經濟部

網際網路零售業

個資與資安管理

參考手冊

網際網路零售業

個資與資安管理

參考手冊

E-commerce

Personal Data and Information Security Management

目錄
CONTENTS

04 個人資料

06 電商網站隱私設計

10 委外資服業者

14 事故通知

18 個資跨境傳輸（歐盟）

22 資訊安全

24 沒有使用防毒軟體的原罪

28 疑點就是不正常

32 認知的不同導致不同的結果

36 資安風險始終來自人性

40 結語

46 參考資料


Secure

個人資料
PERSONAL DATA

電商網站隱私設計

電商網站的設計雖然與個資法比較沒有直接的關聯，但在實務上常常看到網購業者的網站在個資蒐集機制上的設計未盡符合個資法的規範意旨。在此提出2點網站設計上的建議，分別是隱私權政策的設計以及加入會員頁面的資訊欄位設計。希望透過簡單的提醒，使網購業者可以減少個資法遵的負擔，也降低違法的風險。

一、隱私權政策

購物網站的隱私權政策有兩大目的，一是向消費者揭示網站經營者對於個資保護與消費者隱私的重視，並讓消費者對網站如何使用其個資有初步的認知；二是作為我國個資法第8條告知義務的行使媒介。後者在我國個資法上屬於強制的義務，即便在實務上沒有一定的作法，但依法應告知之事項也是缺一不可，計有以下幾項：

1.非公務機關名稱

非公務機關名稱應提供在主管機關商業登記之名稱，例如PChome購物網站上的隱私權政策應揭示網路家庭國際資訊股份有限公司。

2.蒐集之目的

以網路購物網站而言，可以參考法務部公布之「個人資料保護法之特定目的及個人資料之類別」，其中有名為「網路購物及其他電子商務服務」的目的類型，可資業者使用，但業者亦可依業務性質自行撰寫。

3.個人資料之類別

同樣可參考法務部公布之「個人資料保護法之特定目的及個人資料之類別」，通常網路購物業務會使用到的個人資料類別為C001個人辨識資料。

4.個人資料利用之期間、地區、對象及方式

應說明個人資料利用的期間，如無特定期間，可概略說明為業務存續期間；地區可寫台灣或中華民國境內，如可能做境外利用亦應一併揭露；對象則應揭露可能存取當事人個資之第三方，如物流業者或行銷合作對象等等；方式可說明利用之時機或資料流程等。

5.當事人依第三條規定得行使之權利及方式

此處最簡單的方式即將個資法第3條內5款規定原封不動照搬，業者應注意，如自行以使用者條款約定不得行使當事人權利，應為無效。

6.當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

如當事人可以自由選擇不提供某些資料，應說明缺乏這些資料可能影響哪些權益或因此而無法提供服務。

二、加入會員頁面

為了寄送商品的必要，而且一個統一的會員管理系統可以使購物網站業者蒐集與分析會員的消費行為更為便利，購物網站通常會要求消費者結帳前加入會員。我國電商網站要求消費者加入會員大致有兩大機制，第一是連結大型社群網站帳號如Facebook、Google或Line；或是在網站上直接建立會員帳號，兩者可能併用，方便網購業者管理會員。

在網站上建立會員帳號的情形，常常看到網站要求消費者填寫相關資料，以一般網路購物流程而言，大多至少需要下列資訊欄位：

1.帳號（常見以電子信箱或手機號碼作為帳號）

2.設定密碼

3.姓名

4.主要聯絡方式（電子信箱或是手機號碼，通常兩者皆需）

5.地址

許多購物網站在要求消費者加入會員時，即要求填寫上述各項資訊，但加入會員到完成交易其實仍有一段差距，實務上也常見無消費紀錄的網站會員。就個資最小化的原則而言，建議網購業者在設計網站時，僅要求填寫帳號與設定密碼即可。待消費者確定結帳，完成交易前方才蒐集其他必要資訊（如為超商取貨，亦可不蒐集地址）。

此外，因為詐騙集團絕大部分均使用受害者之手機作為主要聯絡方式，如以會員聯絡方式作為帳號，建議使用電子郵件而非手機號碼。

最後，在加入會員頁面中，建議設計一同意勾選欄位（但勿預設勾選），讓消費者可以明確行使同意會員條款或隱私權政策。

委外資服業者

網購業的本質與實體零售並無不同，皆是買進賣出，差別在於網路購物的交易發生在虛擬網路空間。雖然相較實體的店面，網路零售的成本與進入門檻較低，但業者仍然有需要特別注意的部分，尤其是諸如網站設置，使用者操作介面、資料庫管理，當然還有資訊安全等等IT技術相關的種種問題。

