bsi.

個人資料保護
外洩案例分享

2017
個人資料保護教育訓練課程

PIMS ESS Training Course
個人資訊管理系統基礎訓練課程

章鈺　先生
(Mr. Oscar Chang)

BSI 英國標準協會
BSI Taiwan,
Client Manager 客戶經理
BS10012 產品經理
ISO 29100 產品經理

學歷：
- 政治大學 法律碩士
- Baker University, Kansas, U.S.A 管理科學碩士
- 輔仁大學 資訊管理學士

稽核經歷：
- 總統府、行政院、行政院人事總處、行政院主計總處、行政院研考會、考試院、考選部、證交所、期交所、櫃買中心、集保結算所、票交所、財金資訊、聯合信用卡中心、聯合徵信中心、中華電信、遠傳電信、臺灣積體電路、聯華電子、教育部電算中心、Accenture、NIKE、華碩雲端、阿里雲、台北富邦、彰化銀行、台新銀行、群益證券、元富證券、遠雄人壽、安達人壽等。

IT專業領域：
- 開放式作業系統管理/ 資料庫管理/ 應用系統軟體程式開發、系統分析/ SAP 系統管理

稽核資格：
- IRCA ISO 27001 主導稽核員
- ISO 22301 主導稽核員
- BS 10012 主導稽核員
- ISO 29100 主導稽核員
- ISO 20000 稽核員

稽核員相關專業證照：
- ISACA CISA/ CISM/ CGEIT/ CRISC Certified

課程大綱

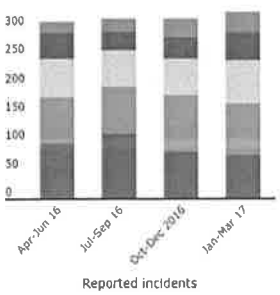
- 新興科技的運用與隱私侵害的平衡
- 從法律與法規看個人資料保護與外洩之責任
- 個人資料外洩因應措施
- 由近期個資新聞檢視應有作為
- Q&A

英國資訊委員公署個資外洩趨勢分析

ico.
Information Commissioner's Office

We received 678 reported incidents; an 18% increase on Q3.

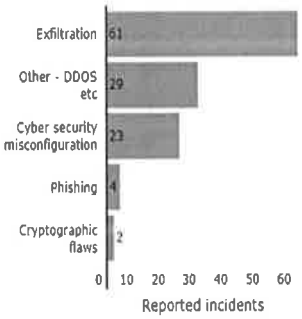
Data security incidents by type



20% increase in data sent by email to the incorrect recipient

32% increase in failure to redact data

Cyber security incidents by type



119 cyber incidents were reported in Q4

Cyber incidents were the most reported incident in Q4

after those defined as other principle seven failures.

Akamai 物聯網趨勢調查：台灣人挑選上網產品首重資安和隱私

數位時代 2017.07.06

- 路流量管理和雲服務供應商Akamai今（6）日公布2017台灣物聯網趨勢調查，發現有84%的受訪者擁有連網裝置，其中每人平均擁有6.7件，例如同時擁有智慧手機、平板電腦、智慧手錶等，而當台灣消費者在選購這些可上網的產品時，最重視資料安全和隱私保障，其次才是內建APP軟體功能，以及資訊分享功能。
- Akamai這項調查是在今年6月進行，隨機用email問卷抽樣314位台灣民眾，值得注意的是，符合調查定義的物聯網裝置或應用範圍甚廣，像是個人用的平板電腦、智慧手機、穿戴式裝置；家用的智慧電視、智慧家庭產品；以及企業用的指紋感應、紅外線感測、恆溫設備等，但不包含桌上型個人電腦。
- Akamai香港暨台灣媒體行銷總監陳秀慧表示，從調查可以清楚發現，使用連網設備已是台灣民眾主要的生活習慣，若依產品別來看，手機穩居普及程度最高的連網設備，其次依序為平板電腦、連網電視、智慧手環、連網家電、連網相機以及車聯網相關產品。
- Garnter預估，今年全球連網裝置達84億台，至2020年，數量更將增至204億台。

Akamai 物聯網趨勢調查：台灣人挑選上網產品首重資安和隱私

- 高度連結下前所未有的資安風險
- 陳秀慧指出，物聯網創造一個高度連結的世界，卻讓個人與企業安全面臨前所未有的資安風險。
- 根據2016安永全球資訊安全調查顯示，49%的企業懷疑自身具備持續辨識可疑流量的能力，44%的企業對追蹤存取公司資料的第三者感到困難，也有40%的企業無法找出隱藏和未知的零時差攻擊（zero-day attack）。
- 陳秀慧提醒，在物聯網時代，企業必須超越消費者期待，需要清楚瞭解產品生命週期、地理涵蓋範圍、技術變化與法規政策等。
- 她舉例，像是下載環境與成本將對消費者定期更新裝置造成挑戰，消費者會期待隨時能獲得迅速且可靠的服務，同時又希冀享受高度個人化的體驗，因此，不管是產品或服務提供者，都必須透過數據資料與分析以更深入瞭解客戶。

雲端服務常見6大安全問題

iThome 2017.06.29

- 近年來，雲端技術發展成熟，許多企業或是政府單位開始將自家資料轉移至雲端資料庫，並委託第三方公司來管理或分析雲端資料，但HITCON CTF領隊李倫銓表示，將雲端資料委外時，若權限設定錯誤時，反而會造成更嚴重的後果。他指出，目前雲端常見資安問題可以歸納成6大類，包含：CDN傳輸層實作問題、權限設定不良、設備解析問題、資料庫問題、網站漏洞、Serverless的架構問題。
- 問題1：CDN傳輸層功能問題
- 第一個問題是CDN傳輸層實作問題。使用者建立雲端架構的時候，經常會使用CDN服務，CDN不僅能夠加速資料的傳遞，也有其他的功能，例如，CDN廠商提供應用程式防火牆（WAF）、DDoS防護，以及提供HTTPS等功能。李倫銓認為，CDN廠商為了商業的利益，演變成CDN提供的附加功能越來越多，導致帶來的風險也變高。
- 舉例來說，今年2月CloudFlare爆發了雲端淌血漏洞事件，造成用戶密碼和個人資料外洩長達5個月。因攻擊手法與2014年心臟淌血（Heartbleed）事件相似，就稱為「Cloudbleed」。李倫銓解釋，CloudFlare 3項功能的Praser程式碼有錯誤，造成使用相同代理伺服器的網站用戶，能夠看到其他網站的資料。

雲端服務常見6大安全問題

- CloudFlare發生資安事件後，修改了包括電子郵件程式碼混淆（obfuscation）、Server-side Excludes，以及Automatic HTTPS Rewrites等3項受影響功能中的HTMLParser程式碼，以及立即關閉其功能，降低了損害程度。
- 李倫銓認為，CloudFlare這次事件凸顯出，用戶太過依賴雲端服務廠商，卻又無法保證雲端服務廠商都能安全無虞。
- 另外，原本企業使用CDN服務的另一個目的是避免自家伺服器直接面對駭客，一旦遇到DDoS攻擊，僅會波及CDN廠商。但是，最近出現一套駭客工具HatCloud，專門挖掘受CloudFlare代管網站的真實IP，讓駭客可以鎖定真實IP位址攻擊。所幸，李倫銓補充，這套駭客工具只會攻擊DNS組態設定錯誤的網站，並非所有CloudFlare代管的網站都能攻擊。

