電子商務交易安全推動計畫

電子商務個資外洩資安防護參考指引

財團法人資訊工業策進會

中華民國104年7月

目　次

壹、 指引訂定說明 1

一、 依據 1

二、 目的 1

三、 本指引參考定位 1

四、 整體指引架構 5

五、 本指引目標使用者與使用說明 6

六、 參考文獻 8

七、 用語與定義 9

貳、 電子商務業者資料外洩現況主要成因分析 15

一、 國際安全組織對於資料外洩成因之分析 15

二、 電子商務交易流程中資訊流、金流與物流 21

三、 交易作業環節之安全問題與弱點 23

參、 主要資料外洩過程分類說明 40

一、 惡意或犯罪攻擊(Malicious or Criminal Attack) 41

二、 系統錯誤(System Glitch) 47

三、 人為錯誤(Human Error) 49

肆、 個資外洩資安防護的參考標準 52

一、 國際標準 ISO/IEC 27001 版 53

二、 產業標準/規範 57

三、 最佳實務 67

四、 VISA 安全規範 68

伍、 事前防禦措施的實施指引 69

一、 事前防禦措施之重點 69

二、 事前防禦策略 69

三、 基本防禦措施 72
四、 事故應變計畫 86

陸、 事中應變措施實施指引 90
一、 事中應變措施的目的與重點 90
二、 個資外洩事故類型 90
三、 個資外洩事故之處理 91

柒、 事後處理實施指引 97
一、 事後處理措施之目的與重點 97
二、 整體事後處理作業說明 97
三、 消費者溝通及處理方式 99

捌、 附件 104
一、 附件 1：電子商務業者個資外洩資安防護查核表(事前資安強化) 104
二、 附件 2：電子商務業者個資外洩資安防護查核表(事中應變) 117

圖　目　次

圖 1　經濟部商業司歷年計畫陸續發展之資安防護規範示意圖 1
圖 2　電子商務個資外洩資安防護參考指引與其他規範關係示意圖 4
圖 3　整體指引架構示意圖 6
圖 4　資料外洩主因分析統計圖 15
圖 5　國際電信通訊公司(Verizon)分析資料外洩之威脅角色統計圖 16
圖 6　國際電信通訊公司(Verizon)分析主要威脅活動統計圖 18
圖 7　資料外洩事故主因 19
圖 8　CVE 公布系統漏洞被利用時間對照統計圖 20
圖 9　2014 年前 5 大零時差系統漏洞被修補的統計圖 21
圖 10 電子商務交易流程與結構化問題分析圖 22
圖 11 電子商務業者系統安全責任範圍示意圖 23
圖 12 國際電信通訊公司(Verizon)分析資料外洩事故分類統計圖 41
圖 13 國際電信通訊公司(Verizon)調查網站攻擊類型統計圖 43
圖 14 惡意攻擊一般流程 44
圖 15 國際組織調查，每筆資料外洩成本金額(單位：美金) 51
圖 16 個資外洩資安防護三個面向示意圖 52
圖 17 ISO/IEC 27001 資訊安全管理領域(14 個) 53
圖 18 ISO/IEC 27001 管理系統框架 54
圖 19 ISO/IEC 27001 與風險評鑑方法架構 55
圖 20 ISO/IEC 27005 風險管理過程 57
圖 21 PCI DSS 信用卡資料儲存規範 58
圖 22 PCI DSS 對 VISA 發卡銀行等級要求 59
圖 23 PCI DSS 標準之特色示意圖 60
圖 24 PCI DSS 的安全防護要求 62
圖 25 PCI DSS SAQ D 查檢表範例 63

圖 26 電子商務資訊安全機制與管理規範-中小企業版資訊安全架構.....65
圖 27 以資料為核心的防禦策略.....70
圖 28 針對發生資料外洩事故企業的調查：資料是否加密.....71
圖 29 安全軟體開發過程.....81
圖 30 個資外洩之事故類型統計.....91
圖 31 資料外洩處理框架與步驟示意圖.....91
圖 32 事後處理實施指引示意圖.....97

表　目　次

表 1　本指引各章節閱讀對象建議 7
表 2　電子商務交易環境 22
表 3　電子商務交易流程及可能問題點分析 37
表 4　個資外洩管理問題對照 38
表 5　電子商務交易安全規範實施策略目標 64
表 6　電子商務資訊安全機制與管理規範發展控制措施與控制目標 65
表 7　電子商務業者個資外洩資安防護查核表(事前資安強化) 104
表 8　電子商務業者個資外洩資安防護查核表(事中應變) 117

壹、指引訂定說明

一、依據

「電子商務個資外洩資安防護參考指引(以下簡稱本指引)」係依據經濟部商業司本(104)年度「電子商務交易安全推動計畫(以下簡稱主計畫)」中「推動電子商務個資外洩防範措施(以下簡稱本計畫)」之分項工作而訂定。

二、目的

本指引之目的在於提供電子商務業者對於保護個人資料外洩之事前、事中、事後之防禦及處理機制，以協助電子商務環境健全及安全的發展。

三、本指引參考定位

(一)已建立之安全防護參考指引

爰經濟部商業司提供電子商務業者資安防護之規範(詳如圖1所示)，說明如下：

資料來源：計畫整理

圖1　經濟部商業司歷年計畫陸續發展之資安防護規範示意圖

1.「交易安全及資安服務平台推動計畫」

針對電子商務交易平台業者，物流商等安全強化指引與上下游安全之自我檢查表，協助平台業者、網路零售業者(使用平台)、供應商及物流商及建立資安防護機制，此計畫提供業者以下規範指引如下：

(1)電子商務交易安全規範-網路平台。

(2)電子商務交易安全規範-供應商。

(3)電子商務交易安全規範-物流商。

2.「資安檢測與輔導計畫」

透過資安檢測技術協助獨立架站之電子商務網站透過檢測方式發現網站問題，並提供業者以下規範指引協助建立資安防護及個資保護能力。

(1)電子商務資訊安全機制與管理規範。

(2)電子商務資訊安全機制查檢表。

(二)本指引之需求

本計畫參考過去發生的電子商務外洩事故中，發現相關業者包括：平台業者、開店零售商(使用平台)，獨立架站電子商務等業者，雖已積極建立安全防護的機制，但於發生資安事故後，仍有問題及需求如下：

1.攻擊來自內部人員或已由直接攻擊網站轉而先入侵及攻擊內部網段、個人電腦後再對網站主機進行攻擊，電子商務業者規劃之網路架構仍不夠安全須要強固。

2.資安事故發生後，電子商務業者未保存足夠 Log 紀錄，導致無法追查、無法確認損失範圍及提出後續補救措施。也由於系統、

安全相關 Log 未能有效保護，部分事故於處理階段，Log 均已遭受破壞。

3.由於系統及安全 Log 部分，過去業者並未積極佈建，因此也無法於系統中透過 Log 分析進行預警提示(例如：資料庫隱碼 SQL Injection 可透過 Balance Log[1]平衡 Log 差異來發覺)，因此部分業者即使已被入侵或資料已外洩，無法即時發現或有可能必須經過長時間才能發現入侵、外洩之範圍。

4.近來由於多個大型資安漏洞接連發生(例如：Shellshock，Heart bleeding，SSL Poodle 等)，由於其影響範圍非常大，因此電子商務業者即使已實施安全管控，但由於漏洞係基於底層技術，無法有效透過安全機制進行防禦，因此對於資料庫、資料加密的技術仍須要求並強化。

5.事故後處理，電子商務業者未能具備發現問題的能力。例如：於客戶撥打客服電話說明其資料遭竊或誤用，電子商務業者缺乏能力進行查證，是否該資料係由其網站所外洩。而此一查證能力須建立於高度安全防護、Log 分析能力、精確的確認安全環節、是否於事故發生期間出現異狀、出現不明之網路流量外流、非授權存取資料等跡證來協助業者判斷，惟過去的指引並未能深入或詳細說明，電子商務業者對於事故中查證的能力非常薄弱。

6.事中處理能力，發生資料外洩作業，由於網路中的跡證會因為電子商務業者之作業而受到破壞，例如：疑似遭受侵入的主機，於處理時應注意必須先將跡證保全，但部分事故中發現，業者

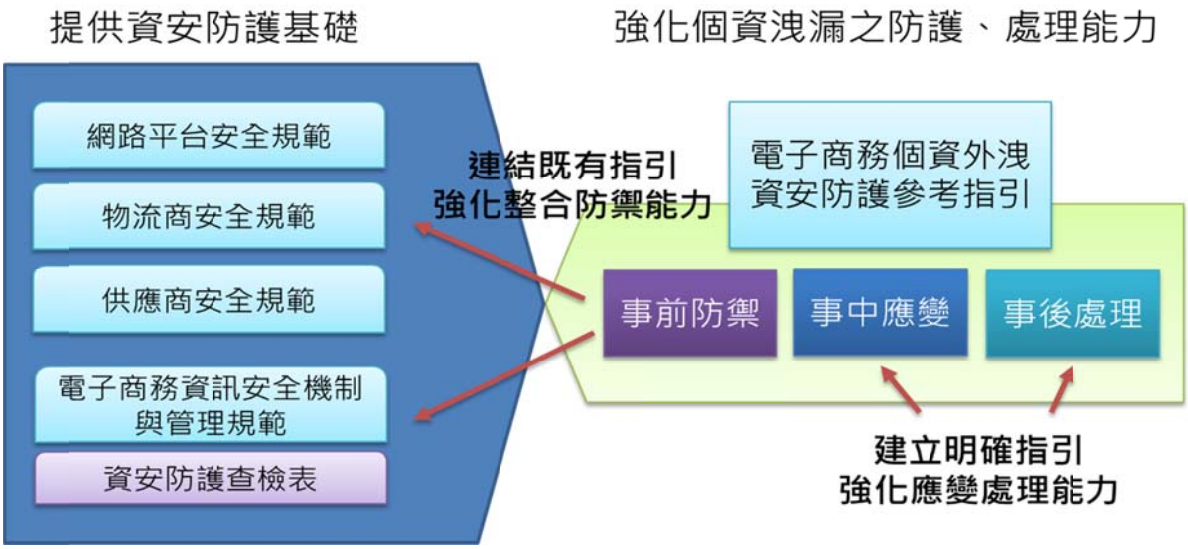
[1] Balance Log 是計算下單量與各主機存取量間之計算，如果遭受駭客直接攻擊資料庫，則下單量與資料庫讀取量的平衡關係會變化，藉由判定這些對應關係來查核可能入侵的點。

於事故期間持續以高權限帳號登入有問題主機，安裝防毒軟體、重啟主機等作業，極可能破壞入侵跡證，因此，電子商務業者極需要有更明確的步驟及提示進行事故之處理。

7.事後處理，目前經濟部商業司、內政部警政署 165 反詐騙等已建立通報體制，並成立「網際網路零售商品之公司行號個資保護行政檢查小組」，將就重大個資外洩或特殊案件之電子商務業者列為檢查對象。然而電子商務業者於面對事故後對於消費者、客戶等因應方式等說明及處理原則均不甚清楚，而導致受害消費者再次受傷害或與電子商務業者發生糾紛，因此極需建立業者事後處理之能力。

(三)本指引與其他規範關係

本指引與過去規範之關係在於強化過去以防禦為主的資安防護規範，其關聯性詳如圖 2 所示：



資料來源：本計畫整理

圖2　電子商務個資外洩資安防護參考指引與其他規範關係示意圖

綜整分析後，電子商務業者仍需積極建立事前防禦、事中應變及事後處理三種能力，茲分述如下：

1.事前防禦能力

(1)依據攻擊型態，積極補強安全架構並採取預防外洩的安全措施，例如：將內網區與主機區做區隔、不使用非安全的通訊協定(例如：FTP)等。

(2)積極於預防階段建立可以支應後續事故調查、事故中應變及事後處理階段需要的 Log、系統狀態，並提高於事故發生前可能的預警能力。

(3)強化資料的安全，透過加密、減量以及降低風險的作為，以因應日趨嚴重的底層技術安全漏洞發生時的衝擊。

2.事中應變能力

建立清楚步驟以協助電子商務業者處理資安事故。

3.事後處理措施

(1)依據本指引協助處理資料外洩。

(2)提供電商業者(資料外洩受害者)處理之溝通技巧。

(四)指引使用限制

1.本指引與其他規範需搭配使用並連結強化，故本指引無法單獨被運用於未建立其他資安防護基本能力之環境。

2.本指引之撰寫係針對資料外洩之防禦,並非全面功能性之指引,僅實施本指引所提示之安全功能並無法得到完整的安全架構。

3.本指引專用於個資外洩安全事故的事前資安防禦、事中及事後處理機制，並不適用於其他類型之安全事故處理。

四、整體指引架構

依據本指引之目的，訂定整體指引架構詳如圖 3 所示：

資料來源：本計畫整理

圖3　整體指引架構示意圖

本指引之整體架構著重目標於「知識建構」，其內容包括：

(一)說明電子商務資料外洩之主要成因。

(二)電子商務環境之問題與威脅。

(三)電子商務環境之弱點與漏洞。

藉由說明電子商務資料外洩現況之成因，與電子商務環境之問題、威脅及弱點與漏洞，以協助電子商務業者瞭解本指引中提示事前、事中及事後之措施必要性與其相對應預防與處理之重點。

五、本指引目標使用者與使用說明

本指引之目標對象為電子商務業者，希透過本指引讓電子商務之經營管理者、系統管理者、安全技術人員等瞭解個資外洩於事前防禦措施、事中應變及事後處理之重點方向。茲將上述人員職務舉例如下：

(一)經營管理者：例如：總經理、副總、經理等人員，為電子商務業務之管理者。

(二)系統管理者：管理電子商務資訊系統維運及安全之主管人員。

(三)安全技術人員：包括網路技術、系統管理技術、資料庫管理技術及系統開發人員。

由於本指引針對電子商務業者的個資洩漏防護提供建議，而防止個資或交易資料洩漏涉及管理、業務、人員以及技術，因此本指引特別將各章節之閱讀對象建議列表，防止外洩階段相較於其他安全保護需要有更深入之管理措施與更嚴密之技術措施，且於部分管理項目涉及技術機制部分，應由系統管理者與技術人員協同管理。

表1　本指引各章節閱讀對象建議

章節	單元名稱	經營管理者	系統管理者	安全技術人員			
				網路技術	系統安全技術	資料庫管理	系統開發
壹	指引訂定說明	V	V				
貳	電子商務業者資料外洩現況主要成因分析	V	V				
參	主要資料外洩過程分類說明	V	V				
肆	個資外洩資安防護的參考標準	V	V				
伍	事前防禦措施的實施指引	V	V	V	V	V	V
陸	事中應變措施實施指引	V	V	V	V	V	V
柒	事後處理實施指引	V	V	V	V	V	V
附件一	電子商務業者個資外洩資安防護查核表(事前資安強化)	V	V	V	V	V	V

章節	單元名稱	經營管理者	系統管理者	安全技術人員			
				網路技術	系統安全技術	資料庫管理	系統開發
附件二	電子商務業者個資外洩資安防護查核表(事中應變)	V	V	V	V	V	V

資料來源：本計畫整理

六、參考文獻

本指引參考國際及產業標準，藉由引用或參考國際及產業標準，使電子商務業者可以使用標準的作法，另外可以作為本指引之延伸，電子商務業者如果有需要進一步的實施全面性的安全措施，也可以經由參考下列本指引參考之國際及產業標準而建立全面性的安全保護作業。

(一)ISO/IEC 27001：2013：Information Security Management System, International Standard Organization, 資訊安全管理系統國際標準組織。

(二)PCI DSS 3.0：Payment Card Industry Data Security Standard, Payment Card Industry Security Standards Council 支付卡產業資料安全標準，支付卡產業安全標準協會。

(三)Visa 國際組織事故應變指引：VISA, What To Do If Compromised Version 4.0, September 2013。

(四)電子商務(B2C)交易安全規範(包括網路平台、供應商及物流商)，經濟部商業司。(下載網址：http://ec-cert.org.tw/公告訊息→檔案

下載)

(五)電子商務資訊安全機制與管理規範，經濟部商業司。(規範索取email：ec-security@mail.cisanet.org.tw)

七、用語與定義

(一)平衡紀錄(Balance Log)

平衡紀錄於電子商務網站管理中，是計算下單量與各主機存取量的平衡關係之計算。如果遭受駭客直接攻擊資料庫主機，則下單量與資料庫讀取量的平衡關係會變化，藉由判定這些對應關係變化來查核可能入侵的點。

(二)識別資料(Credentials)

使用者存取帳戶的使用者帳號和通行碼(Password)資訊。

(三)記憶體刮取(Ram Scraper)

惡意攻擊程式，專門讀取暫存在系統記憶體而未被加密的信用卡資料或交易資料的攻擊方式。

(四)間諜軟體(Spyware)

未經使用者許可的情況下蒐集使用者個人資料或其他財務資訊的電腦程式。

(五)側錄器(Key Logger)

側錄器為軟體或硬體裝置用來在使用者不知情的情況下，錄製使用者系統鍵盤所輸入的所有資訊，藉以分析並取得帳號及通行碼的手段。

(六)釣魚(Phishing)

透過偽造的電子郵件、未授權取得之通訊軟體帳號或假冒、被入侵的網站來誘騙使用者交付個人資料、識別資料或財務資料之手段。

(七)社交工程(Social Engineering)

利用社會關係、人性弱點，應用簡單的溝通和欺騙手段，以獲取個人資料、帳號、通行碼或其他機敏資料並藉由騙取之資料進行下一步驟的攻擊。

(八)進階持續性滲透攻擊 (Advanced Persistent Threat, APT)

針對特定組織，經規劃、多方位、長期性的攻擊行為，通常攻擊者為組織型的犯罪組織。

(九)資料庫隱碼攻擊(SQL Injection)

攻擊者在正常輸入的資料字串之中夾帶惡意的資料庫 SQL 指令，如果網站程式忽略了檢查，那麼這些夾帶進去的指令就會被資料庫伺服器誤認為是正常的 SQL 指令而執行，因而產生資料庫破壞或資料未授權存取的結果。

(十)阻斷式攻擊(DDOS)

攻擊者透過各種手段使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其對目標客戶不可用之攻擊手法。

(十一)零時差攻擊(Zero Day Attack)

在軟體上發現的安全漏洞，攻擊者在問題尚未被廣泛公布或提出問題修正之前，利用該漏洞進行的惡意攻擊。

(十二)跨目錄存取弱點攻擊(Directory Traversal)

網站伺服器或網站應用伺服器的設定未限制網站根目錄以

外的檔案、目錄顯示或是攻擊者透過輸入特殊字元繞過伺服器的安全限制，而對於其他檔案進行存取甚至執行系統指令的攻擊手段。

(十三)跨網站指令碼攻擊(XSS)

是一種網站應用程式的安全漏洞攻擊，攻擊者將惡意程式碼透過資料庫漏洞、系統輸入介面漏洞或其他手法注入或內嵌到正常的網頁上，其他使用者在存取該網頁時就會受到注入的惡意程式之攻擊。

(十四)源碼審查機制(Code Review)

對於原始碼、程式做系統化的審查，通常使用軟體工具掃描或進行同儕審查(Peer Review)的方式進行，其目的是在找出及修正在軟體開發初期未發現的錯誤，提升軟體品質、避免安全漏洞的產生。

(十五)非軍事區(DMZ, Demilitarized Zone)

