2015年(ISC)² Security Congress考察紀要

閻美晴/金融聯合徵信中心 研究部

會議目的

國際資訊系統安全認證協會（International Information Systems Security Certification Consortium, Inc.，以下簡稱(ISC)²）是全球知名非營利性資訊安全專業人員證照組織，擁有將近11萬名會員、遍佈全球160國家。成立願景是希冀建構一個安全可靠的網路世界，並期藉由提供網際網路，資訊，軟硬體等安全相關認證資格、資源與領導管理方針，給予會員及相關機構支援，向社會大眾展現組織價值理念。

(ISC)²自2011年開始，每年定期於美國舉辦全球性資訊安全研討會議（Security Congress），(ISC)²於2015年9月28日至10月1日假加州Anaheim會議中心舉辦第5屆資訊安全研討會議(ISC)² Security Congress，本屆是與ASIS International第61屆年會共同舉辦，恰逢ASIS International慶祝成立60周年慶，共計超過2萬名與會人員，其中包含資安與資訊相關機構及廠商、政府機關、學研界等專業人員參與，為期四天的會議提供超過70堂不同領域與主題的教育訓練課程，並於會場提供職涯輔導與發展機會，本次參與會議主要目的是希望經由各領域資安專家進行實務經驗分享與技術交流，瞭解目前全球資安最新趨勢與熱門議題、最新攻防手法與工具，並提供參考依據以幫助與強化網路安全防禦策略與管理能力。

會議過程[1]

一、會議議程

(ISC)² Security Congress 2015會議總共分為三部分，9月26日至27日是為(ISC)²會員所舉辦為期2天Pre-Conference Training(會前會)，9月28日至10月1日是Conference(正式會議)，最後10月1日至2日亦為(ISC)²會員所舉辦為期2天Post-Conference Training(會後會)，本次參與行程是參加9月28日至10月1日的正式會議，議程詳見表1。

1 會議及其相關資料請詳見網站https://www.isc2.org及http://congress.isc2.org。

表一、會議議程

時間	議程
Monday, September 28th	
07:45 - 09:00	ASIS Opening Ceremony
09:00 – 16:30	1st Day Exhibit Opens, (ISC)² / ASIS Career Pavilion
11:00 – 12:00	Cloud Security：Evaluating the Security of a Potential Partner - Without Permission! Swiss Army Knife：Dissecting Bitcoin Security Healthcare Security：Unsafe Harbor: Will Your Encryption Weather the Storm? Threats-Inside&Out：DDoS: Barbarians at the Gate(way) Malware：Building a Computer Network Immune System People Centric Security：Security Accountability (Not Awareness) Training Application Security/Software Assurance：Cisco's Security Dojo: Raising the Technical Security Development Awareness of 20,000+ Governance, Regulation and Compliance：Are You Really PCI DSS Compliant? Case Studies of PCI DSS Failures!
12:00 – 13:30	Networking Luncheon
13:45 – 15:00	Cloud Security：The Cloud Trust Conundrum: You're Asking All the Wrong Questions Swiss Army Knife：Security from the Trenches - Scrying Security Healthcare Security：Exploring Data and Security Dependencies in the Healthcare Ecosystem Threats-Inside&Out：Living the New Normal of Sophisticated and Determined Attackers Malware：Mobile Malware and Emerging Threats on Mobile Payment Systems People Centric Security：Big Brother Can Leave the Building – Privacy's Got This Governance, Regulation and Compliance：Enterprise Security Governance: State of the Practice and Implementation Guidance
16:30 – 17:30	Cloud Security：Transparency and Trust in the Cloud Swiss Army Knife：Critical Infrastructure: Securing Your Compliance Healthcare Security：Threat Modeling Vignettes for Covered Entities - Real World Use Cases Threats-Inside&Out：Find the Attack in the Haystack By Prioritizing Where to Search Malware：Point of Sale Malware Counter Striking People Centric Security：Leading Cross-Organization Security Change Application Security/Software Assurance：Fast & Secure Application Development – Is It Possible to Have Both? Governance, Regulation and Compliance：Third-Party Risk: How Can We Help Our Business Succeed in an Outsourced Economy
Tuesday, September 29th	
08:00 - 09:00	ASIS Keynote Speaker - Raymond W. Kelly, Former Commissioner of the NYPD
09:00 – 16:30	Exhibit Opens, (ISC)²/ASIS Career Pavilion
11:00 – 12:00	Cloud Security：It's Not You, It's Me - MSSP Couples Counseling Swiss Army Knife：The First 24 Hours of a Breached Company Professional Development：Security MBA – A Crash Course for the Security Professional Threats-Inside&Out：Advanced Dark Web Attacks and Hacker Techniques Mobile Security：Clientless Android Malware Control People Centric Security：Applying Threat Intelligence to Improve Security Awareness Programs Application Security/Software Assurance：OWASP CISO Survey Report 2015 – Tactical Insights for Managers Governance, Regulation and Compliance：SIEM and Data Privacy Violations
12:00 – 13:30	Networking Luncheon