雲端服務常見6大安全問題

- 問題2：權限設定不良
- 李倫銓指出，部分企業或政府單位為了在短時間內，把雲端的資料交給委外公司管理或分析，卻忽略了權限的設定，包括IAM（身分認證管理）權限設定、AWS S3資料夾權限原則設定、防火牆安全群組（security groups）設定、資料庫權限設定，以及應用程式權限設定等5種權限管理的疏忽，造成大量的機密資料外洩。
- 其中，美國近期發生的2起重大資料外洩案，資料儲存在Amazon S3交給第三方單位管理，分別是今年6月初美國國防部軍事衛星情資外洩案，以及6月20日美國共和黨2億筆選民資料外洩案。李倫銓表示，雲端資料委外處理，必須注意委外公司的權限設定，不能開放全部的權限。因為大部分資料外洩案件，歸咎於委外權限設定不良。
- 不僅如此，今年初，一批駭客利用移除公開暴露在網路上的MongoDB內資料，勒贖資料庫所有人需支付0.2個比特幣（約新臺幣1.5萬元），才願意回復資料庫的全部原始資料。李倫銓認為，過去駭客僅會利用釣魚郵件，被動地等待受害者上鉤後，才會啟動勒索攻擊，但現在駭客能夠在「暗黑版Google」的搜尋引擎Shodan，掃描未加密的MongoDB，主動發動勒索攻擊，加密整個資料庫。

雲端服務常見6大安全問題

- 問題3：設備解析問題
- 李倫銓指出，2016年底中國研究人員發表了一篇論文名稱為「Host of Troubles」，揭露了關於不同設備對Host Header解析的歧異，讓駭客可以從中攔截網頁瀏覽請求，轉向偽造網址。例如，NSA（國家安全局）的網頁曾一度被替換成其他的網頁，但是，實際上NSA網頁沒有被替換，只是網址解析出真實IP的過程遭駭客攔截。
- 駭客發現大部分中介服務設備處理Host Header字串時沒有遵守RFC7230協議解析，利用這個漏洞來偽造類似的網域名稱，進而替換正牌網址與真實IP的對應關係，包括了Apache、Nginx網站伺服器、透通式快取服務（Transparent Cache），如ATS、Squid、反向代理服務（Reverse Proxy），如Varnish、Akamai、阿里巴巴、CloudFlare等CDN服務，以及防火牆服務。
- 例如，正常情況下，某一個網站的網域是www.A.com.tw，對應的網路位址是1.1.1.1，使用者輸入A網站網址就會進入網址IP為1.1.1.1的網站，駭客會先註冊一個和目標網站相似的網域名稱為「www. A.com.tw（A前方為空格）」，但對應到IP卻是駭客擁有的1.1.1.2。部分中間服務解析Host Header時，會忽略網址中的空格，導致駭客釣魚網址和正常網站的網址被視為是同一個網站。

雲端服務常見6大安全問題

- 問題3：設備解析問題
- 李倫銓說明，如果駭客在偽造的釣魚網站中植入木馬，使用者進入網站後，電腦就會遭到木馬感染。
- 問題4：DB問題
- 李倫銓指出除了MongoDB資料暴露在外，以及MySQL風險之外，還有一種是RADIUS權限設定有疏失。駭客利用RADIUS的漏洞，植入遠端服務管理SSH金鑰至RADIUS的伺服器，不但能夠取得此伺服器的使用權限，也可以利用相同方式取得其他RADIUS的伺服器權限。
- 問題5：網站系統漏洞
- 李倫銓說明，只要是人就會寫出有問題的程式，有問題的程式就會造成漏洞。在2005年以前，駭客利用網站漏洞來替換網頁，或是直接在網頁掛馬，竊取使用者的個資。但近年來，駭客直接置換在網站的軟體，欺騙使用者下載具有惡意程式的偽造軟體或是作業系統。

雲端服務常見6大安全問題

- 問題5：網站系統漏洞
- 例如，2013年KMPlayer軟體更新程式遭駭事件，駭客直接攻擊官方網站，把開源專案的程式包，全部替換設有後門的KMPlayer軟體程式，使用者安裝了偽造的版本，也相對地安裝了後門。
- 此外，駭客也開始轉往攻擊開發者的環境。李倫銓指出，今年爆發出Samba漏洞後，許多資安研究人員為了探究漏洞產生的原因，紛紛上網下載Python程式碼開發的Samba套件，然而，網路也出現了新釣魚手法「Python package 釣魚」。
- 一名駭客在網路假造了一個Python的Samba套件，並以Python慣用規則命名成的「SMB」，偽裝成官方提供的套件，上傳至Python套件索引平臺PyPI上提供下載。當研究員使用Python套件管理工具「pip」下載「SMB」時，駭客也能順便竊取了研究人員回傳的Username、Hostname、IP位址和其他主機資訊。不僅如此，2015年發生的XcodeGhost風暴事件也都透露出，攻擊開發環境已經成為一種風潮。

雲端服務常見6大安全問題

- 問題6：Serverless的安全問題
- 2014年AWS推出了Serverless的運算架構，李倫銓指出，從資安觀點來看，使用者不會擁有伺服器，一旦發生DDoS攻擊，都由雲端廠商負全責，但除了DDoS問題，Serverless架構仍然有其他的安全問題，如Lambda功能的存取控管風險（Funtion Access）、AWS資源權限管理風險（Resource Permisson）、資源濫用（Resorce Abuse）、Container 安全性，以及程式碼注入（Code injection）風險等問題。
- 李倫銓表示，公有雲的安全性是一種假設，仍在許多環節會出現意外或繞過管制的可能，而且無論是管理憑證的機構、網路營運商、雲端服務商，甚至自家開發者都可能會發生疏失。而駭客不僅攻擊使用者，也開始轉而攻擊外包商，以及系統架構業者，所以，最好的方法就是接受資安問題的存在，尋找適合的處理方式正面迎戰。

新興科技的運用與隱私侵害的平衡

bsi.