IT技術在現代社會相當重要，但對於沒有相關專業背景或無經驗的一般民眾而言，並無法在短時間內掌握精熟。網購業的經營者或許較之一般民眾對資訊科技較為熟悉，但也未必具有高度IT技術專業。對於大型業者而言，當然可以在事業內部成立專責的技術部門，但對於中小企業而言，委託外部資訊服務業者建置與維護電商系統似乎是兼顧營運彈性與效率的作法。

在網購業者委託外部資服業者維護其電商系統的情形下，資服業者如有權限存取含有個人資料之資料庫，則應適用個資法上委外的規定。

一、案例

網購業者X委託資訊服務業者Y建置購物網站Z網站，委託範圍除Z網站以外，亦包含APP以及ERP系統之建置與維護，但Y公司所設置之系統卻因為有漏洞，導致Z網站遭駭客入侵，大量消費者個資被竊取。

二、法令規範

個資法第4條規定「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關」，在本案例中以白話解釋就是資服業者需依照網購業者應遵守之規範為蒐集、處理、利用。

此外，在個資法施行細則第8條第1項亦要求委託機關應對受其委託蒐集、處理或利用個資者為適當之監督；同條第3項亦要求委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。

因此資服業者如因有故意或重大過失而造成系統漏洞，導致個資外洩事故，將可能違反個資法規定，且此時網購業者也應負擔相關民事或行政上責任。故網購業者對於委外資服業者的選任勢必謹慎為之。

三、法遵建議

一般而言，個資法上的委託條款不外乎注重個資法施行細則第8條第2項之各款規定，例如明確約定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間，或是採行適當的安全維護措施等等。但在資服業者受委託建置與維護各項電商系統時，如網購業者缺乏高度IT技術專業，監督能量不足時，可特別參考下列幾點建議：

1.系統建置或維護契約上之權利義務

個資／資安事故的發生或許是由系統漏洞導致，但網購業者日常對人員、設備如疏於管理，亦很可能是事故發生之原因，為避免事故發生時雙方推諉責任，應明確劃分雙方應負之責任或義務，如應使用正版作業系統並隨時更新、防毒軟體應定期更新病毒碼、合理範圍內應確保網路設備韌體正常等等。

2. 事故可歸責於資服業者時之賠償責任

個資事故發生時，如依照契約內容可認為資服業者有責任時，應規定資服業者對網購業者因個資事故所導致之有形或無形損失予以賠償的義務。

3. 契約期限屆期後之處理

實務上常見系統之建置或維護契約訂有一定期限，而在契約結束後，如因為系統固有之漏洞（特別是可歸責於資服業者時）導致之個資事故，雙方應就法律責任的劃分在契約內加以明確規範。

事故通知

通常談論到網購業者個人資料保護法上的責任時，多數人一開始會先想到防止個人資料外洩，防止個人資料外洩固然重要，然而人有旦夕禍福，即便業者已經盡到相當的注意義務，例如訂定合理的個資標準作業程序（SOP）或採用高標準的資安防護措施。實際上仍然可能因為內部員工疏失，或是被外部的駭客入侵而發生個資外洩事故，此時事後的補救措施就相當重要。由於事故通知對於各網購業者而言為為常見的問題，此處就不以個別案例為例來說明。

以實務上而言，事後的補救措施中，一般最常被業者誤解的部分就是個資事故發生後對當事人為通知的部分。所謂被誤解，指的是業者自認已經達到法令規定的要求，但事實上卻與確實合法有所落差。以下先說明實務常見情形與理論上法規要求的作法，再予以分析。

一、案例

發生個資事故後，網購業者可能會在網站上張貼宣導防詐騙訊息，並且以簡訊或電子郵件方式發送上述防詐騙訊息至會員所留存之行動電話。

通常業者在網站上公告，或發送的訊息內容可能是請消費者注意，如接獲自稱是購物網站工作人員，告知消費者因內部系統問題，其刷卡金額被誤設定為分期付款，或是重複扣款，要求消費者至ATM時解除設定時，請務必不要相信，諸如此類性質上偏向政令宣導的警語。