是一種安全網絡架構的方式，非軍事區網段被建立在不信任的外部網路和可信任的內部網路之間，該網段接受來自外部網路的存取，並允許進行內部網段之存取，這樣區域設立可形成一個保護內部網段不被外部直接攻擊的安全措施。

(十六)入侵防禦系統(Intrusion Prevention System)

透過監視網路或網路裝置的網路資料存取或傳輸行為，並與惡意攻擊的模式資料庫進行比對，能夠即時的偵測、中斷、調整或隔離一些不正常或是具有傷害性的網路資料存取或傳輸行為。

(十七)網站應用程式防火牆(Web Application Firewall)

通常架設於網站伺服器之前端，監視流向網站的 Http/Https 指令要求，透過行為的分析及防禦政策的建立，保護網站伺服器不被惡意攻擊。

(十八)安全架構(Security Architecture)

一種依據安全原理規劃出的系統或網路結構，此結構描述中包括達到安全所必須之元件、配置方法或效能、層級等要件，依據安全架構建立網路或系統，可獲得較全面的安全防護功能。

(十九)自有設備使用(Bring Your Own Device)

一種管理政策，允許組織內的員工或工作者攜帶自己擁有的電腦或資料處理設備到組織擁有的辦公環境作業，並允許接上組織的內部網路或專有網路的管理方式。

(二十)資料庫設計(Schema)

資料庫的設計通常只針對資料欄位(或稱為 Schema 綱目)進行之規劃及建置。

(二十一)軌跡資料(Trail files)

電腦、網路系統的存取、變更、使用等紀錄組合，可用於事後進行對於系統事件的追蹤。

(二十二)中間人攻擊(Man-in-the-middle-attack)

攻擊者惡意介入資料傳輸者及接受者之間，對傳輸者假冒其為接收者，並對接收者假冒其為傳輸者，因此攻擊者可以對資料惡意的存取或變造，因此達到竊取資料或變更資料之目的。

(二十三)暴力破解(Brute-force)

透過持續的錯誤嘗試或攻擊演算法弱點的方式進行通行碼

的破解之攻擊手法。

(二十四)弱點掃描(Vulnerability Scan)

弱點掃描通常透過自動化工具，基於已知的系統漏洞或弱點資料庫，針對被掃描的系統做系統化的評估、測試以判斷該系統是否存在系統的漏洞或弱點的方式。

(二十五)滲透測試(Penetration Test)

滲透測試通常由專業的安全顧問以人工方式，模擬攻擊者的思維進行對於系統的攻擊測試，透過利用現有系統的漏洞或弱點，嘗試組合現有漏洞或弱點，並透過測試發現新的漏洞或弱點以達到模擬攻擊的測試目的，找出系統的安全問題。

(二十六)網站應用程式安全掃描(Application Security Scan)

特別針對網站應用程式端進行的弱點掃描作業，專門針對網站於應用程式(例如：JavaScript、AJAX 等)進行弱點的評估作業。

(二十七)安全軟體開發生命週期管理(Secure Software Development Life Cycle)

將安全管理、安全需求融入軟體開發流程作業中(例如：在系統分析階段產出系統安全需求)，以開發出安全的軟體。

(二十八)政府組態基準(GCB)

由行政院資通安全辦公室制定，目的在於規範資通訊終端設備(如：個人電腦)的一致性安全設定(如：密碼長度、更新期限等)，以降低駭客入侵管道並進而引發資安事件之疑慮。

(二十九)數位鑑識(Digital Forensic)

以周延的方法及程序來保存、識別、抽取、記載及解讀數位資料證據，用以保留數位證據的完整性和正確性，及建構資訊安全事件發生的過程，以做為資訊安全事件及司法單位調查判決電腦網路犯罪之依據。[2]

[2]軍事院校資安管制措施之探討-以數位證據鑑識標準作業程序為例,林宜隆, 周彥霖, 2013

貳、電子商務業者資料外洩現況主要成因分析

電子商務業者資料外洩現況主要成因分析，主要依據以下步驟進行說明，摘錄分析國際安全組織之成因分析，透過分析近期之安全組織、公司針對網路環境中的資料外洩事故進行分析，並摘錄其中主要與電子商務業者相關之成因。

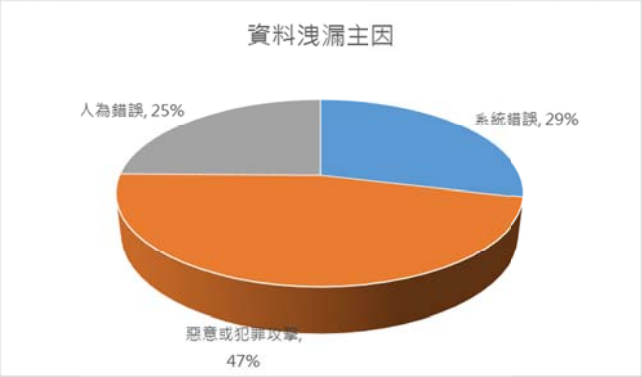
分析電子商務業者交易環境中資訊流與金流之特點，並藉以說明其可能之問題、威脅、漏洞與弱點。

一、國際安全組織對於資料外洩成因之分析

本指引參考以下國際組織之報告進行本次成因之分析如下：

(一)資料外洩主因統計

依據國際組織 Ponemon Institute 針對全球資料外洩事故的主因分析，資料外洩主因有 3 類，分別為：惡意或犯罪攻擊(Malicious or Criminal Attacks)(佔 47%)、系統錯誤(System Glitch)(佔 29%)以及人為錯誤(Human Error)(佔 25%)，分析資料外洩主因統計詳如圖 4 所示。



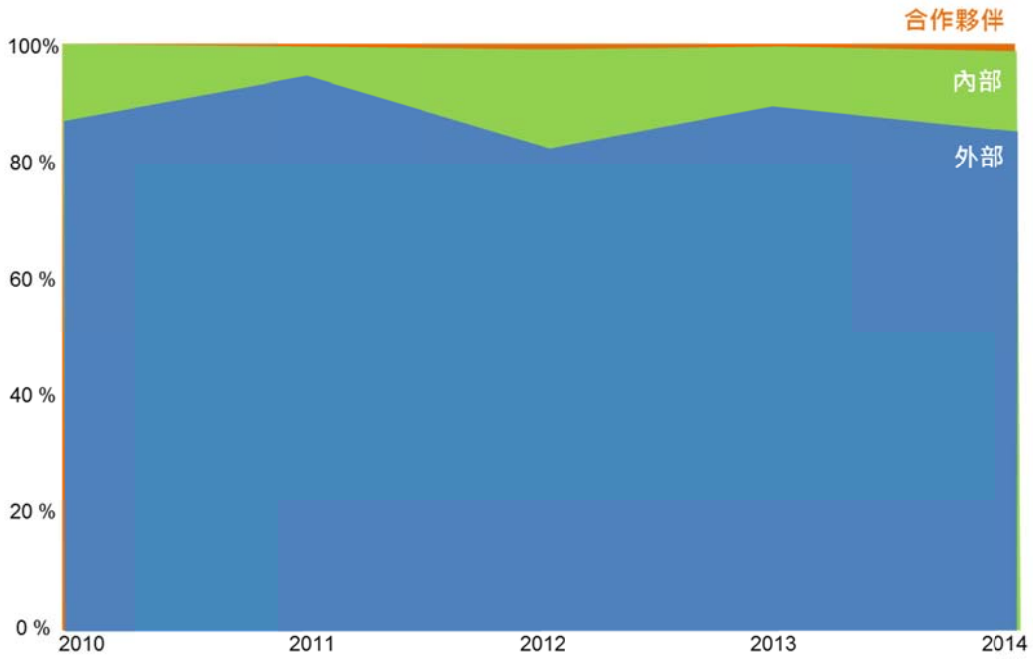
資料來源： 2015 Cost of Data Breach Study, Global Analysis　Ponemon Institute

圖4　資料外洩主因分析統計圖[3]

[3] 此圖中之總和數字大於 100%，係為原始資料單位之錯誤。

(二)資料外洩之威脅角色(Threat Actors)

電子商務業者應瞭解，依據國際組織的調查與統計，所有的外洩事故中，威脅角色(Threat Actor)大部分來自外部，但其中約莫13~15%事故的成因是來自於內部人員。另外，合作夥伴(Partner)近年來慢慢的在其間扮演一定比例的來源，因此對於後續的安全防禦工作上，應注意其順序與資源的投入比例，防禦的範圍也不可以忽略夥伴關係的廠商或合作組織。資料外洩之威脅角色分析詳如圖 5 所示。



資料來源： 2015 Data Breach Investigation Report, Verizon

圖5 國際電信通訊公司(Verizon)分析資料外洩之威脅角色統計圖

(三)威脅活動(Threat Actions)

依據國際電信通訊公司(Verizon)調查(註：該公司之報告係針對廣泛業者、非特定針對電子商務業者)，識別資料(Credentials)、記憶體刮取(Ram Scraper)、間諜軟體(Spyware/Key logger)及釣魚(Phishing)等威脅活動為過去主要的資料外洩事故中關鍵活動，也是威脅角色(Threat Actors)使用的主要入侵或取得資料之方法。其

中記憶體刮取(Ram Scraper)係特定指入侵大型零售業的前端銷售電腦(POS)、刷卡設備中，並由該等設備之記憶體中進行資料竊取的行為，近年各國大型零售業經常遭受此等的威脅。以上四類的活動，電子商務業者除了 Ram Scraper 僅發生於具備現場交易之環境，其餘的發生成因應值得注意及避免。依據國際電信通訊公司(Verizon)於 2015 年統計 2010~2014 年主要威脅活動分析詳如圖 6 所示。並將上述四類之威脅活動說明如下：

1.識別資料(Credential)

此種活動手法是最常見的攻擊手法，藉由竊取、入侵或其他方式取得登入所需的識別、帳號密碼資料進行資料的竊取是資料外洩事故中最主要的活動。

2.記憶體刮取(Ram Scraper)

透過該活動手法竊取大量的信用卡或支付卡資料。

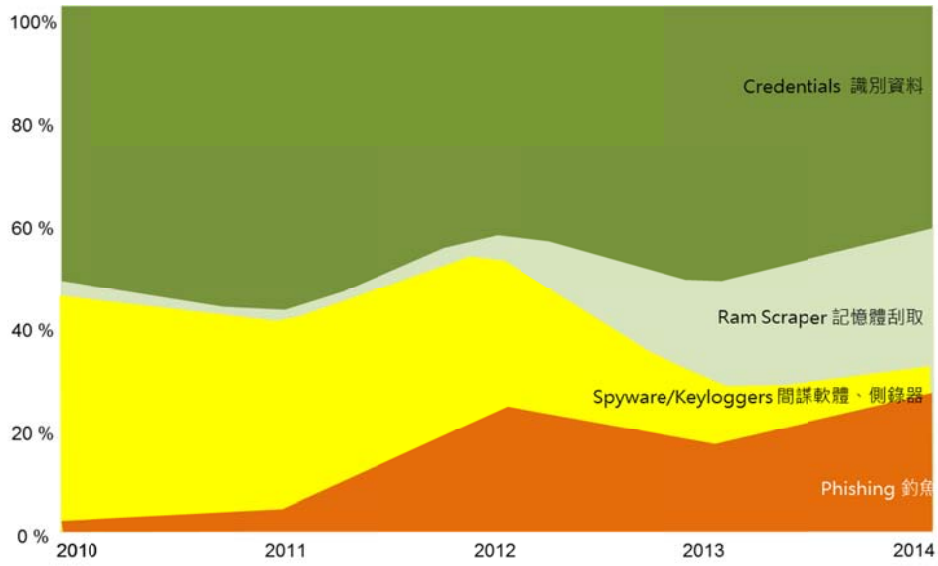
3.間諜軟體與側錄軟體(Spyware/Key logger)

間諜軟體與側錄軟體仍為主要的攻擊作業，藉由病毒、遠端或實體入侵後建立側錄之機制，或透過間諜軟體遙控或監視資料所有者的活動藉以竊取資料。

4.釣魚(Phishing)

是近年來非常盛行的作業也是主要的社交工程活動，藉由 email 或其他方式接觸持有資料或內部員工(持有必要登入資訊)，竊取、騙取資料或登入識別資料。上述社交工程活動包括近年來最常見的進階持續性滲透攻擊(Advanced Persistent Threat, APT)有 91%的攻擊利用電子郵件作為開始的進入點，電子郵件是阻力最小的攻擊路徑，可以用來避開現有的安全防禦，以相關的電子郵件形式出現，其中包含惡意電子郵件附加

檔案或網址來合成引誘收件者打開的內容，進而竊取敏感的客戶資料、商業祕密等。



資料來源： 2015 Data Breach Investigation Report, Verizon

圖6　國際電信通訊公司(Verizon)分析主要威脅活動統計圖

(四)資料外洩安全事故分類

依據國際電信通訊公司(Verizon)於 2015 年的調查報告顯示，統計資料外洩安全事故主要原因及所佔比率詳如圖 7 所示，主要成因包含：

1.其他類錯誤(佔 29.4%)，例如：錯誤寄送到不正確的收件人、銷毀錯誤、錯誤公告、實體意外及資料銷毀錯誤等與人員疏忽。

2.惡意程式(佔 25.1%)，木馬、綁架軟體及後門等惡意軟體。

3.內部人員誤用(佔 20.6%)，包括各級員工、內部人員(例如：櫃台人員及經理等)以合法之存取授權將資料誤用、交付外部等違法行為[4]等。

[4] Ponemon Institute 國際組織的外洩主因統計(本指引第 15 頁)將內部誤用之惡意、違法行為歸入「惡意或違法之攻擊」。

4.實體遭竊或遺失(佔 15.3%)，實體資料儲存媒體或設備遭竊取或遺失。

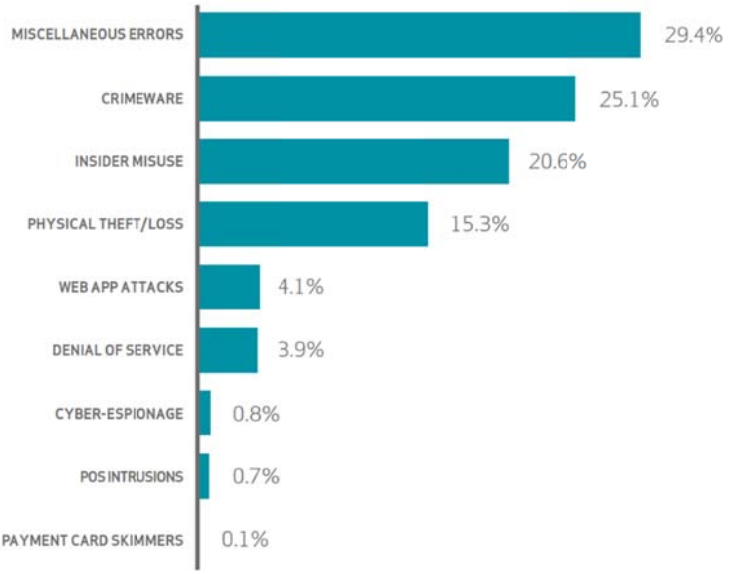
5.網路系統攻擊(佔 4.1%)，包括以竊取的身分登錄資料進行網站登入，使用網站後門漏洞、資料庫隱碼 SQL Injection 等與網站應用程式(Web APP)相關之攻擊。

6.阻斷服務攻擊(佔 3.9%)，透過 DDOS 分散式阻絕服務。

7.網路間諜活動(佔 0.8%)，例如：常見的釣魚攻擊等活動，其行為包括以郵件夾檔進行攻擊、郵件中夾帶連結、遠端植入等方式。

8.收銀系統入侵(佔 0.7%)，攻擊 POS 收銀系統。

9.支付卡側錄(佔 0.1%)，以側錄設備進行側錄卡號。



資料來源： 2015 Data Breach Investigation Report, Verizon

圖7　資料外洩事故主因

(五)系統之安全漏洞

系統的安全漏洞、弱點是系統遭受攻擊的主要原因，國際組織統計系統漏洞遭受攻擊的相關統計分析如下：

1.CVE(Common Vulnerability Exposure)是國際組織用來描述系統漏洞的標準，所有國際安全社群所發現的系統漏洞，都會公布於此組織，對於系統漏洞被利用(Exploit)的分析統計，詳如圖8 所示。

在系統弱點被公布後，約有 50%的系統漏洞在被公布後2~4 週就被利用，因此，電子商務業者必須注意對於系統漏洞的管理，在 CVE 發布後，應儘速進行系統的補強措施。

資料來源： 2015 Data Breach Investigation Report, Verizon

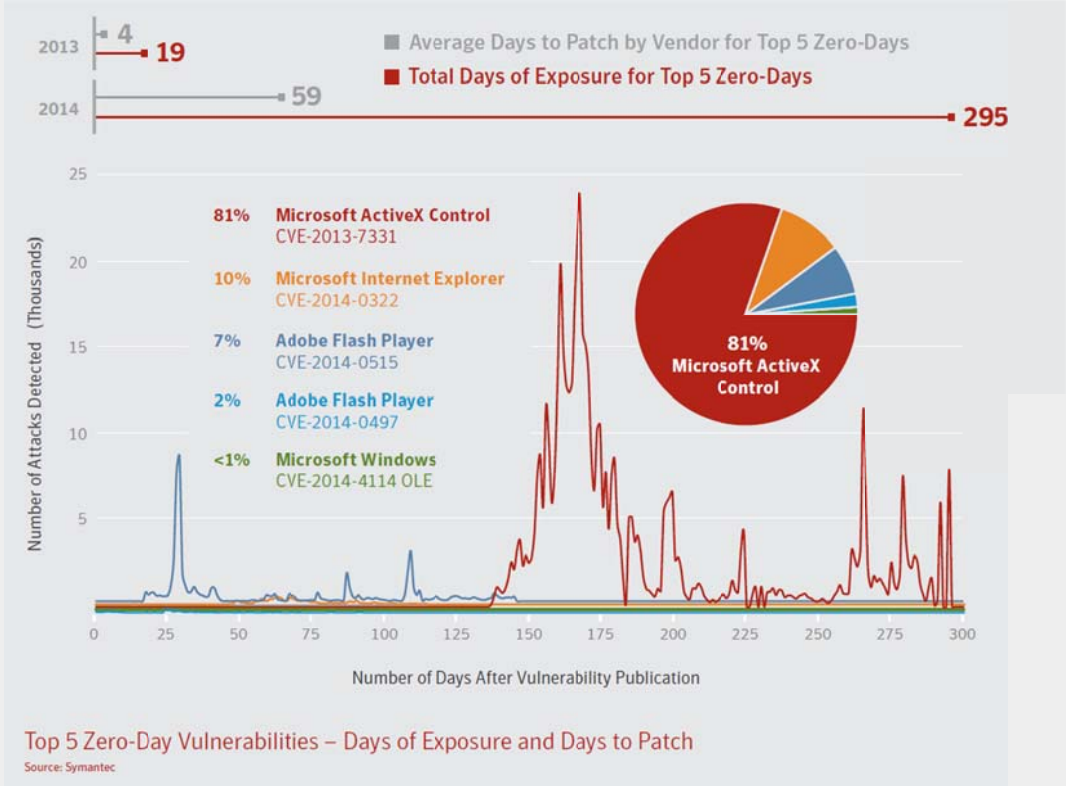
圖8 CVE 公布系統漏洞被利用時間對照統計圖

2.系統漏洞被修補的時間

Symantec 公司針對 2014 年系統漏洞被修補的時間進行統計，發現前 5 名零時差攻擊[5]Zero Day Attack 的系統漏洞在發布後，需要 295 天原廠才提供系統修補。因此電子商務業者須注意，系統原廠對於系統漏洞的修補能力，如果尚未能適當的系

