經濟部

2020 網際網路零售業 個資與資安管理

參考手冊

2020 網際網路零售業個資與資安管理

參考手冊

目錄 CONTENTS

1

電商業者的
個人資料檔案安全維護計畫

從個人資料保護的法遵面來看，電商業者內部有沒有依照「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（下稱本辦法）」訂定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（下稱安全維護計畫辦法）等規範，是業者證明已落實個人資料保護法（下稱個資法）的一大重點，在此針對本辦法所規範事項，簡要提醒業者制定個人資料檔案安全維護計畫（下稱安全維護計畫）的重點。

一、業者未制定安全維護計畫的法遵風險

依照個資法第48條第4款，業者如果沒有依個資法第27條第2項訂定安全維護計畫，可能會受到按次處新臺幣2萬元以上20萬元以下的罰鍰，同時業者在個資事故消費者求償案件中也有可能會因此被認為沒有盡到個資法第27條關於適當安全措施的義務，被法院認定有過失，而應負擔損害賠償責任（臺灣臺北地方法院106年度北小字第2161號民事判決參照）。

二、個人資料保護管理政策

業者應依其業務規模及特性，衡酌經營資源之合理分配，設置個人資料管理單位或適當組織，並配置適當資源，由該單位負責個人資料保護管理政策與安全維護計畫之訂定及修正。

三、個人資料盤點

業者應適時並每年定期清查其所保有之個人資料檔案及其蒐集、處理或利用個人資料之作業流程，據以建立個人資料檔案清冊及個人資料作業流程說明文件。

四、個人資料風險評鑑

業者應適時並每年定期評估其因蒐集、處理或利用個人資料可能面臨的法律或其他風險，並訂定適當之管控及因應措施。

五、個人資料蒐集、處理與利用等程序規範

業者應就下列事項訂定具體程序或機制，並提出有效方式維持其運作：

1. 檢視個人資料之蒐集、處理與利用是否符合個資法第19條與第20條規定
2. 檢視是否已依便利當事人之適當方式，踐行個資法第8條及第9條所定之告知義務；如有免為告知之情形，應確認其合法依據。
3. 檢視已於首次行銷時提供當事人表示拒絕行銷之管道，並由業者支付所需費用。
4. 檢視當事人已拒絕接受行銷時，即停止利用其個人資料為行銷，並周知所屬人員或採行防範所屬人員再次行銷之措施。
5. 檢視個人資料之蒐集、處理、利用與符合個資法第5條誠實信用等原則。
6. 對個人資料進行國際傳輸前，應針對該次傳輸進行可能之影響及風險分析，並採取適當安全保護措施。
7. 特定目的消失、期限屆滿、有個資法第19條第2項所定情形，或有違反個資法規定而為個人資料之蒐集、處理或利用時之處理程序。
8. 檢視個人資料是否正確，有不正確或正確性有爭議者，應分別依個資法第11條第1項、第2項與第5項之規定辦理。

9. 當事人依個資法第3條權利行使事宜：

(1)提供行使權利之方式應考量個人資料安全管理之必要性及當事人之便利性。

(2)應依適當之方式確認，或請求當事人或代為行使權利之人說明，其確為當事人本人或有權代為行使權利之人。

(3)於提供查詢或製給複製本時，得收取成本費用，但應事先明確告知。

(4)應遵守個資法第13條有關處理期限之規定。

(5)於得合法拒絕權利行使或得延長處理期限之情形，應將拒絕之理由或延長之原因，以書面通知當事人。

10. 委託他人蒐集、處理或利用個人資料之全部或一部時，應有選任受託人之標準及評估機制，且應於委託契約或相關文件明確約定適當之監督方式，並確實執行。
11. 受他人委託處理個人資料之全部或一部時，如認委託機關之指示有違反個資法或其他個人資料保護相關法令者，應立即通知委託機關。

六、保護消費者個人資料機制

業者如有保護消費者個人資料之機制（例如多因素認證），應適時提醒消費者應用，並為適當之公告。

七、安全管理措施

業者應考量業務性質、個人資料存取環境、個人資料傳輸之工具與方法及個人資料之種類、數量等因素，採取適當之人員、作業、設備及技術之安全管理措施。

八、教育訓練

業者應每年定期實施所屬人員之個人資料保護與管理認知宣導及教育訓練，使其明瞭個人資料保護相關法令之要求、人員之責任範圍及各項個人資料保護相關作業程序。另外，對代表人、負責人或個人資料管理單位人員，應依其於安全維護計畫所擔負之任務及角色，每年定期實施必要之教育訓練。

九、內部稽核

業者應每年定期由個人資料管理單位或適當組織執行安全維護計畫之內部稽核。

十、紀錄與證據留存

網際網路零售業執行安全維護計畫，除其他法令另有規定外，原則應留存以下紀錄或證據：

1. 個人資料提供或移轉第三人之紀錄，該紀錄應包括提供或移轉之對象、依據、原因、方法、時間及地點等資訊。
2. 確認個人資料正確性及補充、更正之紀錄。
3. 當事人行使個資法第3條之權利及處理過程之紀錄。
4. 個人資料或儲存個人資料媒體之刪除、停止處理、利用或銷毀之原因、方法、時間及地點等紀錄。
5. 存取個人資料系統之紀錄。
6. 資料備份及確認其有效性之紀錄。
7. 人員權限新增、變動及刪除之紀錄。
8. 因應事故發生所採取行為之紀錄。
9. 定期檢查處理個人資料之資訊系統之紀錄。
10. 認知宣導及教育訓練之紀錄。
11. 稽核及改善安全維護計畫之紀錄。
12. 其他必要紀錄或證據。

十一、網際網路零售服務平臺業者責任

網際網路零售服務平臺業者亦應制定安全維護計畫並依循相關事項，同時其安全維護計畫還必須包含下列事項：

1. 對其平台使用者，進行適當之個人資料保護及管理之認知宣導或教育訓練。
2. 訂定個人資料保護守則，要求平台使用者遵守。


Mobile Wallet
Credit Card
1234 5678 9012 3456
09/18
1234
Touch and Pay

2

個資事故通知

「月有陰晴圓缺，人有旦夕禍福。」，完善的個資管理制度儘管能控制個資事故發生的風險，卻無法將風險完全降到零風險，實際上除了因為內部員工疏失，同時由於科技的進步與駭客技術的提升，也能可會被外部的駭客入侵而發生個資外洩事故。當業者遇到個資事故時，建議應秉持著「坦率面對、努力解決與儘速通知」的原則處理。以下本文將就業者遇到個資事故後，針對個資事故通知應注意的事項為說明。