二、法令規範

我國個人資料保護法第12條規定「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」；此外對於登記資本額在新臺幣

1,000萬以上的網路購物業者，另應適用網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法，其所保有之個人資料發生被竊取、竄改、毀損、滅失或洩漏等事故時，應訂定因應措施，其內容包含適時以電子郵件、簡訊、電話或其他便利當事人知悉之適當方式，通知當事人事故之發生與處理情形，及後續供當事人查詢之專線與其他查詢管道。

三、法遵建議

發生個資事故時，應該要先查明事故原因，並以適當方式通知當事人，雖然某些業者可能對於個資法第12條中「違反本法規定」之要件有疑慮，但站在維護當事人知情權的立場，如事後查明業者並不違反個資法，亦不會因此受罰。

而所謂適當方式，一般包含當面、電話、簡訊、電子郵件甚至通訊軟體等種種可有效通知當事人的方式。就網購業者而言，由於其消費者或會員多為網路會員，因此以電子郵件或手機簡訊方式發送通知或許較可兼顧經濟與實效，實務上亦有推出購物app的業者以app推播方式通知，但用戶不見得會將購物app的通知打開，購物app也不是每日都會使用的app，因此app推播較適宜做為補充的手段。

而在通知的內容方面，建議應包含：

1.事故情形與對當事人之影響；

2.業者因應事故之作為或處理方式；

3.事件窗口。

如此可以讓受事故影響之當事人了解情形，並在接到可能的詐騙電話時有反映或查證的窗口。

個資跨境傳輸（歐盟）

個資跨境傳輸，顧名思義即為將個人資料傳輸至境外，此處境外指的是我國法律管轄範圍以外的國家或地區。而所謂傳輸並不限於任何方法，但是在網路科技高度發展的現代，個人資料的跨境傳輸絕大部分都是使用網路傳輸，尤其商業規模的個人資料傳輸，幾乎已經不可能有實體傳輸的情形。

個資跨境傳輸較常見的情形有幾種，第一是跨國企業內部，散布各國的分公司互相傳輸個人資料或將個人資料傳輸回總部；第二種是不同企業間所為的互相傳輸，但以目前國際資料隱

私法制發展的現況來看，相對先進的國家均設有嚴謹的個資保護法規，如歐盟諸國、日本、韓國、加拿大、澳洲、紐西蘭等等，即便美國在聯邦層級並未訂有一般性的個資保護法規，也與歐盟簽訂隱私盾協議以限制個人資料的跨境傳輸，不同企業間的跨境傳輸也時常受到這些法令限制。

因此更為常見的狀態是，企業組織可能將伺服器或者資料庫建置於境外，當組織將所保有的個人資料存放於境外之伺服器或者資料中心時，即可認為有跨境傳輸之情形。

除此之外，包含不同國家政府機關內傳輸、為委託他國公司處理個人資料而傳輸，又或者不同國家之公司為了達成與當事人簽訂之契約內容而為之跨境傳輸，皆為目前常見之跨國傳輸個人資料之類型。

一、案例

我國A公司開設的B購物網站主要以販賣女性服裝為主，雖然提供國外寄送服務，但目標客群仍以我國民眾為主，因此網站使用的語言為繁體中文，結算貨幣也是新臺幣。

A公司內負責B網站營運的C經理最近得知歐盟在2018年已施行歐盟一般資料保護規則（General Data Protection Regulation, GDPR）。C經理同時也曉得GDPR設有許多嚴格的個資保護規範，也可能適用於歐盟境外的企業，並對於違法的企業課與高額罰金。

於是C經理檢視了B網站蒐集、處理或利用消費者個人資料的各項管理政策與流程，發現雖然可以符合我國個資法規定，但無法完全符合GDPR規範。網站也的確有極少數來自歐盟的會員，使C經理相當苦惱。

二、法令規範

1.我國

我國規定非公務機關為國際傳輸個人資料，而有第21條所列舉4種情形之1者，中央目的事業主管機關得限制之。亦即原則上並不限制非公務機關將個人資料傳輸至境外，一般企業傳輸個人資料通常不受限制。

2.歐盟

雖然A公司為我國企業，然而依據GDPR第3條規定，不在歐盟範圍內設立業務據點的控管者或處理者，向歐盟境內的個人資料當事人提供商品或服務亦應遵守GDPR規範。

三、法遵建議

在2018年11月，歐盟資料保護委員會（European Data Protection Board, EDPB）針對上述的GPPR第3條公布了指引草案，其中對於第3條的地域規範的適用有做出解釋，可供我國網購或電商業者參考。