[5] 零時差攻擊： 指駭客針對尚未修補的漏洞進行攻擊

統修補前，應儘速採取其他方式以避免該系統漏洞被利用造成資料的外洩。2014 年前 5 大系統漏洞被修補的統計詳如圖 9 所示。



資料來源： Internet Security Threat Report, Symantec

圖9　2014 年前 5 大零時差系統漏洞被修補的統計圖

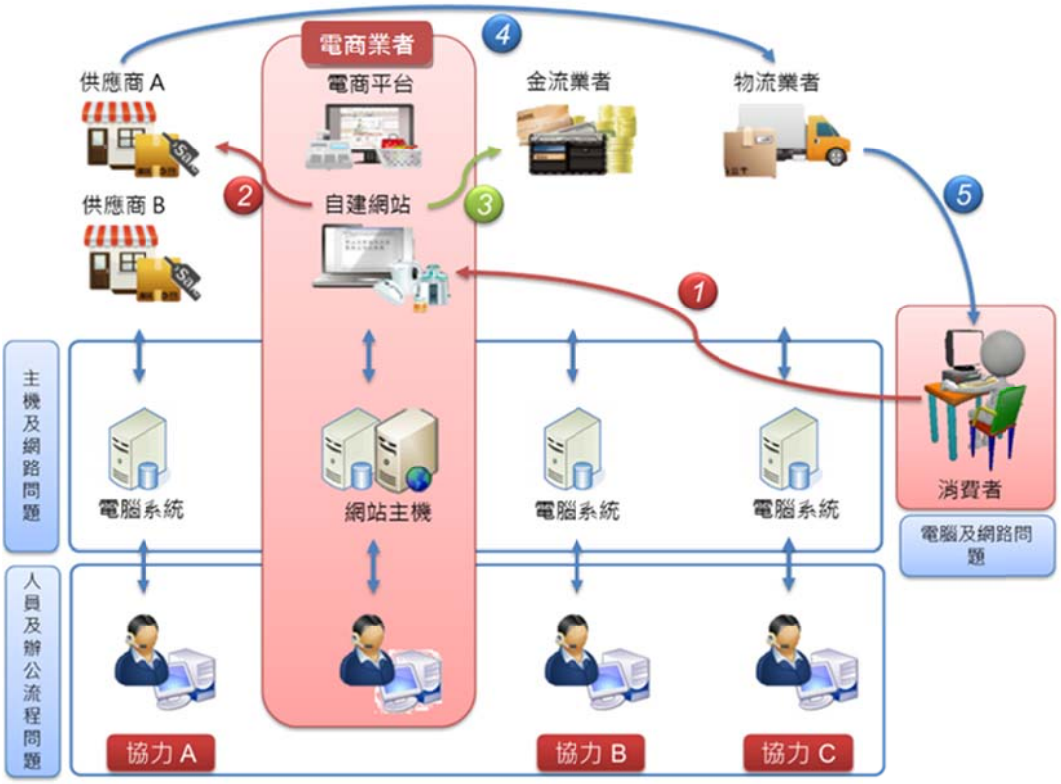
二、電子商務交易流程中資訊流、金流與物流

電子商務業者的特性在於透過系統及網路進行電子商務的交易，其中包括：金流、物流與資訊流，本指引說明如下：

交易過程中，由於包括自消費者與電子商務業者間的資訊流及金流作業，訂購完成後，物流自電子商務業者向消費者端進行。

期間多數電子商務業者廣泛與協力廠商(Third parties)包括金流業者(例如：銀行、第三方支付等)與物流業者(貨運、便利商店)進行合作，部分電子商務業者屬平台業者，故另包含上游供應商，因此電子商務產業的資訊將依使用的合作夥伴與選擇的管理方式而

不同，其交易與資訊流向示意圖詳如圖 10 所示，以下針對電子商務交易環境之問題及弱點進行分析。



資料來源：本計畫整理

圖10　電子商務交易流程與結構化問題分析圖

電子商務交易環境可以歸結為：消費者、電子商務業者及協力廠商 3 種角色並說明詳如表 2 所示。

表2　電子商務交易環境

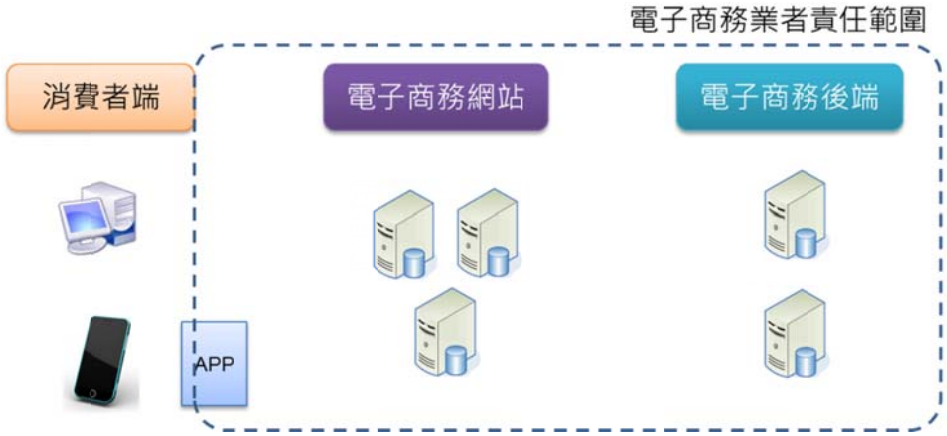
角色	說明	備註
消費者	交易之購買端，提供本身之個人資料及金流所需金融資料給賣方電子商務業者。	
電子商務業者	提供交易商品，維護電子商務交易環境與管理協力廠商。於交易成立後提供產品	

角色	說明	備註
	(有形、無形)予消費者。	
協力廠商	主要為電子商務業者選擇於電子商務交易過程中提供部分交易服務	包括： ▪ 供貨商 ▪ 金流服務業者 ▪ 物流服務商 (備註：由於本計畫以電商業者角度審視個資外洩資安防護相關事宜，因此系統服務、平台服務之協力廠商之角度並不在本指引中進行討論)

資料來源：本計畫整理

三、交易作業環節之安全問題與弱點

由於目前電子商務業者除提供網站服務外，另可能包含提供 APP 軟體供消費者使用，因此電子商務業者的安全防守區與責任範圍應包含到 APP 軟體之安全性，而非僅有網站及內部作業區，其責任範圍示意圖詳如圖 11 所示並說明如下。



資料來源： 本計畫整理

圖11 電子商務業者系統安全責任範圍示意圖

(一)電子範圍

1.前端主機、系統(包括：主機硬體及軟體、OS 作業系統)

(1)網站伺服器(Web Servers)：用於提供電子商務交易服務之網頁服務。

(2)應用程式伺服器(Application Servers)：電子商務交易環境中，提供商業邏輯(Business Logic)、交易流程管控、服務流程之控制伺服器，通常也是主要交易服務程式存放及執行之位置。

(3)資料庫伺服器等(Database Servers)：電子商務交易環境中，提供交易資料之消費者個人資料，及其他電子商務業者商業資訊存放的位置。

(4)檔案伺服器(File Servers)：電子商務業者於管理交易流程中用於存放對消費者或內部管理、交易管理檔案所在之主機。

(5)郵件伺服器(Mail Servers)：提供郵件寄送或內部人員郵件接收之主機。

(6)其他主機：包括名稱伺服器 DNS (Domain Name Server)、日誌紀錄伺服器(Log Servers)及備份設備主機等。

2.電子商務業者後端管理主機、系統

(1)財務管理系統：用於處理交易過程中支付、金額、會計作業等各類用於財務管理之會計系統、財務系統等主機及其應用程式，此類系統可能包含交易資料、信用卡或其他支付方式資料、客戶交易明細等重要資料。

(2)人員管理系統：用於人事行政管理之系統，其中包括：電子商務人員管理作業所需之資料。

(3)客服管理系統：使用於管理客戶交易，提供客戶詢問、處理訂單問題等，此系統將可以進行客戶基本資料之查詢、連接前端系統查詢訂單、交易狀況及產出相關報表等。

(4)客戶交易處理管理：用於交易之管理包括：查詢訂單、出貨及退貨等與客戶訂單處理相關之作業流程使用。

3.消費者端應用系統(APP)

近期，由於行動設備普及，前端交易使用之 APP 軟體係屬於電子商務業者提供消費者使用之訂購工具，APP 軟體並取代電子商務網站，成為第一手接受消費者鍵入資料、付款資訊的起點，因此該APP系統的(裝置於消費者行動設備)之系統安全，應納入電子商務業者之資安管理範圍。

例如：電子商務業者提供 APP 服務供消費者進行商品訂購，或其他服務功能涉及消費者個人資料之使用，請參閱經濟部工業局訂定之「行動應用 App 基本資安規範」。

(二)電子商務安全問題

1.主機及系統問題

由於系統錯誤與惡意與犯罪攻擊佔資料外洩事故的主要原因(76%，依據 2015 Cost of Data Breach Study, Global Analysis Ponemon Institute 之統計報告)，因此交易環境中的電子商務系統安全，是電子商務業者最須要注意的安全問題，電子商務業者可能有的主機、系統問題與資料外洩相關之說明如下：

(1)主機弱點管理問題

由於電子商務系統之前端系統置放於網路接受消費者之連線，因此系統將有部分曝露在對外公開網路上，因此主機之弱點管理，將可能嚴重影響主機之安全。部分統計資料

亦顯示，駭客或其他惡意攻擊透過工具或其他方式隨機攻擊具備弱點之主機。電子商務業者於此部分的管理，通常問題如下：

A.管理人員缺乏足夠能力進行弱點之管理

電子商務業者管理人員未具備足夠能力，導致未能發現所有之弱點，或於發現漏洞時未能有足夠之能力進行補強。

B.缺乏足夠之安全意識

電子商務業者對於安全組織所發布之弱點訊息(例如：CVE)，或經由弱點掃描工具發現之弱點，系統安全人員或主管人員並未予以重視，導致後續未能投入足夠資源或及時進行各項弱點修補。

C.投入不足之經費於弱點管理

部分弱點管理需依賴工具或外部資源，高度安全的弱點管理需要高價的服務，電子商務業者投入的資源(例如：經費)不足時將無法獲得有效的弱點管理成效。部分弱點之補強作業需要耗費許多資源，包括：經費投入及系統改制、暫時停機等，因此電子商務業者於發現、或被通知系統弱點訊息後，仍無法進行系統弱點的補強或修復。

D.未有持續與及時之管理

部分電子商務業者以兼職人員進行弱點管理，但由於未能及時發現或持續對於此項目進行管理，因此未能有效及時的偵測弱點並進行補強，而產生空隙、空窗時間遭受弱點利用攻擊。

(2)系統規劃、建置管理問題

電子商務相關系統(軟體、硬體)於建置、規劃時未配置足夠之系統安全，例如：未有足夠之安全管理功能、配置系統錯誤、系統容載不足(例如：不足夠的儲存空間規劃)等，造成系統配置的弱點或漏洞，導致後續資料外洩。

軟體及 OS 部分，於規劃建置期間，未考慮適合配合組織管理能力與交易需求使用 OS 或軟體，導致後續管理漏洞與軟體能力弱點等。

(3)系統組態管理問題

交易系統之系統組態未依據安全需求進行設定、錯誤設定或因為設定錯誤導致之問題(例如：Directory Traversal、錯誤導向設定，SSL 設定)，組態管理除設定錯誤外，也常見於管理人員之知識或能力不足，導致無法設定系統至安全之組態。

(4)系統程式開發問題

電子商務交易系統由於開發之語言、技術、平台之不同，需要具備高度安全系統開發技術，系統程式開發產生安全漏洞(例如:資料庫隱碼 SQL Injection、跨網站攻擊 XSS)造成應用系統於交易過程產生可被利用的弱點或漏洞，導致惡意人士可以透過程式的漏洞進行攻擊。部分系統開發、程式語言撰寫方式(例如：使用 Get 或於網址使用參數)將資料之存取方式曝露，或於交易過程中揭露交易資訊、個人資料等，導致資料外洩。

另系統開發完成後，未進行源碼審查機制(Code Review)，無法檢查程式碼中產生的錯誤及漏洞，導致系統的錯誤或產生可被利用的弱點，導致資料外洩。

(5)系統存取權限管理問題

交易系統常見包括：消費者帳號、管理者帳號(包括：網站、系統、交易處理人員及客服人員等)或其他協力廠商使用存取權限，常因為權限設定錯誤，存取控管安全等級設定(帳號長度、通行碼長度、定期更換及審查)不安全，或於管理存取權限中允許使用共用帳號等管理問題，導致重要消費者或管理者權限之錯誤，或過於簡單被破解而產生資料外洩問題。

部分系統未更改廠商預設之存取權限，導致系統帳號密碼遭利用，進而產生資料外洩問題。

(6)病毒及其他惡意軟體

部分電子商務業者未建置足夠之病毒、惡意程式之防禦能力或管理病毒碼更新等管理問題，以及部分系統未設置安全防護機制(例如：Linux 系統未安裝防毒軟體)，導致病毒、木馬程式等由外部或內部進行系統攻擊或資料竊取。

電子商務業者未於後端管理系統、作業管理使用系統及個人電腦等建置足夠的病毒、惡意軟體防禦機制，導致入侵或攻擊發生自後端管理及作業環境，進而產生資料外洩。

2.網路管理問題

(1)網路架構設計問題

未依據安全原理進行網路規劃，舉例說明如下：

A.未規劃適當之網路區隔、安全區域(例如：未設置 DMZ 或安全內網區)。

B.未依據各區域之安全等級進行路由之限制(例如：未限制客服作業區連線至非必要存取的內網區，導致其他網路攻擊

之風險、或部分業者提供無線網路於內網區)。

C.錯誤網路架構及規劃致使重要主機設備曝險於高風險網段(例如：忽略或錯誤將重要資料庫置放於 DMZ 區域)。

(2)網路存取權限設置問題

A.網路存取權限設置錯誤，導致部分未授權人員得以進入重要主機管理區域、或低權限等級人員得以進入高度安全需求區域(例如：機房、主機區)、或管理權限開放過於寬鬆，導致網路安全等級降低等。

B.未有效管理網路政策，未進行網路服務之協定(Protocol)之來源、目的地、通訊連接埠(port)等設定，導致外部可進入內部區域，或入侵者可輕易將竊取之資料向外搬移。

(3)未有足夠資通安全設備

電子商務業者經常未設置足夠之資通安全設備，導致安全防禦能力之不足，常見之資通安全設備應包括：

A.防火牆設備(Firewall System)

防火牆設備為主要之安全防禦設備，用來區隔外部與內部網路，並限制資料之進出。各安全區域(例如：主機區、人員作業區)應以防火牆(或路由、交換設備)建立管制機制，以確保各區域之網路安全。

B.路由及交換設備

路由器(Router)及交換器(Switch)為網路基本之管理元件，電子商務業者應依據需求建置相關網路路由及交換設備。

C.入侵防禦系統(Intrusion Prevention System, IPS)

入侵防禦系統用於偵測網路行為、特徵作為判定入侵之依據，並阻絕或告警管理人員可能的入侵事故。

D.網站應用程式防火牆(Web Application Firewall)

電子商務交易系統依賴大部分的網頁、網站程式及系統，網站應用程式防火牆(WAF)可以補強一般防火牆僅針對協定(Protocol)、網路位址(IP)、通訊連接埠(Port)進行管制的弱點，進一步針對被允許的網路流量內容進行過濾，並阻擋針對網站應用程式攻擊。

E.入侵偵測系統(Intrusion Detection System, IDS)

入侵偵測系統透過偵測網路行為、主機行為及特徵作為判定入侵之依據，並依據通報機制進行對於管理人員之告警或記錄相關資訊做為後續事故追查之依據。

F.資料外洩防護系統(Data Loss Prevention)

此類資通安全設備可設置於網路或主機上，針對特定的資料傳輸行為進行與允許政策(Permission Policy)的比對，並於違反政策時進行資料傳輸之阻擋，確保資料不違反政策，以防止被利用或傳輸。

G.其他安全系統

其他安全系統包括:控制網路連線之資通安全設備(例如：NAT 等)，以及網路監控機制，可以確保人員連線、網路存取控制以及建立即時反應之機制。

(4)無線網路之使用

A.無線網路由於其傳輸協定本身的安全問題，以及對於無線傳輸協定的安全規格選擇，電子商務業者經常使用無線網

路於內部管理環境，但疏於進行對無線網路的安全管理，或因為對於無線網路存取控管的鬆散，導致於無線網路傳輸的資料遭側錄或被竊取。

B.無線網路由於其無法有效控管邊界(Boundry)，導致惡意人士可以於實體環境外存取，或以技術機制破解電子商務業者已實施安全管控的無線訊號，而導致惡意人士得以於外部存取內部網路區域，或藉以攻擊使用無線網路之內部使用者。

C.人員使用未授權的無線網路機制，由於手機設備目前可以設定成為無線設備，電子商務業者之內部人員如果使用未授權(未安全管制)的無線網路(例如：於內部開通無線上網服務，並可連上組織其他設備)，將造成內部原有安全控管機制遭破壞而導致外部入侵、因使用該未授權之無線網路(未有安全管控)而導致傳輸資料遭惡意人士竊取之可能。

(5)網路設備組態設定問題

網路設備除須依據安全架構(Secure Architecture)進行設置外，對於網路設備的組態安全更須注意，不安全的網路設備組態，經常導致該網路設備本身被攻破、入侵或無法發揮安全控管之功能，致使網路產生弱點、漏洞進而產生入侵及資料外洩之可能。

(6)遠端登入或遠端管理(Remote Login and Management)

電子商務業者充分使用網路進行各項管理，常見於網路設備端或交易系統所提供遠端登入之機制，遠端登入由於常伴隨非組織管制之設備(例如：私人電腦、公共電腦)因此容易產生帳號、通行碼遭惡意人士或機器側錄或破解之可能。因此電子商務業者若必須使用遠端登入，應搭配相關安全機

制(例如：使用雙因子機制、OTP 一次性密碼)搭配原有之帳號、通行碼管制以確保遠端登入之安全。

(7)使用不安全的網路協定

部分網路之協定(Protocol)，例如：FTP(檔案傳輸協定)、Telnet(終端模擬協定)等，使用明碼傳輸登入過程所需要的帳號及通行碼、或協定本身傳輸資料時並未進行安全管控，以致可以側錄監聽其網路傳輸內容或帳號、通行碼，如果電子商務業者於組織內部或外部允許使用非安全協定，將產生極高之風險。