13:45 – 15:00	Cloud Security：The Anatomy of a Cloud Data Breach Swiss Army Knife：Security on a Shoestring: Twelve Low-Cost Solutions That Can Dramatically Improve Enterprise Security Professional Development：Career Advice From Two Old Dinosaur-ettes Threats-Inside&Out：Adventures in Threat Intel, Volumes I and II Mobile Security：Cellular and Online Cyber Security Risks People Centric Security：FUD or Fact: The Role of the News Media in Security Application Security/Software Assurance：Case Study: Securing the Software Supply Chain Governance, Regulation and Compliance：'Is This Thing On?' What Your Employees Are Really Doing Online at Work
16:30 – 17:30	Cloud Security：SDN Security: Two Sides of the Same Coin Swiss Army Knife：The Hunt for Patient Zero-Operating Under Assumption of Compromise with EDR Technology Professional Development：Status of the Industry: 2015 Global Information Security Workforce Study Threats-Inside&Out：Passive Information Leakage: A New Threat to Sensitive Business Information Mobile Security：Mobile Innovation and Security People Centric Security：Under the Unfluence: The Dark Side of Influence Application Security/Software Assurance：Vulnerability Tracking and Mitigation Associated with Open Source Software Governance, Regulation and Compliance：Security Risk Modeling: Advanced Techniques and Tools for Supercharging Your Risk Management Program
Wednesday, September 30th	
08:00 - 09:00	Keynote Speaker - General Michael Hayden
09:00 – 15:30	Last Day of Exhibit, (ISC)²/ASIS Career Pavilion
11:00 – 12:00	Cloud Security：Internet of Things Security Assessment - Frameworks, Skills and Controversy Swiss Army Knife：If You Only Had $1 for Security, What Would You Spend It On? Professional Development：Guest to Root – How to Hack Your Own Career Path and Stand Out Threats-Inside&Out：The Threat Landscape – Insights from Symantec Global Intelligence Network Forensics：Digital Forensics 3.0 - How Technology and Regulation Is Changing the Game People Centric Security：Rebuilding the Credibility of a Security Team Application Security/Software Assurance：Security Comparison of Web Application Programming Languages Governance, Regulation and Compliance：Secure Compliant Data Reduction for Global Governance, Regulation and Compliance
12:00 – 13:30	Networking Luncheon
13:45 – 14:45	Cloud Security：The Researcher's Guide to the IoT Galaxy Swiss Army Knife：A Glimpse into the Future Direction of Card Not Present Authentication Professional Development：Communicating Risk to Executive Leadership Threats-Inside&Out：Threat Detection Via Text Mining Forensics：File System Journaling Forensics People Centric Security：People-Centric Security: Measuring and Transforming Your Security Culture Application Security/Software Assurance：The State of Bug Bounties Governance, Regulation and Compliance：Panopticon 2015: Continued Erosion of Privacy Rights (and Occasional Victories)
15:30 – 16:30	Cloud Security：Advancements in Web Systems Security: The Cloud is Your New DMZ Swiss Army Knife：Bringing IT and OT Together: Trends in the industry Professional Development： Mentoring Fundamentals for the Security Professional Threats-Inside&Out：Hacking the Internet of Things: Now Everything Is Hackable Forensics：Cryptanalysis for Forensics People Centric Security：Implementing Gamification and Other Creative Security Awareness Methods Application Security/Software Assurance：How to Scale an AppSec Program Governance, Regulation and Compliance：Information Security Regulatory and Legal Environment