桃機自動通關系統 8日提升為雙重認證

自由時報 2017.03.08

- 為有效提升旅客入出境通關效能，移民署自即日起，自動查驗通關系統改採臉部與指紋同步辨識，通關時間再縮短，預計可以提升通關效率。
- 移民署去年8月在高雄機場試辦的F-Gate（外國人出境自動通關系統）也將在今年8月在桃園機場提供外國人出境自動通關出境服務，不過剛開始因為經費關係只能在1期安裝8台F-Gate供外國人出境通關使用，目前還在尋找經費在2期航廈安裝，外籍旅客只要入境完成臉部照相及指紋按壓記錄，出境時就可以使用移動通關系統。
- 針對經費問題，許多機場單位指出，這些服務外國人的設施就是提高桃園機場及觀光客的品質，每年從機場服務費取得百分之40經費的觀光局應該負擔這些費用，再來就是桃園機場的世界機場名次評比，移民署的通關速度也榜上有名，桃園機場是否也以提升服務品質的目的，提供經費完成這些設施，

桃機自動通關系統 8日提升為雙重認證

- 自動查驗通關系統主要是透過臉部特徵辨識身分，若旅客因頭髮遮眉或臉部有表情笑容等其他因素致臉部辨識未成功，可再以食指指紋輔助辨識即可通關。
- 由於採分段辨識，故須等候臉部連續辨識不成功之後，始能進入指紋辨識模式。為縮短系統辨識時間，以提高通關效率，自即日起，自動查驗通關系統改採臉部與指紋同步辨識，全程僅需10秒鐘，旅客可享有更便利快速的通關品質。
- 旅客已申辦自動查驗通關且留有指紋者不用再申請；之前申請僅留臉部影像未留存指紋者，仍可以辨識通關，如欲再縮短通關時間，則可選擇重新註冊同時留存指紋，以節省通關時間。
- 移民署也提醒旅客，尚未申辦自動查驗通關系統的旅客，國人只要年滿14歲，身高140公分以上，攜帶護照及第2證件（身分證、健保卡或駕照擇一）；14歲以上外國人、大陸地區人民及港澳居民具有在臺居留資格且有多次重入國許可者，亦可攜帶護照及居留證至移民署各地註冊櫃檯免費申辦。

Netflix 是如何用大數據捧紅「紙牌屋」的

Inside 2013.02.26

- 現在網路上最熱門的美國影集，可以說就是「紙牌屋」，在美國知名的影評網站 IMDb 上，在 15,000 個評分中獲得 9.0 高分，你就可以知道這部美劇現在熱門程度。
- 這部影集是由 Netflix 這個線上影音服務，用一億元美金買下版權，打破過去美國網路影音服務是先跟 HBO、FOX 或者是其他大電視頻道買節目後，才在網路上播出的模式，直接是由網路首播；跟過去一週一集不同，影迷們不用每週苦苦等待，「紙牌屋」當天一口氣就推出一季 13 集（所以很多字幕組都在哀號），而紙牌屋本身更是請來**大衛芬奇**作為導演（社群網戰、班傑明的奇幻旅程、鬥陣俱樂部）以及知名演員**凱文史貝西**作為劇中扮演美國多數黨黨鞭的角色，話題性十足；一推出後，在美國等地就成為熱門討論焦點。

Netflix 是如何用大數據捧紅「紙牌屋」的

- 那麼 Netflix 是否在買下本劇開拍前就知道這部片會不會紅呢？紐約時報在近期的文章中 Give Viewers What They Want，如此評論：
『在美國的電視業裡，沒有什麼事是確定的，也許你找齊金牌導演、實力派演員跟熱門劇本，但還是跟擲骰子一樣，都是在賭。但是不是有破解之道呢？任何一門生意中，如果可以預見未來，是相當有殺傷力的，而 Netflix 可能靠著「紙牌屋」辦到了這點』。
- 以下為 IT 經理網編譯自 SALON 的內容 ，早在一年前，Netflix 就開始利用大數據分析，對節目的進行安排，透過對觀眾收看習慣的了解， Netflix 發現， 那些喜歡看 BBC 舊版「紙牌屋」的觀眾，同樣也喜歡大衛芬奇導演的電視劇， 或者凱文史貝西主演的電視劇。
- 因此， 對 Netflix 的高層來說， 購買這部由大衛芬奇導演，凱文史貝西主演的同名電視劇就是合理的。而這也最終也讓他們決定花一億美元來購買這個 1990 年 BBC 同名電視劇的重製版。

Netflix 是如何用大數據捧紅「紙牌屋」的

- 新版「紙牌屋」一共兩季，第一季已經在 2 月 1 日在 Netflix 平台上獨家播出，第一季一共 13 集，北美、英國、愛爾蘭、拉丁美洲和斯堪的納維亞半島的會員都可以點播觀看。在去年 11 月，Netflix 的公關總監 Jonathan Friedland 在接受「連線」雜誌採訪的時候說：
『我們知道觀眾在 Netflix 上的觀看習慣，所以，透過觀眾收視分析，我們對哪些劇集會受歡迎很有信心。隨著時間過去，我們能夠針對不同觀眾推出他們更加喜歡的節目』。
- 除了節目自身的受歡迎程度外，大數據戰略還有一個優勢，就是 Netflix 的推薦引擎也會有很大作用，這可以使 Netflix 節省不少行銷成本。Netflix 的數據表示，75%的觀眾都會被 Netflix 推薦觀看所影響。
- Netflix 的公關副總裁 Steve Swasey 說：「透過我們的演算法，我們可以發現那些可能喜歡凱文史貝西或者政治題材電視劇的觀眾，進而推薦給他們喜歡的劇集。」雖然具體的數據還得過一段時間才會揭曉，但觀眾對新版「紙牌屋」的最初評價相當正面。而人們不禁要問，大數據分析究竟給影視創作帶來了什麼？

Netflix 是如何用大數據捧紅「紙牌屋」的

- Netflix 的數據來自於它的 2900 萬觀眾。每次觀眾的搜尋，正評或負評，這些數據也會和第三方數據，如尼爾森的收視數據綜合起來，此外，再加上地理位置數據、裝置數據，社群媒體分享數據，觀眾加書籤數據、每次觀眾登入授權的數據，以及每部影片或者劇集的數據，都會進入 Netflix 龐大的數據分析系統裡去。
- 通過 Netflix 的演算法，Netflix 不僅僅知道你星期天晚上比星期一下午更可能會看恐怖片。也可能知道你更喜歡用平板電腦來看片。哪些地方的人們更加喜歡在星期天下午，用平板電腦觀看。Netflix 甚至能夠記錄哪些使用者當節目結束，幕後人員表開始跑時，就停止觀看。
- 分析凱文史貝西，大衛芬奇的粉絲與政治題材電視劇的相關性，僅僅是很小的一個應用方式。Netflix 透過對觀眾習慣了解，足夠它判斷某些特定內容對觀眾吸引程度。
- Netflix 的資深數據科學家 Mohammed Sabah 在去年夏天的一個研討會上指出，Netflix 可以針對某一幀畫面進行內容分析，分析當時的觀看習慣。這些數據，可以和其他數據關聯起來，得到更加完整的分析。而根據 Sabah 的演講看來，這裡的「其他數據」可能包括音量、顏色、背景等等數據，這些數據可能綜合起來，得出關於觀眾喜歡內容的有價值的資訊。