3.人員問題

電子商務作業環節涉及之相當多的內外部人員(例如：客服人員、作業員、業務人員及資訊人員等)，人員之行為可分為故意或疏失行為而導致相關資料外洩問題如下：

(1)蓄意行為

A.員工或內部工作人員蓄意竊取業務經手之客戶資料、交易細節，並向外提供或為自我非法之利益而利用電子商務業者資料。

B.員工為自我目的或利益進行或協助他人進行電子商務業者之客戶或交易資料。

C.員工或內部人員蓄意破壞組織之安全機制、資料或協助外部惡意人士提供管道、漏洞資訊等惡意行為。

D.員工違反組織規定使用自我設備、連接網路或存取未授權之資料導致資料外洩。

(2)非蓄意行為

A.作業疏失，員工或內部人員於作業流程中因疏失或非蓄意行為產生資料、系統錯誤或錯誤交付資料等。

B.員工因安全意識之不足，遭社交工程、點選釣魚郵件或惡意網站導致系統被入侵或引入病毒等惡意程式。

C.員工因使用帳號、通行碼疏於防範，導致帳號、通行碼遭竊，或與他人共用帳號、通行碼而產生資料外洩之風險。

D.員工於進行資料傳輸、郵寄(紙本、或電子格式)期間因疏於管控或作業疏失導致資料外洩或遭竊取等。

E.技術人員因未遵循安全開發作業流程，導致在程式撰寫或上版作業中，因未能檢查出之系統漏洞而造成個資外洩問題。

(3)BYOD (Bring Your Own Device)自有設備使用

部分電子商務業者允許或未管制員工使用私人之電腦、手持或其他終端設備及網路設備等，連接入電子商務作業環境、網路或系統，由於該等設備未有足夠或組織規範之安全管制，常因設備之安全問題導致帳號、通行碼遭盜用、惡意程式竊取或破壞組織資料或引入病毒等惡意程式。

(4)員工安全意識及安全保護知識、技術

A.電子商務業者如未提供適當之訓練、認知建立員工或內部人員足夠之安全意識，員工常因疏忽造成非蓄意的資料外洩或遭受外部之惡意攻擊(例如：社交工程、惡意網站及病毒)而造成資料外洩。

B.員工、內部人員或系統、網路管理人員如未有足夠之安全防禦技術及知識，將無法建立、設定、維運及監控電子商

務交易系統及網路環境之安全機制，因而產生弱點、漏洞或因管理疏失而導致資料外洩。

4.資料及資料庫安全管理問題

(1)資料庫安全管理

電子商務業者建立之資料庫含有大量的消費者個人資料及交易資料，資料庫系統本身需要高安全性的管理，包括：

A.資料庫系統安全組態之設置：不安全的資料庫系統安全組態設計，將導致資料庫系統本身之安全弱點及漏洞遭致惡意攻擊之利用。

B.資料庫存取權限管理：不足夠之資料庫存取權限，將導致系統程式、管理人員、程式開發人員等得以藉權限為由，進行對於資料的授權或非授權存取。

C.資料庫設計(Schema)：錯誤的資料庫規劃(DB、Table、Field)將導致系統錯誤的存取或意外的揭露，因而產生資料外洩。

D.資料存取紀錄：資料庫應建立人員、作業與資料存取之關聯性管理，並留存適當之存取紀錄，並由關聯性、存取紀錄進而能判定或預防非法之存取，有效的紀錄更可以協助事後的調查及作業的修正；若未能有效建立資料存取紀錄將導致系統未能於事後追查、或於事前預防未授權的存取或攻擊。

(2)資料安全

電子商務業者之消費者個人資料或交易資料，除集中存放於資料庫外，尚可能出現於下列位置：

A.以檔案形式存放於主機或個人電腦(例如：人員製作之報表、系統產出之檔案、報告檔)。

B.各類 Log 檔：交易應用系統 Log、付款閘道器 Log、資通安全設備 Log (Firewall, WAF.....)、網頁伺服器 Log。

C.歷史檔案：各類由交易應用系統、管理系統、資料庫系統產出之歷史檔案、郵件寄、收支歷史檔案。

D.軌跡資料(Trail files)：系統因管理或安全目的產出之軌跡資料檔。

E.作業交換及交換過程產出之檔案：系統於例行、或臨時產出的交換作業檔案，或於交換過程間產出之檔案。

F.錯誤過程產出之檔案：系統於進入偵錯(Debug)模式產出之檔案或系統當機產出之傾印(Dump)檔。

G.備份檔案：資料之備份檔案，以及因為虛擬化技術或備份作業產出之系統影像檔(System image, Snapshot file)。

針對以上可能出現消費者個人資料或交易資料之可能位置、檔案，電子商務業者應進行管理或定期檢視，以確保資料未被遺漏或未管制而導致後續資料外洩。

5.環境管理問題

電子商務整體環境除前述針對系統、網路、人員、資料等管理問題，尚有對於電子商務實體環境以及作業環境之安全管理問題，例如：電子商務業者作業包括與其他協力廠商之合作，應包括與協力廠商合作之方式、介面等管理問題：

(1)實體安全管控

電子商務業者作業中包括許多作業設備(包含資料之設

備)、電子檔案(儲存媒體、系統)、紙本表單、產品包裝之客戶資訊等，須進行實體之安全管控。

A.設備安全管控

對於存放消費者個人資料、交易資料之設備或系統：

a.主機設備。

b.資料庫系統。

c.個人電腦及終端設備(桌上、筆記型電腦、點貨終端設備)。

d.列印設備(印表機、影印機等設備)。

e.電信設備(如交換機、電信設備)。

應建立安全管制區域(如機房、作業區)並進行管制，未有足夠的實體安全防護機制，管制授權人員進出，將導致設備之遭竊取或遺失等情事。

B.儲存媒體

電子商務業者將消費者個人資料或交易資料存放於媒體，例如：

a.可移除式媒體：USB、外接硬碟機等。

b.光碟、磁帶等儲存媒體。

由於此類儲存媒體均為可攜帶或高度移動性，未有足夠之安全管制，包括：安全存放、紀錄、盤點以及存取控制將導致資料儲存媒體遭竊取或進行未授權之存取。

儲存媒體於運送過程應進行適當之遮蔽保護，並以專人或可信賴之傳送機制(例如：掛號等可追蹤之機制)，重要資料傳送並應配合加密機制之實施，以避免資料遭竊取

或被非法存取。儲存媒體遭竊或遺失為過去資料外洩之主因之一。

C.列印設備

部分列印設備設置於公共區，其列印未有適當之管制，導致非業管人員能窺視或竊取列印之資料。列印設備部分具備儲存功能，應於該等設備移除、汰換、送修前應將內部儲存資料消除，以避免資料外洩。

D.電信設備

電信設備除可能存放消費者聯絡資訊外(例如：Log)，亦可能有被竊聽、側錄之風險，應定期進行檢查並設置防禦機制，除內部之電信設備外，應注意大樓電信機房等可能被竊聽或側錄之位置安全。

(2)實體進出管制

電子商務業者除應建立進出管制、人員識別及資料應保存適當之時間，若未能有效管制或記錄，將造成後續追查困難。

(三)電子商務作業環節可能存在之安全弱點

綜合上述之管理問題，電子商務業者應於下列所列出之安全弱點區域及項目，進行相對應的弱點管制(詳如表 3 所示)，以防範惡意攻擊或人為蓄意或非蓄意的行為導致資料外洩。

表3　電子商務交易流程及可能問題點分析

編號	起點	終點	說明	資訊	可能弱點
1	消費者	商家	消費者上網，選購產品及輸入消	▪消費者資料 ▪交易金	▪消費者本身電腦或網路問題。 ▪電子商務網站系統及網路

編號	起點	終點	說明	資訊	可能弱點
			費者資訊及交易資訊	流資料	安全。 ▪電商業者人員及環境安全。
2	商家	供應商	商家將資料轉給供應商，由供應商直接出貨	消費者訂購資料及送貨資訊	▪電商業者人員及環境安全。 ▪供應商系統及網路安全。 ▪供應商人員及環境安全。
3	商家	金流業者	商家將交易資料轉給金流業者	交易金流資料	▪金流業者系統及網路安全。 ▪金流業者人員及環境安全。
4	供應商	物流商	物流商至供應商取貨寄送	消費者送貨資料	▪供應商系統及網路安全。 ▪供應商人員及環境安全。 ▪物流商系統及網路安全。 ▪物流商人員及環境安全(包含司機)。
5	物流商	消費者	物流作業	消費者送貨資料	▪物流商系統及網路安全。 ▪物流商人員及環境安全(包含司機)。

資料來源：本計畫整理

(四)個資外洩管理問題對照

除本指引前段所分析之資料外洩可能之成因外，針對電子商務實體運作過程以及電子商務作業特性，將依據不同類型之管理問題可能發生資料外洩問題對照列表詳如表 4 所示。

表4　個資外洩管理問題對照

問題 / 角色		系統	網路	人員	資料	環境
消費者		☑	☑			
電子商務業者		☑	☑	☑	☑	☑
協力商	供應商	☑	☑	☑	☑	☑

問題 角色		系統	網路	人員	資料	環境
	物流商	☑	☑	☑	☑	☑
	金流業者	☑	☑	☑	☑	☑

資料來源：本計畫整理

參、主要資料外洩過程分類說明

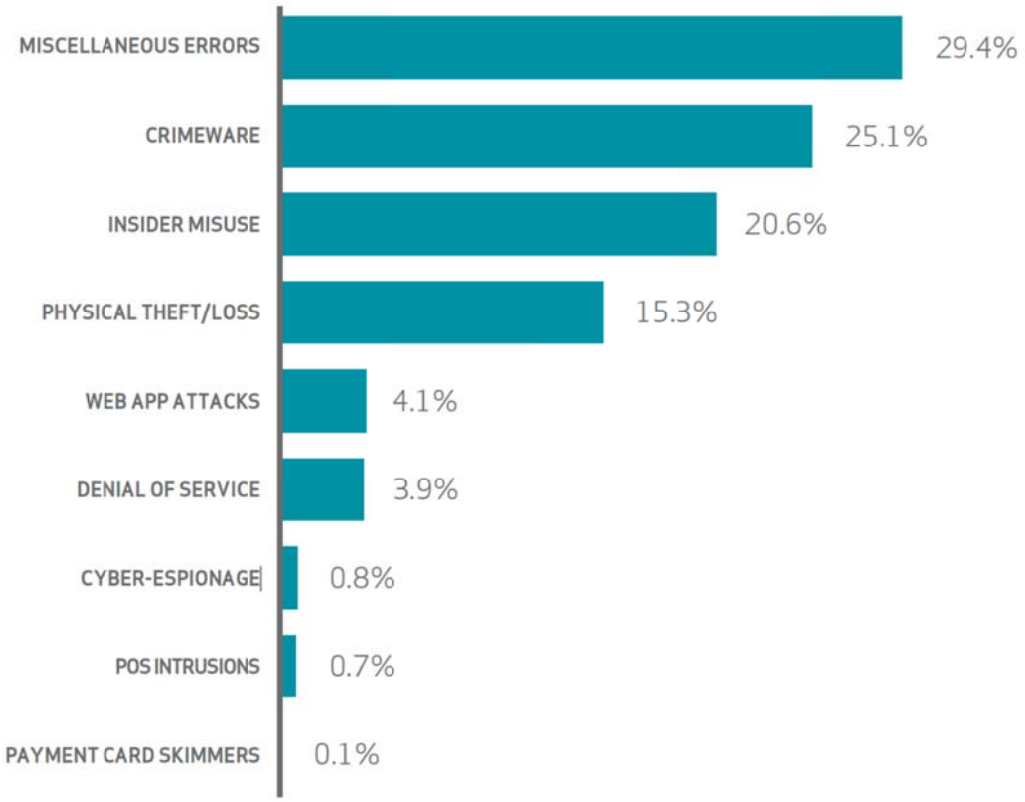
本章主要針對電子商務消費者個人資料及交易資料可能的外洩事故成因分類，進行其類型、行為的說明，以利後續建立管制與防護機制。

依據本指引之資料外洩主要成因分析，可以分為三大分類：1.惡意或犯罪攻擊(Malicious or Criminal Attack)、2.系統錯誤(System Glitch)、3.人為錯誤(Human Error)。

依據國際電信通訊公司(Verizon)對於資安事故之統計，資料外洩事故發生的統計依據其資安事故分類可歸類於以下九大主要分類，分析統計詳如圖 12 所示。

- 其他類錯誤(Miscellaneous Errors)。
- 犯罪軟體(Crimeware)。
- 內部錯誤使用(Insider Misuse)。
- 實體遭竊或損失(Physical Theft/Loss)。
- 網站應用程式攻擊(Web Application Attacks)。
- 拒絕服務(Denial of Service)。
- 網路間諜活動(Cyber-Espionage)。
- 收銀系統入侵(POS-Intrusion)。
- 支付卡側錄(Payment Card Skimmer)。

其中除第 1 項綜合人為錯誤及系統錯誤，以及第 9 項支付卡側錄屬於實體攻擊外，其餘均屬於本指引分析三大分類之惡意或犯罪攻擊之領域。



資料來源： 2015 Data Breach Investigation Report, Verizon

圖12 國際電信通訊公司(Verizon)分析資料外洩事故分類統計圖

一、惡意或犯罪攻擊(Malicious or Criminal Attack)

依據本指引前段之統計資料分析結果，兩種分類方式之結果均指向惡意或犯罪攻擊係屬資料外洩中最主要及最頻繁之類型，其中不論其意圖屬一般攻擊或犯罪攻擊，本指引以下以「駭客入侵」或「駭客攻擊」說明「惡意或犯罪攻擊」項目：

(一)常見的惡意攻擊的資安事故分類

依據統計 96%以上資料外洩攻擊手法均可以歸類為以下分類[6]

1.各類錯誤(Miscellaneous Errors)。

2.犯罪軟體(Crimeware)。

[6] 2015 Data Breach Investigation Report, Verizon

3.內部錯誤使用(Insider Misuse)。

4.實體遭竊或損失(Physical Theft/Loss)。

5.網站應用程式攻擊(Web Application Attacks)。

6.拒絕服務(Denial of Service)。

7.網路間諜活動(Cyber-Espionage)。

8.收銀系統入侵(POS-Intrusion)。

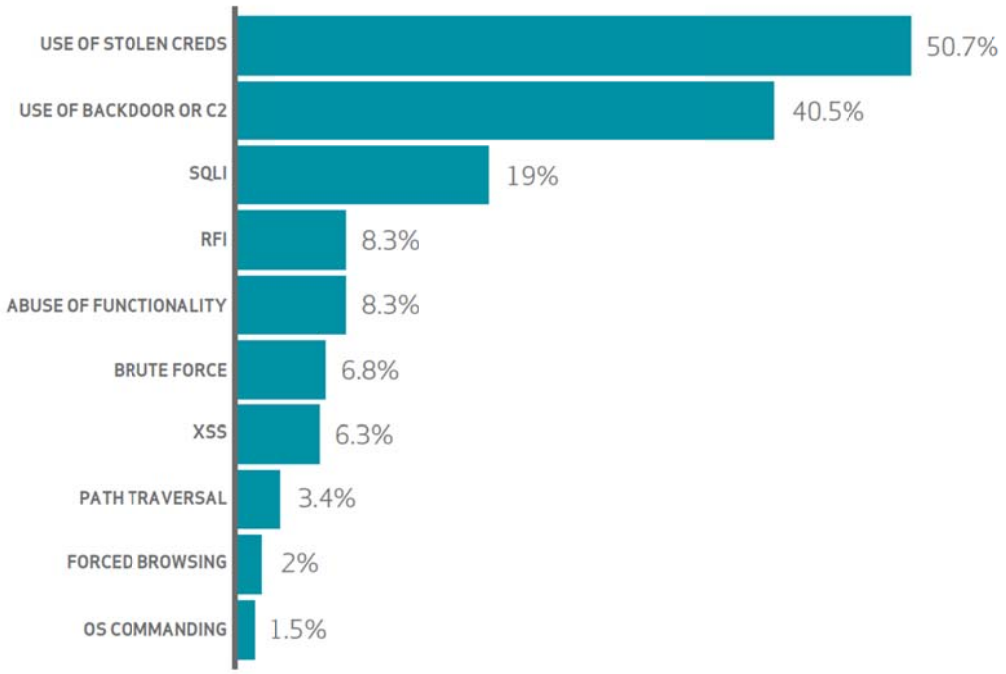
9.支付卡側錄(Payment Card Skimmer)。

其中第 1 類的「各類錯誤」及第 4 類「實體遭竊或損失」包括：員工及系統錯誤導致，將於後續「人為錯誤」及「系統錯誤」之章節進行說明，第 6 類「拒絕服務」由於不涉及資料外洩，將不在本指引的討論，其餘各類將被歸類「惡意或犯罪攻擊」(本章節)範疇。

(二)惡意攻擊常見步驟說明

1.網站的攻擊

由於電子商務業者主要的服務窗口為網站，因此網站的攻擊為最主要的惡意攻擊類型，依據國際電信通訊公司(Verizon)之調查，網站部分的攻擊經統計詳如圖 13 所示並將主要成因說明如下：



資料來源： 2015 Data Breach Investigations Report, Verizon

圖13　國際電信通訊公司(Verizon)調查網站攻擊類型統計圖

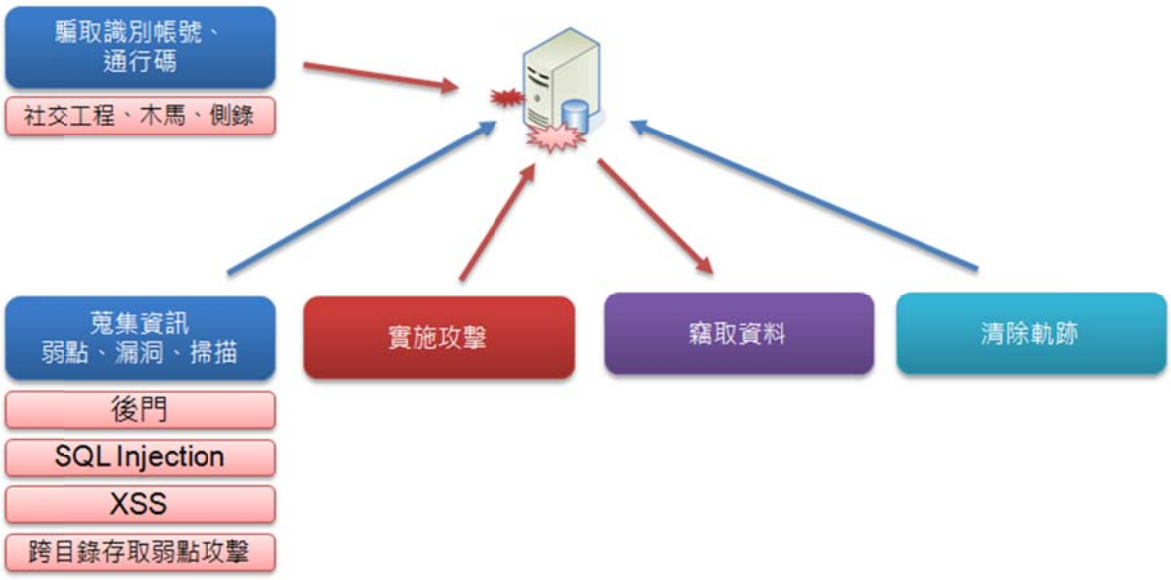
(1)使用竊取的識別帳號資料：網站攻擊的類型中，最主要還是惡意攻擊者先取得被害者或被害網站的識別帳號資料，進而登入網站竊取資料。手法包括：使用社交工程、木馬、側錄等各類型可能的攻擊手法。