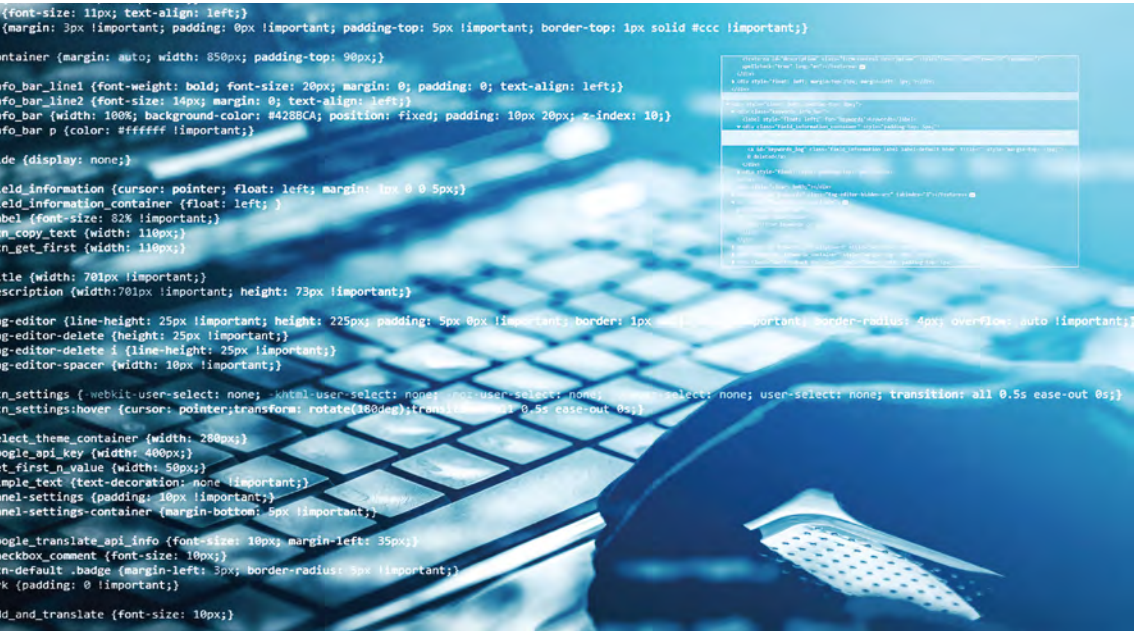
一、案例

網購業者A公司於年中發生個資事故，A公司接到消費者投訴電話後便委託資安公司進行調查，經調查後，初步研判是因為其中一名員工未能安裝防毒軟體且於網路上下載不明軟體，導致駭客入侵電腦成功竊取消費者個資。

A公司知道前述情形後，隨即於網站上張貼宣導防詐騙訊息：「親愛的會員您好，提醒您，最近詐騙集團猖獗，本公司絕對不會通知您訂單設定錯誤、錯誤設定分期付款、請您更改付款條件或於電話中要求您提供信用卡號碼、銀行帳號等資訊。如您接獲自稱是本公司人員，告知您因內部系統問題，其刷卡金額被誤設定為分期付款，或是重複扣款，要求您至ATM時解除設定時，請務必不要理會。」，並且以簡訊與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與電子郵件地址。

二、法令規範

個資法第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」，同時依照個資法施行細則第22條第2項，其通知應包含個人資料被侵害之事實及已採取之因應措施。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，尚應適用「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

1. 通知當事人時間點

發生個資事故時，應該要先查明事故原因，並即時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」之文字有疑慮，但站在維護當事人知情權的立場，同時避免延遲通知而致當事人遭受其他不測侵害或損失之虞的情形，業者是否違反個資法並非個資法第12條通知義務的前提要件，因此，業者於發現有個資外洩情形時，即必須查明事實後，以適當方式迅速通知當事人，如果事後查明業者並沒有違反個資法的情形，亦不會因此受罰。

2. 通知當事人的方式

個資法第12條所謂以適當方式通知當事人，一般包含當面、電話、簡訊、電子郵件甚至通訊軟體等方式。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。

3. 通知當事人的內容

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) 事件聯繫窗口。

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。

四、個資事故通知範本

親愛的消費者／會員您好：

非常抱歉，（公司與網站名稱）於000年00月00日接獲消費者投訴，經本公司調查後，疑似於000年00月00日至000年00月00日期間，因○○原因發生個人資料外洩事故，本公司依個人資料保護法第12條及施行細則第22條規定通知您相關事項如下：

一、影響範圍：000年00月00日至000年00月00日之消費者訂單，實際影響人數為000000人，欄位包含姓名、電話、電子信箱、○○○與○○○等個人資料。

二、已採取因應措施

本公司目前已就本次個資外洩事故委請○○單位調查事故發生原因，後續查明事故發生原因後將會以適當方式通知您。本公司並已採取弱點掃描、漏洞修補、○○○與○○○等因應措施，並加強○○○、○○○與○○○等個人資料管理與安全防護措施，未來本公司也會持續加強資訊安全防護與個人資料保護管理，並持續遵循個人

資料保護法等規範，以降低消費者個資被侵害之風險，保障您的個人資料安全。

三、目前已有消費者接獲詐騙集團電話。提醒您，詐騙集團通常於週末或下班時間以（手法）誆騙消費者。如接獲疑似詐騙電話，請不要聽從指示操作ATM、付款或提供任何個人資料，並立即通報165警政署反詐騙專線。

四、如有關於訂單或本次個資事故之疑問，請於（上班時間）與本公司客服人員聯絡（電話與電子信箱）；上班時間以外請以（提供其他可行方式）聯絡本公司。

（公司名稱）敬上

日期000年00月00日

3

跨境傳輸國際法遵

在電子商務盛行的現代，從網路購物、運貨、網站系統與資料庫存取甚至於消費者購物行為分析，均可能涉及個人資料跨境傳輸的行為，而需特別注意國內外相關法律規定。

一、案例

我國A公司開設的B購物網站主要以販賣居家生活用品為主，B網站於國內、新加坡、美國加州與歐盟均可瀏覽網頁與購物，並提供國外寄送服務。

二、法令遵循注意事項

1. 我國個資法

我國規定非公務機關為國際傳輸個人資料，而有個資法第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. 歐盟一般資料保護規則

