個人資料保護管理制度
現況及挑戰
------以資安層面探討

李相臣

銓敘部資安重大疏漏 59萬筆文官個資外洩

- 政府資安再傳重大疏漏！銓敘部驚傳有高達五十九萬筆文官服務單位、職稱等個資外洩，並遭國外網站揭露，銓敘部已緊急依資通安全管理法向行政院國家資通安全會報技術服務中心通報，銓敘部昨也指出，目前已請資安部門進行資料外洩原因調查，將確實檢討改進，另也依個人資料保護法規定，針對二十多萬受影響的當事人展開通知作業。

北市府紅隊演練發現衛生局公衛系統 市民個資於暗網兜售，檢調發動調查

北市政府衛生局驚傳，公共衛生資訊管理系統的個人資料遭到外洩，並且在暗網中，以100筆個資要價1千美元的價格對外販售。

該起資安事件的通報，起因是臺北市政府配合行政院執行資安前瞻計畫，由資訊局委由資安業者戴夫寇爾進行紅隊演練期間，進行相關情資蒐集時，在地下網站發現有人販售臺北市衛生局個資，戴夫寇爾並第一時間通報臺北市資訊局進行後續的調查。

臺北市衛生局的公共衛生資訊管理系統於2015年委由慧智達科技進行開發，據媒體報導，該系統有超過70個子系統，包含藥物及化粧品線上查詢暨申辦、行政資訊、健康管理個案管理系統、精神病患管理系統等。

李維斌表示，已經委由資安業者提供客製化的工具進行掃毒。但是，能否據此確認這是所謂的APT（進階持續性威脅）或是針對式攻擊，李維斌認為，一切都得等調查局調查結果出爐之後，才能確認真正的事發原因。

報告：個資外洩最多的產業是?

根據Verizon最近的一份報告顯示：

- **政府機關**所發生的資料外洩案件最多 **(303 起)**，
- 其次是**銀行 (277 起)** 和
- **零售業 (164 起)**。

政府機關應更注意供應鏈的資安狀況

政府機關和企業機構都必須更注意其委外廠商的資安狀況，尤其是那些能夠存取其敏感資料的關鍵廠商。

相對的，Unisys表示，消費者認為最可能發生資料外洩的產業分別為：

- **電信 (59%)**、
- **政府 (49%)** 及
- **銀行 (48%)**。

在最近一項針對40家公司共25萬台端點裝置的分析發現，**每一家公司的企業網路都有遭到「進階持續性滲透攻擊」**（Advanced Persistent Threat，簡稱APT攻擊）入侵的跡象，但大多數仍未發展到最危險的資料外傳階段。

企業發現新型態的銀行惡意程式非常難以防範，而且其技術在 Zeus 出現之後更不斷精進，**這類惡意程式專門暗中竊取使用者的網路銀行帳號登入資訊**。

Big Data

- 個資（去識別化）
- 整合、集體性資料
- 分析、決策性資料
- 存放地點、設備
- 多組合硬/軟體
- 特殊性分析工具

大數據來源(DMP 外部合作)

- 以站外實際行為，每日更新人群興趣、屬性、消費意圖...等，強化會員經營/行銷
- **名單管理平台**
- 可即時分析、篩選、編輯的人群名單管理系統，更可將人群名單推送到廣告平台供後續廣告投放使用
- **廣告投放專案**
- 與Cookie裝置辨識
- 上千追蹤網站活躍裝置2300萬/月
- 每日3000萬筆以上行為資料
- 深度學習語意分析解析行為與內容
- 250+ 機器學習標籤資料每日即時更新

- **紀錄多元行為的跨資料源數據**
- 記錄通話分類資料
- 位置紀錄
- 上網紀錄
- 收視廣告互動
- 瀏覽行為
- 其他資料夥伴持續洽談中

- …**AI** 技術進行資料**Mapping**與標籤化處理
- 人群資料匯送、名單管理平台與廣告投放專案彈性服務客戶、展現資料價值

我們可以從臉書和劍橋分析事件中學到什麼？

三個新興技術的發展：

1. 從網路上可獲得大量個人資訊(同意?)
2. 現代機器學習算法可使用這些資訊，來學習、建立複雜的人格檔案
3. 而社群平臺，能讓根據複雜人格檔案建立的客製化政治或行銷訊息，有效發送給對應的民眾