Thursday, October 1st	
08:00 - 09:00	(ISC)² General Session - Galina Antova
09:30 – 10:30	ASIS General Session - IP Protection: Lessons Learned from the Sony Hack
11:00 – 12:00	ASIS General Session - The Terrorist's Son
12:00 – 14:00	Closing Luncheon, Keynote Speaker - General James Mattis

二、會議內容

本次會議內容包含應用程式安全(Application Security)、雲端安全(Cloud Security)、公司治理與法令遵循(Compliance, Regulation, Governance)、數位鑑識(Digital Forensics)、國家安全(Government Security)、醫護安全(Healthcare Security)、惡意軟體(Malware)、行動裝置安全(Mobile Security)、軟體安全(Software Security)、資訊安全工具(Swiss Army Knife)和威脅(Threats)等11個主要議題，本次分享其中三場有關公司治理與法令遵循，行動裝置安全和威脅議題之摘要及內容：

(一) DDoS: Barbarians At The Gate(way)

講者：Dave Lewis

資歷：CISSP®, Global Security Advocate, Akamai Technologies

摘要：Dave Lewis介紹DDoS[2]目前攻擊手法與工具，分享DDoS最新攻擊趨勢，瞭解發動DDoS攻擊動機與偵測攻擊模式的原理，以提供組織建立較佳的防禦策略。

內容：Dave Lewis說明DDoS攻擊者及其動機、攻擊手法、攻擊工具、目前趨勢與相關資料，最後給予組織防禦策略之建議，說明分述如下：

1.DDoS攻擊者(Actors)與攻擊動機：

(1)受雇者(mercenaries)：

例如俄羅斯地下市場，聘雇一個DDoS攻擊一天$30~$70美元，一個月$1200美元，入侵組織郵件$500美元，2000個殭屍電腦(bots)$200美元等；除了非法組織，一般合法組織亦有駭客網站提供人力資源服務聘請駭客(如Hackerslist.com)。

(2)青年孩童(Bored Kids)：

例如2014年利用Heartbleed漏洞入侵加拿大國稅局之加拿大青年，或是2000年Mafiaboy事件，這些青少年或孩童花很多時間於網路，其特徵是這些攻擊者對於攻擊目標並無明顯動機，使用的攻擊工具亦非高難度或特殊資訊技術，純粹只是利用網路取得之攻擊工具發動攻擊；(ISC)2 safe

2 分散式阻斷服務攻擊（Distributed Denial of Service，簡稱DDoS），主要為駭客利用分散於不同地方的多台電腦主機(一般會以「殭屍」向特定的目標)，發送大量偽造來源地址（spoofed source IP addresses）的封包，癱瘓受害者所在的網路電腦主機伺服器，導致無法服務。

and secure program提供協助幫助這些網路犯罪之青年孩童。

(3)駭客主義者(Hacktivists)：

例如anonymous、lulzsec，積極參與政治和社會運動，無特定組織層面；或是基於政治目的而發動的DDoS攻擊者，例如主要針對美國與加拿大發動攻擊之Qassam Cyber Fighters(簡稱QCF)，這類型組織有明顯政治動機並有良好財務支援與組織結構。