本案中，A公司就其所經營的B網站業務是否應適用GDPR規定，關

鍵爭點即在於是否符合GDPR第3條所稱「向歐盟境內當事人提供商品或服務」。EDPB認為此處提供商品或服務必須有針對性，亦即主觀上是有將歐盟人民當成目標客群，由於網站可自由進出的特性，可在歐盟境內進入該網站並無法作為該網站有意向歐盟人民提供商品或服務。

因此以下列出EDPB認為應該參考的幾個判斷因素：

1.網站是否指定歐盟或至少一個成員國是服務或商品的提供對象；

2.是否向搜尋引擎支付參考費用以便歐盟消費者搜尋該網站；

3.對歐盟消費者發起廣告或行銷活動；

4.業務具有國際性質；

5.網站有歐盟境內的聯絡窗口；

6.使用歐盟或歐盟會員國的頂級網域；

7.提供從歐盟至商品服務提供地區之路線指示；

8.提及歐盟境內的客戶，或是其經驗分享或見證；

9.服務不使用當地國家之語言或貨幣，反而使用歐盟語言或貨幣；

10.提供在歐盟成員國內交付貨物的服務。

上述因素必須綜合判斷，因此以我國網購業者的情形而言，如業務不以歐盟為主，且組織目前尚未準備好適用GDPR規範，即應該避免網站符合太多項上述判斷指標。

資訊安全
INFORMATION SECURITY


Uploading ...
INFORMATION SECURITY
Login Problem,
Wrong username or password
MESSENGER
LOGIN

沒有使用防毒軟體的原罪

一、案例

今年以來有三家電商發生個資外洩的模式完全相同，都是沒有使用防毒軟體所導致。但從另一個角度，我們有可以發現其實駭客的攻擊都是很有耐性，長期佈置，而且有針對性的對象，聽起來很像所謂的APT進階持續性威脅，但是真的沒有那可怕，只要電商都使用合格的防毒軟體，這些個資外洩風險都可能降到最低。為何提到模式相同? 因為遭受攻擊的電商所使用的平台都是同一家。

台灣這家平台商提供國內眾多的電商使用，資安防護技術能力超強，駭客從前台無法攻擊，減弱防護能力。 因此，攻擊的目標往往從後台進行。這也是資安界所研究，滲透測試應該從內部進行，因為往往攻擊大部分發生於內部。內部與外部的差別在於，內部的攻擊通常是先取得授權。

這三家電商其中一家向電子商務資安服務中心（EC-CERT）通報，發生了個資外洩的事件， 起因於，它的客服部門以往都設使用網路白名單，就是白名單內的IP才可以連到後台，其中一部電腦未裝防毒軟體，又剛好是新人值班沒有經驗，當開啟一封社交工程的信件，電腦中毒了，也看到游標游動。向客服經理報告這個現象， 剛好當天外包的IT工程師遠端連線進入維護系統， 直到下午客服經理覺的時間過長，再次跟外包的IT工程師聯絡才發現，維護的主機在倉庫而不是客服部門。此時，拔掉網路線已經來不及了，晚上開始接到客訴電話。經過調查，他們發現駭客取得電腦控制權，利用客服人員已經建立的議程，直接從後台下載訂單資料。

這家電商以前使用另外一家開發商的系統，因為屢次發生資安事件，毅然改用這家平台商的系統。它進入後台除了帳號與密碼也必須使用手機驗證碼雙重認證，甚至於與這家平台商合作ERP的系統， 因此出貨帳單根本不需要下載，按個鍵直接用API轉過去就可以出貨。所以，沒有訂單資料為何發生個資外洩呢?