這些訊息引的效用非常大，原因：

1. 這些訊息是根據每個人的人格特質所發送的(客製化)
2. 這種行為很難審查，因為這些訊息是直接發送給個人，而不是公開在平臺上、讓第三方看得到

App隱私條款 個資賣身契

網路公司有哪些爭議手段

- 即使未經允許，也能追蹤用戶所在位置
- 將用戶個資和關係企業分享
- 讓用戶無意中同意第三方利用
- 就算是用戶已經刪除的搜尋歷史，仍被網路業者保留
- 用戶未開啟App，依然會被追蹤
- 用戶的私人訊息其實沒那麼「私人」

Fyodor

5.5萬　抹黑一人
20萬　煽動街頭抗議活動

劍橋分析

65個讚　跟你朋友一樣認識你
300個讚　跟你配偶一樣認識你 → FB告你或加入

尤其藥物使用、政治立場、健康

大數據信用風險待解決之問題

01

數據共享(黑心科技公司)

網路巨頭變成了數據黑洞，用戶的數據進得去、出不來，可以為企業自身而用，但不能為整個行業或社會而用。此外，散落在稅務、公積金、海關、工商等領域的數據梳理和整合，也是漫長的過程。

02

數據保護(雲端 倉儲等)

數據既是寶貴的資產，也可能演變成為聲譽風險、合規風險、用戶訴訟風險等各類問題的潛在來源，是福是禍，尚是未知之數。」

BRUCE SCHNEIER：萬物都是電腦，所有事也都變成了資安事

第1堂課是：大多數軟體都寫的很不安全。所有軟體都有漏洞

第2堂課是：網際網路不是為安全設計的(初期為封閉使用)

第3堂課是電腦具有擴充性

第4堂課，電腦系統很複雜

第5堂課是，互連之後會帶來新弱點

最後一堂課是，要發動資安攻擊，總是越來越容易、越厲害、也越快速，這就是我們面對的真實世界

- 科技是以功能導向開發運用的而非安全
- 使用 一段時間 會發現漏洞
- 有利可圖會驅動駭客入侵
- 使用者的疏忽或使用不當
- 所以美政府資安長說 只有被入侵
- (或不知被入侵)與即將被入侵者
- 風險控管 VS 風險防制 VS 沒有風險

KYC

- IP、3G 、4G 、費率
- 上網時間
- 使用設備、廠商型號
- 搜尋引擎、軟體功能(APP)
- GPS (活動範圍(內容隱私))
- 使用服務、輸入關鍵字查詢資料
- 網頁、廣告、購物、音樂、影片...、花費
- Cookie Log 讚 自填 他說...

EX：Apple Pay你看到什麼

手機不設防(丹麥-公共電視)