(2)透過網站主機、系統的後門漏洞對網站進行控管，竊取資料。

(3)透過網站的漏洞，例如：最常見的資料庫隱碼 SQL Injection、跨網站攻擊 XSS 等手法進行資料竊取。

(4)另外主機設定錯誤所致之跨目錄存取弱點攻擊，因為未設定主機目錄瀏覽的保護，因此機密資料可透過瀏覽目錄方式，直接或透過取得部分系統資訊、程式內容進而竊取資料。

2.惡意攻擊一般流程說明，示意圖詳如圖 14 所示。



資料來源：本計畫整理

圖14　惡意攻擊一般流程

(1)竊取識別帳號、通行碼

惡意攻擊人士透過各類方式，例如：

A.社交工程(Social Engineering)。

B.釣魚(Phishing)。

C.側錄(Sniffing)。

D.中間人攻擊(Man-in-the-middle-attack)。

E.植入惡意程式或木馬程式至使用者電腦。

F.部分網站主機、資通安全設備、管理網頁由於帳號、通行碼使用預設值(Vendor default)，因此相當容易被利用。

G.網站設定之通行碼過於簡單或使用懶人通行碼等。

H.網站未設定防止機器人之安全機制，透過暴力破解(Brute-force)方式進行帳號通行碼破解。

因此防止資料的外洩，利用被竊取的帳號密碼佔整體事故的 50%以上，因此除了主機、網路的安全防護，人員的資安意識、安全防護更為重要。

(2)蒐集資訊(弱點、漏洞、掃描)

A.蒐集各類的主機、人員資訊的弱點

惡意攻擊於攻擊前均會對攻擊目標進行系統資訊的蒐集，例如：透過 Google 等搜尋引擎蒐集各類的主機、人員資訊，包括：

a.主機數量。

b.主機名稱。

c.網站進入點、後台系統進入點。

d.管理人員帳號、email。

e.系統使用軟體、硬體、網路設備等相關資訊。

B.透過工具進行掃描

由於電子商務網站多半對外開放，因此透過工具進行遠端的掃描作業可以得到更多的系統資訊，包括：

a.網站及各類主機數量使用 IP 等。

b.網站使用連接埠、協定(Port, Protocol)。

c.網站系統使用 OS、網站系統版本、應用程式版本等。

d.資通安全設備類型。

C.蒐集系統漏洞資訊及可以利用的攻擊方法

a.在蒐集完相關資訊後，可以依據網站主機目前使用的 IP，協定(Protocol)、連接埠(Port)、服務(Services)進行初步研

判，判斷是否有未關閉、不安全(in-secure)協定使用等可以利用的方式。

b.依據網站使用的資通安全設備，研判攻擊進入的路徑、方法。

c.依據網站主機、相關主機目前使用的作業系統、網站軟體、其他服務的軟體(例如：FTP Server)，進行訊息弱點、漏洞及攻擊工具的資訊蒐集(例如：透過 CVE 資料庫進行資訊蒐集)。

(3)進行攻擊

依據蒐集得到的資訊，進行攻擊作業，入侵主機，包括：

A.使用竊取的識別資料例如：帳號進行登入嘗試，例如：以取得帳號、通行碼(password)直接登入。

B.透過登入的帳號，透過攻擊方式取得較高之權限，或透過該帳號進行其他帳號之竊取。

C.透過系統的弱點進行攻擊，例如：

a.資料庫隱碼攻擊(SQL Injection)。

b.跨網站指令碼攻擊(XSS)。

c.跨目錄存取弱點攻擊(Directory Traversal)。

d.透過網站軟體、使用工具的弱點、後門進行入侵。

e.透過已滲透進入組織的木馬程式、惡意程式，或透過以控管的內網系統進行網站之攻擊。

(4)竊取資料

一般而言，惡意攻擊者在入侵網站主機、或相關服務主機後會開始進行資料的竊取，包括：利用該主機進行正常的讀寫、尋找資料檔案或其他管理帳號、通行碼等以進行資料

的讀取。

如果系統內的資料庫主機遭入侵，則資料又未經過加密處理，則資料將被直接竊取。惡意入侵後的資料竊取常見手法如下：

A.進行資料搬運，透過工具(例如：FTP、email 或其他網路工具)將資料進行搬運出主機至指定之區域,通常為了避開資訊資通安全設備(例如：DLP 等)之監控，可能還會將資料處理為加密封包或分散切割成更小資料封包方式，已達成竊取目的。資料搬運的終點一般也會透過多個網站、公共空間或其他受害主機以躲避追查。

B.部分惡意攻擊會在主機留下後門、木馬之類的惡意程式以利後續進入，並調整系統主機安全設定或於系統後端直接建立可信任之帳號，後續便可自網站外部直接竊取資料。

(5)清除軌跡資料

惡意攻擊在成功達成竊取資料之目的後，會進行相關軌跡之清除，經驗豐富的攻擊者通常在入侵後立即進行各項安全 Log 的停止以避免被追蹤記錄或因而觸發其他的警訊裝置。

於成功竊取資料後，惡意攻擊者會清除可能留下軌跡之處，清除紀錄的系統 Log，移除攻擊期間使用的各種工具或帳號等，避免後續遭到追蹤；或透過清除各類軌跡使網站擁有者無法得知系統曾經被入侵或攻擊，可延長竊取資料期間。

二、系統錯誤(System Glitch)

系統錯誤常見的類型包括：

(一)硬體設備、軟體設備發生故障

由於系統故障時，部分組織為求持續營運，使用備援或關閉部分資通安全設備繼續進行相關服務，由於未有完整之安全機制，因此容易因為系統漏洞或防禦不足而產生資料外洩。軟體系統部分出現錯誤時，有時導致系統進行記憶體 Dump 而該檔案內包含各種資料，因而造成資料外洩。

(二)錯誤系統設定

另一類的系統問題，來自管理人員因為經驗、知識不足或疏忽設定錯誤的系統組態導致之系統錯誤或漏洞，例如：

1.錯誤設定檔案之分享、權限設定錯誤。
2.網站主機的錯誤處理(Error Handling)，導致網站系統發生錯誤時顯示系統內部敏感資訊或程式碼等資訊。
3.錯誤開啟或未關閉跨目錄存取(Directory Traversal)。
4.設定連線時，誤用了不安全的協定(例如：FTP、Telnet 等)。
5.常見的系統設定錯誤，包括：設定 FTP Server 但選取匿名者登入(Anonymous Login)功能，使得該系統之 FTP Server 不需要取得通行碼就可以登入。
6.防火牆等資通安全設備組態設定錯誤，導致網路安全及防護降低或失效，亦會造成資料外洩問題。
7.設置系統預設帳號及密碼過於簡單或容易猜測(例如：admin/123456)，導致外部惡意攻擊者可以推測出帳密並登入。

(三)程式設計錯誤

系統程式設計錯誤常見於電子商務及各類型組織，例如：

1.程式錯誤使用資料欄位導致網頁出現使用者資料。
2.使用不安全的程式編寫指令，例如：使用 Get 等方式於網址欄

傳送資料等。

3.程式設計錯誤導致將消費者信件寄送給他人，或錯誤迴圈設計導致同地址寄送多份其他人之個人資料等。

三、人為錯誤(Human Error)

依據國際組織調查，62%的員工認為在公司以外的場合使用公司資料是可接受的，其中多數員工使用資料完畢後並不會將資料進行刪除[7]。

(一)常見的人為錯誤造成資料外洩

1.將資料錯發給不對的接收者。

2.將資料不小心公布於外部網路導致外洩。

3.人為疏失導致系統傾印資料。

4.運送資料備份媒體中遺失。

5.於組織外部使用資料時遭竊取。

6.個人電腦存放組織相關資料，遭惡意程式或病毒入侵後竊取。

7.個人對於帳號與通行碼之管理或保管不當。

(二)資料外洩事故衝擊說明

資料外洩事故可能會造成組織許多的衝擊，以及後續的賠償，往往電子商務業者在事故前並未確實瞭解事故的衝擊大小，導致沒有積極建立足夠的事前防禦，或者在資料外洩後未重視並預防衝擊的擴大。

1.資料外洩可能的衝擊

資料外洩所造成的衝擊大致可分為：

[7] 2013 Cost of Data Breach Study： Global Analysis, Ponemon Institute

(1)金錢損失

資料外洩造事故衝擊組織需對於受害消費者進行賠償、因為資料外洩遭受主管機關的罰款、或因為服務中斷而造成的直接業務損失。

(2)後續業務或客戶流失

通常在資料外洩後，組織除直接的商譽損失外，衝擊於後續發酵並造成消費者採購該組織服務的意願降低，訂閱客戶或會員數的降低等，造成後續的業績下滑。

(3)處理成本

A.事故後需要進行消費者通知(依據信用卡收單合約規定或依據個資法等)，如果外洩的資料筆數眾多，公告和逐一通知消費者需要一定的成本。

B.後續協助消費者進行資料變更(例如:更換帳號)、變更密碼等。

C.進行系統復原、服務恢復等成本，例如：資料外洩涉及系統攻擊，將該因為攻擊產生的問題(例如：後門植入、資料被竄改等)需要各類技術人員或服務協助處理需要一定成本。

D.如需要進行鑑識、數位內容保存需要其他技術專家、服務的成本。

E.涉及訴訟當地法律顧問、律師費用等。

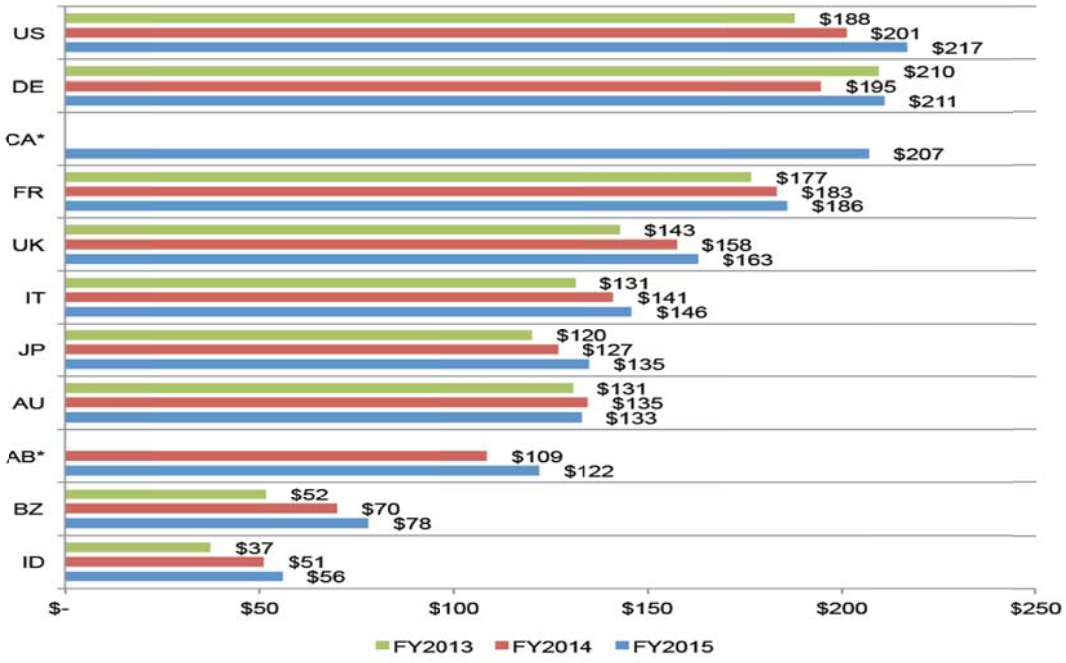
F.透過稽核作業進行對於內部的作業進行檢視之稽核作業成本。

G.聘請各類顧問，包括：技術顧問、安全顧問或管理顧問等進行系統或服務流程之改善。

H.部分資料外洩事故涉及內部人員之問題，必須針對人員進行其他的訓練補強等訓練成本。

2.資料外洩的損失

國際組織 Ponemon Institute 進行對於資料外洩成本的分析中，表示 2013~2015 年間調查顯示，資料外洩平均成本金額詳如圖 15 所示。



資料來源： 2015 Cost of Data Breach Study, Phonmon Institute

圖15 國際組織調查，每筆資料外洩成本金額(單位：美金)

肆、個資外洩資安防護的參考標準

應如何防止消費者個人資料以及交易資料外洩呢？依據統計、資料處理過程分析，可找出個資外洩發生的原因及可管理的控制點，進一步進行防護及控制，事前的防禦永遠是安全手段中成本最低的作法。本指引除分析資料外洩的成因與過程外，透過本章節介紹國際、產業標準/規範，及其他關於資料保護的參考資源，並將資料外洩資安防護的整體作業分為事前防禦、事中應變及事後處理等三個面向，以利電子商務業者能夠依序參考並進行預防及解決問題，示意圖詳如圖 16 所示。

資料來源：本計畫整理

圖16 個資外洩資安防護三個面向示意圖

本指引參考國際及產業標準/規範，藉由引用或參考國際及產業標準/規範，使電子商務業者可以使用標準的作法，另外可以作為本指引之延伸。電子商務業者如果有需要進一步的實施全面性的安全措施，也可以經由參考以下本指引所參考之國際及產業標準而建立全面性的安全保護作業。本指引參考及介紹範圍，包括：

- 國際標準，例如：ISO 標準等。
- 產業標準/規範，例如：PCI DSS 支付卡產業標準、電子商務(B2C)交易安全規範(包括：網路平台、供應商及物流商)、電子商務資訊安全機制與管理規範(中小企業版)。
- 最佳實務(Best Practice)：由各安全組織研究發表，例如：SANS 組

織。

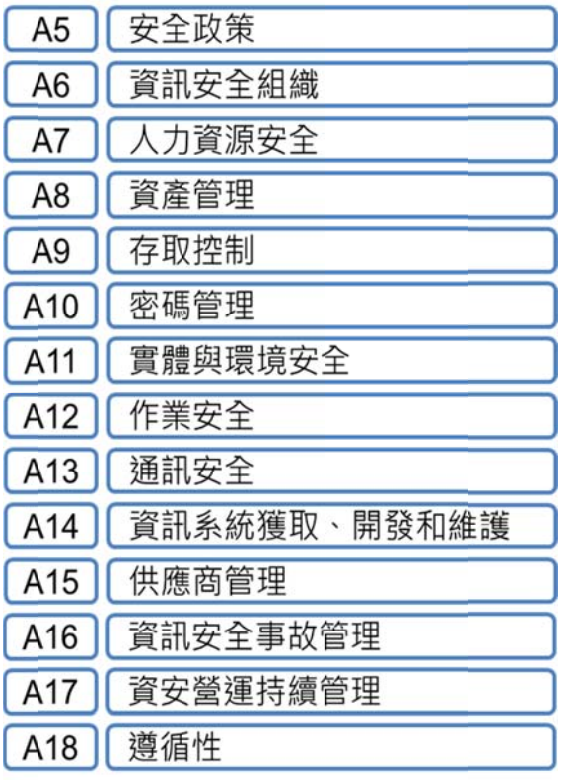
- 企業規範：部分企業例如：VISA、Master 等組織，發表的相關安全規定。

一、國際標準 ISO/IEC 27001 版

ISO/IEC 27001 Information Security Management System 為目前國際上最多組織使用於資訊安全管理的管理系統。

(一)ISO/IEC 27001 與本指引之搭配

ISO/IEC 27001 將資訊安全管理分為十四個領域，作為組織維持資訊的機密性、完整性與可用性的標準，詳如圖 17 所示。



資料來源：本計畫整理

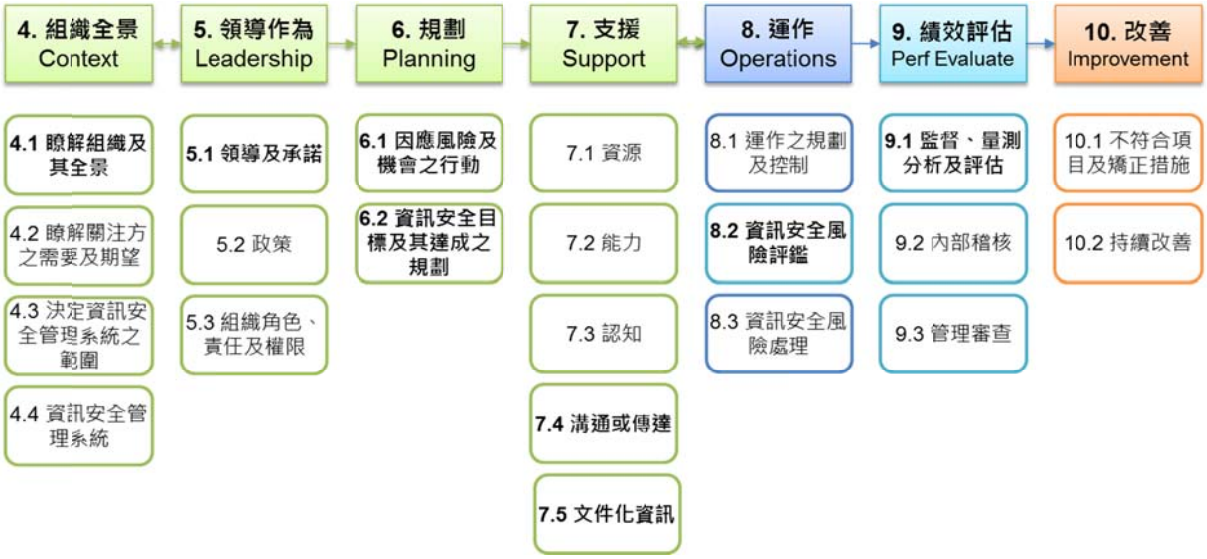
圖17 ISO/IEC 27001 資訊安全管理領域(14 個)

本指引將參考引用 ISO/IEC 27001 之各項管控措施於「事前防禦措施」的各項預防作業，以及運用 ISO/IEC 27001 於資訊安全事故管理的框架及要求於「事後處理措施」中。

(二)ISO/IEC 27001 的管理制度參考

ISO/IEC 27001 與本指引參考的其他國際標準或產業標準最大不同的點在於 ISO/IEC 27001 提供一個管理制度的框架，依據 PDCA 的作業，與透過管理機制來讓資訊安全管控作業能夠上軌道並持續有效。以下為 ISO/IEC 27001 的管理框架說明(詳如圖 18 所示)。

組織於應用本參考指引同時，也可進一步藉助 ISO/IEC 27001 的管理系統框架建立組織完整的管理制度，能夠更完整的強化整體資安管理體系。

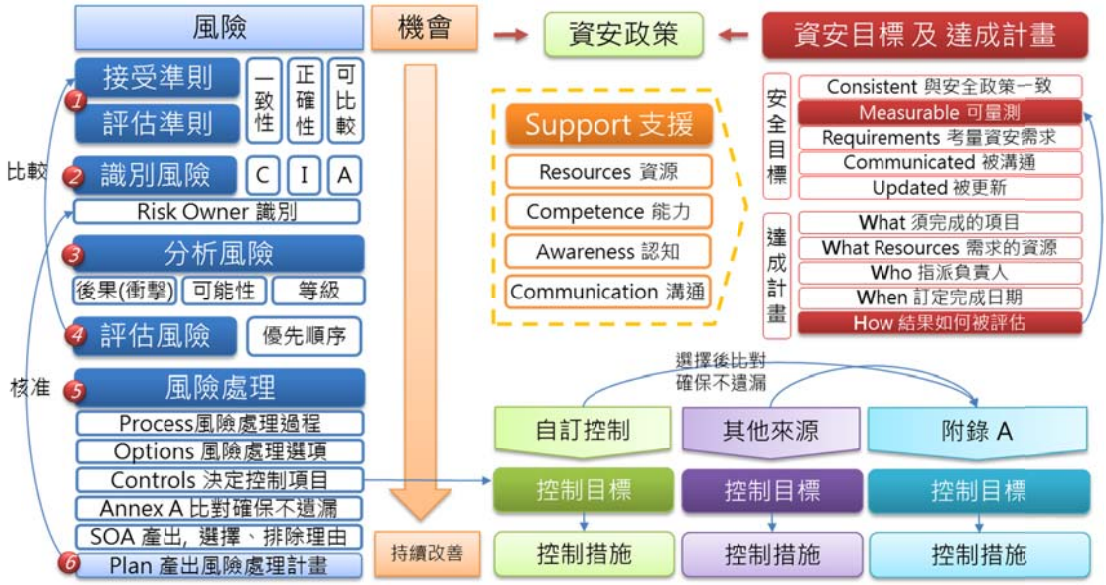


資料來源：本計畫整理

圖18 ISO/IEC 27001 管理系統框架

(三)ISO/IEC 27001 的風險評鑑與風險管理

此外 ISO/IEC 27001 也提供一個風險評鑑的方法論，以及風險處理的管控建議(於該標準的附錄 A 中)，整體 ISO/IEC 27001 與風險評鑑方法之架構示意圖詳如圖 19 所示。