整個後台系統功能十分完整，不僅有API將帳單直接轉到ERP的系統，也有帳單下載的功能，以因應其他電商與其他物流出貨的需求，但是它不知道，可是駭客都知道。平台商很快的應變處理， 對於要求下載訂單一律要求再次輸入手機驗證碼，立刻封鎖了這個系統應用的弱點。

二、分析與建議

駭客真的是有計畫的對這家平台商進行攻擊，但是也必須依靠電商不使用防毒軟體，才比較有勝算的機會。經過檢討平台商對於電商進入後台，每次的議程時間往往超過6小時，有必要強迫登出再次認證進入系統。EC-CERT也知道迫於現實，平台商也會開放某些電商不用雙重驗證，單憑帳號與密碼就進入後台的做法。我們建議一律強迫使用雙重驗證。

這個案例可能很瞎，不過真的在8個月連續發生三次，對於電商節省成本的做法，過去曾發現：

1. 電商使用盜版的作業系統，當然不會購買合格的防毒軟體
2. 電商不使用防毒軟體，導致電腦中毒，發生個資外洩
3. 電商使用盜版的應用軟體

其實，往往小聰明比不過駭客的企圖，從網路上可以輕易取得的金鑰系統或者應用系統，往往都是有心的駭客刻意製作的，就是希望貪小便宜的人使用，製造後門，方便駭客後續的攻擊。

疑點就是不正常

一、案例

今年有一家電商，發生個資外洩事件後， 立即聘請國內有名的資安公司進行事件的鑑識，結果未發現任何異狀。當EC-CERT前往資安訪視，業者表示一共接獲600多件客訴電話，數件財損發生。根據報告的內容確實沒有疑點的可能性，後續怎麼辦呢? 雖然資安專家找不到事件原因，但是電商本身不能就放著不管，一定有個地方沒有被發現。

這家電商是外商公司，也都遵循母公司的資安稽核標準，而且每年都會查核，已經進行網購的業務13年了，以往都未曾發生資安事件。 網站一共有四台主機都是Windows 2012的版本，談到對於主機的系統更新大約每半年實施一次，因為以往曾有一次更新後無法上線，因此沒有每月定期實施。這是很重要的線索，但是在鑑識報告卻未提及，這極可能是導致個資外洩的原因。

該公司的網站由PHP的程式語言開發，已經有7年未升級了，從時間點研判，應該是5.x的版本，但今年開始PHP 5.x系列已經不


Target Security
LOCKED
LEVEL
STD

再獲得支援了，這也是可能的線索之一， 但是，鑑識報告上也未提及。網站日誌的分析倒是提到來自大陸的IP排名占據來訪的第6名，其他都無異狀。

EC-CERT也提供資安協處，結束訪談後，就對這家電商進行弱點掃描， 確實未發現任何中高以上的弱點，也間接證實資安公司的判斷， 由於，資安公司已經對前台系統做了日誌分析，因此要求提供系統的event log進行分析，該公司的資安聯絡人坦白說明，後台還是使用Windows 2003，沒有辦法提供Event log。由於 Windows 2003已在2015年7月14日結束延長支援，這當然是另一個個資外洩可能的事件原因。

既然後台找不到event log，不妨就找後台的網站日誌是否有疑點？以往，最容易入手就是找尋是否有外部的IP可以成功的執行， 一旦後台被外部IP 入侵這就是個資外洩的最直接的證據。

經過分析後只找到內部IP成功存取的紀錄，且也沒有攻擊的樣式紀錄，再次驗證資安公司的報告確實找不到外洩的原因。承辦人說明，5月底前他們公司的客服部門放在電信公司的機房，6月之後，客服部門才搬回公司總部。但是，承辦人補充一點，因為後台系統記錄時間沒有正時，因此時間必須加8計算，這點倒是提供了另外一個方向。不是可以尋找是否有晚上8點之後到隔日清晨7點的紀錄?

果真一大堆的加班紀錄，甚至隔日的凌晨3點都有下載訂單的紀錄。

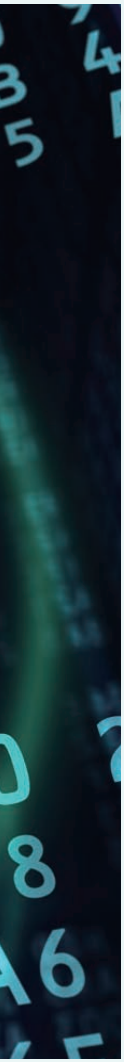
承辦人接著提供6月之後的日誌，也有相同的現象。這當然不是客服人員辛苦加班，而是客服人員所使用的電腦遭入侵感染惡意軟體，後續就由這家電商自行處理了。

二、分析與建議

其實網站後台的疑點往往來自以下，

1. 理論上，後台可以提供網站機敏性的資料，因此，應該只限制公司內部的IP，即使見到外部IP，它的記錄傳回值屬於失敗（不是200）。
2. 異常時間存取，就是在非上班時間，不論是外部IP或者內部IP，後台在這段時間，不可能有公司合法員工正常使用，非法使用的可能非常高。
3. 由於後台本應限制性的使用， 因此既然可以成功存取，表示已經獲得授權，因此看不到攻擊性的代碼，反而在一段單位時間內，同一個IP連續的下載訂單資料，客戶資料。