App普及率

隱私

技術

駭客攻擊之變遷

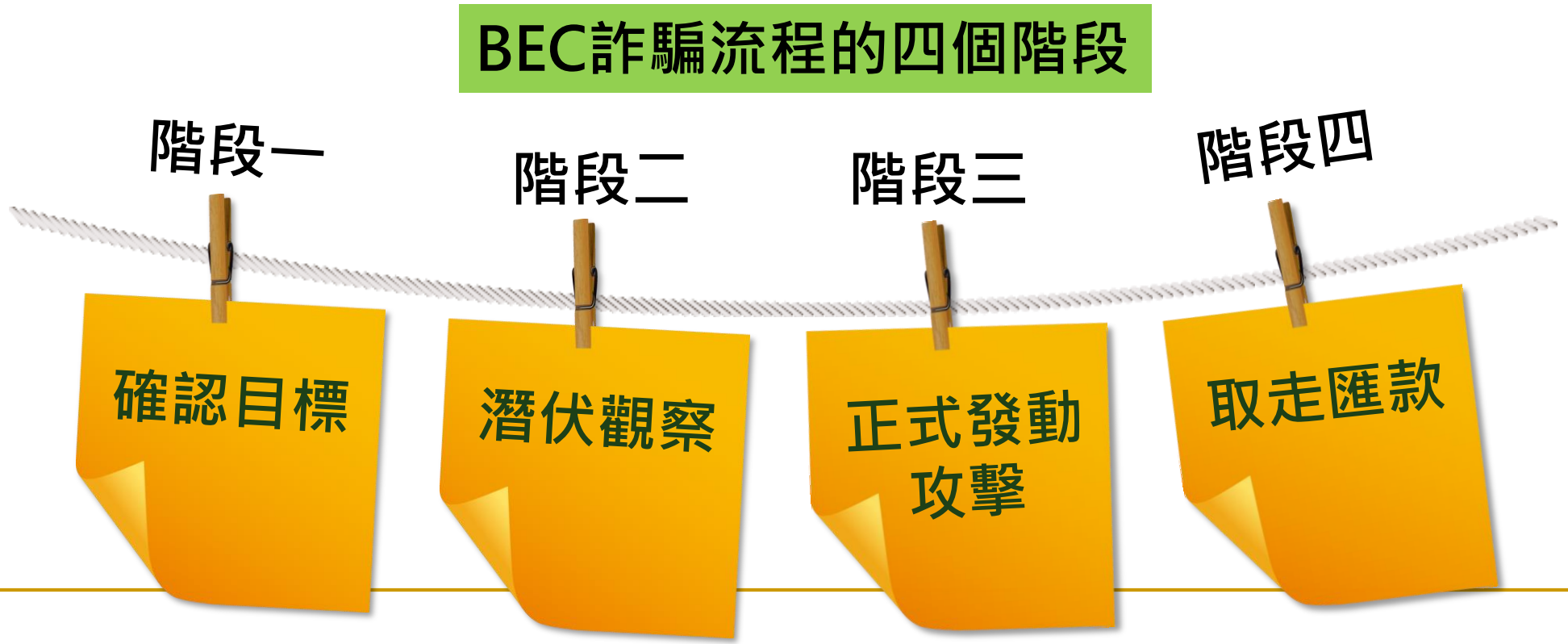
1. 工具愈來愈普遍、易得、交流與秩智慧
2. 高技術、精緻性手法與工具亦開始變多
3. 容易取得被害目標（人、企業與系統）等，更多相關資訊較易成功（客製化）
4. 目標式隨機與目標式聚焦攻擊增加
5. 使用暗網（如Tor）與比特幣，難以追查來源與目的
6. 孤鳥駭客＋工具流（製造）＋資訊流（攻擊）＋物流（收穫）＋金流　之產業生態鏈已形成

詐騙集團以AI軟體偽裝成老板聲音指示匯錢

- 詐騙集團發展出語音網釣攻擊，利用AI軟體模擬企業主管語音來要求下屬匯款，英國已有一家能源公司受騙

BEC常見詐騙方式(變臉)

駭入被害人公司的電子郵件系統，並偽冒其真實身份或電子郵件帳號，要求更改匯款內容。



俄羅斯駭客組織攻擊全球30國銀行掠財，臺灣為亞洲首要目標

- 安全公司Group-IB偵測到名為Silence的俄羅斯駭客組織，近年對全球超過30國銀行發動攻擊以竊取財產，而臺灣是這個組織在亞洲攻擊最頻繁的目標。

- 根據該公司分析，Silence曾在近期的一個月內，發出17萬封偵察式電子郵件，其中亞洲有8萬封，而臺灣以2.1萬封居榜首，其次是馬來西亞（1.6萬封）及南韓（8,800封）。值得注意的是，一旦驗證為有效電子郵件信箱後，駭客就開始發送附有攻擊程式的惡意郵件，接著以其工具滲透受害銀行的內部網路及橫向移動，如果金融機構安全防護技術未能偵測到，最後駭客得以控制信用卡處理中心、並以Atmosphere木馬或名為xfs-disp.exe的程式控制提款機在特定時間吐鈔，並由外部車手取款。更多內容