2.DDoS攻擊形式主要可分為三大類型：

流量攻擊(Volumetric attack)、應用層攻擊(Application layer attack)及網路協定攻擊(Protocol attacks)。攻擊手法多為以下方法：(1)SYN Floods；(2)UDP Floods；(3)ICMP Floods；(4)NTP Amplification；(5)HTTP Flood。在2015年第2季各類DDoS攻擊手法中，SYD與SSDP是最常見的攻擊方法，其中SSDP在2014年第1季尚未出現，到2015年已有顯著比例。

DDoS攻擊手法日新月異，除以往大多針對Layer 3（網路層）、Layer 4（傳輸層）的通訊協定進行攻擊，逐漸轉向針對應用層發動攻擊，亦稱為Layer 7攻擊，應用層攻擊主要是在癱瘓目標主機之網路應用服務能力，與其他攻擊手法不同的是，常用於竊取金融機構資料，轉移資訊與資安人員注意力所使用之手段。分析2015年第2季DDoS應用層攻擊與基礎建設層攻擊所佔比例顯示，現階段應用層攻擊約佔10%，基礎建設層攻擊佔近90%，其中應用層攻擊方法主要是利用HTTP GET。

Dave Lewis在此提出有些DDoS攻擊是由網路幫派份子所為，例如：DD4BC。他們威脅受害者必須支付相當比特幣，否則將發動DDoS，一旦發動DDoS攻擊，受害者必須支付更高額費用給與DD4BC。

另外一種攻擊手法稱為放大攻擊（Amplification Attack），例如NTP，SNMP及DNS，此類攻擊手法是以多個假IP，用小封包製造數百倍頻寬流量傳至攻擊目標主機，藉以癱瘓目標主機。

3.攻擊工具有下列幾種：如Havij、HULK、Torshammer、、LOIC、HOIC、Brobot及WGET等。

4.DDoS近期攻擊趨勢：

(1)譁眾取寵(Media Grandstanding)：

2014年第4季 DDoS攻擊傾向於博得媒體版面或是破壞大型遊戲業者名譽而進行的惡意攻擊，此一偏好於2015年第1季持續下去，特別於2015年1月。

(2)商品化(Commoditization of DDoS)：

在網路上有些駭客組織推出各種月付方案，如月付$69.99美元，每天只需付出$2.33美元，客戶即可使用

DDoS攻擊服務，如2014年聖誕節爆發的Sony PSN遭DDoS攻擊事件，便是駭客組織Lizard Squad展現自家DDoS攻擊服務的確有效的宣傳式攻擊。

5.攻擊趨勢分析：

在2015年第2季，發動攻擊來源國家仍是中國大陸，約有37.01%， 其次為美國的17%，英國是第三，約有10%，然而在Dave Lewis的工作經驗中，曾經服務的公司於遭受DDoS攻擊進行分析時，發現來源IP位址雖來自於中國大陸，但是此位址為跳板(open relay)，最終可以追蹤至歐洲地區。從講者的經驗分享得知，網路世界的既有認知可能會有誤導我們實際的判斷與分析結果。

在2015第1季與第2季，網路電信業者及遊戲業者比其他產業遭受到更多DDoS，遊戲業者自2014年第2季之後就是最大的攻擊目標，每季攻擊皆有35%是針對遊戲業者；由網路應用層攻擊面來看，零售業者與金融服務業是目前主要攻擊目標。