雖然A公司為我國企業，然而依據歐盟一般資料保護規則（General Data Protection Regulation, 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，其向歐盟境內的個人資料當事人提供商品或服務，甚至是對於當事人於歐盟內所為行為進行監控，均應遵守GDPR規範。

依據歐盟資料保護委員會（European Data Protection Board, EDPB）針對上述GPPR第3條所公布的指引，GDPR第3條所謂「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。

EDPB同時也提出9項關於「向歐盟境內當事人提供商品或服務」判斷指標，包含(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費用以便歐盟消費者搜尋該網站；(3)業務具有國際性質；(4)網站有歐盟境內的聯絡窗口；(5)使用歐盟或歐盟會員國的頂級網域；(6)提供從歐盟至商品服務提供地區之路線指示；(7)提及歐盟境內的客戶；(8)使用歐盟語言或貨幣；(9)提供在歐盟成員國內交付貨物的服務。前述9項判斷標準必須綜合考量，進而判斷是否屬於「向歐盟境內當事人提供商品或服務」的情形。

另EDPB也指出，GDPR第3條所謂「對於當事人於歐盟內所為行為進行監控」涵蓋透過穿戴式裝置或其他智能設備所為的追蹤、行為定向廣告、地理定位、運用cookie或其他跟蹤技術、個人化的飲食與健康分析服務、閉路監視系統、基於個人資料所進行的市場調查等行為研究與對個人健康監測。

以我國業者而言，如業務不以歐盟為主，且組織目前尚未做好GDPR相關準備時，即應該避免網站及所提供的商品或服務符合前述情形。

3. 美國加州消費者隱私保護法

號稱全美國最嚴格消費者隱私法的「加州消費者隱私保護法」(California Consumer Privacy Act, CCPA) 已經於今 (2020) 年1月1日正式施行。

與GDPR相同，CCPA也具有域外效力。位於美國加州以外的企業，只要於加州內有營業行為 (does business in the State of California)，且符合(1)年度總收入超過2500萬美元；(2)基於商業目的，每年購買、基於商業目的接收 (receive)、銷售、分享5萬筆以上加州消費者、「家庭」(household) 或裝置上之「個人資料」(personal information)；(3)銷售加州消費者個人資料獲得之收入佔該企業年收入50%以上等特定情況，該企業也會受到CCPA的規範。除此之外，控制符合前述條件的企業，或受該等企業控制的企業，若與該企業「共用品牌」(shares common branding)，同樣屬於受CCPA規範之企業。

因此，即便是我國業者，只要符合前述情形，便有CCPA的適用，而必須遵循CCPA的相關規定，否則，違反CCPA的企業可能受到最高7500美元的民事罰款，另加州消費者亦得請求實際損害賠償金額或法定賠償金額（每一加州消費者就單一事件最高可請求750美元）。

4. 跨境隱私保護規則

亞太經濟合作組織（Asia Pacific Economic Cooperation, APEC）跨境隱私保護規則（Cross Border Privacy Rules, CBPR）體系為美國主導推行的跨境隱私保護制度，我國於2018年12月獲准加入該體系，目前我國、美國、墨西哥、日本、加拿大、南韓、新加坡、澳洲與菲律賓等國均為APEC CBPR體系的成員。

以新加坡為例，依據新加坡個人資料保護法（Personal Data Protection Act, PDPA）第26條，除符合特定條件外，組織原則不得將個人資料傳輸到新加坡以外的國家或地區。

而新加坡個人資料保護委員會（Personal Data Protection Commission, PDPC）於今（2020）年6月2日宣布增修個人資料保護規則（Personal Data Protection Regulations），將APEC CBPR與資料處理者隱私認可（Privacy Recognition for Processors, PRP）體系的認證（Certifications）納入新加坡跨境傳輸的合法方式之一。

依照新修正的新加坡個人資料保護規則，通過CBPR或PRP認證的組織被視為符合提供相當於PDPA保護的法律義務，新加坡的組織可以將個人資料傳輸給這些經認證的海外接收者，而不需要再額外滿足其他條件。

因此我國業者倘有與新加坡或其他CBPR體系成員的企業進行個人資料跨境傳輸，未來可以取得APEC CBPR認證，以證明自身符合相當的個資保護水準。

4

委外業者的監督管理

網購業者在處理交易時，往往需要面對網站設置，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。

然而隔行如隔山，對於這種與IT技術有關的事情，實務上有許多網購業者會委託外部資訊服務業者（下稱資服業者）協助維護其電商系統。同時，網購業者在委託資服業者維護管理電商系統，由於涉及到個人資料的處理，因此必須善盡監督管理的責任，才能符合個資法適當安全措施的要求。

由於實務上時常發生因資服業者緣故所導致的個資事故，因此，以下本文將介紹於委託資服業者維護管理電商系統時，必須注意的事項。

一、案例

網購業者X公司委託資服業者Y公司建置購物網站Z網站，委託範圍包含Z網站、ERP系統與手機APP應用程式的建置、維護與管理。然而Y公司所設置的系統存有漏洞，且Y公司並沒有適時修補該漏洞，導致駭客利用該漏洞入侵Z網站，使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」，換句話說，受委託的資服

業者，必須依循委託者所應遵守的個資法等規定，進行個人資料的蒐集、處理與利用。

同時，個資法施行細則第8條第1項也規定委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當的監督。其監督事項至少應包含：

1. 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。
2. 受託者就個資法施行細則第12條第2項採取之措施。
3. 有複委託者，其約定之受託者。
4. 受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。
5. 委託機關如對受託者有保留指示者，其保留指示之事項。
6. 委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。

同條第3項更要求委託機關對於監督事項應定期確認受託者執行之狀況，並將確認結果記錄之。

由於個資法施行細則要求委託機關必須對受託者為前述的適當監督，因此，當因資服業者的故意或過失行為（例如未適時修補系統漏洞）導致個資事故的發生時，倘網購業者沒有善盡對於受託者的監督管理責任，不僅不符合個資法關於適當安全措施的要求，網購業者也應就個資事故的發生負擔相對應的責任。所以網購業者對於委外資服業者的選任、監督與管理勢必應謹慎為之。

