現況問題篇

層層揭開都是洞 都是駭客惹的禍？

購物平台不僅牽涉組織眾多，關係網絡複雜，變化的速度也相當快，本篇主要揭露電子商務面臨到的資安現況。

文 | 吳依恂

最近，購物平台又出事了。

資料外洩的購物平台換了一個，依然可以看見各大新聞報紙紛紛報導，不過出事的原因還是一樣－沒人搞得清楚。電子商務依然是一個混亂而新興的產業，很多事情都還在發展中，即使是同一家公司，過去曾經出過問題的癥結也難保下次不會再有，這個產業是一個複雜、變化快速且蘊含商機的新平台，無法用時間或環節來統一歸類，發生事情原因多半是混合型的，無法單一歸類的個資外洩原因，其實是一個很接近現實的狀況。

「我們每天關在房間裡跟客戶開會，就是想要知道到底是哪裡出問題啊！」KPMG資訊科技諮詢服務協理謝昀澤說。警政署犯罪預防科警務正常金蘭提到，EC特性是客戶族群大且不容易掌握。除此之外，其整個物流的末端也是資安較不嚴密的部份，以過去追查的經驗來看，還曾經有詐騙集團可以清楚說出是在哪間超商取貨？幾點幾分？哪個工讀生負責簽收等資訊。

目前問題可分作個資外洩與ATM詐騙，而個資外洩可能會導致ATM詐騙，形成治安問題。在外洩的環節當中，最末端的個人安全往往都是一個難以控管的死角，有時候的確是個人電腦被植入木馬造成資料外洩，單一個人問題還好，如果這個「個人電腦」是購物平台上的一個小供應商，就有可能會成為其中一個入侵的漏洞。

近來亦有EC業者針對資安規範與物流業者重新訂定、審視合約，目標希望物流業者在明年中之前可以導入國際驗證標準，不過細節仍在評估中。

內政部警政署資訊室主任李相臣從治安的觀點看資安，他說，網路犯罪率一直持續上升，而這其中罪犯的未成年比率已達1/2，網路犯罪的形成是犯罪集團金主與駭客集團的結合，兩種智慧加在一起，在網路世界形成一股犯罪新勢力，而一般的使用者卻還沒有跟上來，以為只要設帳號密碼，以為只要有防火牆、防毒就安全

了，資安的數位落差已經造成一般使用者受害的原因之一。他甚至建議，如果有重要的轉帳交易，不如在公司電腦做，平常至少有資訊人員幫忙把關，還比在家上網來得安全。

不被揭露的真相　看不見的資安

KPMG資訊科技諮詢服務執行副總張允洸提到，台灣對消費者保護的法律並不足夠，例如新的個人資料保護法一直遲遲未通過，舉證責任依然在消費者身上。又，當發生了資安事件，或許通報給主管機關、受害者，或許新聞媒體會自己去挖出一些真相。但資訊並未透明化，受害的購物平台自然也是草草遮掩、不欲人知。張允洸認為，政府應該主動且積極的將這些資料開放給大家查詢，例如歐美國家就有資料遺失資料庫(Data Loss Database) http://datalossdb.org/，裡頭可以查詢每筆個資外洩事件背後的始末，現在台灣有「政府資訊公開法」，但雖然有這樣的精神卻沒有執行力，若想要了解台灣的個資外洩事件，就必須要通過政府複雜的申請程序，卻還沒有辦法看清楚事件的全貌。