6.Dave Lewis最後提出防範DDoS攻擊防禦措施：

(1)與服務供應商協助並合作。

(2)SQL INJECTION是可解的問題

(3)強化系統。

(4)與網際網路服務提供者（Internet Service Provider，簡稱 ISP）研議DDoS緩解措施解決方案。

(5)針對IP Spoof的問題，網路管理者可以在路由器(router)或防火牆設定相關的ACL rule，將不可能出現的封包全部擋掉。

(6)速率限制：控管每一秒鐘可以發出的連線數。

(7)及時安裝系統補丁程序。

Dave Lewis提醒目前為止還沒有發現對DDoS攻擊行為有效的解決方法，但採取上述的防禦措施仍對於組織防禦DDoS有相當助益。

(二)Third Party Risk: How to Help Our Business Succeed in an Outsourced Economy

講者：William O’Connell

資歷：CISSP®, VP, Global Trust, ADP

摘要：目前企業委外作業是很普及的一種方式，但是企業針對委外作業並無足夠人力去進行實地稽核作業，William O’Connell以自身經驗分享對於委外作業應如何決定其委外管理方式，並能進行有效與合適的稽核作業。

內容：William O’Connell首先提出目前他在委外管理作業方面常遇到的10種議題與爭議，如：

1.風險永遠都存在，所以何必庸人自擾?

2.供應鏈風險是言過其實的一種風險。

3.我們只跟大公司做生意。

4.進行委外管理會阻斷我們談生意。
5. 我們有風險計劃與安全評估計畫，哪個要優先評估?
6. 請委外廠商填寫評估問卷即可。
7. 對於委外風險一籌莫展，我們只能夠選擇接受。
8. 所有委外廠商皆須進行實地查核。
9. 我們沒有多餘時間能辦理委外監督作業。
10.我們沒有足夠資源能進行委外管理。

針對上述10種議題與爭議，William O’Connell以自身經驗及蒐集到的相關研究，給予相關問題釐清、回覆與建議，例如沒有時間進行委外管理，組織應該爭取高階領導階承的承諾，釐清RACI(Responsible，Accountable，Consult，Inform)及時間承諾；亦或對於所有委外管理作業，都以實地查核進行管理時，當組織有1000家委外廠商，不可能對於每家廠商一一進行實地查核，則可以選擇分析ROI來決定查核優先順序。

接者，講者引用「與成功有約：高效能人士的七個習慣」(Steven Covey, 1989)「Begin with the END in Mind.」(以終為始、成果導向)，亦即於任何事情開始進行前，要先瞭解終點（目的地、目標）在哪裡；如此，我們才知道目前身處何處，也才能夠往正確的方向向前邁進。William O’Connell認為組織辦理委外管理時，需要回頭思考委外管理的主要目標到底為何，是為了滿足主管機關要求？還是為了保全自己的工作飯碗？或是替組織做好風險控管呢？

講者再以馬斯洛的鎚子（Maslow's hammer)理論來說明，「When all you have is a HAMMER, Everything looks like a NAIL.」(如果你唯一的工具是把錘子，你很容易把每件事情都當成釘子來處理)。對於專業人員有時於考量委外管理時，很容易出現盲點，William O’Connell提出兩個委外管理常用的方法為例：「問卷調查」與「實地查核」。「問卷調查」方法，有時很容易受到委外業務性質不同而進行客制化問卷，但其實委外作業的評量問卷應該要有標準化的文件，以進行確實並客觀的管理；在「實地查核」方面，如一般組織認知，作業環境面的檢視是很重要的並有其必要性，但有效率的委外管理亦是很重要的一個原則，如果一大型組織在AP系統上有5萬家產品或服務合作夥伴的製造廠商，要一一完成實地查核是很耗費資源的一件事。因此，William O’Connell提出三種委外管理之建議方法：

1.Risk Based Approach。
2.A Common Assessment。
3.Taking actions that add value (ROI)。

在Risk Based Approach，講者認為應先辨識重要作業或指標，依照風險高低排序，利用風險評等進行分類並依分類進

行不同的管理方式，將高風險廠商進行同樣的風險管理，在ROI，組織可以先定義出ROI矩陣，並考量幾個面向，如目前的委外廠商對於業務的影響程度與成本，當委外廠商發生資料外洩事件或是倒閉，對於組織的影響。提出委外管理的步驟如下所述：