三、法遵建議

一般而言，委託機關對於受託者的適當監督，大致可分為選商前與選商後的監督管理：

1. 選商前監督管理

X公司內部應制定個資管理程序規範委外廠商之選商程序，依循該程序選擇信譽優良的委外廠商，例如選擇其個資管理制度經過公證第三方驗證之廠商，或是請廠商針對其公司內部個資與資安保護的情況提供自我查核表，使X公司得就廠商內部個資保護與資安保護的情況得以審慎評估，以作為選商依據，並留存相關紀錄。同時依照個資法施行細則第8條第1項規定，透過契約方式約定相關事項確保委外廠商採取適當方式保護個人資料，以及接受X公司之定期監督。

2. 選商後監督管理

X公司應於選商後落實定期且有效之監督，要求受委託的廠商確實落實雙方委外契約所約定事項，具體方式包括但不限於現場稽核、由廠商定期提供自評表或提供有效的第三方驗證以供查驗。

同時，對於倘因委外廠商緣故屢屢導致個資事故的發生，則X公司也應該要善盡其監督管理的責任，另行選任合適的委外廠商。

另外當個資事故發生時，如認為資服業者有責任時，委託機關也可以對資服業者依契約關係或法律規定請求損害賠償，實務上最近即有一間公司向提供不符合現行科技水準網站系統的委外廠商成功求償新臺幣1,021,976元（臺灣臺北地方法院108年度訴字第1721號民事判決），該判決認為該委外廠商並沒有做好事前防禦措施導致公司個資外洩，而其他使用該委外廠商所提供電子商務平台的業者，均曾發生遭駭客入侵竊取消費者個人資料的情形，且其資訊安全保護經OWASP標準檢測為最低的F等級，顯然不符合現行科技水準，因此判決認定該公司得向委託機關主張解除契約返還報酬、請求已經賠償第三人的和解金與該公司的商譽損失。

5

電商平台與賣家的賽局理論

一、電商的兩種角色

根據資安專家長期輔導電商的多年經驗，最常遇到電商平台所發生的資安問題，往往來自兩個不同角色的衝突。

一個是電商平台本身，面對付費的賣家或者供應商，平台商往往無法要求賣家自願性的選擇更多的資安控制措施；例如，賣家進入後台貪圖方便好記，使用弱密碼，經過一段時間之後，往往被駭客發現。加以賣家只想以快速、省錢，方便的方式使用平台的功能。當平台要求更嚴謹資安防護措施時，就容易遇到招商不易的窘境，而影響市佔。

況且網路賣家本身，大多數缺乏資訊安全的認知，對於個資保護措施意識不足。甚至少數賣家往往使用沒有版權的作業系統，也不知道為何需要更新，乃至於沒有購買防毒軟體。對於所持有的電腦是否遭受惡意軟體感染也不太重視，同時因為成本考量，普遍缺乏個資保護、安全使用資訊設備的教育，這是目前在賣家這端最大的資安困境。

然而，這些賣家本質上是創業家，他們的專業是拓展營業額，將產品推陳出新，滿足買家的需求，更是新型態電商的骨幹。原本與平台商是互補的功能，為何會不願意配合加強平台的安全性，因為賣家欠缺對資訊科技的瞭解，而需要個資保護教育的落實。

二、平台的困境

電商平台一旦建置完成後，積極招商增加收入是首要目標，當然是來者不拒。基於付費是老大的心態，對於賣家的要求， 盡可能予以滿足。更為了擴大市場佔有率，有的平台必須遷就賣家的要求。

例如明明以限制固定IP的方式登入後台是很好的優點。以往資安協處經驗，有的賣家經費拮据只有使用浮動IP，單單只用帳號密碼控制後台登入，容易遭受攻擊。甚至於這些少數賣家使用未獲授權的盜版軟體，以至於帳號密碼被盜取。

三、不應該同意賣家用盜版軟體

平台對於賣家使用盜版軟體不能視若無睹，這理應是在平台上合法買賣最基本的要求，應該簽訂合約時予以規範。網路賣家本身大多數缺乏資訊安全的認知，對於個資保護措施意識不足。甚至少數賣家往往使用沒有版權的作業系統，也不知道為何需要更新？乃至於沒有購買防毒軟體。對於所持有的電腦是否遭受惡意軟體感染也不太重視。貪圖一時方便，且普遍缺乏個資保護、安全使用資訊設備的教育，是目前平台上多數賣家的困境。

曾經認識一個受駭的賣家，強調本身只是賣果乾的商家，也沒有得罪別人，為什麼網站會受駭客攻擊？該公司當初也是使用顧問公司的資源，如設立免費網站。然而，實際分析該商家的出貨數量，其實賣家只需要靜態網頁接受匯款方式訂單，無須在網站上使用資料庫收接受訂單，徒增被駭的風險程度。

四、平台的最佳的防護措施

有不少的平台業者，對於軟體更新的執行，始終抱持可有可無的觀念，一年可能只做兩次。其實平台整體的架構，類似房屋維護的概念，經過風吹日曬雨淋，結構逐漸出現漏洞，軟體更新就是修補安全漏洞。

五、軟體更新有以下的好處

1. 修復已發現的安全漏洞以及修復或消除錯誤；
2. 駭客喜歡安全漏洞，又稱為軟體漏洞。軟體漏洞是在軟體程序或操作系統中發現的安全漏洞或弱點。駭客可以設計針對漏洞的程式來利用漏洞；
3. 更新不僅修補安全漏洞，還可以添加新功能並改進現有功能。

大型平台業者處理個資外洩事件方法，其實都具有完善的事件處理機制。當發現客戶外洩的來源限縮於一個賣家，往往會派出資安人員前往，做

一次完整的資安檢測。資安事件報告中所發掘的問題十之八九都是來自賣家沒有使用防毒軟體以及使用沒有合法版權的作業系統，於是賣家使用網路往往遭受各種惡意攻擊，當然形成駭客的跳板；以至於當後台的帳號與密碼被竊，甚至於電腦的控制權被駭客所操控，進入後台非法下載訂單資料。

六、電商後台的強化方法

如果賣家願意加強控制措施，例如使用固定IP要求進入後台限制IP白名單，駭客即使取得後台的帳號與密碼，還得必須入侵電商的內部網路，但因盜取賣家的訂單資料有不少金錢利益，這是駭客必須克服的困難。當賣家進一步控制措施，例如下載訂單增加手機驗證碼，駭客必須面對難度顯然提高許多，如果下載的訂單又是加密，資訊外洩的可能性越來越低。