Netflix 是如何用大數據捧紅「紙牌屋」的

- Netflix 的首席內容官 Ted Sarandos 表示：
『Netflix 對觀眾非常有針對性。不像其他傳統電視台或者有線電視營運商， Netflix 不需要把內容先放出去後才知道觀眾喜好程度，Netflix 在內容播給觀眾前就已經知道這些』。
- 當然， 以數據為中心的決策也不一定能夠保證成功。凱文史貝西甚至大衛芬奇的參與， 也不能保證一定成功。作為 Netflix， 它的目標是要挑戰 HBO 在高品質影片的地位。這需要對大數據分析進行精益求精的優化。要記住的是， 任何大數據分析，也不可能避免小概率事件的發生。
- 不過， Netflix 這次在「紙牌屋」上的嘗試，對於製片業即將迎來一個重要轉折。新媒體公司過去幾年來， 已經在利用大數據分析的推薦引擎， 向觀眾推薦他們喜歡的節目。而現在， 大數據分析正深入到電影的創作環節， 這對將來整個影視創作行業從劇本選擇、 導演與演員的選擇， 拍攝和後期製作， 乃至行銷， 都會產生深刻的影響。

解密改變貨幣流通方式的新名詞

財經新報 2016.05.03

- 有一天，當你要辦理銀行業務時，卻發現一隻手機就能解決一切。有一天，當你正要踏入分行，卻發現銀行已經搬離原本的據點。這時，恭喜你來到金融科技（FinTech）的年代。金融和科技撞擊出來的火花正逐步改變你我的生活，究竟什麼是金融科技？它的重要性為何？本篇將依次為您解析。

金融與科技的結合

- 金融科技（Fintech）結合金融（Finance）和科技（Tecnology）兩字，由愛爾蘭的 National Digital Research Centre in Dublin 定義為將創新的元素融入金融服務。意味著以科技的方式，針對無效率的金融服務（例如：業務模式、產品、流程、應用系統等）作出改善。舉例來說我們常見的銀行叫號服務、電話下單交易等，都是科技和金融相互應用的例子。
- 「金融服務將不只是一個『地方』，而是一種『行為』！」，這句耳熟能詳的話，點出了金融科技未來的走向。金融科技崛起的核心價值，正是因為它能降低營運成本、差異化服務內容以及增加顧客的黏著度。

解密改變貨幣流通方式的新名詞

從信用卡開始，不斷跨越演進

- 金融科技的概念及應用已存在六十多個年頭。故事從 1950 年代說起，當時美國加利福尼亞洲的富蘭克林國民銀行首先發行了信用卡，讓人們出外購物時，不再需要以實體貨幣的形式支付。
- 1960 年代，英國倫敦北部的巴克萊銀行出現第一台自動提款的 ATM ，取代銀行櫃台和分行的角色。隨後的十幾年，Charles Schwab 成了第一個擁抱新的交易規則的證券交易商。這個新規定廢除了固定佣金。在此之前，數以百萬計家戶的投資機會是受到限制的。遊戲規則在 1975 年被改變，當證券交易商對於佣金的限制被 SEC 打破。
- 1990 年代，網路和電子商務發展日新月異，且線上股票交易改變佣金的形式。很多公司被包含在這波線上交易行動的浪潮。例如 1994 年的八月，K. Aufhauser & Company 成為第一家透過自身的WealthWEB 提供線上交易的券商，或者像 Datek 是一家在 1970 年建立的證券經紀商，並在 1996 年提供了線上零售交易的服務。

解密改變貨幣流通方式的新名詞

從信用卡開始，不斷跨越演進

- 當 PayPal 在 1998 年 12 月成立，意味著第一個給網路客戶的銀行品牌成立。當時大家沒有辦法把這概念和科技做連結，因為「金融科技」這概念當時尚未被提及。PayPal 並沒有受到如同銀行的管制，但它是和線上銀行最接近的一種形式。一開始以 Confinity 的名稱成立，接著才和 X.com 合併。這是一個非常遠大的目標-透過 email 寄送現金，並且這家公司藉由 eBay 的買賣雙方找到了利基市場。PayPal 在 2002 年 IPO，接著變成 eBay 完全持有的子公司。
- 「網路 2.0」從 2004 年開始變成一個非常受歡迎的階段，用來描述網路的第二次崛起。千禧年的第一個十年，P2P 借貸模式、機器人顧問、比特幣、支付等金融科技的崛起，搭配 iPhone 的推出，代表了一種所有產業很會就會被科技打亂的前奏。智慧型手機在這個階段允許所有產業的創新可以百花齊放。人們隨身攜帶智慧型手機，如同個人電腦可以隨時連接到網路。
- 一直到今天，無數的金融科技公司（例如：LendingClub 、OnDeck ）逐漸踏上 IPO 的階段。相信金融科技的創新還會再延續到未來，創造出更多的改變。

解密改變貨幣流通方式的新名詞

傳統銀行首當其衝

- 根據《Business Insider》的調查，我們可以發現傳統的金融產業面臨迫切危機，因為在 2020 年有四分之一的業務會受到金融科技公司影響，當中又以付款與交易被侵蝕的最嚴重，資產管理業務與保險則在其次。
- 分行轉型、裁減人力已經變成金融業棘手的問題。相對於極盛時期的聘用人數，英國金融時報觀察到美、歐已裁減約 73 萬人，預估未來 10 年還會因為金融科技崛起的關係大量裁減 170 萬人，佔比約目前人員數的 30% 。
- 2016 年開始，丹麥開始採行貨幣無紙化的交易形式。無紙化可以消除過往現金會有的問題（例如：易竊、衛生、偽造貨幣等）。然而凡事都有一體兩面，無紙化的過程會透過留存消費者每筆交易紀錄作為根據，此時個人隱私將被國家、金融機構掌握得一清二楚。另外，小型攤販及收入不多的家戶在無紙化交易過程中可能會遇到的問題也未被納入考量。
- 崛起的中國和印度，成為亞洲在金融科技浪潮下被關注的區域。以中國為例，經濟成長快速有助於吸引投資。印度，則是因為銀行帳戶和上網普及率尚低，被視為待開發的市場。

解密改變貨幣流通方式的新名詞

銀行被迫轉型跟進

- 被侵蝕營收、市場佔有率下滑以及資安隱私保障，成了金融體系轉變原因。Uber 的出現威脅著計程車產業，金融科技讓金融業產生了 Uber 時刻，徹底影響就業人數。
- 元大寶華經濟綜合研究院 院長梁國源，發布「金融業因應數位金融崛起的轉型之道」報告，針對台灣發展較其他國家落後的金融科技提出 5 大建議：
  1. 收購或投資適用的相關技術
  2. 盡快培養相關數位人才
  3. 鼓勵業務模式的開拓與創新
  4. 善用子公司跨業經營模式
  5. 確保數位金融的安全性
- 為了培育金融科技人才，並且串起產業和學界的橋樑，玉山銀行以「玉山黑客松」的商業競賽形式推廣 Fintech 並延攬相關學子。國泰金控更和政大科智所簽訂合作契約，開設課程增加競爭力。

解密改變貨幣流通方式的新名詞

政府修訂相關法規、成立金融科技公司

- 2016 年 4 月 6 日正式成立了臺灣金融科技股份有限公司，整合台灣的金融和科技產業，串連金融科技生態圈，讓金融科技可以在台灣開花結果。台灣金融科技股份有限公司未來將從大數據著手，廣泛搜集產業和政府的相關數據。此外，也會以 PaaS 平台為輔助，讓 P2P 的創新可以更快速。
- 另外，金融業本身為受管制的特許行業，政府法規上的與時俱進，也是發展金融科技的一大關鍵。政府目前已積極打造有利於金融科技發展的環境，呼應外界希望政策可以朝諸如放寬非金融行業經營 P2P、開放機器人理財顧問、純網銀等方向改進的期許。