資料來源：本計畫整理

圖19 ISO/IEC 27001 與風險評鑑方法架構

其中電子商務業者對於消費者個人資料或交易資料的保護，本指引僅能依據國際組織統計分析之結論提示可能的成因與風險，並無法於本指引提供全面性、針對使用者組織的風險提示。因此如電子商務業者需依據自我現況進行更全面的風險評估，ISO/IEC 27001 具備高度成熟的風險評鑑要求可以協助組織進行全面性的風險評鑑。

ISO/IEC 27001 所提供之風險管理過程實施之步驟如下：

1.依據組織的特性及目標提出風險評鑑及風險接受的準則，以作為後續風險評鑑過程評估及接受依據。

2.依據評鑑準則進行組織內風險的識別，並建立或指派風險擁有者，須確保風險管理責任被指派。

3.依據風險及風險實現時可能的潛在後果分析風險、風險發生的可能性決定風險等級。

4.將決定之風險等級與原訂之風險接受準則進行比較，並產出風險分析結果以及風險處理的優先順序。

5.依據風險評鑑結果，進行風險處理，可由 ISO/IEC 27001 標準(參

考該標準之附錄 A 控制措施)或其他業界標準等方式進行資訊安全風險的處理。

6.產出風險處理計畫，並依據該計畫實施，組織應進行對於風險處理計畫的監視以及審查，確保風險有效控管。

透過風險評鑑過程所識別出的風險，也可以進一步的與本指引之事前防禦措施章節，所提示的控管措施進行整合及補強，以強化本指引未能依據個別組織客製化相關管控措施之不足。

(四)ISO/IEC 27005：2011 資訊安全風險管理標準

ISO 組織於 2008 年提出風險管理標準並於 2011 年修訂作為組織於風險管理的參考標準。其標準之重點包括：

1.組織的風險是可被系統化、有效率識別的。

2.企業應根據風險發生的可能性與導致結果設定風險評估的標的及範圍。

3.識別出風險發生的可能性與導致結果，應被溝通並被組織及成員了解。

4.透過管理需求與組織目標建立風險處理的優先處理順序。

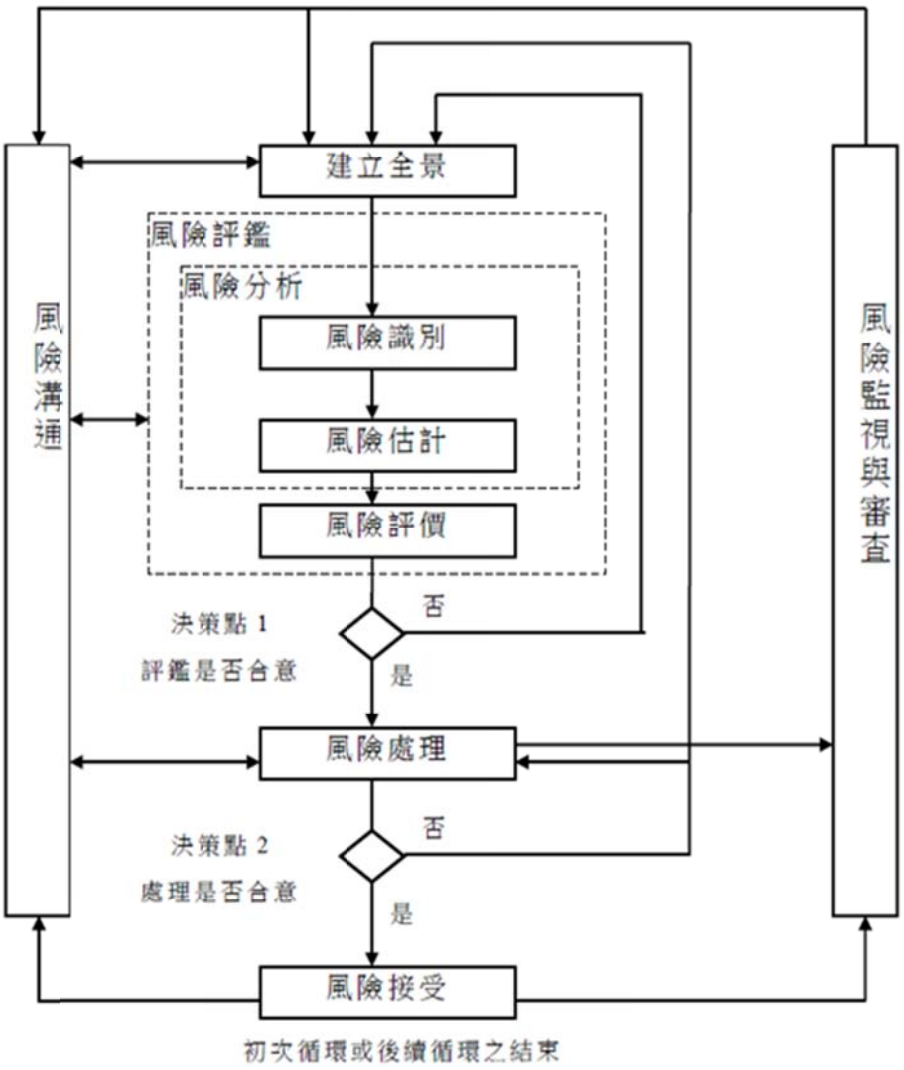
5.組織管理人員應參與風險管理決策之制定，並持續關注直到風險被有效控制。

6.建立有效率的監督與檢視風險處理的管理方式。

7.風險與風險管理過程需要被檢視與定期查核。

8.風險管理與風險、事故發生後的行動，組織管理者與成員須被訓練確保有足夠的能力進行風險管控。

ISO/IEC 27005 並提出對於風險管理的整體流程，詳如圖 20 所示。



資料來源：ISO/IEC 27005

圖20 ISO/IEC 27005 風險管理過程

電子商務業者可以參照此標準進行組織風險的管理依據，並依據該標準的方式進行風險評鑑、風險處理以確保所有安全風險均被識別及管控。

其中 ISO/IEC 27005 可與 ISO/IEC 27001 搭配或合併使用以達到最佳成效。

二、產業標準/規範

(一)PCI DSS(Payment Card Industry Data Security Standard)標準簡介

PCI DSS 支付卡產業安全標準是由五大信用卡發卡組織所組成之 PCI SSC(Payment Card Industry Security Standards Council)支付卡產業安全標準協會所制定頒布。

五大主要發卡組織，面對其發行的信用卡或現金卡等支付工具於運行時之安全管控，PCI SSC 透過 PCI DSS 標準來約束規範處理、傳輸、儲存支付卡資訊(以此五大發卡組織所屬卡片為限)的特約商店(Merchant)或服務提供者(Service Provider)。

對於支付卡的資料以信用卡為例，包括：信用卡卡號、服務代碼、有效日期，客戶姓名、以及記錄於磁條或晶片內部之信用卡資料。PCI DSS 標準嚴格管控相關資料是否得被儲存(詳如圖 21 所示)。

		Items 項目	Storage Permission 儲存允許	Render Stored Data Unreadable 加密
Account Data 帳戶資料	Cardholder Data 用戶資料	Primary Account Number (PAN) 卡號	Yes	Yes
		Cardholder Name 姓名	Yes	No
		Service Code 服務代碼	Yes	No
		Expiration Date 失效日	Yes	No
	Sensitive Auth Data 敏感授權資料	Full Track Data 全軌資料	No	不得儲存
		CAV2/CVC2/CVV2/CID 後三碼	No	不得儲存
		PIN/PIN Block 密碼	No	不得儲存

資料來源： PCI DSS V3.0

圖21 PCI DSS 信用卡資料儲存規範

對於組織是否需依據 PCI DSS 標準進行管理，PCI SSC 也訂定出相關標準(其中要求等級依據各發卡組織略有不同，以下以 VISA 為例)。依據該組織保存、處理或傳輸的支付卡交易數量進行不同等級的要求(詳如圖 22 所示)。

等級	認證應執行作業	有權執行認證單位
1 600 萬筆交易/ 每年 以上	每年一次進行 PCI DSS 現場稽核，並且每季進行 ASV 網路掃描	合格評核機構或由公司高階主管簽署之內部稽核報告 授權掃描供應商
2 100 萬筆/ 每年 以上	每年完成 PCI DSS 自我評估問卷 (SAQ) 並且每季進行 ASV 網路掃描	商店本身自我檢查 授權掃描供應商
3 2 萬筆/ 每年 以上	每年完成 PCI DSS 自我評估問卷 (SAQ) 並且每季進行 ASV 網路掃描	商店本身自我檢查 授權掃描供應商
4* 2 萬筆/ 每年 以下	每年完成 PCI DSS 自我評估問卷(SAQ)，並且每季進行 ASV 網路掃描（選項）	商店本身自我檢查 授權掃描供應商

資料來源： PCI SSC and VISA

圖22 PCI DSS 對 VISA 發卡銀行等級要求

1.PCI DSS 標準與本指引之關係

電子商務業者普遍使用或提供信用卡交易蒐集之消費者資訊，包括：金融付款相關資訊，其所保護的資料對象，與 PCI DSS 所保護之持卡人具備高度的重疊性。PCI DSS 的特約商店中，台灣目前電子商務交易中最常使用的金融工具，高達 76.5%使用信用卡作為支付工具[8]。

本指引透過引用 PCI DSS 對於組織安全的要求事項來進行指引的「事前防禦措施」之主軸、技術要求以及運用 PCI DSS 標準所提示之保護策略，來引導電子商務業者進行更有效的資料保護措施。

2.PCI DSS 標準之特色

[8] 2013 年 B2C 網路商店調查報告，資策會 MIC

由於本標準以保護支付卡資料為主，因此標準整體以資料為核心的防護標準。

由於 PCI DSS 規範的組織均處理或儲存大量的消費者支付卡資料，因此 PCI DSS 相較於其他安全標準或相較於本指引參考之 ISO/IEC 27001 標準，PCI DSS 較為嚴謹、強制以及較偏技術性要求。

資料來源：本計畫整理

圖23 PCI DSS 標準之特色示意圖

(1)強制性要求

對於安全防護的部分，PCI DSS 由於針對支付卡產業，其作業及流程具備高度相似度，因此對於安全結構，例如：必須有兩道防火牆，對於具備風險的不安全協定、或加密密碼強度等均以強制性規定，要求組織遵循。

(2)技術性要求

技術性的要求，除了在每一個安全領域中被要求外，例如：要求資料庫或資料存放的空間須使用加密機制；要求須使用資料正確性比對機制(File Integrity Management)，另外大量使用技術檢查機制，例如：要求定期的內部、外部弱點

掃描，以及內外部滲透測試等技術安全評估，以確保組織的資訊系統安全。

(3)高強度機制

另外由於支付卡產業的個人資料及交易資料均屬於高風險的範疇，因此 PCI DSS 另外一個特色是所有的安全保護均為高強度之要求，例如：加密密碼，目前須為 AES128 以上 RSA 2048 以上，並隨著業界安全水準而提升(或因為技術被破解而禁止)。

(4)監控及測試作業

PCI DSS 要求高度的監控，並要求蒐集大量的系統安全及交易 Log，以利於發現相關攻擊或系統異常狀況。Log 的蒐集存放並需要做到不被惡意竄改，監控系統並必須具備告警之能力，由於資料外洩事故，惡意攻擊者通常在非常短的時間就竊取大量的資料，因此 PCI DSS 要求在監控告警後，管理人員必須於 24 小時內進行反應[9]。

(5)標準定期更新

PCI DSS 由於強調技術及高強度，因此其標準須隨著技術機制的演化、駭客攻擊技術的進步、資料風險環境的變化而進行調整，目前 PCI DSS 標準每三年固定發行新版並實施。相較於 ISO 等管理性標準，以 ISO/IEC 27001 為例，目前版本距離前一版相差八年，因此電子商務業者可於定期至 PCI DSS 標準下載最新版本，目前(2015 年 5 月)，PCI DSS 為 3.0 版，目前已有 3.1 版進入意見回饋階段(廣納各界的修改意見)。

[9] PCI DSS V3.0 12.10.3 Designated specific personnel to be availability on a 24/7 basis to respond to alerts.

本指引將參考並引用與電子商務業者較相關，並與本指引前段分析之成因與提示可能有之問題進行比對後，建議出一般管理要求以及強化型安全防護要求。依據 PCI DSS 標準的特色，本指引中將 PCI DSS 高強度技術性要求機制訂定為強化型的安全管控，將 ISO/IEC 27001 的相關要求訂定為一般的安全管控。

3.PCI DSS 的安全防護要求

PCI DSS 總計分為 6 個框架及 12 個要求項目(Requirements)，電子商務業者除參考本指引所參照的條文或控管措施外，也可以直接利用該標準進行對於自我的檢查(PCI DSS 是一個安全評估標準)，對於部分交易量較小的業者，PCI DSS 僅要求組織進行自我評估表，因此業者也可以利用該評估表進行相關的自我評估作業(詳如圖 24 所示)。

PCIDSS要求之框架	12項要求項目
建立並維護網路與系統的安全	1. 安裝並維護防火牆設定，以保護持卡人資料 2. 不使用供應商提供的預設的系統密碼和其他參數
保護持卡人資料	3. 保護儲存的持卡人資料 4. 在公共網路中傳輸加密的持卡人資料
維護弱點管理計畫	5. 保護資訊系統避免惡意程式攻擊並定期更新防毒軟體之病毒碼及程式 6. 開發並維護系統與應用程式之安全
實施嚴格的存取控制措施	7. 限制僅有業務需求的人存取持卡人資料 8. 識別與授權可存取的資訊系統 9. 限制持卡人資料的實體存取
定期監控和測試網路	10. 追蹤和監控網路環境和持卡人資料的所有操作紀錄 11. 定期測試系統和作業流程之安全
維護資訊安全政策	12. 維護對於所有人員的資訊安全政策

資料來源： PCI DSS V3.0

圖24 PCI DSS 的安全防護要求

4.PCI DSS SAQ(Self Assessment Questionnaire)

PCI DSS 依據不同類型的商家要求使用不同的自我評估表，其中電子商務商家應使用的是 SAQ D，查檢表格式範例(詳如

圖 25 所示)，電子商務業者，可自行至 PCI SSC 網站中下載相關文件進行自我評估作業。

Build and Maintain a Secure Network and Systems

• Requirement 1: Install and maintain a firewall configuration to protect data

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
1.1	Are firewall and router configuration standards established and implemented to include the following:						
1.1.1	Is there a formal process for approving and testing all network connections and changes to the firewall and router configurations?	• Review documented process • Interview personnel • Examine network configurations	☐	☐	☐	☐	☐
1.1.2	(a) Is there a current network diagram that documents all connections between the cardholder data environment and other networks, including any wireless networks?	• Review current network diagram • Examine network configurations	☐	☐	☐	☐	☐
	(b) Is there a process to ensure the diagram is kept current?	• Interview responsible personnel	☐	☐	☐	☐	☐
1.1.3	(a) Is there a current diagram that shows all cardholder data flows across systems and networks?	• Review current dataflow diagram • Examine network configurations	☐	☐	☐	☐	☐
	(b) Is there a process to ensure the diagram is kept current?	• Interview personnel	☐	☐	☐	☐	☐
1.1.4	(a) Is a firewall required and implemented at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone?	• Review firewall configuration standards • Observe network configurations to verify that a firewall(s) is in place	☐	☐	☐	☐	☐

資料來源： PCI DSS SAQ D

圖25 PCI DSS SAQ D 查檢表範例

(二)電子商務(B2C)交易安全規範(包括：網路平台、供應商及物流商)

本規範文件之框架為依據電子商務業者之營業額、個資量、作業特性等分級分類，不同等級給予不同的資安防護實施建議，訂定適合企業交易安全實務操作之文件。交易安全規範包含網路平台、供應商及物流商 3 份並包含以下作業流程，以利電子商務業者掌握上下游作業之資訊安全。

1.電子商務供應鏈之中大型電子商務平台業者之資訊安全管理。

2.含內部資訊流管理。

3.交易網站安全機制管理。

4.有效的交易網站安全機制。

5.與供應鏈的協同資訊作業管理。

6.商品供應商(或賣家)的資訊管理(含交易資訊管理流程)。

7.物流商資訊管理流程(含客戶資料保護管理)。

8.作業安全需包含交易資訊之機密性、交易平台之可用性、交易

內容之完整性、與交易作業之適法性等需求。

依據規範適用範圍之電子商務業者，所涵蓋之交易服務上下游作業流程，依據上下游作業流程中，應予以保護之重要資訊流，訂定相對應之實施策略目標，詳如表 5 所示。

可參考本規範中與資訊流相關部分，可供事前防禦參考之用，並於事中應變部分納入資安通報管理機制。

表5　電子商務交易安全規範實施策略目標

文件名稱	電子商務交易安全規範-網路平台	電子商務交易安全規範-物流商	電子商務交易安全規範-供應商
實施策略目標	1.促進組織資訊安全管理。	1.促進組織資訊安全管理。	1.促進組織資訊安全管理。
	2.加強核心營運系統與資料庫之安全管理。	2.加強核心資訊系統安全管理。	2.建立營業資訊設備管理。
	3.強化客戶個人資料安全管理。	3.保護客戶個人資料檔案安全。	3.保護客戶個資及作業資料安全。
	4.提升企業內資訊環境安全管理。	4.建立託運單安全管理。	
		5.加強作業環境安全管理。	4.加強作業環境安全管理。
		6.加強網路安全管理。	5.加強網路安全管理。
	5.強化對外網站交易平台安全管理。	7.建立外部單位資料交換安全管理。	6.建立外部單位資料交換安全管理。
	6.建立資安通報管理機制。	8.建立資安通報管理機制。	7.建立資安通報管理機制。

資料來源： 本計畫整理

(三)電子商務資訊安全機制與管理規範(中小企業版)

管理規範的資訊安全控制項目針對內容安全、網路安全、及應用安全三大領域編列，並配合電子商務業者之業務流程，分為

交易環境安全及交易過程安全兩個過程。資訊安全架構示意圖詳如圖 26 所示。

資料來源：本計畫整理

圖26　電子商務資訊安全機制與管理規範-中小企業版資訊安全架構

依據電子商務業者資安控管需求、個資法對電子商務業者新增的要求，訂定資安控制目標、資安控制措施，進一步產出資訊安全進階基準(Baseline+)。電子商務資訊安全機制與管理規範(中小企業版)發展之控制措施分項與控制目標詳如表 6 所示。