對於賣家，基本資安要求如下：

1. 所有電腦使用有合格授權的軟體包括作業系統以及Office。
2. 購買授權的防毒軟體。
3. 以上的網路設備和軟體應該維持更新。
4. 如此， 至少降低70% 以上的個資外洩風險。

更進一步，進階資安要求如下：

1. 公司盡可能使用固定IP，連接後台限定使用IP白名單。
2. 接收電子郵件的電腦，通常是客服使用最容易遭受社交工程攻擊，單純用於電子郵件收與送，不做其他用途。
3. 連接後台的電腦最好與其他電腦網路彼此隔離，這阻絕惡意軟體竊取訂單資料的可能。萬一網路無法彼此隔絕，訂單下載要求配合手機驗證碼，或者訂單下載加密。

全部都符合以上要求，網路的賣家已經善盡其資訊安全的責任，畢竟賣家不是資安專家或者資訊工程師，與平台商各自專業分工。發生個資外洩的可能，只有賣家內部的不良員工，或者平台本身漏洞才可能導致個資外洩。

七、賣家如何選擇優良平台

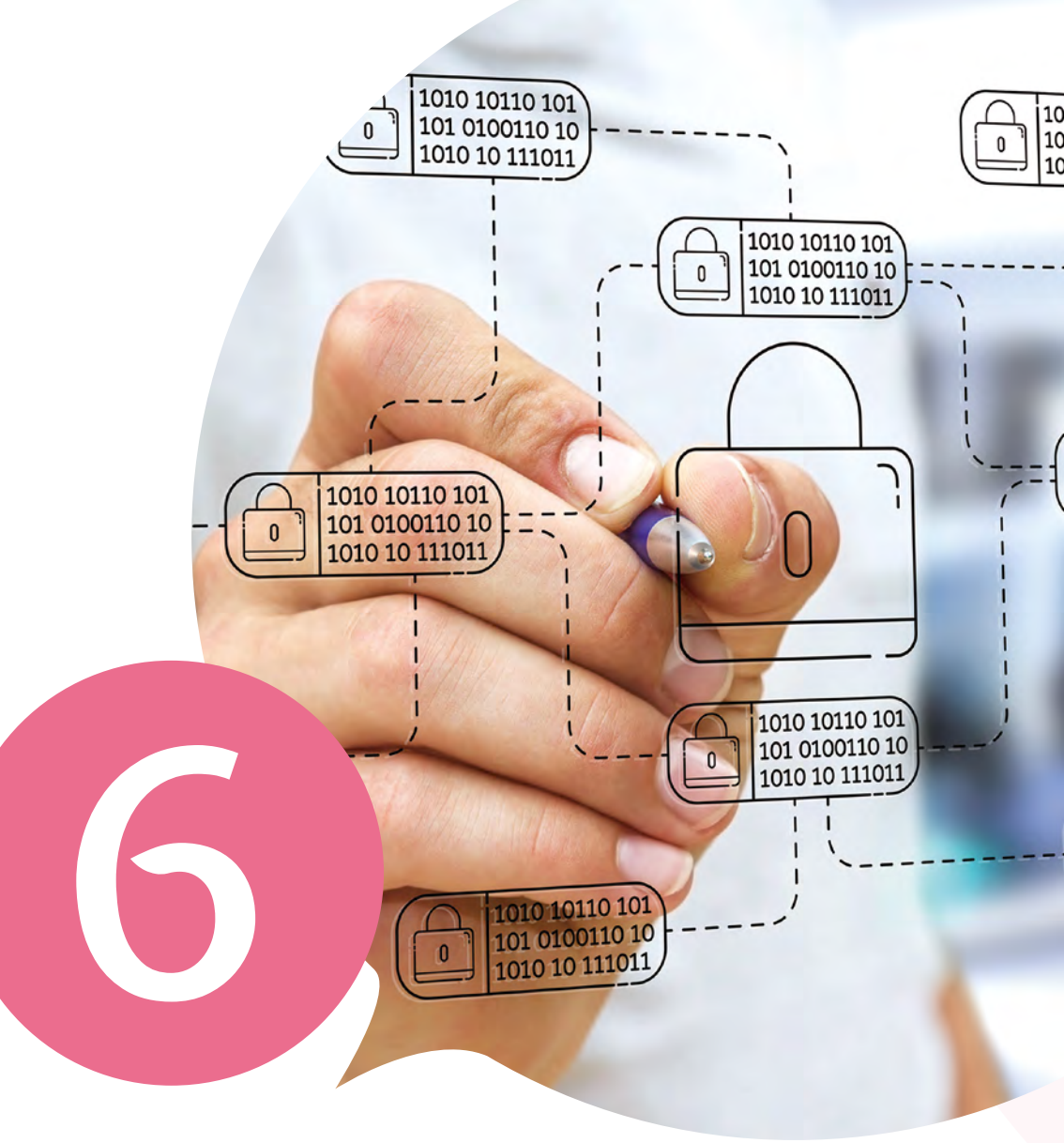
我國大型平台前後台通常維持得不錯，如果平台控制措施失效，個資外洩的數量將會相當可觀。確實有中小平台因為無法發現已存在漏洞或不知道如何修復安全漏洞的困境，這是因為中小平台不具經濟規模無法加入更多人才參與系統開發、整合運作維運，系統管理。這可以尋求主管機關、EC-CERT或個資與資安輔導團隊的協助，提供源碼檢測、弱點掃描、社交工程、資訊架構檢視等資安檢測項目，或者由民間資安組織滲透測試都可以提升中小平台降低個資外洩的風險。

電子商務資安服務中心EC-CERT聯絡方式：service@ec-cert.org.tw

八、優良賣家的特點

1. 資訊公開透明。
2. 對於個資的取得處理利用等遵循個資法要求。
3. 發生資安事件會進行調查以及應變措施。
4. 資安防護措施縱深防禦並可供稽核。

電商平台與賣家是雙方都採取背離其共同利益的行動，要達成共同的利益，最好的方式是溝通與坦白，明白雖然一時會犧牲本身少數利益，但長遠看整個網路購物市場將是生機蓬勃，消費者不會失去個資遭詐騙集團騷擾，更加樂於網路購物，平台商經營運作更加順暢安全吸引更多的賣家，賣家也因此業務興隆，唯一的輸家是詐騙集團。



