主加入物聯網資安基礎聯盟（IoT security foundation），期對所產製或提供的物聯網商品、服務之資

安防護有所助益。但還有成千上萬的物聯網商品或服務提供者及資安防護觀念薄弱的廣大消費者仍待發掘。崙此，本會已責成「數位匯流/IoT資安威脅防禦機制暨資安實驗室建置與服務」計畫之委辦商財團法人電信技術中心（TTC），就其物聯網資安產出及資安防護意識進行推廣。今年12月所舉辦的資安成果發表及參加總統府資安週活動，並演示資安攻擊案例及資安防護有獎徵答活動等，只是推廣物聯網資安防護的起點，未來更可將觸角深入校園或併入本會電磁波宣導，將資安觀念植入人心。

相關宣導內容，以此次高峰會為例，部分講者提供智慧家庭變成鬼屋、加護病房生理監視器（監測病人的生命徵象，包括：心電圖、心跳、血壓、呼吸、血氧濃度等）遭駭引發誤診情事發生的案例；另電影《玩命關頭8》（英語：The Fate of the Furious）壞人駭入紐約市區數百輛自駕車圍堵俄國國防部長；又消費者自己就可以進行的資安防護措施，如物聯網設備首次連網前變更初始密碼或弱密碼、關閉telnet功能、透過https連網、關閉多重接取、不同帳號之權限控管、配合廠商召回、適時軟體更新、只連接安全的接取網路等講者建議，都是很不錯的宣導教材，可供日後推廣物聯網資安防護之用。