不過，往往電商的維運人員不知道如何檢查後台的紀錄，這是很可惜的。對於系統的資安管理，最重要的應該維持紀錄的一致性，就是時間連續，內容完整，維運人員或者資安公司藉由紀錄可以檢查系統的防護是否有效? 整個事件應變的流程， 都是周而復始，經過經驗學習之後，改善流程，再回到預備的階段，都應該重視檢查系統記錄的任何不正常的事件發生，及早應變以控制事件。



認知的不同導致不同的結果

一、案例

近期拜訪兩家電商，起因都是個資外洩事件，購物用戶財務受損。 其中一家很快的控制事件，迅速降低次數，另外一家電商受駭的用戶人數不僅較多， 所花費的成本相當高，時間也比較久。發生的原因都是源自對系統軟體更新作業執行的忽視。經過輔導之後，一家電商認同更新作業的必要性，確實按時執行之後，已經超過10個月完全沒有個資外洩的事件，幾乎沒有花費多少成本， 事情就完全或的控制。另外一家時程上額外花了8個月，重新購置伺服器，系統重新調整，人力以及物力投入相當的成本，其實他們使用是相同的一套網站系統軟體，所有的架構完全相同。

談起先前這家業者，員工人數超過上兩百名，也是國內有名的百大電商。去年底發生個資外洩事件，資安經理依照規定通報EC-CERT， 並約好前往資安訪視。 除了在辦公室內網對所有的內部電腦系統檢查是否安裝防毒軟體之外，EC-CERT也使用鑑識專用的惡意軟體行檢測，僅發現少數廣告軟體，研判內部網路以及電腦均未遭受惡意軟體感染。

EC-CERT也分析網站日誌，意外的發現有一天大約25分鐘出現了來自同一個IP，但分別使用了GET與POST對一支執行歷史購物清單程式，這家電商使用asp.net 開發的程式，日誌的紀錄顯示time-taken以微秒為單位， 但這段時間內所執行的歷史購物清單程式執行時間至少都超過數秒以上，大多數都執行數十秒，雖然資安經理解釋，每一個用戶只能讀取自己的購物紀錄，無法接觸其他用戶的資料，這點雖然無法提出有力的反駁，不過清查當時這個IP的登入紀錄， 卻發現當天只有三次登入，所以在這段時間內，不論用GET或POST執行的歷史購物清單肯定來自同一人。有人會對三個月之內的歷史購物紀錄反覆查詢，讚25分鐘內查詢將近40次且每次都花費10餘秒？還是駭客…

倒是資安經理提到一個人事簽到系統，提供員工簽到或者請假必須開放在網路上， 經常受到攻擊，但是未入侵內部網路，卻提到那個系統經常重灌，而且更新作業三個月才執行一起，後續討論所有的系統因為擔心更新之後上線困難，所以並不是按時執行。因此，EC-CERT建議務必不要延期三個月才執行更新作業， 敦促資安經理每個月確認當期更新沒有問題就執行更新， 理由是每次更新後駭客透過逆向工程可以知道當期修補的弱點， 累積三個月所暴露的弱點越多，讓駭客利用的機會就越大，更新作業可以適時彌平作業系統的漏洞，使駭客愈不容易減弱網站的系統，網站會更安全。之後，資安經理接受這個理由，10個月都未曾有任何個資外洩事件。

至於另外一家電商，過去也做了很多的努力與改善以保護個資，包括用戶訂單成立之後，立即將電話號碼拋轉到其他雲端平台，訂單上完全沒有電話號碼，經過10分鐘後，訂單立即加密到資料庫，金鑰另外由開發商保管，除非經由內部的ERP系統否則無法讀取訂單資料，因此駭客即使入侵網站與資料庫都無法接觸到客戶的個資。但是，還是發生了令人遺憾的事情。

二、分析與建議

後來終於在網站上找到了木馬，它以圖形的方式包藏攻擊的代碼，駭客以固定的樣式可以遠端執行程式，或者上傳其他程式。系統成交後的訂單可以以明碼的方式存在10分鐘，只要駭客上傳攔截的程式，應該可以攔截訂單資料，經過日誌分析也發現許多購物車程式異常的執行超過數10秒以上。