表6　電子商務資訊安全機制與管理規範發展控制措施與控制目標

類別	控制措施大分項	控制目標
交易環境及營運安全	人員安全	確保電子商務管理人員有足夠的資訊安全認知、管理知識及能力。
		確保電子商務管理人員瞭解其資訊安全責任，並遵守組織之管理政策或要求。
		確保電子商務於資訊安全或個人資料事故發生時，能迅速處理並控制事故。
	實體及環境安全	防止組織場所與資訊遭未經授權的實體存取、損害及干擾。
		防止資產的遺失、損害、竊盜或破解，並防

類別	控制措施大分項	控制目標
		止組織活動的中斷。
	存取控管安全	確保經授權使用者對電子商務系統的存取，與防止未經授權的存取。
		確保電子商務系統之存取權限配置之正確性。
	網路安全	防止電子商務服務使用網路遭未經授權的存取、破壞或惡意攻擊。
		確保網路資源的使用符合組織之管理目標。
	個人電腦、資訊處理設備安全	防止個人電腦、資訊處理設施遭未經授權之存取、破壞、攻擊或竊盜。
		確保個人電腦、資訊處理設施處理、保存之資訊的機密、完整及可用性。
	網站/伺服器安全	防止電子商務網站、伺服器遭未經授權之存取、破壞、攻擊或竊盜。
	程式碼/系統安全	防止電子商務網站使用之程式碼及系統遭未經授權之存取、破壞並降低因利用系統技術脆弱性所導致的風險。
	行動安全及 BYOD	確保行動處理裝置之網路連線安全及其處理資訊之機密、完整及可用性。
	第三方管理	確保第三方之服務或資訊處理、使用符合組織之安全要求。
交易過程安全	資料傳輸安全	確保電子郵件之使用符合組織控制目標，並防止電子郵件遭未授權存取、攻擊或破壞。
	郵件安全	確保電子郵件之使用，符合組織控制目標並防止電子郵件遭未授權存取、攻擊或破壞。
		防止組織，遭垃圾郵件或其他透過電子郵件方式的惡意攻擊。
	交易主體及身分識別安全	建立機制，識別交易之主體及消費者身分識別以確保交易之安全及不可否認性。
	交易過程安全	防止交易過程中資訊遭竊取或惡意破壞，並維持交易資訊之機密性及完整性。
其他安全	安全評估/弱點掃描/漏洞管理	偵測、評估及維持電子商務系統之安全性。

類別	控制措施大分項	控制目標
控制	個人資料保護安全	確保電子商務管理及交易過程中之個人資料使用，符合個人資料保護法之規定。
	證據保全/數位鑑識	確保電子商務管理及交易過程中之證據之完整保存及有效性。
資料及個人資料安全	資料/文件/資料庫安全	確保電子商務系統中及營運中使用資訊之存取安全及合理使用。
		藉由加密密碼方式以保護資訊的機密性。
	儲存/備份安全	維持資訊及資訊處理設施的完整性與可用性。
	個人資料安全	維持個人資料之正確性及完整性。
		預防個人資料遭非法存取、竄改、遺失或外洩。
		確保存放個人資料之儲存空間及實體安全。
		確保個人資料之傳輸安全。
	個人資料安全法律遵循	確保組織遵循個人資料相關法規。

資料來源：本計畫整理

針對上述控制措施提供明確清楚說明，對於控制措施的要求及目的應清楚描述，並且針對每個控制措施的實作方式提供建議方案。並透過進階基準(Baseline+)控管方式，電子商務業者可以由建議使用的控制目標及建議使用的控制項目中，選出合適自己規模、安全需求的類別項目進行控管，以達到規範所要求的控制目標。

透過這些控制項目的選擇結合管理規範範例，電子商務業者可以快速採用或修改後建立自己的管理系統規範及文件或作業流程。

三、最佳實務

SANS Incident Handling：PCI DSS and Incident Handling：What is required before, during and after and incident. SANS(SysAdmin,

Audit, Networking, and Security)是個專門進行資訊安全教育、安全技術之研究機構，透過 SANS 位於全球安全專家針對特定安全議題提供許多安全的報告以及相關安全管控方法研究。

SANS Incident Handling 與本指引之關係本篇專題報告針對 PCI DSS 標準所要求之事故處理(Incident Management)進行事故前、中、後的處理方式說明，本指引將參考及引用部分本報告中提示之方法，尤其事故中之應變機制。

四、VISA 安全規範

(一)VISA：What To Do If Compromised，VISA 事故處理指引

VISA 事故處理指引，是一個針對 VISA 客戶、商店或服務商提供的指引，主要在透過清楚的指示在遭到安全攻擊、系統遭到入侵後該組織應該如何因應的手冊。本指引最主要參考及引用部分 VISA 組織要求其業者在系統遭入侵後的作業指導內容，轉化為電子商務業者在系統入侵事故、資料外洩事故後應執行(或不應進行)的作業項目及方法。

如電子商務業者本身也提供信用卡交易，並且在系統被入侵後涉及 VISA 卡的資料外洩，可進一步完整參考本文件以符合 VISA 組織之要求。

(二)VISA：Responding to a Data Breach，VISA 資料外洩後處理指引 (Guidance)

本手冊係 VISA 提供給特約商店的一個指引，提供在事故後一個與消費者、主要利害關係者、信用卡組織間的反應指引。本指引主要參考及引用其中對於事故後處理機制的策略，以及對消費者溝通的方式，可作為電子商務業者在事故後進行處理的原則及指引。

伍、事前防禦措施的實施指引

依據本指引之分析，資料外洩事故的成因主要分為三大分類：惡意或犯罪攻擊、系統錯誤及人為錯誤，示意圖詳如圖 4 所示。本指引之事前防禦措施的實施指引章節撰寫也將依據此三大類別提供事前防禦。

一、事前防禦措施之重點

事前的防禦，主要目的如下所述：

(一)預防資料洩漏事故的發生。

(二)降低事故發生的可能性。

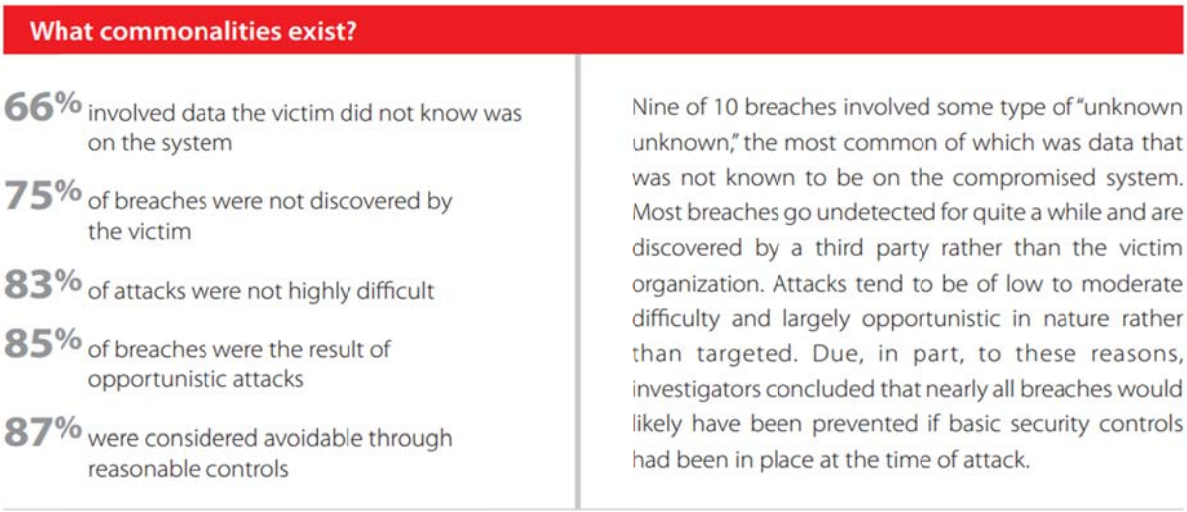
(三)減少事故發生後的衝擊、損失。

因此本指引撰寫，以遵循標準或最佳實務(Best Practice)作為實施的重點，電子商務可以藉此來降低資料洩漏事故發生的可能性。國際標準或產業標準係累積國際或產業組織對於資訊安全的最低要求，最佳實務(Best Practice)則指示最佳的安全管控做法。因此，藉由參考標準與最佳實務(Best Practice)，可以讓電子商務業者引進標準化的要求。

二、事前防禦策略

(一)以資料為核心的防禦策略

本指引以防止資料外洩為主軸，因此選擇所有保護將以資料(消費者個人資料與交易資料)為核心，此防禦策略建立以資料為中心，過去的安全管理，由於並非以資料為核心進行各項安全管控，國際電信通訊公司(Verizon)調查中發現過去外洩事故中發現66%的受害者並不知道資料在系統上(統計分析詳如圖 27 所示)。



資料來源： Verizon Data Breach Investigation Report, 2008

圖27　以資料為核心的防禦策略

以資料為核心的策略有別於過去保護系統、網路為主的方式，將資料當成是保護實施的標的，將安全控管措施實施於資料本身，因此所有控制措施將以資料為中心構築，包括：

1.資料本身就具備安全的管控，例如：加密控制。

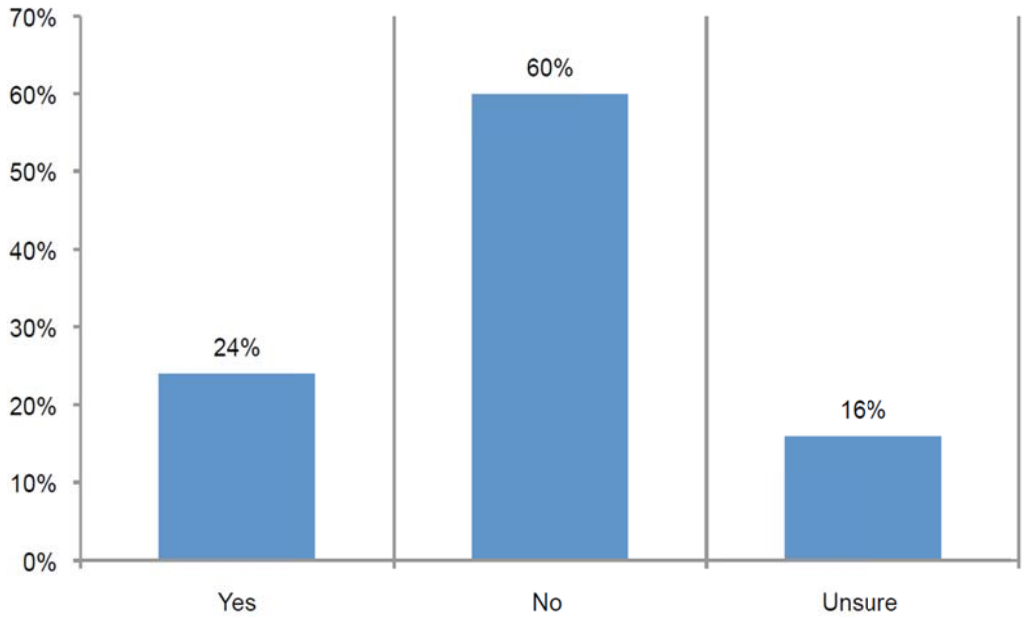
2.依據對資料的需求進行存取控制。

3.存放資料的系統需有相對資料安全等級的防護。

4.所有資料流經的網路及資通安全設備均需符合對應的安全政策及管控措施。

5.依據最小化原則進行資料的蒐集、保存。

過去組織僅重視建構資訊安全環境，但對於資料本身的保護卻相對薄弱，依據國際組織針對發生資料外洩事故企業的調查中發現僅有 24%的組織遺失或遭竊的資料是經過加密，76%未加密或不清楚是否加密的部分，其資料在遺失或被惡意攻擊者偷竊後即可被惡意攻擊者所使用。分析統計詳如圖 28 所示。



資料來源： Aftermath of a Data Breach Study, Phonemon Institute, 2012

圖28 針對發生資料外洩事故企業的調查：資料是否加密

(二)資料減量降低衝擊

電子商務業者對於交易內容，應僅存放必要的資料，以降低保護資料之成本及減少資料外洩的風險。

越多的資料代表越高的風險，於資料外洩的衝擊分析中，每一筆資料在外洩後的代價包括：直接衝擊、間接處理成本等，國際組織調查之結果，每筆資料外洩後的代價金額統計，詳如圖 15 所示。

(三)降低入侵動機

電子商務業者遭惡意攻擊被竊取之資料，最主要目的皆使用於後續詐騙及金融盜刷等，透過降低惡意攻擊的意圖(Intention)或動機，可以有效的減少被攻擊的機會，或降低資料遭竊後的風險。

例如：詐騙組織均於接近客服人員下班時間以手機聯絡當事

人進行刷卡分期交易設定錯誤的詐術，如果在資料庫中的資料僅有 email 或地址，即可大幅降低該資料被竊取的動機，並且降低資料被竊取後當事人受到詐騙的可能。

三、基本防禦措施

(一)基本防禦類型

本指引之撰寫目的在提供電子商務業者一個事前、中、後所需要的資安防護強化措施，因此本章節中提示之事前防禦措施，除了依據前段之防禦策略作為主軸外，所有措施也可以大體分為以下的防禦類型：

1.強化安全架構：電子商務業者應積極強化整體的安全架構，透過安全的架構設計可以有效產生整體的安全防禦效果。缺乏完整的安全架構設計，往往無法形成全面性的安全防護效果。

2.提高知覺：藉由建立良好的知覺系統，本指引提出強化系統 Log 分析與組態檔案安全，建立能夠察覺惡意攻擊者入侵的跡象，而進一步達到防止或降低外洩衝擊之可能。

3.降低入侵動機及損失：本指引提出在事前預防階段，透過加密、減量資料等方式來達到降低入侵動機及損失之方式。

4.建立事中應變及事後處理之能力：本指引提供建立事前防禦措施或作業，有效協助事中應變以及事後處理能力。

(二)整體防禦措施結構

由於本指引之防禦措施僅在強化防止資料外洩以及建立後續事中、事後的處理能力，因此整體防禦措施之結構包含：

1.相關參考指引

本指引之規範將依據先前相關規範或標準建立之基礎，並

提示相關安全措施已於先前之規範中提及，藉以整合經濟部商業司先前對於電子商務安全相關之指引以及安全規範。

2.「基礎」以及「強化」分類

由於本指引將適用於不同規模之組織，由於組織規模的大小，以及電子商務業者風險的考量，為使此指引以及後續查檢表能夠一體適用於各種類型之風險及規模組合，因此，本指引將透過標示「強化」之選項，協助電子商務管理業者選擇本指引所提示之選項做法。未標示「強化」之基礎選項表示為本指引提示一般風險等級業者均應實施之措施，「強化」等級表示高風險業者所必須實施，或一般風險業者想要進一步達到較高安全等級所必須實施。

3.基本防禦措施參考說明

本指引主要參考 PCI DSS 標準建立以下基本防禦措施之管理標準依據，並依據此管理框架建立以資料為核心之保護策略，並確實防範人為錯誤、系統錯誤以及惡意攻擊三大類之資料外洩原因分類。電子商務業者如需進一步強化資料之安全也可以直接引用完整之 PCI DSS 標準進行安全管控。

(三)強化安全架構

1.建立安全架構(Security Architecture)，安全區域以及網路區隔 DMZ 區、內網區及依據作業目的、需求區隔無線網路區段以確保安全。

2.建立強固的網路安全控管，包括：不安全的協定不得使用，遠端連線安全以及公眾網路存取需使用加密通道等。

3.透過資料加密進一步強化資料本身的安全措施。

4.透過定期弱點掃描以及滲透測試發現安全漏洞並補強。

5.依據本指引實施 Log 紀錄強化機制，強化 Log 的留存，並透過 Log 的分析預警機制，提早發現入侵之跡證。保護 Log 不被竄改，以因應事中的應變需求以及事後處理之舉證需求等。

(四)建立並維護網路與系統安全

1.網路安全

由於電子商務業者均使用網路進行交易行為，主要交易之場所在網站或 APP 端，因此網路的攻擊為主要的攻擊方式，網路的安全應注意以下項目：

(1)建立網路安全控管政策，包括：網路區隔方式、存取控制方式。

(2)應建立安全網路架構，包括：依據電子商業業務流程建立安全區域，例如：DMZ 區、內部網路區、辦公作業區、系統開發區、客服作業區及出貨作業區等。

(3)維持最新之網路架構圖，以確認網路架構符合組織之網路安全需求，網路架構圖應包括：所有對外及內部連線現況。

(4)各安全區域應進行適度之網路區隔，並嚴格限制各安全區域之網路存取控制措施。

(5)僅使用安全之網路通訊協定，使用不安全之網路安全協定應有相對應之安全管控。

(6)僅於業務所必須(Business Justification)原則開放使用服務(Service)，協定(Protocol)以及連接埠(Port)，網路連線之開放應僅開放必須之來源與目的 IP 位置。

(7)使用無線網路應僅於必要的目的，無線網路與各安全區域應建立以適度之網路區隔，無線網路區段應建立必要之網路進出管制。

(8)辦公作業區，如需提供訪客使用無線網路等，應避免與辦公區域使用相同之網路或以資通安全設備進行區隔。

(9)所有對外連線與 DMZ 區僅限制安全、核可之網路流量。

(10)所有對外連線應設置DMZ區以區隔內部網路與外部網路，並僅於業務所必須開放進出 DMZ 區之網路流量。

(11)基於安全網路架構，外部網路(Internet)僅允許連線至 DMZ 區，不應開放任何外部網路連線至內網區；內部網路區僅允許連線至 DMZ 區，內部網路區不應開放直接連線至外部網路區。

(12)主要資料存放區域應設置於內網區，非有對外連線必要之主機不應置放於 DMZ 區，資料庫主機或其他存放重要、大量消費者個資或交易資料主機應設置於內網區，並以網路區隔與外網及其他非安全網路(untrusted network)。

(13)應限制所有進出主要資料存放區之網路流量，並限制遠端管理連線(如：SSH, RDP, VNC)及後台系統的存取來源位址，並採取強固的身分認證及失敗鎖定機制。

(14)定期審查網路架構、防火牆政策(Policy)及相關路由或交換器設備之設定，確保組態之正確與需求相符。

(15)關閉所有未授權之對外流量，僅開放符合業務所必須之對外流量。

(16)連接外部網路之個人電腦應設置個人防火牆，避免惡意攻擊。

(17)所有遠端登入(Remote Control)應搭配雙因子認證之存取控制，所有非本機之登入僅於安全的網路協定下執行。

(18)消費者輸入個人資料或交易資料的連線應僅於安全、加密的網路連線下進行。

2.系統及設備安全

(1)應維持主機及系統、設備之清冊，並盤點各系統、主機、設備之功能、設置位置、網路相關資訊及已實施之安全管理機制。

(2)不使用軟體供應廠商已停止安全支援或更新服務之軟體(例如：Windows XP, Windows 2000 server)。

(3)所有主機及設備在接入網路前應變更預設(Default)之帳號或通行碼，並移除非必要之所有帳號。

(4)應依據最佳實務(Best Practice)進行主機(OS)、應用系統以及資通安全設備建立安全組態標準，並依據該安全組態標準進行主機、應用系統設備之組態設定並定期查核其正確性。

(5)主機系統應僅安裝一個主要功能，以避免不同安全等級要求之應用系統安裝於同一主機降低該主機之安全等級。

(6)主機僅開放必要之服務(Service)、協定(Protocol)、連接埠(Port)。

(7)應移除所有主機上非必要之功能、服務(Service or Daemon)、介面、子系統、檔案系統。

(8)應加密所有非本機登入(non-console login)之管理權限活動(Administrative activities)，非本機登入僅限制使用安全之協定(例如：SSH, VPN, TLS)。