監測四億多用戶的瀏覽行為，連看英文影片都知道

螞蟻金服用大資料偵測金融犯罪

掌握大量用戶動態資料　需快速判斷異常交易

擁有四億多用戶的螞蟻金服，經營著中國最大的線上支付平臺支付寶與餘額寶等，供用戶在網路上進行購物、借貸甚至投資等多元金融服務，不過，在複雜的網路金融交易中，也暗藏著許多詐欺、賭博與貪污等行為，螞蟻金服到底如何在錯綜複雜的交易中判斷非法交易行為？

螞蟻金服法務及合規部高級經理黃元駿表示，掌握用戶交易與網路搜尋行為等大量資料，就是在網路中建構交易監控與建構風險評級的關鍵。在分析用戶龐大的資料時，為了了解關鍵數據為何，首先必須要判斷哪一些是公司關鍵的服務，其包括購買、支付行為、信用卡發卡與收單、物流與網路瀏覽行為等。「對於螞蟻金服來說，不管用戶進行轉帳、投資或消費，只要能夠佐證此筆交易為真實的，就認為是關鍵資料。」，他說。

在數位金融時代，黃元駿表示，進行反洗錢工作最大的挑戰為，由於用戶在螞蟻金服開設戶頭，只需要30秒左右，而不需到傳統銀行臨櫃辦理，導致反洗錢工作人員無法辨識用戶填寫的資料，包括性別、地址等是否正確，且透過用戶電腦申辦帳戶，也難確定操作系統的人是否就是用戶本人。

另一方面，在網路交易平臺上，因為用戶可利用手機隨時隨地進行交易使得工作人員必須在短時間內判斷交易是否存在異常，且由於交易日趨多元，能在網路上進行購物、轉帳、投資與借貸等，難定義交易是否異常，而帶給反洗錢工作很大的挑戰。

數位金融時代最大的特色在於，能夠取得大量的用戶資料，來分析交易是否存在異常，不同於傳統銀行大多僅只於使用靜態資料，如用戶的性別、年齡、地區與職業等。

由於阿里巴巴集團旗下經營包括搜尋引擎、淘寶網、網商銀行、餘額寶等，因此可以透過這些網路平臺取得用戶的動態資料，包括，線上購物、轉帳匯款、投資理財、瀏覽網站、觀看影音網站、消費行為與購物產生的物流過程與使用時間、位置等資料，因此，「對於數位金融反洗錢來說，最關鍵的就是掌握資料。」。

以用戶的影音網站觀看資料來說，如有一位60歲、受國中教育且在工廠工作的男士，但某天卻開始收看英文影音內容，就會懷疑此交易帳號是否被其他人使用，而非同一人，而認為此帳號存在異常行為。另外，也可以透過手機定位系統能來判斷用戶交易位置與移動情況，以判斷每一次交易是否有地緣關係，如A正在北京用手機購物，但十分鐘後，就出現在新疆，因不可能10分鐘後就移動到新疆，代表利用此交易帳號進行交易者應非同一人，而判斷此交易存在異常。

圖片來源／勤業眾信

螞蟻金服法務及合規部高級經理黃元駿表示，掌握用戶交易與網路搜尋行為等大量資料，就是在網路中建構交易監控與建構風險評級的關鍵。

不光蒐集用戶瀏覽行為，黃元駿表示，也會藉由判斷此商品交易使用的物流服務，透過商品賣方與物流商提供的商品運送等相關數據，再加以比對，來判斷此商品交易是否為真，或是假交易。

黃元駿表示，螞蟻金服是針對一般的民眾，而以巴拿馬文件風暴來說，其暴露了1千多萬筆國際政要與富豪等避稅資料，對傳統銀行產生比較大的衝擊，對於螞蟻金服則影響不大。**文⊙胡瑋佳**

1. Deep Learning → Hacking Learning
2. Machine Learning → Machine Bot
3. Big Data → Hacker掌握更多攻擊、漏洞與行為特徵
4. 各行各業都在進步，駭客自不例外

當科技愈來愈進步，使用愈來愈廣泛，比較有效的方法還是要聚焦使用前、中、後所產生的紀錄分析

- AI + Big Data

  =

  Open Data

太多科技來不及學或搞懂就出事了

敬請指教！

認知

學習

警覺

防護