當然，去年剛發生個資外洩事件，當時尚未認知系統的弱點可能是木馬入侵的途徑，誤認為可能是規模的問題，樹大招風，應變方向錯誤，直到今年大量的個資外洩，才開始重新檢視，終於更換了所有系統額外購置備援主機，解決問題時程延長，商譽的受損。

電商的工程師解釋，經過其他資安公司檢視，系統的架構沒有顯著的問題，甚至建議應該要規律的執行更新的作業，終於接受這個觀點。因此，認知的不同導致不同的結果。

資安風險始終來自人性

一、案例

執行計畫經常分析網站的日誌，經常有惡意攻擊的樣式出現於網站的前台，如果網站已經建置網頁防火牆（WAF），或者購買雲端的網頁防火牆，這些惡意樣式就會少一點。如果再加上IPS的過濾與防堵效果就更加的良好，就是所謂的縱深防禦。至於網站的後台，往往儲存網站的交易資料以及用戶的個資，往往是駭客覬覦的主要對象，可惜，大多數受駭的網站後台，都發現外部IP存取的紀錄，這裡所謂的外部IP就是根本不屬於電商所使用的IP，往往來自國外IP。由於司法管轄的範圍以及認定，一旦牽涉國外的IP，追查就停頓下來。

不過要防範後續的駭客攻擊，追查這些法的IP往往不是重點，只要防堵非法IP進入的後台的管道，往往事半功倍。有個案例可以說明這種範例，一家電商的前台經過工程師以及包商的努力，將WAF調教成防護嚴密的狀態，它的交易資料不存在前台的資料庫，而是先加密成檔案在後送回公司總部的資料庫，中間經過對稱加密，非對稱加密兩道程序，資料庫與公司內部網路形成實體分離，


48%
System HACKED

只能由客服到固定位置的電腦查詢訂單資料服務客戶，至於出貨物流公司在這部電腦打包一個非對稱的加密壓縮程式，將訂單加密壓縮後，客服用USB將複製的訂單帶到客服的電腦，直接寄給物流公司出貨。

以上的架構的重點在於資料庫與公司內網的其他裝置實體隔離，雖然這家電商以往在內網曾經發生過因為使用遠端桌面連線軟體，駭客入侵並擴散到其他的主機，使用這樣的方式確實杜絕個資外洩的機會。但是，今年老闆買了一套NAS系統，這個系統功能很不錯，甚至也有網頁的介面，使用真的很方便，公司工作效率也大大的提升，老闆覺得要是能夠在家裡也能使用網頁這不是更加方便嗎?既然如此，不如將資料庫和這套NAS系統串在一起，要這麼做，就開放網頁的存取途徑，但是，開放的途徑並未遵循只開放老闆家裡的IP，而是全部開放，再加上NAS的超級使用者的帳號與密碼原廠設定為變更。以往熟門熟路的駭客，又再度回來。

二、分析與建議

資安風險始終來自人性，就是一個定律。這家電商的經營者事業有成，對於電商的營運也很有想法，態度很好。但是，過往資安訪視發現使用非法的作業系統，就是一種貪小便宜的心態，也使用免費的防毒軟體，三個月換一次金鑰，其實網路上也有小紅傘的免費軟體，但就是不願意使用。寧可冒險也不願意保險的心態。為了方便自己網路上使用公

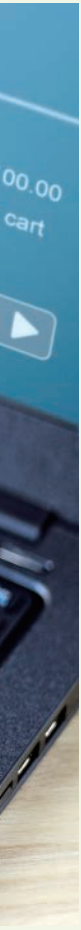
司的資源，大開方便之門，就是一種走捷徑的心態，原廠設定的密碼使用後沒有立即更換，就是一種輕忽的心態。

這些心態就是造成這家電商持續的個資外洩的原因。不是軟體外包商的問題，不是網頁程式的弱點，不是資料庫加密的問題，也不是客服電腦中毒……都是老闆的不正確心態導致這種情況。

結語
EPILOGUE


Order total: $1
3 items in your
Edit your cart
Checkout

結語



到了2019年的今天，網路購物已經不再稀罕，甚至成為很多人日常生活不可或缺的一部份，但根據市場研究機構eMarketer預估，全球網路零售市場銷售額將從2017年的2.29兆美元，成長至2021年的4.48兆元；而臺灣電子零售商務也預估將於於未來5年間，每年將成長7%，從2018年之美金65.3億元成長至2022年之84.1億元，成長潛力不可小覷。