6

撞庫攻擊

一、撞庫攻擊的真實案例

個資外洩案件數量逐年增加，猶有過之而無不及。而且發生外洩的公司更是知名商家，網站存取紀錄號稱一天超過200G，並未發現所謂的SQL Injection或XSS等惡意攻擊成功的紀錄，然而這些連續時間大量的成功登入紀錄都是來自相同IP。這家公司的資安主管，判斷這是很明顯的惡意攻擊行為。

這些透過相同IP連續時間大量登入的紀錄，應該是使用程式輸入用戶帳號，以及密碼，密集進行網頁的登入，進入之後查詢這個帳戶的歷史購物紀錄。而且為了效率就使用同一個IP位址發送登入的查詢。如果因此取得用戶的相關個資與訂單資訊，就可以作為詐騙集團使用電話詐騙的有利資訊，這樣就是所謂的撞庫攻擊。

二、撞庫攻擊的根本原因

帳號密碼是一般的用戶的通病，也是人性的弱點，用戶就是無法同時記住不同的網站所有的用戶帳號與密碼，乾脆一個帳號與密碼通用於各個購物網站。導致密碼不夠複雜，用戶選個容易記的通用密碼，卻反受撞庫攻擊之害。

當然，駭客也注意了這個現象，並且加以利用。只要使用程式輸入帳號再配合500大弱密碼，目前網站的回應處理速度很快，可能幾分鐘以內，就可以完成數百甚至上千個帳號的成功配對，同時駭客也能以此方式存取到消費者其他網站的資料。對

於網站而言，由於難以辨認是否為真正消費者登入的行為，只是登入的數量較多，難以判斷是否屬於惡意樣式的行為模式，難以預防。

對於這種的網路攻擊手法，是否有對應的策略呢？首先，問題來自一個密碼通行於各大網站，這是人性，儘管三令五申要求購物網站定期要求用戶更換密碼，但經營者為了避免影響用戶使用的便利，依舊不願意配合強制定期更換密碼，這種營業營利的需求很難由主管機關強制實施。

三、電商針對撞庫攻擊的作為

大部分的電商都不願意主動要求用戶更改密碼，認為這會影響其業務，因此不會將定期密碼的更換當作資安防護工作。但從另外一個角度來看，有的電商願意定期提供優惠方式，主動聯絡客戶，只要願意更換密碼，就提供折價的優惠，這是蠻主動積極的作法。其實，國內有數家電商就依照這種模式，不僅維持客戶的關係，也促進營業額的增長，更保護客戶的密碼安全性。

四、應用防護措施的加強

至於資訊安全的控制措施，因為這種攻擊方式來自網頁的查詢，倒是可以利用網頁應用防火牆（WAF）予以阻擋，鑑於部分用戶沒有使用防毒軟體，以至於電腦遭惡意軟體挾持，登入網站單憑用戶帳號與密碼無法確定是用戶本人。

第一，用戶登入增加OTP（one time password），進行二次驗證，網站檢驗登入帳號與密碼後，用戶還需要輸入手機驗證碼。

第二，用戶帳號一天以內重複三次登入失敗，必須強制要求用戶修改密碼。

第三，目前的WAF可以設定每秒鐘同一個IP登入的要求超過7次就認定為是不懷好意的行為，可以暫時停止這個IP登入的查詢一天。

第四，WAF也可判斷對於每三秒鐘頁面查詢30次以上的IP，視為機器人自動阻擋，人類的使用速度沒這麼快，這也是針對機器人很好處理方式。

第五，針對網路機器人登入之後立即切換查詢頁面到會員專區， 因此，可以要求用戶再輸入OTP，確認用戶本人。

五、善用機器人偵測

對於大量網頁的登入是採取程式極短時間連續執行，也就是網路機器人。Google於2018年11月所提供reCaptcha v3是在網站中所有的頁面都會有reCaptcha的追蹤功能，讓網站的每一個位置都能夠分析惡意程式的存在。用過的資安人員都讚不絕口，覺得reCaptcha做了很多事情，遠超過想像，這也是防止撞庫攻擊的一項很好的工具。

六、良好的密碼使用

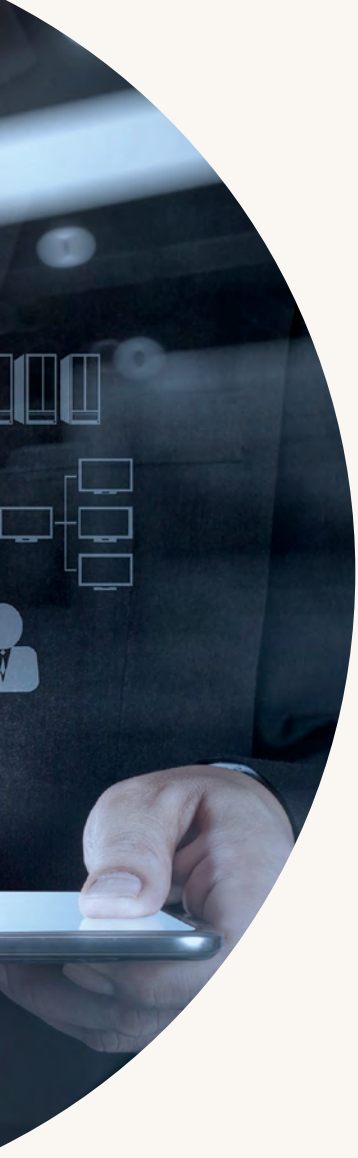
以上提到撞庫攻擊，本質上是針對一種不良的密碼管理方式。如果密碼不是輕易被猜測，這種攻擊就會消失。 因此，良好的密碼使用習慣應該是：

1. 所有的帳號不要使用相同的密碼。
2. 使用長度較長（12位元以上）的密碼，英文數字混用，長度比複雜度更重要。
3. 密碼不要告訴別人，否則請立即更換。
4. 定期更換密碼。

對於密碼這件事，用戶可以做到以上幾點來保護自己的帳戶安全。

7

網站後台
控制措施與對策



一、網站後台的通病

通常企業的網站系統後台絕大多數為企業內部人員所使用，進入後台的路徑只有企業的對外IP，如果實施網站的前台與後台分離的機制，經過網路層的路由限制，以應用層的角度其實外界無法存取後台的資源。