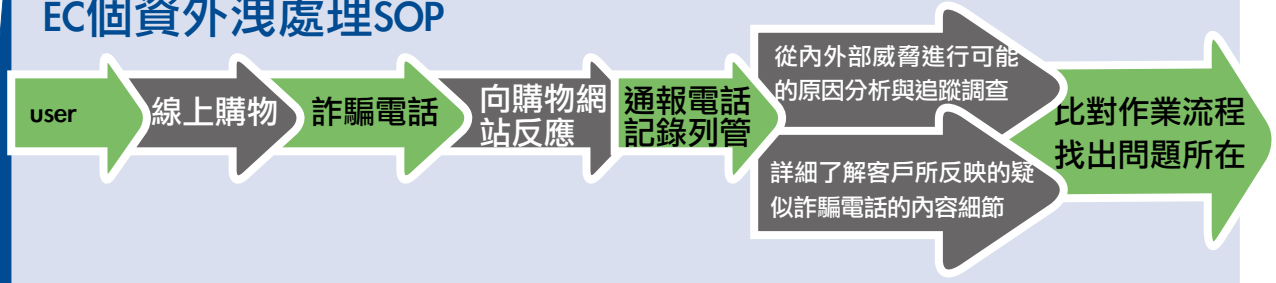
他舉例，有些金鑰的演算法是公開的，讓大家審視、挑戰，卻依然無法破解，這才是真正的安全，絕不是把事件掩蓋起來就會安全了。今日我們的資安事件依然不夠透明化，所以一個資安事件甚至會在同一個地方一而再、再而三的發生。

“Security based on visibility.” 張允洸如是說。

當我們要購物的時候，可以在網路上比價，看看哪個比較便宜？配送品質如何？但是我們對於網站資訊安全的程度完全無法掌握，因為資安資訊是不透明的，每個人對各網站的安全度，都是看新聞、聽小道消息，或是憑感覺得來，消費者無法挑選比較安全的網站來購物。在採訪過程中，我們追問資安專家、顧問們，他們或許可以說出片段原因，但卻鮮少可以就整起事件明確的剖析，如果人們只能了解片段，也就只能從片段來解決。

Payeasy公共事務推展部協理陳中興說，各種環節都有可能出錯，payeasy在線上購物平台的詐騙成功率是零，這是由於當時payeasy一發現異常，在犯罪集團尚未行動時就趕緊開記者會跟消費者示警。

EC個資外洩處理SOP



例如，疑似詐騙電話所描述的訂購流程、付款方式、消費者相關資訊的完整度，甚至來電者的口音、語氣、用詞等，都是業者可以用來比對內部作業流程及管控方式，找出可能的來源以進行追蹤調查。即便是外部威脅所致，也能分析出一些蛛絲馬跡，確認相關防範措施是否仍有弱點。

終極目標

建立涵蓋全面性的資訊安全管理系統，從企業經營者的角度，由上而下檢視組織的資訊安全管理是否有漏洞，並且建立起防範資料外洩的管控措施及資安事件時的標準處理流程。

資料提供：KPMG，吳依恂整理。

但是，曾有某次與電視節目合作，透過電話銷售，結果有三名payeasy的客戶（但非網購會員）遭到詐騙成功，事後經過調查，發現該節目委外的行銷公司有問題，與之配合的其他網購、電視購物業者資料也都遭到外洩。當時payeasy也針對此三名受害者贈送慰問金，但是發現受害者多半不願意報案覺得很丟臉，甚至有名婦女因瞞著丈夫購物且被詐騙，事後不僅被丈夫毆打，甚至鬧得要離婚，更堅持不肯報案。受詐騙者所受到的心理、社會衝擊其實是很大的，雖然僅僅只是三萬元。（ATM轉帳最多三萬）

而現在的狀況是，出過事、願意改善的購物平台，可能較有豐富的處理經驗，多付出一點努力來防禦，於是犯罪集團發現必須要付出較多成本才能再次得逞，就轉向尚未「開發」過的購物平台處女地，於是大家變成輪流中獎，於是後來受害的人，去向之前出事的人請教該怎麼辦？如何對付這些惡意的集團、駭客？要怎麼做才可以讓商譽損失降到最低？企業內部應該有什麼樣的流程可以因應？這些受害經驗的處理很寶貴，但是僅有部份業界私下累積，難以公開分享，如果再有人受害，誰可以幫助他們？常金蘭說，很可惜，政府甚至沒有一個專門處理的單位可以協助這些業者，有些人會向她請教，但更多人會選擇悶著頭自己做，這之中有著同業競爭等等的考量，就算是私底下的管道，也不見得暢通，還得看人脈、看管道，能不能找到人來解決。

受害業者處理的經驗很寶貴，但僅有部份業者私下交流，難以公開分享經驗，很可惜。 ～內政部警政署警務正常金蘭

特殊產業特性
組織變動大、權限難掌控

曾經去處理過這些購物平台個資外洩的資安業者說，他說，不少次其實都是上游的供應商或下游的物流業出事情，不過大家難免還是抓著這些比較知名、大的平台打。當然，有時候這些平台業者是自己真的出事，有時候也很無辜，如果是跟一般中小型的電子商務業者比起來，資安算好的了，但由於目標大，相對攻擊也就多。