中國瘋刷臉、孕育出全球第一個臉部辨識獨角獸 Face++

MoneyDJ 新聞 2017.06.09

中國瘋刷臉、孕育出全球第一個臉部辨識獨角獸 Face++

- 鴻海於2016年10月代子公司FOXTEQ HOLDINGS INC.公告取得曠視科技特別股股權。
- 根據Omnico在6月7日發布的調查報告，85%的美國、英國、中國、日本以及馬來西亞消費者希望主題樂園能夠採用AI身份辨識系統。
- 中國消費者對高科技的接受度最高、高達92%願意讓AI藉由身體特徵進行身分辨識。與五國整體調查趨勢(指紋辨識)不同的是，中國主題樂園訪客最能接受的是臉部辨識、支持佔比達41%。
- 南華早報5月19日報導，艾瑞咨詢預估中國AI市場規模平均複合年增率將高達50%、2020年產值上看91億美元。根據瑞銀財富管理公司報告，2030年AI在亞洲將可創造出1.8-3.0兆美元的價值、中國預估將可拿下8千億美元至1.25兆美元的產值。
- 雲天勵飛執行長陳寧表示，公司研發的人工智慧晶片比傳統的 CPU、GPU 還要有效率。內建雲天勵飛晶片的安全監控攝影機能大幅加快人臉辨識速度、在數秒內便可從群眾中找出嫌疑犯。

從法律與法規看個人資料保護與外洩之責任

bsi.

確保個人資料安全責任

第十八條

- 公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

第二十七條

- 非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
- 中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。
- 前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。

第十二條

- 公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

特種個人資料事前與事後安全保護要求

第六條第一項

- 有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

一. 法律明文規定。

二. 公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且**事前或事後**有適當安全維護措施。

三. 當事人自行公開或其他已合法公開之個人資料。

四. 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

五. 為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內**且事前或事後有適當安全維護措施**。

六. 經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

個人資料安全保護應有之施行

個人資料保護法施行細則第十二條

- 本法第六條第一項但書第二款及第五款所稱適當安全維護措施、第十八條所稱安全維護事項、第十九條第一項第二款及第二十七條第一項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取**技術上及組織上**之措施。
- 前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有**適當比例為原則**：

一. 配置管理之人員及相當資源。
二. 界定個人資料之範圍。
三. 個人資料之風險評估及管理機制。
四. 事故之預防、通報及應變機制。
五. 個人資料蒐集、處理及利用之內部管理程序。
六. 資料安全管理及人員管理。
七. 認知宣導及教育訓練。
八. 設備安全管理。
九. 資料安全稽核機制。
十. 使用紀錄、軌跡資料及證據保存。
十一. 個人資料安全維護之整體持續改善。

私立專科以上學校及學術研究機構個資安全保護

私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法第五條

- 學校、機構得指定或設**管理單位，或指定專人**，負責個人資料檔案安全維護；其任務如下：

一. 訂定及執行安全維護計畫，包括業務終止後個人資料處理方法。
二. 定期就個人資料檔案安全維護管理情形，向管理人提出書面報告。
三. 依據稽核人員就計畫執行之評核，於進行檢討改進後，向管理人及稽核人員提出書面報告。

私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法第六條

- 學校、機構應確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍，並**定期清查**所保有之個人資料現況。
- 學校、機構經定期檢視，**發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置**。

私立專科以上學校及學術研究機構個資安全保護

私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法第十二條

- 學校、機構對所保有之個人資料檔案，應設置必要之安全設備及採取必要之防護措施。
- 前項安全設備或防護措施應包括下列事項：
  一. 紙本資料檔案之**安全保護設施及管理程序**。
  二. 電子資料檔案存放之電腦或自動化機器相關設備，配置**安全防護系統或加密機制**。
  三. 訂定紙本資料之銷毀程序；電腦、自動化機器或其他儲存媒介物需報廢汰換或轉作其他用途時，應採取適當**防範措施，避免洩漏個人資料**。

私立專科以上學校及學術研究機構個資安全保護

私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法第十三條

- 學校、機構為確實保護個人資料之安全，應對其**所屬人員**採取下列措施：
  一. 依據業務作業需要，建立管理機制，設定所屬人員不同之權限，以控管其接觸個人資料之情形，並定期確認權限內容之適當性及必要性。
  二. 檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。
  三. 要求所屬人員妥善保管個人資料之儲存媒介物，並約定保管及保密義務。
  四. 所屬人員離職時取消其識別碼，並應要求將執行業務所持有之個人資料（包括紙本及儲存媒介物）辦理交接，不得攜離使用，並應簽訂保密切結書。

私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法第十六條

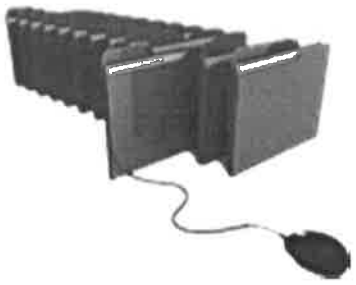
- 學校、機構應訂定個人資料檔案安全**稽核機制**，定期或不定期檢查安全維護計畫所定相關事項是否落實執行。

私立專科以上學校及學術研究機構個資安全保護

私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法第十七條

- 學校、機構執行安全維護計畫各項程序及措施，應**保存下列紀錄**：

一. 個人資料之交付及傳輸。
二. 個人資料之維護、修正、刪除、銷毀及轉移。
三. 提供當事人行使之權利。
四. 存取個人資料系統之紀錄。
五. 備份及還原之測試。
六. 所屬人員權限之異動。
七. 所屬人員違反權限之行為。
八. 因應事故發生所採取之措施。
九. 定期檢查處理個人資料之資訊系統。
十. 教育訓練。
十一.安全維護計畫稽核及改善措施之執行。
十二.業務終止後處理紀錄。



私立專科以上學校及學術研究機構個資安全保護

私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法第八條

- 學校、機構應訂定應變機制，在發生個人資料被竊取、洩露、竄改或其他侵害事故時，迅速處理以保護當事人之權益。
- 前項應變機制，應包括下列事項：

一. 採取適當之措施，控制事故對當事人造成之損害。
二. 查明事故發生原因及損害狀況，並以適當方式通知當事人。
三. 研議改進措施，避免事故再度發生。

個資外洩有損及當事人之虞時應有之通報義務

個人資料保護法施行細則第二十二條

- 本法第十二條所稱適當方式通知，指**即時**以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他**足以使當事人知悉**或**可得知悉之方式**為之。但**需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之**。
- 依本法第十二條規定通知當事人，其**內容應包括個人資料被侵害之事實及已採取之因應措施**。

個人資料外洩因應措施

bsi.