但是台灣的中小企業大多無法實施以上的網站前後台分離的機制，理由在於成本。目前網站雲端化已成為主流，成本包括虛擬機、作業系統版權，網路流量計價、多一個後台多一筆費用等。因此，幾乎都前後台共用以路徑名稱區分。

因此，這樣形成了惡性循環的現象：

1. 無法限定一個固定IP存取後台以保護帳號與密碼。
2. 因為網路都可以任意存取後台，以致於帳號與密碼可以不斷的重複猜測，大多數企業的後台帳號密碼並非固定更換。
3. 無法使用WAF（網頁應用防火牆）。

一旦，發生後台資源遭非來自公司的IP甚至來自國外的IP多次使用，企業的資訊資產就因此蒙受損失。

二、個資外洩案例

一家電商的後台系統除了公司自用之外，也提供供應商共同使用。過去三年從未發生任何個資外

洩紀錄。依照網站存取紀錄定期檢查並未發現惡意攻擊成功的紀錄，後台雖然無法使用網頁應用防火牆（WAF）限制電商的IP，開發商自行撰寫應用層的用戶登入認證與授權系統，配合一次性驗證碼（time-based one-time password algorithm, TOTP）強化了認證，因為這是以時間配合雜湊函數（hash function）所產生的一次性密碼，無法持續猜測。認證的系統一併驗證電商內網IP以及供應商的IP，剛好彌補了網站後台的缺點。

但是，該公司還是發生了個資外洩，類似這樣的事件是因為資訊系統防護措施出現漏洞並遭駭客成功利用。

三、事件處理與分析根因

資安協處首先透過訪談的方式了解整個企業的資訊架構，以及資安管理如何運作，這家公司的資訊系統更新正常，也經常性的執行弱點掃描。不過，訪談發現他的後台認證系統並沒有限制國外的IP登入，而是認為認證的優點已經足以彌補帳號與密碼的不足。

企業內部人員和供應商共同使用後台，而且沒有限制特定IP，這意味著無法單單只由IP發現不合法的使用情形。

並藉這家電商所提供網站存取紀錄，經過分析之後意外的發現後台在兩個月中幾乎都是國內的IP存取，可是有兩天居然出現來自國外IP成功存取後台的紀錄，而且過了三天之後開始出現大量的個資外洩事件。今年因為疫情的因素，供應商無法出國，所以可以判斷來自國外的IP，肯定不是合法使用的人員。

對於IP的分析，國內企業發生資安事件的模式，往往初期可以發現一些網路測試，大多來自國內的IP，這無傷大雅算不上惡意攻擊。 但是，當駭客找到漏洞之後，最後的攻擊就是來自國外的IP，這是為了要規避國內執法機關的追查。不過，這樣的模式可以想像，這是多國的合作，有人找

漏洞，有人寫腳本程式，有人負責測試， 但主要的竊取個資的源頭肯定大多來自台灣與大陸。

如進一步再仔細檢查日誌的紀錄，往往可發現一共有多個國外IP查詢，如果有一個IP不需經過登入的頁面，這就是說他不需登入的檢驗，那麼之前應用程式對IP的檢查以及TOTP的認證機制，不就是被繞過了嗎？開發商根據這個線索發現找到可能的弱點並且立即進行改善措施，一般經過兩周後外洩數量確實可以開始大幅降低，有效改善外洩的情形。

針對類似的攻擊，我們可以深入研究是否可能避免？在資安訪視的時候，後台沒有限制國外的IP存取，這樣不予設限往往提供駭客進行持續測試的條件，密碼無法被猜中並不意謂認證系統其他的弱點不被駭客發現。

試想國外的IP可以對後台持續查詢但不會引起系統管理人員的注意，這是不是這個網站的使用軌跡查核沒有被落實？

國內最常見的網站安全威脅就屬SQL Injection，發動之前往往要做所謂網頁弱點探勘（web scraping），就是針對一個網頁發動多次的查詢，夾帶各種參數的資料，以獲得各種可能的結果。真正進入攻擊的時候就是夾帶攻擊的參數，送進有弱點的網頁，得到預期的結果。所以，往往一個負責的系統管理人，會計算一天之內每個網頁被存取的次數，當出現超過正常次數10%， 即視為惡意的測試弱點行為，如果又來自同一個IP，那就是很可疑的行為，可以使用防火牆停止這個IP的查詢。

研究資安事件所導致個資外洩的案件，其中因為網站後台控制措施不足，產生的弱點讓駭客有機會利用，進入後台查詢訂單交易資料，這個比率其實很大。大多數的電商特別是中小規模往往因為無力負擔較高的費用，所以幾乎都選擇網站前後台位於同一主機，僅用路徑區分，大多數的後台路徑名稱都以/admin開頭。

所以如果後台的路徑名稱選擇用一個較普通的名稱，的確駭客要多費時間尋找，為了更精準的找出後台的路徑名稱，駭客也會使用目錄搜尋等方式，這種搜尋大多會集中在一個IP，因為駭客使用程式工作，無法中斷或經常更換IP以達到目標，所以一個經驗豐富的系統管理人員，也會計算一個正常使用的用戶，一天在紀錄中出現的IP次數， 如果超過10%以上，大多會特別觀察這個IP做了哪些的查詢。

所謂的後台都具有網站的系統管理、產品管理、企業公告、訂單管理，會員管理等。其中訂單資料以及會員資料是詐騙集團最想要的目標，以往最常做的就是對後台限制IP，只提供電商的內部IP存取，但是因為後台的路徑屬於應用層，一般的防火牆對來源IP， PORT做限制，但防火牆不懂網頁路徑名稱，所以無法有效的設限。

四、後台的防護控制措施

所以，強化後台的改善措施就是前後台分離，使用網路層的路由機制，限制企業後台的存取。

其次，若後台不只一個單位使用，認證的機制可以考慮使用2FA（two factor authentication），除了輸入帳號與密碼之外另外增加手機驗證。

第三，系統維持更新以及固定作弱點掃描。

對於平台的資安需求，電商必須依賴網頁開發人員在應用程式給予後台的路徑提供認證以及授權，但是網站系統本身的作業系統以及應用框架，再加上所使用的套件，檔案數量往往超過數十萬件以上。這次的事件可能駭客找到這個網頁的某一個弱點，可以規避認證系統的檢查機制，因此，一個網站應用系統每年應該定期弱點掃描，應用程式變動頻繁的系統一年應該要做一次源碼檢測，甚至進行滲透測試以發現可能的弱點，進而降低風險。一般電商限於經費經常無力，也不願意執行。