1.檢視合約。

2.統一詞彙與用語。

3.儲備委外廠商名單。

4.決定關鍵性的服務。

5.決定委外監督管理之工具。

6.發展委外作業服務計畫。

7.提倡委外作業服務計畫：對於委外作業服務計畫要堅定有信心，利用事實與數據證明計畫成果，取代對於委外管理可能有的FUD(意即Fear, Uncertainty, Doubt)。

講者最後以「It will all be ok in the end. So if things are not okay, It’s not the end」勉勵在場所有與會人員。

(三)Mobile Innovation and Security

講者：Spencer Wilcox

資歷：CISSP®, SSCP®, Managing Security Strategist, Exelon

摘要：行動裝置(mobile space)目前為一蓬勃發展的領域，持續不斷地創新改革給予資訊產業帶來龐大商機，同時卻也使得資訊安全、資料隱私與資訊整合面臨巨大的挑戰。企業使用行動裝置，一方面要確保資訊與個資資產的資訊安全(機密性、完整性、可用性)，一方面也希冀能隨時隨地安全地利用行動裝置獲取資訊，資安人員能否找出面臨此難題的解決方法，Spencer Wilcox提出個人實務上建議供與會人員參考。

內容：行動裝置於近期主要有幾種創新應用為人悉知，列舉如：行動支付（Mobile Payments）、行動裝置應用程式（App Stores）、物聯網（IoT）、地理位址定位（Geo-location）、生物辨識（Biometrics）、雲端儲存（Cloud Storage）、社群網路（Social Media）、線上遊戲（Games）、小額支付（Micropayments）、近距離無線通訊（Near Field Communications）及公用充電（Public Charging station）等。因此行動裝置安全問題亦是所有資安人員所需面臨的一巨大挑戰；行動裝置的資訊安全風險，一般多為下列8種風險因子進行分析考量：

1.營造商（Carrier）。

2.使用者經驗（User Experience）。

3.行動裝置管理（Mobile Device Management）。

4.應用程式（Applications / App Store）。

5.惡意軟體（Malware）。

6.脆弱性管理(Vulnerability Management)。

7. 供應鏈（Supply Chain）。

8. 隱私權（Privacy）。

例如：在應用程式方面，研究指出4分之1的Google Play上的免費app是重複的，另外無論是在Apple、Android或是blackberry上，皆有惡意程式的存在，有超過80%的的惡意程式是源自於自行開發之app，而供應商本身的品質管理及國家亦是風險分析的重要因子；在資料隱私權與使用者經驗方面，行動裝置難以完全區隔企業資料與個人資料，另社群網路的使用、雲端儲存集中化管理等亦會提高行動裝置資安風險。

講者分析使用Apple、Android以及blackberry的不同OS之風險，他認為Android雖公認為風險較高之作業系統，然而因此停止使用Android多少有些不符合實際市場情況，因為大多數的手機使用者並沒有辦法付出高額費用購買Apple及blackberry所生產的智慧型裝置，另一方面Google針對Android使用上的各項弱點亦有持續在進行改善，透過病毒掃描與即時更新補丁程式等方法，Android實際上並沒有想像中的風險高；另一方面，iOS是目前風險較低的作業系統，也因此容易造成使用者本身在管理與使用行動裝置之認知上容易有所疏忽，而RIM(Research in motion)雖於blackberry上開發出可使用Android之作業系統，但是其目前最大風險應是慢慢流失其市場。

講者最後對於行動裝置的資安風險提出下述三點建議提供給與會人員參考：

1. 有效整合行動裝置各項創新應用會成為組織之競爭優勢。
2. 組織在行動裝置上的風險，主要歸於其管理策略與使用方式，作業系統本身風險其實沒有上述來得大。
3. 組織只要有公務用的行動裝置，行動裝置的風險就會永遠存在。