英國資訊委員公署對個資外洩的因應建議

Guidance on data security breach management, Ver. 2.1, 2012.12.12

- 資料外洩的原因：
  - 對未經授權存取許可的不當存取行為
  - 設備無預警故障、失靈
  - 人為操作錯誤
  - 非預期的災害，例如：火災、洪水、颶風、地震等
  - 駭客攻擊
  - 社交工程
- 資料外洩未必為單一原因發生，對於複合性的威脅將更難完全避免資料外洩

英國資訊委員公署對個資外洩的因應建議

Guidance on data security breach management, Ver. 2.1, 2012.12.12

- 資料外洩時的管理程序：
  - Containment and recovery 遏制與復原
  - Assessment of ongoing risk 持續進行風險評鑑
  - Notification of breach 個人資料外洩通知
  - Evaluation and response 評估與回應

英國資訊委員公署對個資外洩的因應建議

- Containment and recovery 遏制與復原：
  對個人資料外洩的初期不僅只有調查和情況的遏制，尚有復原計劃的實施，及必要的損害控制，這階段可能需要資訊部門、人事部門及法律專業領域的投入，特殊狀況下可能還要包含與關注方和廠商的聯繫。並需注意下列事項：
  - 決定負責調查原因部門，並投入適當資源
  - 確定哪些部門需要了解個人資料外洩情形，通知相關部門作為遏制工作的實施
  - 確認有無可能降低損失，並限制可能造成的損害
  - 通報執法機關

英國資訊委員公署對個資外洩的因應建議

- Assessment of ongoing risk 持續進行風險評鑑：
  個人資料外洩可能造成的影響與一般設備故障是不同的，在決定後續應評估各式可能的風險。 也許最重要的是對個人的潛在不利後果的評估，包含嚴重程度、實質影響，以及其發生的可能性，並確認下列事項：
  - 確認外洩的個人資料內容與數量
  - 有無特種個人資料或可能對資料主體造成重大影響的資料？
  - 外洩的個人資料有無任何保護措施，例如：資料加密？
  - 洩漏個人資料的資料主體是是誰？例如：員工、客戶或供應商
  - 洩漏的個人資料會對資料主體造成什麼傷害？ 例如：身體、心理、精神、財務，或其他？
  - 有無可能造成信心的淪喪？
  - 是否需防止身份欺詐的可能？

英國資訊委員公署對個資外洩的因應建議

- Notification of breach 個人資料外洩通知：
  通知當事人個人資料外洩在資料外洩管理策略中的重要一環，但通知當事人並非目的，為了使受影響的當事人能夠採取措施保護自己，或者允許適當的監管機構履行職能，作為隨之將來提供諮詢和處理投訴的作業，並考量下列事項：
  - 是否有法律或合約要求？
  - 通知的及時對於當事人的重要性，例如：取消信用卡或變更密碼。
  - 選擇適當的通知方式。
  - 通知的內容至少應包括如何以及何時發生個人資料外洩、涉及哪些資料的說明，以及已採行的補救措施等資訊。
  - 提醒當事人可採取的保護措施，並提供具體和明確的協助與建議。
  - 提供聯絡的管道以更新資訊或聯繫所用，例如：免付費電話或網頁。

英國資訊委員公署對個資外洩的因應建議

- Evaluation and response 評估與回應：
  不僅查明造成個人資料外洩原因，還要評估因應措施的有效性，並注意下列事項：
  - 確認掌握個人資料的保存及儲存方式。
  - 鑑別風險，例如：有多少特種個人資料？個人資料是否統一集中保管在一個地點？
  - 與他人分享個人資料時，需確保傳輸方法是安全的，並確保只分享所需的最少個人資料。
  - 識別現有安全措施中的弱點與盲點。
  - 監督工作人員對安全的認知，透過教育訓練或宣導來彌補差距。
  - 評估配置技術和非技術人員的必要。
  - 在既有的營運持續計畫中考量個人資料外洩的情境。
  - 評估因應未來個人資料外洩時的一線的人員。

香港私隱公署對個資外洩的因應建議

資料外洩事故的處理及通報指引

- 步驟1：立即蒐集有關資料外洩事故的重要資料
  - 事故於何時發生？
  - 事故在哪裡發生？
  - 事故如何被發現及由誰發現？
  - 事故的肇因是什麼？
  - 涉及什麼種類的個人資料及範圍有多大？
  - 受影響的資料當事人有多少？

香港私隱公署對個資外洩的因應建議

- 步驟2：聯絡相關人士及採取措施遏止事件擴大
  資料使用者在發現資料外洩後，應採取步驟以杜絕事件的肇因，這可能需要聯絡執法不怎、相關的歸管機構、互聯網公司及 / 或資訊科技專家，作出報告、尋求建議及協助。 遏止措施可考慮：
  - 如果資料外洩是系統故障造成，應停只有關系統的操作
  - 更改用戶密碼及系統配置，以控制查閱及使用資料
  - 考慮是否需要尋求內部或外部的技術協助，以修補系統上的漏洞及 / 或組織黑客入侵
  - 停止或更改涉嫌作出或導致資料外洩的人事的查閱權
  - 如已發生或相當可能發生身份盜竊或其他犯罪活動，應通知有關執法部門
  - 保留資料外洩的證據，這可能會有力調查及採取糾正行動
  - 如資料外洩是因資料處理者的作為或不作為而造成，資料處理者需立即採取補救措施及將進度告知資料使用者

香港私隱公署對個資外洩的因應建議

- 步驟3：評估事件可能造成的損害
  資料外洩事故可能導致以下的損害：
  - 人身安全受到威脅
  - 身份盜竊
  - 財務損失
  - 受辱或喪失尊嚴、名譽或關係受損
  - 失去生意或聘用機會

- 當事人可能蒙受傷害程度取決於：
  - 外洩個人資料的種類
  - 涉及個人資料的數量
  - 資料外洩的情況
  - 身份被盜或假冒的可能
  - 外洩資料是否加密、匿名而令其不能查閱？
  - 資料外洩是否持續，及會否進一步曝光？
  - 有關事故是獨立事件，抑或屬於系統性問題？
  - 如屬實物遺失，是否有機會使用前尋回？
  - 相關補救措施？
  - 當事人可避免或減輕傷害的能力？
  - 當事人對個人資料私隱的合理期望

香港私隱公署對個資外洩的因應建議

- 步驟4：考慮作出資料外洩通報
  在資料外洩事故中，如可以辨識資料當事人並能合理地估計實在的傷害風險，資料使用者應考慮通知資料當事人及相關人士。資料使用者在作出決定前，應恰當地考慮不作出通知的後果，並考慮下列事項：
  - 向誰通報？當事人？執法部門？私隱專員？相關規管機構？其他可採取補救行動以保障受影響資料當事人的個人資料私隱及利益人士，例如：互聯網公司。
  - 通報應包含什麼？視個案情況，通報可包含下述資料：
    1. 事件的概況
    2. 外洩日期及時間，及持續時間
    3. 發現事故的日期及時間
    4. 外洩的源頭
    5. 表列所涉及的個人資料類別
    6. 對外謝事件導致傷害的風險評估
    7. 未防止個人資料進一步遺失或未經授權下查閱或洩漏所採取的措施
    8. 指派機構內部門或個人的聯絡資料
    9. 資料當事人可如核保障自己免受事故的不利影響及身份不被盜用的指引
    10. 通知執法部門、私隱專員或其他有關人士是否獲通知

何時通報
如何通報

由近期個資外洩新聞檢視應有作為

bsi.