中小企業確實有這種困難，不過政府或者公協會大多可以提供這樣的協助，至少可以做一次弱點掃描。中小企業可以把這種弱點掃描當作網站的健康檢查，弱點掃描是根據以往所發生過的各種弱點，以系統性的檢查方式，逐一進行檢查，並區分弱點為極端、高、中、低風險等級。一旦發現極端風險或者高風險必須立即修復，以避免可能立即的風險，至於中度風險，時效性雖不即時，但也應該規劃修復的時程，這就是風險管理最首要的目標。

弱點掃描聯繫窗口：alex@iii.org.tw（財團法人資訊工業策進會資安所）

8

有待改進的
企業網站管理

一、案例

曾經有間資本額達1,500萬的電商公司，其所經營的網站發生個資外洩事件，但公司無法提供網站運作的軌跡紀錄，也無法證明網站的安全，且負責該公司網站維護的網站開發商，依照經濟部工商登記的網站查詢顯示該網站開發商公司已解散。

二、委外但無法管理

雖然這家電商的資本額不屬於小型電商，但是他的內部電腦管理連同網站的開發維運均採用委外，與小型電商的運作方式相仿。雖然只維持核心業務，除了能賺錢的本業以外，能委外幾乎全都外包出去了。至於個資保護項目，從個資的蒐集、處理與利用，以至於訂單下載從公司處理出貨，甚至公司內部電腦的防毒掃描也都委外。因此，許多經手個資的人員都不是該電商公司的員工。究竟個資外洩來源發生於網站的防護不夠周全，抑或從電商內部外洩，原因變得相當複雜。

三、對於電商與軟體開發商的建議

對於電商的建議如下：

1. 如果防毒軟體更新都委外，要確定是否使用有版權的作業系統？是否購買有版權的防毒軟體，且可以設定成自動更新。
2. 電商可在委外合約中載明有關個人資料的保密義務、個人資料安全相關責任，規範開發商違反相關規定的罰則。

3. 因為資本額已達1,000萬，需要建立並落實個資檔案安全維護計畫，可以尋求財團法人資訊工業策進會科技法律研究所、資安科技研究所諮詢。

四、對於軟體開發商最基本的要求

1. 考慮升級PHP程式語言到PHP 7之後，這是目前的主流，也仍在支援。超過保固的程式語言，更新不再支援，原有的弱點經過一段時間後，容易被惡意人士掌握。
2. 封閉網站表頭的資訊洩漏，不要讓外界知道網站使用哪種程式語言以及應用伺服器。這是一種態度，謹慎的資安管理人員不會輕易讓外界知道與網站業務無關的任何資訊。
3. 線上營運網站如果不希望進行弱點掃描，也可以對測試機進行測試，依掃描結果進行改善再上線。駭客是根據軟體的弱點予以利用再滲透成功，因此趁早發現弱點，及早降低風險的發生。
4. 網站存取紀錄是很重要的資訊軌跡，每個網站都必須予以保存6個月，分析內容有助於事件應變程序，追蹤攻擊路徑，發現資安防護的弱點，事件發生的數位鑑識都很重要。
5. 網站的設定可以用Lynis這項免費的安全性檢測工具，協助對Linux作業系統進行檢測。對於軟體開發商，經常對於安全的設定，僅憑工程師的個人經驗，容易產生疏忽，因此，開發與維運無法兼顧，使用工具作為設定檢查，這是好的選擇。
6. 可以採用雲端WAF（網頁應用防火牆），有的品牌不僅功能良好而且價格便宜，每月不到600元。


SOCIAL NETWORK
SOCIAL NETWORK

結語

隨著網際網路的發達以及消費者購物習慣的改變，近年來全球電子商務的營業額持續增長。根據市場研究機構eMarketer於2019年6月的預估，全球電子商務市場規模將自2019年的3.53兆美元，將於2023年成長至6.54兆美元；此外，電商銷售佔零售業之比重逐年提升，2019年為14.1%，2023年將成長到22%。電子商務產業的成長性與重要性不言可喻。

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，個資保護與資訊安全是主管機關經濟部、產業與消費者都很重視的一個議題，尤其國際間對於隱私保護的議題越來越重視，除了歐盟GDPR、加州CCPA等法律，國際間已有許多國家開始針對隱私保護議題調修國內法令，以加強對於隱

私保護的水準。另外亞太地區已有許多國家開始正視APEC CBPR體系，新加坡甚至將CBPR認證納入其國內跨境傳輸的合法要件。我國國內網際網路業者如何在各國法令間生存並且開拓市場，將是業者需要面對的挑戰。

電子商務隨著網路科技發展蓬勃，但水可載舟，亦可覆舟。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。在電子商務市場規模逐年擴大的同時，國內電子商務交易網路詐騙事件也層出不窮。近年來，在內政部警政署大力宣導之下，許多民眾接到詐騙集團電話，已逐漸建立於第一時間撥打165反詐騙專線諮詢的習慣，但是由於詐騙集團手法不斷演變，仍有不少民眾不慎誤入詐騙集團陷阱，造成實質金錢損失。

檢視我國法務部及內政部警政署刑事警察局165反詐騙等相關統計資訊，因網際網路零售業者暨相關電商企業個資保護不力，或資安管理能量不足，造成消費者個資外洩而導致網路詐騙頻傳，或對於已蒐集之資料進

行不當行銷，致引發不小民怨，而我國法院實務亦指出業者應針對個人資料保護建置完善、嚴格之管理制度，方可謂已採取個資法第27條之適當安全措施，可預期未來個資及資安保護與管理等需求將日益重要。

個資保護有如逆水行舟，不進則退。駭客技術無時無刻都在提升，我國業者倘仍原地踏步，則雙方的差距將不只是「道高一尺，魔高一丈。」業者應積極檢視自身關於個資保護管理的制度與措施，進行超前部署，如此才能落實個資法的要求、保障消費者權益以及維護自身商譽。

經濟部目前除積極針對疑似個資外洩之網購業者實施行政檢查外，同時也在「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與個資法遵的輔導。因此彙整這些輔導查訪的結果並加以出版，希冀達到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。

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/

參考資料

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：109年12月

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

CSTI 資安科技研究所 CyberSecurity Technology Institute

經濟部商業司廣告