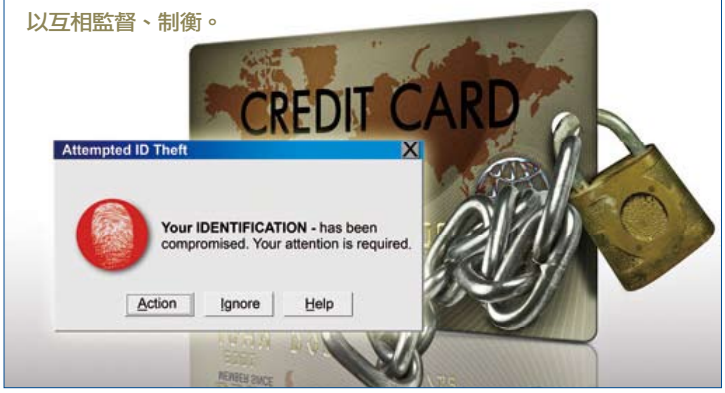
柿子，當然是挑軟的吃。Yahoo！奇摩電子商務事業群總經理何英圻曾說過，詐騙是有相對成本的，假設安全可以做得跟銀行一樣的話，駭客為什麼不乾脆去找銀行就好了？他認為推動資安，只要公司重視的層級夠高，投入足夠的資源以及有效徹底的執行，時間就會站在投入的那一邊。

先談外部攻擊。面對駭客攻擊的主因已經比過去少很多，尤其是大型的EC業者，各式各樣的資安技術、軟、硬體設備在這些電子商務的業界裡都不缺乏。資安顧問楊伯瀚表示，有兩點是近來電子商務業者比較強力防護的部份，Web Security 一 過去常見的網頁安全威脅如SQL Injection、XSS等幾乎已經很少見到。電子商務業者已經關注到網頁應用程式安全的部份，有些業者不僅會做滲透測試、原碼

▲ 張允洸說，由於資安資訊不透明，消費者無法挑選比較安全的網站來購物。（左起：KPMG資訊科技諮詢服務執行副總張允洸、協理謝昀澤。）

檢測，包括架設網頁應用程式防火牆等。DB欄位加密 － 有些是資料庫自己支援這樣的功能，有些則是透過第三方軟體做，而大部分都是寫程式的廠商來做，簡單的說，其實是存已加密的資料到資料庫裡去。一般來說並不會直接加密資料庫，對資料庫的負擔將會過重且不切實際。至於傳輸過程中運用SSL VPN加密、權限控管使用token或OTP雙因素認證密碼等，也依各EC業者資安程度的不同而有所運用。近來，亦有業者開始預備資料庫稽核的導入，不僅能夠因應未來個資法令的需求，亦能防範內部資料外洩，這也是過去比較少著墨的地方。

公司內應該有職權區分(SOD, Separation of Duty)的觀念，要可以互相監督、制衡。



這些IT資安防禦解決方案也是具有IT背景的業者在第一時間就會馬上去佈署的部份，尤其是台灣公司。張允洸觀察，若是外商則會先研究其問題原因、流程管理等。不過，道高一尺、魔高一丈，面對新的入侵攻擊總是會有需要改進的地方，所以投入資源的點要對，且承認自己的架構並不安全、持續改善。此外，即使是大型的平台業者也會面臨到一些基本的系統問題，例如部分系統或許是原生，但部分則可能是購自國外，像有些ERP系統來自國外，如果該公司對該系統的控制力不夠時也容易發生問題。此外，資安顧問李柏逸表示仍然還有一些小型的電子商務業者，由於沒錢、沒人、沒資源，所以網站上依然還存在著漏洞，甚至開始在會員條款上面鑽漏洞，明定「會員資料被第三人以非法的方式進入系統，對資料庫做修改、破壞、複製會員資料等動作，會員不能對公司要求任何賠償或補償。」，以求規避未來個資法可能衍生的法律責任。