1 委外旅行社的外包商訂房系統遭駭，Google 員工資料外洩！

iThome 2017.07.04

- 專門為Google提供員工差旅訂房服務的旅行社CWT，因為使用的訂房服務供應商Sabre Hospitality Solutions發現系統遭到非法存取，經調查Google委託的訂房資料、包含員工姓名、聯絡資訊、信用卡等資料外洩。
- 受這起事件所累，Google委外旅行社處理的多筆數目不詳的訂房資料，以及Google員工姓名、聯絡資訊、信用卡資訊等外洩。Google已於上周通知受影響的員工及加州主管機關。
- Google指出，為該公司負責差旅訂房、訂票的旅行社Carlson Wagonlit Travel (CWT)使用訂房服務供應商Sabre Hospitality Solutions開發及營運的SynXis Central Reservations系統（CRS）。Sabre發現SynXis CRS的內部帳號在2016年8月10日到2017年3月9日遭非授權存取，該名未獲授權人士得以存取經由CWT完成的數宗訂房客戶的個人資料。CWT也在得知此事後於6月16日通知Google。Google並在CWT和Sabre配合下證實Google的員工受到影響。

1 委外旅行社的外包商訂房系統遭駭，Google員工資料外洩！

- 除了上述資料，Sabre的調查未發現員工社會安全號碼、護照、駕駛執照遭存取的證據。但因為SynXis CRS會在住房過後60天內刪除訂房資料，因此無法證實是否還有其他員工或其他類型資料外洩。
- 針對本外洩案，在CWT及Sabre合作下，Google提供受影響員工一旦發生詐欺及身份盜竊導致的財務損失賠償、信用回復及長達二年的信用卡資料監控服務。
- 資料外洩難防，而外包商更使資料盜竊事件防不勝防。去年以來，美國特種作戰司令部及海軍分別因為外包商Booz Allen 及HPE未做好資料防護導致外洩11GB與13萬筆官兵資料。

2 Android用戶小心個資被看光 逾800款App遭植惡意程式

NewTalk 2017.06.18

- Android的愛用者要小心了！資安業者趨勢科技（Trend Micro）在偵測Android平台時發現，有逾800個手機App廣告中內嵌有木馬程式「Xavier」，並利用這些App暗中竊取用戶個資，目前這些App已累積有數百萬人次下載，相當可觀。
- 根據趨勢科技調查，兩年前「Xavier」原本僅是一款合法無害的廣告庫，可以內嵌在各種免費的應用程式，讓應用程式的開發者能夠輕鬆地透過廣告賺取費用，而目前使用這個廣告庫逾有800 個應用程式，其中包括相片編輯程式、桌布程式等，但隨著時間發展，「Xavier」逐漸變種為危險又複雜的軟體，Xavier可以躲過 Google Play 的安全檢測，所以駭客可以利用它來蒐集用戶的裝置資料、個人化設定、使用語言、作業系統版本、已安裝應用程式，甚至是電子郵件地址和Google Play帳號，駭客都能輕易到手。

2 Android用戶小心個資被看光 逾800款App遭植惡意程式

- 除了盜取個人重要資訊之外，駭客也可以遠端鎖定行動裝置，並安裝指定應用程式套至裝置內部，駭客多半會將該程式偽裝成Android系統清理工具「Ks Clean」，並於安裝完成後跳出通知，要求使用者進行更新，多數使用者都會不假思索地按下更新後，該程式便會安裝另一個假冒檔案，並要求使用者授權管理權限。造成用戶難以察覺中毒，而這個「Ks Clean」目前該惡意程式的主要功能為不論何時何地都能跳出廣告視窗，而且可執行各種惡意行為，諸如讀取書籤歷史紀錄、覆蓋系統視窗、變更裝置設定，或是逕自下載其他檔案等，令人髮指。
- 目前大多數下載遭Xavier感染App的用戶，都來自越南、菲律賓等東南亞國家，台灣也有 5.36% 的受害比例，所以用戶應要隨時保持手機系統更新，在下載應用程式時一定要特別小心，千萬不要下載來路不明的應用程式，在下載之前，也請先看清楚該應用程式要求開啟的權限，以免個人資料被駭客看光光。

3 駭客入侵出國登錄系統 領務局公開致歉

自由時報 2017.02.08

- 外交部領務局推廣「出國登錄」，民眾出國前登錄個人資訊，旅遊目的地外館的領務專用電子信箱就會收到資料，倘若民眾在海外遭遇急難，即可立刻獲得協助。然而外交部日前進行安全查核時，卻發現有不明來源 IP 成功駭入數十個外館領務信箱。領務局估算，最多可能使近 3 個月以來登錄的 1 萬 5000 筆人次個資遭竊取。領務局今上午召開記者會致歉，並表示已通報行政院資安辦、提升伺服器防護等級、要求外館立刻更改信箱密碼，現正研擬調整登錄項目中。領務局強調，遭駭系統是獨立的，與外交部其他資料均無關。
- 外交部今證實，領務局近日在資通安全檢查時，發現領務專用電子郵件系統有異常活動情形，初步研判領務局發送給駐外館處的國人出國登錄資料，可能遭不明人士攔截。領務局除通報行政院資安辦公室、提升伺服器防護外，也立即停止傳送出國登錄資料至外館，改由外館於緊急狀況時直接向領務局查詢資料。

3 駭客入侵出國登錄系統 領務局公開致歉

- 領務局今上午召開緊急記者會說明此案。領務局副局長鍾文正表示，領務局已委請資安專家到局內進行數位鑑識，並確認領務局電郵及護照簽證等主機，並無遭駭客入侵跡象，確認受影響的資料是出國登錄的範圍，其他個人資料均安全無虞。領務系統異常活動時間範圍是最近3個月，範圍是民眾經常出國旅遊的國家或地區，如日本、英國、東南亞等。領務局表示，駭客是以浮動 IP、每天駭入不同館處。估算可能遭竊取筆數約 1 萬 5000 筆，然而確切被截取的資料數量，仍需要進一步清查。鍾文正也解釋，如果駐館比駭客更早收信的話，相關資料就會被清除，也就不會被擷取。所以清查完後，受影響筆數可能還會下修。

- 鍾文正表示，此次發生資安事件非常遺憾，對於造成民眾不安與困擾，他代表領務局，致上最深歉意。然而出國登錄真的是對國人旅外安全有幫助的措施，因此領務局會繼續辦理，但為維護國人個資安全，防範有心人士不當截取，未來考慮調整登錄項目，以降低風險。目前「出國登錄」網站需登錄中英文姓名、出生年月日、身分證字號、護照號碼與電子信箱等資訊；據了解，領務局內部正研議將登錄項目減至最低，可能會將登錄所需資料項目減少至姓名、護照號碼與緊急連絡人等內容。