心得及建議

一、參與本會議能使與會人員瞭解目前國際資訊安全最新發展趨勢，同時亦提供各界專業人士經驗分享與交流的機會；每場議題除有明確的主題外，議題內容亦提供不同深淺內容，部分專題與議題亦較偏向座談會形態，與會人員能有更多的實質討論與溝通。

二、近幾年各大企業遭逢DDoS攻擊時有所聞，例如2015年5月香港發生中國銀行與東亞銀行DDoS攻擊勒索事件，2015年8月國際駭客組織「匿名者」癱瘓我國政府部會多個網站。任職於Kaspersky Lab的Evgeny Vigovsky對於2015年第3季DDoS報告表示目前DDoS攻擊數量仍在增長，多數攻擊目的是進行短時間(不超過24小時)的攻擊以干擾企業服務，另一方面，攻擊時間持續較長，並以摧毀大型企業為攻擊目的的攻擊數量亦持續上升；Akamai Technologies亦於近期之網路安全威脅建議書中提出近幾個月內已觀測到 3 種新

型反射DDoS攻擊。顯示DDoS攻擊頻率越來越高，攻擊技術日新月異並使用聲東擊西手法，以獲取目標系統資訊或進行恐嚇威脅，尤其是從國際資安新聞可推測以大型零售業者與金融業者為攻擊目標的DDoS攻擊，竊取大量個人資料應為其主要動機與目標。

三、美國證券交易委員會在2015年針對網路安全訂定一套指導原則，裡面提出幾項建議要點，例如定期進行資安評估作業，建立一套面臨資安威脅的反應策略，明訂實施資安防護的政策和程序[3]；聯徵中心保有全國性信用資料，對於網路犯罪者而言，實屬一明確目標。在資安防護上，聯徵中心目前有良好監控及防禦機制，然而面對不斷變化和推陳出新的惡意程式與攻擊手法，在資安防護上仍應抱持著戰戰兢兢、如履薄冰的心態。另一方面，聯徵中心於2015年已正式列為「資安責任等級A級機構」，遵循「政府機關(構)資通安全責任等級分級作業規定」之A級機構應辦理工作事項及相關要求（如：訂定電腦系統資訊安全評估辦法、進行資訊系統分級及後續資安防護基準），與美國證券交易委員會之建議不謀而合，伴隨著網際網路的快速發展，面對資安風險之日增，良好的風險評估與檢視機制，持續改善實為資安管理的重點。

四、美國第二大連鎖零售商Target在2013年年底發生個資外洩事件，駭客透過竄改POS系統取得卡片磁條上的資料，而在個資外洩事件前2個月，駭客已利用夾帶惡意程式的電子郵件入侵Target空調服務供應商的電腦系統，此一事件使得Target付出巨大代價，顯示企業除對於自身於資安規範之要求外，委外廠商亦為一不可輕忽的風險來源；委外管理，實際依然是在論述企業本身的風險管理，作業或資訊系統的委外對於一家企業的責任與角色不會改變或減少，所需承擔的風險與減少的人力成本等是否對等，尚需回到委外的目的到底為何去進行檢視。

五、聯徵中心目前並無行動化服務，然而行動化、雲端化、物聯網、虛擬化等新興議題正持續發燒，盡早培訓相關領域專業資訊人才，惟有透過持續不斷之訓練與精進，才能因應未來可能之各種發展趨勢，例如可取得本會議之主辦單位(ISC)²所提供之各項國際資安認證：CISSP資訊安全系統專家認證（Certified Information Systems Security Professional）、與軟體安全開發有關的CSSLP資訊安全軟體開發專家認證（Certified Secure Software Lifecycle Professional），CCSP雲端資安專家認證（Certified Cloud Security Professional）等。

3 參考資料：https://www.informationsecurity.com.tw/seminar/news_detail.aspx?tv=41&aid=8128。