再談內部資安控管的問題。EC產業特性與其他產業不同，可能全公司都多少具有IT背景，甚至總經理可能是IT技術最強的那個。曾有過一個案例是一總經理特助擁有全公司所有系統所有的權限，原因是，總經理隨時都要看。張允洸說，「這是相當荒繆的事情，應該要有職權區分(SOD, Separation of Duty)的觀念，要可以互相監督、制衡。」

但其實，電子商務產業對權限的界定是非常複雜而困難的，這個產業的特性就是組織變動非常快且巨大，電子商務時常要推出新的業務，像是貨物迅速拓展到香港、大陸等通路，可能就會有輪調的狀況出現。即使是IT人員也是，可能沒多久就又換了一批人或身兼數職。謝昀澤舉例，有時候甚至於連角色的都很難描述得清楚，最後只好說「我的

重點事項提醒

電子商務業者

應有職權區分(SOD, Separation of Duty)的觀念，互相監督、制衡；並且於企業內部應制訂資安危機處理流程以因應個資外洩事件。

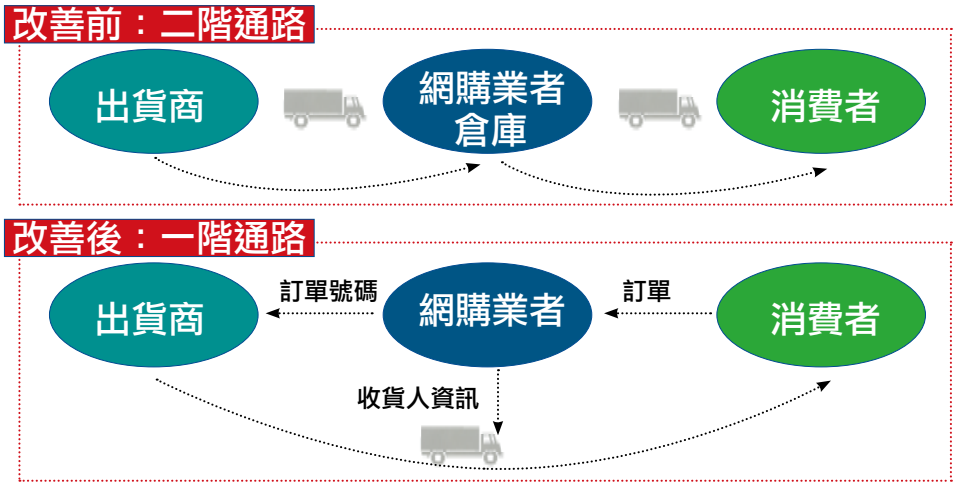
供應商

使用一次性的動態密碼工具(one-time password)避免帳號密碼被竊，盡量將出貨用電腦、資料庫隔離。

物流業

以資安觀點優化物流、資料流，落實改善資安環境。

圖1 物流簡化圖



資料來源：新竹貨運提供，吳依恂整理

各大電子商務業者目前多半已針對委外作業進行更細微的檢討，由於每家電子商務配合的物流大致上都會有3家以上，金流約有5家以上，而這都是比較容易一一開會、檢討、要求的部份，檢討的程度更是到達相當細微的程度，包括表單內容、列印、流程等，IT技術要求已經是很基礎的，例如加密，甚至像是SCM供應鏈管理的模式，電子商務業者甚至會去設計一套流程搭配管理、系統設定等方法，讓物流業者可以低成本卻依然有效率的將客戶貨物送達（見圖1）。

謝昀澤覺得在今年可以感覺到，物流業者真的已經受到EC業者的很大壓力。尤其在經濟不景氣之下，物流業靠著電子商務「宅經濟」的影響，還可以生存得不錯，如此看起來，EC業者已經是相對的強勢。物流業雖然較為傳統，但其實大部分的物流業者都已經「知道資安」了。

舉例來說，KPMG去年底也審視了一些物流業者，有幾個狀況出現，例如物流業知道機敏資料要加密、備份，但是金鑰的管理卻可能全都繫在一個工程師身上。另外，也有3家物流業者，也知道電腦要做權限的控管，但是列印端卻沒有鎖或是USB沒有控制。多半都處於「知道資安重要性，可是卻沒能執行得徹底。」的狀況。此外，物流業也有不少老舊的小系統，可能無法支援安全設定，例如密碼設定的原則等，結構上的問題。又例如購物網站PayEasy就