3 駭客入侵出國登錄系統 領務局公開致歉

- 領務局資安系統除依規定定期監控、並使用 SALT 加密外，也不定期進行檢測，此次是外館同仁發現異狀，因此進一步檢查。領務局強調，遭駭系統是獨立的，與外交部其他資料均無關。對於可能遭駭、即近 3 個月登錄的民眾，領務局已發送警示電郵，提醒民眾的其餘個人密碼，若有使用到登錄的資訊，建議儘速更換密碼；而若國人仍在海外旅遊，建議儘快和家人報平安。

- 倘若民眾因此受害該如何賠償？鍾文正表示，針對此次資安事件，已經成立專案小組因應，如果民眾有需要、或因此造成損害，可透過電郵 info@boca.gov.tw 或專線電話 02-2343-2868、02-2343-2922、02-3343-5551等管道和領務局聯繫，將依法律規定進行處理。鍾文正表示目前還沒有收到民眾回報有受害情形。

4 監理站美女 洩漏個資被訴

自由時報 2017.06.05

- 代表台灣參加東亞運榮獲銀牌的龍舟國手呂維鈞，與男子洪楚源，因健身房有經營權糾紛，洪當時的女友、也是桃園監理站監理員龔詩茜，竟利用職權，查詢呂男名下車牌是否變更登記等個資；新北地檢署今依刑法洩密罪嫌及個人資料保護法起訴龔女。
- 檢警調查，呂維鈞、洪楚源等人合夥在新北土城經營健身房，由呂男擔任登記負責人並管理財物，洪男與其他股東另於桃園開設分店。
- 因健身房自營運起至104年8月均未發放紅利，引發洪男等5位股東不滿，洪懷疑呂男掏空公司，遂於104年8月22日晚間，在土城健身房召開財務說明會議，要求呂男說明，雙方爆發口角，洪出手毆打呂男，要求交出公司大小章、存摺等，還要呂簽下50萬本票，才讓他離去。

4 監理站美女 洩漏個資被訴

- 事後，呂怒控對方侵占、背信、傷害、強制，另又指控龔女利用在監理所系統查詢他的個資，提供給洪男。
- 檢方日前已依傷害、強制罪嫌起訴洪男，侵占、背信另案偵辦；龔女部分，檢方調查認為，她確實利用監理系統，查詢呂的個資，並將呂已將名下汽車變更登記給家人，及車藉資料提供給洪男；也因此，洪男能依此質問呂男為何脫產。
- 龔女否認犯行，辯稱可能在聊天過程告知此事；檢方認定龔女所為觸犯刑法洩密罪及個人資料保護法，因而起訴，至於洪男則因無法證明是指使所為，而不起訴。

5 北市智慧支付平台傳外洩個資 資訊局否認

聯合新聞網 2017.6.28

- 台北市推出「pay.taipei」平台支付水費等費用，卻傳出平台未加密，恐讓個資外洩。資訊局副局長高永煌今天說，是平台安全出現漏洞，但不會洩漏個資，現已逐漸完成修復。
- 台北市政府25日開記者會宣布智慧支付平台「pay.taipei」正式上線服務，民眾可下載「pay.taipei」行動App或上網站一鍵繳納水費、停車費及聯合醫院醫療費用，推出首波也結合支付業者各項優惠，但27日卻傳出App存在資安風險，
- 高永煌說，該平台作為支付業者及各機關的服務中介，並不會處理金流，也不會儲存會員個資，使用者所輸入的資料僅用身分確認。
- 至於為何發生安全漏洞，高永煌表示，廠商選擇不安全傳輸且未有加密協定，但不會洩漏個資問題，因為平台沒有個資資料，民眾不會從平台頁面看到相關資料，需要特定技術人員在特定環境和時間點和工具才可看到片面資料，但到目前為止，都沒有類似的安全疑慮。

5 北市智慧支付平台傳外洩個資 資訊局否認

- 高永煌說，昨天下午2時發現App有資安風險，下午4時就完成防毒，後續做好網站修改及App更新，資訊局在App上線前沒有做好更徹底檢查，坦然接受外界批評，會積極維修改善。
- 他表示，市長柯文哲也在上午舉行會議特別指示，若有錯就要虛心檢討，但也希望民眾不要對該平台失去信心，目前App有約1000人下載，包含向市府測試工程人員，現都已完成修復，且不排除會向廠商求償。

6 史上最大宗 美2億選民個資外洩

自由時報 2017.6.21

- 美國資安研究人員證實，一家為共和黨全國委員會和其他共和黨人士服務的資料分析公司「深根（Deep Root）」，疑似在一次更新時不小心解除檔案的加密保護，本月1日起把1.1TB檔案，包括約佔62%美國人口的1.98億選民姓名、生日、住家地址、電話號碼等個資，暴露在公開的網路世界12天，期間任何人都能輕易下載這些資料。該起事件據信為史上最大宗的美國選民資料外洩案。

- 美國矽谷新創資安公司「守衛（UpGuard）」安全風險分析師維克里（Chris Vickery）12日在亞馬遜雲端服務中發現大筆選民資料，只要連上正確路徑就可以讓人隨意下載，這些資料不同於一般外洩的商業資料，不包括社會安全號碼或信用卡資訊，但有諸多選民登記的細節，以及共和黨用來識別並分類選民的資料與模型。維克里指出，有些檔案針對選民回答議題的觀點打分數、分類，議題包括2012年美國大選的投票情況，對移民、貿易、汽車製造業的觀感，對美國總統川普口號「美國優先」的認同度等，還有超過170GB的檔案專門蒐集選民在社群媒體的貼文，「你可以利用這些資料鎖定特定群體或個人.....，我甚至可以給你共和黨全國委員會認為票投川普的所有選民的住址。」

6 史上最大宗 美2億選民個資外洩

- 維克里發現問題後，立即通報警方及相關單位，「深根」已在14日修正問題，並發表聲明表示正與外部專家合作調查此事，「我們將為此狀況負起全責」，指出至今仍未發現駭客入侵系統的跡象，聲稱被取得的資料包括「限閱資訊以及公開可用與州政府官員欣然提供的選民資料」。共和黨全國委員會表示，他們已暫停與「深根」的合作，會靜待調查結果。「深根」和其他兩家同屬共和黨的承包商「目標諮詢」及「數據信賴」合作建立這個選民分析資料庫，這批資料被形容是「川普陣營所用的政治資料和模擬偏好一大寶庫」。

- 該起個資外洩案曝光後，引發社會關注。民眾擔心這些資訊會被壞人加以利用，進行詐欺、騷擾，或是因此能加以威脅不同政治傾向的人。隱私政策專家卡瑟納告訴英國廣播公司，共和黨依靠公開取得、商業提供的資訊來進行分析並利用電腦模式來預測選民行為，「沒有人能想到，提供給某個機構的資料，最後會被放進資料庫，用來預測他們的政治傾向」，「這威脅民主的運作」。

bsi.

...making excellence a habit.™