經濟部作為網路零售業主管機關，為強化網路購物產業環境，近年皆委託資策會科法所執行「網路購物產業價值升級與環境建構計畫」，內容包含：

一、觀測與研析國際與我國法制暨產業生態，協處法制與市場發展障礙，促進產業結構優化。

二、協助企業檢視需求，鏈結政府或民間資金資源，運用智慧科技提升產品或服務附加價值。

三、結合網購業者鼓勵網路開店，及強化中南東部數位行銷能力，活絡網路購物產業能量。

四、強化電商資安與個資之規範推廣、平台維運、聯盟運作、行政檢查，提升民眾對電子交易安全的信賴。

其中加強資訊安全與個人資料保護更是產業與消費者都很重視的一個議題，尤其近年來隨著網路購物扮演更為重要的角色，市場變大的情形下也導致許多不法份子針對網購業者，透過社交工程、撞庫攻擊或相關駭客手法，竊取其擁有的龐大消費者資料以施行詐騙。網路與資訊科技也同時帶來層出不窮的資訊安全問題，帳號密碼被盜用、個資外洩、網路詐騙、釣魚郵件、網站掛馬等情事不勝枚舉。

觀察近期國內外所發生之個資外洩事件，其中有部分是網站交易內容遭到側錄所導致。例如，2018年9月英國航空（British Airways）網站遭到駭客入侵，並在該網站所使用的程式庫裡，埋入了惡意程式碼，進而竊取38萬名旅客的個資與付款資訊。而香港國泰航空亦在2018年10月發表聲明承認，有940萬乘客資料曾在未授權的狀況下被取用，包含乘客的電話、電子郵件、地址、護照號碼、身分證號碼等。

2018年11月全球最大飯店集團萬豪國際集團（Marriott）公佈，集團下喜達屋連鎖包括W Hotels、喜來登、威斯汀、艾美等知名飯店的訂房系統客戶資料庫遭到駭客入侵，恐已導致5億住客個資外洩，包括姓名、郵寄地址、電話號碼、電子郵件和護照號碼，以及帳戶資訊、出生日期、性別、客戶入住與退房資訊、預訂日期和郵件通訊偏好的組合等，部分顧客信用卡付款資訊也恐遭竊。

在國內方面，個資相關犯罪以詐騙最為常見。駭客利用購物網站系統資安漏洞，運用攻擊手法入侵系統後台，竊取消費者個資及訂單資料，轉售給詐騙集團後。再進一步冒充購物網站客服人員打電話給受害民眾，利用各種詐騙話術，例如：佯稱因工作人員操作錯誤，導致訂單變成分期付款，往後每月將重複扣款，誘騙消費者前往ATM解除分期設定。

這些由個資所衍生的犯罪問題，對消費者及電子商務企業經營者產生衝擊影響，甚或鉅額財物損失。經濟部目前也在「網路購物產業價值升級與環境建構計畫」下委託資策會對疑似個資外洩之網購業者進行資安或個資法遵的輔導。因此彙整這些輔導查訪的結果並加以出版，或可有宣導個資法遵與資安防護的效果，進而防止潛在的個資事故，為資策會執行本計畫時，不可或缺之任務。

DATA REFERENCE

參考資料

個人資料保護法
https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021

個人資料保護法施行細則
https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=I0050022

網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法
https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=J0080052

經濟部商業司電商、智慧商業及物流業個人資料管理資源專區
https://gcis.nat.gov.tw/mainNew/subclassNAction.do?method=getFile&pk=859

電子商務資安服務中心EC-CERT
https://ec-cert.org.tw/


mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True
mirror_ob.select= 1
modifier_ob.select=1
except:
print("please select exactly two
OPERATOR CLASSES
Mirror Tool
E-commerce
Personal Data and
Information Security
Management

E-commerce Personal Data and Information Security Management

財團法人資訊工業策進會
INSTITUTE FOR INFORMATION INDUSTRY

地址：106台北市敦化南路二段216號22樓
電話：(02)6631-1000　傳真：(02)6631-1001
網址：stli.iii.org.tw

出版日期：108年11月

stli 科技法律研究所 SCIENCE & TECHNOLOGY LAW INSTITUTE

CSTI 資安科技研究所 CyberSecurity Technology Institute