職權跟某某一樣」。為了要達到「最少的資訊揭露原則」，就要一一審視每個人的工作需求為何？之後，又要再對應到可能會有什麼樣的存取權限。而在組織變動如此大的環境下，可能就得定期審視工作說明書，才能確保人員權限都能適得其所，這並不是一件容易的事情。

最後，是上下游的協力廠商。可分成兩個部份，物流業者及供應商。

物流業者雖具資安意識　還有待落實強化

物流業在今年以前是較為脆弱的，但如今都有所改善。物流業今年重視資安的驅動力，主要是來自主要業主－也就是契約客戶或企業客戶，對於電子商務供應鏈客戶資料保護的共同要求，甚至部份EC業者已經將物流業資訊管理與資安執行指標，做為配送運量配置的重要參考。

供應商有大有小且數量眾多，供應商較強勢者可能無法在合約裡規範，又或者供應商太小，亦無法要求對方投入過多成本。

曾經在審視某合作物流業的網頁，發現線上查詢貨物進度，輸入訂單編號後即可show出當時簽收的影像原始檔。問題在於，只要輸入訂單編號+1或-1，就可以看到別人的簽收單。在這起事件發現後，物流業就第一時間被要求將該功能下架，然後雙方開會建議改善。

而原先，就有些EC業者便會不定期去稽核物流業者？但是多久稽核一次？是否徹底？則要看各家的執行力而有所不同。近來，亦有不少EC業者與物流業者針對資安規範重新訂定、審視合約，並且開始進行協商，目標希望物流業者在明年中之前可以導入國際驗證標準，如ISO 27001，不過細節也都尚在評估中。

▲ Payeasy積極與會員互動，保持對話暢通。

供應商有大有小　難以對付的危險個體戶

由於供應商有大有小，且數量眾多，不容易去討論或要求，有些供應商賣的產品相對強勢，購物平台業者可能無法在合約裡要求太多，又或者供應商太小，也無法要求對方投入過多成本，這都是平台業者較難掌控的一塊。

「那陣子平台業者、我們、警察都有人分批去處理過，去看過後你就知道多慘了，供貨商常常都是一、兩台電腦，一間小倉庫，打電動跟處理訂單都用同一台電腦，而實際出貨的也都是供應商，所以供應商手上會有詳細的客戶資料，輪替率又很高，不少還是上班族兼差的副業...」資安業者如此形容。

現在也有些網購平台業者提出辦法，例如要求供應商將與電子商務資料庫相連的電腦進行實體隔離，並且透過權限控管，例如payeasy就主動提供該供應商一次性的動態密碼工具(one-time password)，規範其供應商需使用OTP Token才能夠與之進行資料交換。也有的業者改善其供貨流程，減少供應商直接觸碰到客戶個資，例如說透過與物流業，片段給予供應商與物流商資料，供應商可能僅握有出貨數量與物品種類，物流商可能僅有訂單編號資料，並直接從供應商取貨再交付予消費者，盡量減少每段流程中可能接觸客戶資料的單位，擁有完整的資料，僅提供所需資料，切割成片段亦有助於事後追蹤外洩管道，並持續改善。不過，這些要求看起來都還僅能規範到稍具企業規模的供應商，供應商越接近「個人」規模，就越難以要求，這也都必須返回至自提升資安意識做起。

至於責任歸屬問題，購物平台業者多半在合約裡與供應商有保密協定的規範，但由於個人資料保護法遲遲未通過，多數業者還在觀望，目前並沒有明確規範未來違反個資法時，需付損害賠償責任各自的範疇。然而這是一個相當現實的問題，沒有法律合約的規範，誰理你？

結論

各購物平台在幾年前開始輪流出事，雖然剛開始都態度不佳予以否認，不過在社會輿論下、商業形象、主管機關要求等因素驅使下，也都開始默默的進行一些管理制度、系統導入等，可以收緊、收攏的部份也緊鑼密鼓進行，只是，還有許多溝通、人為的環節，還需要政府大力協助，還需要標準來規範。