(五)保護消費者資料安全

1.消費者資料保護

(1)作業流程盤點：由於電子商務業者之消費者或交易資料經常須流經組織中不同部門、系統或作業流程，因此於進行資料盤點作業前，建議應進行作業流程盤點，依循資料流經的作業進行識別，確認那些作業流程使用消費者個資或交易資料，進而了解資料可能被存放、利用的情形，將有助於後續的資料盤點進行。

(2)資料及資料存放位置盤點：盤點所有消費者個人資料及交易資料存放位置，包括：主機系統、資通安全設備、資料備份及其他可能存放資料之位置產出清冊，並進行定期的查核作業以確保資料存放位置之正確性及必要性。

(3)考量業務、法律或法規要求，依據最小化原則蒐集與保存消費者個人及交易資料，包括：數量、欄位等。

(4)資料應設定保存期限，並定期檢視並刪除超過保存期限之資料。

(5)消費者個人與交易資料，存放於資料庫或檔案、備份媒體時應視需求採取加密保護措施，該密碼應具備足夠安全強度。

(6)上述加密機制，應建立管理程序以有效管理密碼之產生、保管、使用、保存及廢止等，以確保加密機制之有效性。

(7)如果系統同時使用明碼資料儲存及密碼資料儲存，應做區隔並避免交互參照破解加密之可能。

(8)消費者個人與交易資料於業務執行階段(例如：螢幕顯示、列印報表等)應依據需求採取單向雜湊(One-way Hash)或遮罩方式處理。

2.消費者個人資料或交易資料傳輸安全

(1)於公眾網路傳輸消費者個人資料或交易資料應使用高強度加密之傳輸機制(例如：SSH、SFTP、VPN、TLS 等)。

(2)使用無線網路傳輸消費者資料或交易資料，應使用高強度加密機制(例如：IEEE 802.11i/WPA2[10])。

(3)嚴禁使用一般傳輸工具進行傳輸未經保護的消費者個資或交易資料。

---

[10] Three levels of IEEE 802.11 Security, WEP(weak), WPA(OK), WPA2(best)<IEEE 802.11i>, 2010/11, National Instruments Corporation

3.個資法對於消費者資料保護之規定

個資法要求蒐集、處理、利用個人資料之組織進行對於個人資料之適當安全維護，並於個資法施行細則中針對適當安全維護進行要求，包括：

(1)配置管理之人員及相當資源。

(2)界定個人資料之範圍。

(3)個人資料之風險評估及管理機制。

(4)事故之預防、通報及應變機制。

(5)個人資料蒐集、處理及利用之內部管理程序。

(6)資料安全管理及人員管理。

(7)認知宣導及教育訓練。

(8)設備安全管理。

(9)資料安全稽核機制。

(10)使用紀錄、軌跡資料及證據保存。

(11)個人資料安全維護之整體持續改善。

(12)電子商務業者應注意對於該等法律要求之安全保護項目是否已實施，以確保本身之合法性，對於適當安全維護之具體做法，以及相關程序及表單建議參考經濟部商業司頒定「電子商務交易安全規範」與「電子商務資訊安全機制與管理規範」。

(六)維護弱點管理計畫

1.防範病毒及惡意軟體

(1)應於所有可能遭受病毒或惡意軟體之主機系統(包括：Linux 或其他平台 OS 主機)安裝防毒軟體。

(2)於所有個人電腦設備及其他資料處理設備安裝防毒軟體，並確保所有個人電腦安裝之防毒軟體不被使用者自行停止或移除。

(3)防毒軟體應定期更新病毒碼作業。

(4)確保所有安裝之防毒軟體，具備偵測、移除及保護系統之功能，並可以因應所有已知之病毒、惡意軟體類型(請電子商務業者，應安裝可靠、具備可信賴度之防毒軟體)。

2.維持安全之系統或應用系統

應用系統本身的安全性無法以資通安全設備做到全面性的防禦，由於此類的攻擊直接針對網站系統，因此建立安全應用系統，透過安全的系統開發過程控管才能達到對系統安全的全面防禦。

電子商務業者如果委外開發或購買其他已開發完成的系統，應依據本指引檢視委外開發作業或開發完成之應用系統。

(1)應定期針對網站使用之系統(包括：網站主機、資料庫及資通安全設備等)進行安全性弱點掃描，並針對掃描結果進行修正，如果原廠尚未提供修正程式時，應由系統開發人員進行補強措施或暫停使用該功能或元件。其中弱點掃描之次數應依據組織之風險進行，可參考 PCI DSS 標準之規定，外部掃描(自外網區進行對組織網站掃描)規定為每季一次；內網掃描(自內網區對所有主機進行掃描)需每季進行一次。

(2)應定期針對重要對外主機進行滲透測試(Penetration Test)，並依據滲透測試結果進行修正，如果原廠尚未提供修正程式時，應由系統開發人員進行補強措施或暫停使用該功能或元件。其中滲透測試之次數應依據組織之風險進行，可參考 PCI DSS 標準之規定，外部滲透測試(自外網區進行對組織網站掃描)規定為至少每年一次。

(3)所有原廠提供(Vendor Supplied)安全更新應最遲於發布後一個月內安裝更新。

(4)對外服務之網站應用程式，應定期及於網站應用系統或軟體元件重大更新上線前，進行網站應用程式安全掃描(Application Security Scan)，並依據掃描結果，排除可能的安全弱點或漏洞。

(5)對外服務之網站應用程式(Public Facing)，應使用或安裝網路應用程式防火牆(Web Application Firewall)並定期更新其偵測防禦所需資訊，以有效防止針對網站應用程式之攻擊。

3.應用系統開發安全

(1)應依據標準或產業最佳實務進行系統開發作業(例如：OWASP, NIST 等)以確保系統開發之安全。

(2)於應用系統上線前，應移除測試或非必要之帳號、通行碼及測試資料。

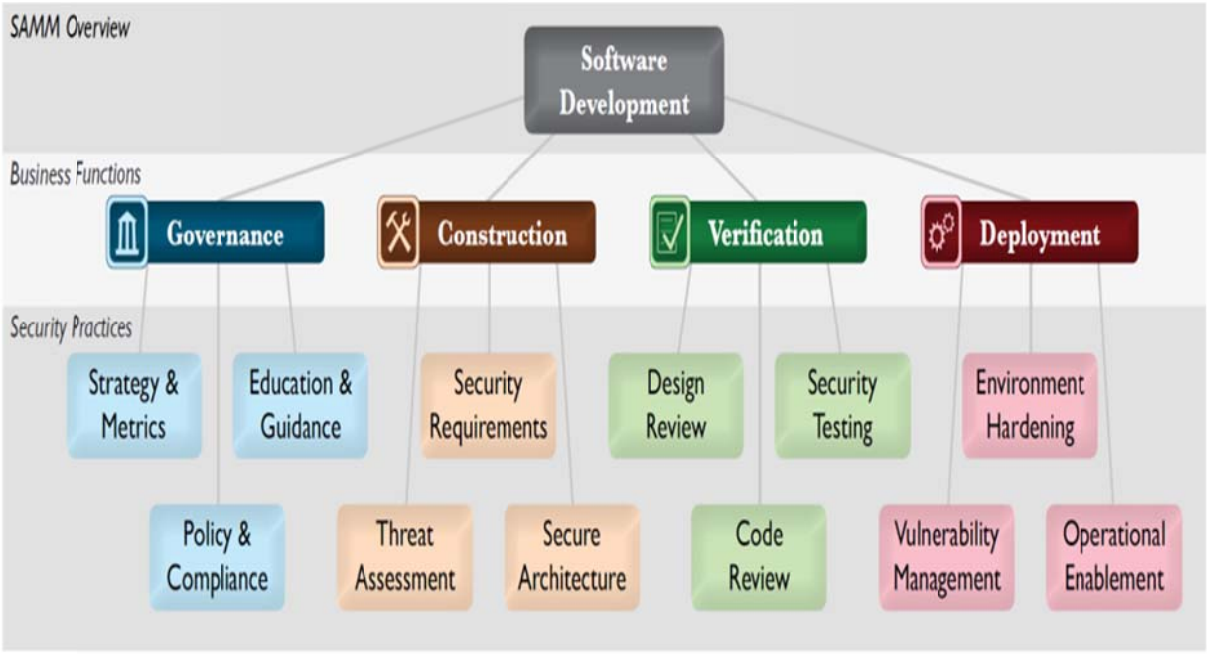
(3)應用系統上線前，應進行源碼檢查(Code Review)，源碼檢查應至少能偵測使用網路應用程式主要的漏洞或安全弱點(例如：OWASP Web Application TOP 10)

(4)應進行應用系統開發人員之系統開發安全防護訓練，以確保該人員具備安全系統開發之能力(Secure coding)。

(5)應區隔測試區與正式區之管理權限，如為同一人執行，應分別建立不同的帳號並使用不同的通行碼，以避免誤用或遭惡意攻擊利用。

(6)安全軟體開發生命週期管理(Secure SDLC)

建議電子商務業者於軟體開發過程中導入安全的軟體開發管理，例如：OWASP 的 SAMM(Software Assurance Maturity Model)等協助電子商務業者進行安全的開發作業流程。



資料來源：OWASP, SAMM V1.0

圖29 安全軟體開發過程

4.委外開發系統之安全要求

電子商務業者如委外開發或取得外部開發使用之電子商務系統應注意要求以下項目，以確保所有系統之安全：

(1)應評估該委外開發公司或該產品之安全風評，是否曾經發生安全事故等；或諮詢該公司之其他客戶以確保該軟體安全可靠。

(2)電子商務委外開發合約中，必須訂定保固期間、維護方式尤其與資料外洩事故中需配合的緊急處理支援服務，應明訂於合約中，確保外洩事故中可獲得及時且足夠的支援。

(3)電子商務委外或購買合約中應注意提示「如本軟體使用之所有元件、開發工具或指定之系統使用平台或伺服器軟體於保固期間或後續使用其間內出現安全問題，該委外廠商或軟體供應商應提供相關的弱點補強、系統更改或更改使用平台之服務」，以確保所使用的軟體不因為安全問題而無法使用(注意：保固期後的修改可能涉及其他費用)。

(4)依據個人資料保護法，委外開發廠商或軟體供應廠商如果與開發或維護的階段可以接觸或存取到電子商務業者的消費者個人資料，應於合約中要求遵循個人資料保護法之規定(詳細作法及範本合約可以參考經濟部商業司「電子商務資訊安全機制與管理規範」)。

(5)業務單位須要求承包廠商參與開發案之相關工作人員，均須簽署保密切結書。承包廠商處理委託事務，涉及個人資料時，須遵守「個人資料保護法」規定。業務單位應視資料之重要性，訂定廠商違反規定時之罰則及賠償責任。

(6)建議於委外系統或購買自外部系統驗收前，請該委外廠商或軟體供應商提供下列安全性報告：

A.完整的軟體源碼掃描報告(Code Review Report)，並檢視存在中高風險之安全問題。

B.提供該軟體中使用的相關元件、平台，以利後續追蹤該軟體可能有的安全弱點或漏洞。

a.開發工具或語言(例如:.net, php 等)。

b.該軟體中使用之外部元件、函式庫(Library)。

c.該軟體所需使用之系統架構可能包括：前端網站伺服器(Web Server)，應用伺服器(Application Server)、中介軟體(Middle Ware)，及後段資料庫(Database Server)。

這些資料的提供，最主要在於後續了解該軟體中可能有的弱點，由於軟體交付時可能未有漏洞被發現，但隨著軟體的使用時間，可能才發現該電子商務系統使用了一些包含漏洞、弱點存在的問題。

C.建議要求委外廠商或軟體供應商應提供「系統設計規格書」、「資料庫綱要說明(欄位及關聯)」、「系統測試報告」、「系統安裝及維護管理手冊」、「系統備份及還原說明書」、

「系統操作使用手冊」及「教育訓練教材」等文件，於驗收時連同「系統原始碼光碟」，以利電子商務業者可以進行後續之軟體維護作業。

以上之軟體、元件及文件等訊息，應清楚提供名稱、版本、適用平台等資訊。

(7)建議於系統進入電子商務業者環境後，正式上線前協請委外廠商或軟體公司提供，針對該軟體之系統弱點掃描報告(Vulnerability Scan)，如系統屬於網站應用程式，建立要求提供網站應用程式安全掃描報告(Web Application Vulnerability Scan Report)。

(8)系統於移交給電子商務業者後，應要求委外廠商或軟體供應商刪除或停用所有該廠商使用或預設之帳號。

(七)存取控制

1.安全區域內的重要主機、資通安全設備應設置高強度通行碼，至少為 12 碼[11]以上並包含複雜度(包含英文大小寫字元、10 進位數字及非英文字母字元)且不可包含使用者帳戶名稱全名，至少每 60 天更換通行碼，且不得與前 5 次使用過之密碼相同。

2.鎖定系統或應用程式重複錯誤登入次數超過 5 次以上之帳號。

3.系統或應用程式登入後不使用超過 15 分鐘，應強制登出或於恢復使用時以帳號、通行碼管制。

4.所有系統傳輸帳號、通行碼均應使用高強度密碼進行加密或於安全協定、通道下傳送帳號、通行碼等識別資料。

[11] 參考政府組態基準(GCB)建議密碼設定原則，於密碼歷程記錄部分，政府組態基準要求不得與前 24 次密碼相同，考量電子商務業者實作，故訂定不得與前 5 次密碼相同。

5.所有重要主機、資通安全設備遠端登入應使用安全協定外，並使用雙因子認證以確保安全。

(八)實體及人員管控措施

1.實體及人員管控安全措施，可參照經濟部商業司頒訂之「電子商務交易安全規範」與「電子商務資訊安全機制與管理規範」中已有的基本安全措施，並實施以下防止洩漏強化措施：

(1)環境安全管理措施

A.應強化實體安全，避免惡意攻擊者透過實體進入辦公區域竊取資訊、設備或安裝網路監聽設備、入侵設備等。

B.辦公區域中不使用之網路線及網路接口，應以安全設備控管其連線能力或以實體方式阻絕以避免未授權之使用。

(2)人員安全管理措施

應要求注意人員使用社群網路工具、電子傳訊工具中之釣魚(Phishing)或詐騙之行為。

(九)監控及測試系統及網路

1.記錄及監控網路及資料存取活動

(1)所有安全紀錄(Log)應可對應到應被記錄監控的個人，不應只記錄群組、共用帳號或其他無法識別實際使用者的代號。

(2)電子商務業者應建立自動機制或其他方式記錄以下 Log，應設置集中存放之 Log 紀錄於內網區，集中蒐集各主機及 Log 紀錄並避免未經授權的修改。

A.所有個人對於消費者個人資料或交易資料之存取。

B.所有個人執行以管理者權限(Administrator 或 root)的所有活動，包括：以提升權限或最高權限執行程式。

C.對任何系統之稽核軌跡(Audit Trail)之存取動作，包含啟動、暫停或停止稽核記錄機制(Audit Log)。

D.所有提升權限的動作，包含任何對於具備系統 Root 或 Administrator 權限帳號的新增、修改、刪除動作。

E.新增或移除系統元件動作。

(3)所有稽核紀錄應設置避免管理人員或具備管理權限之其他人員進行任何變更。

(4)所有紀錄應至少保留至少一年。

(5)所有系統應進行同步校時，並應設定可靠之校時主機(Time Server)。

(6)應設置檔案變更管理監視機制(File Integrity Management)監控重要主機設備、資通安全設備之 Log，並在 Log 被未授權變更、刪除時預警通知管理人員。

(十)資訊安全教育訓練

電子商務業者應進行對於內部管理、作業、技術人員施予資訊安全、如何防止洩漏之教育訓練措施，建議應包括以下面向：

1.組織之安全目標及目前實施之安全管控措施。

2.人員於安全管理中扮演的角色與其責任。

3.提供資料安全保護的知識與技能訓練。

4.提供組織使用之安全機制與操作設定說明。

5.提供個人資料安全保護的法律知識與相關管理措施。

6.透過安全事故、案例之說明，強化人員應注意或應避免之事項。

7.配合應變計畫管理進行事前應變程序演練。

四、事故應變計畫

為了降低事故發生的衝擊與減少事故的應變時間、做好應變的準備，電子商務業者應於事前預防措施中，預先準備事故應變(Incident Response Plan)，以確保在緊急狀況下，可依據事先規劃的步驟及準備的資源進行事故處理。

(一)事故應變組織

電子商務業者應建立事故應變組織，其中應包括角色如下：

1.事故應變小組召集人

應指派一人並備妥備援名單，擔任事故應變小組召集人，召集人應具備指揮、調度能力，並於事故應變階段進行重要決策。建議人員應為組織負責電子商務業務之最高主管或公司高層人員。

2.管理階層

事故應變小組應由各業務執行之管理階層所組成，包括：業務、客服、系統、程式等部門主管人員，以提供相關重要決策之意見提供。

3.技術人員

熟悉組織電子商務系統之技術人員，包括系統維運、網路以及系統開發人員。

4.法務人員

由於個資外洩事故經常涉及相關對於消費者之法律責任、賠償責任，因此事故應變小組內，應有熟悉相關法律事務之人進行法律責任之判定，對外發言之內容、與消費者間的溝通內容以及對於主管機關之溝通協調。

5.公關/對外發言窗口

由於事故中應變可能需應對媒體及廣大消費者，因此事故應變小組應指派公關或對外發言窗口，以避免因人員之不慎發言引發更多衍生問題。

6.外部專家

由於資料外洩事故經常涉及複雜及高度技術難度、法律及媒體關係等議題，電子商務業者應考慮於事故處理小組中納入外部資源與專家以確保事故處理之有效性，建議可考量下列外部資源：

(1)法律面

電子商務業者應視外洩內容、範圍大小以及嚴重程度判斷是否需要外部法律諮詢資源的介入。此外部資源應於平常即備妥，進行相關合約簽訂等，以免於緊急狀況下無法取得支援。

(2)技術支援

電子商務業者，應於平時就準備與技術相關之支援，技術支援包括：技術原廠供應商、系統供應商、資料庫專門技術人員、系統開發技術、資訊安全專家等。安全技術專家可以協助技術的調查與後續防禦措施之建立。

(3)事故處理人員

電子商務業者應視本身的事故處理能力與事故的狀況，考慮委託專門的事故處理專家進行事故協助處理，事故處理專家可協助事故應變的流程、根因調查、消費者溝通、公關/媒體關係等作業。

電子商務業者涉及之外洩事故，例如：信用卡號，注意

部分信用卡品牌(例如：Visa、Master 等)依據事故之嚴重要求須由其授權核可之事故處理人員進行事故處理，組織並提供相關名單[12]。發卡組織並要求於一定時間(例如：72 小時內[13])內提出事故調查報告。

(4)鑑識專家

電子商務業者應視外洩事故的嚴重程度以及其所涉及的法律層面、責任，考量聘請獨立之數位鑑識專家進行證據之保全，數位鑑識專家並可以協助進行根因調查。

如電子商務業者無固定之安全應變組織，應以本指引之建議盡量於事故發生時備齊相關功能，或委由外部之安全服務機構進行相關安全事故之處理。

(二)事故應變處理

電子商務業者除組成事故處理小組外，應針對事故應變做出相關事前的計畫，其中應至少包括：

1.消費者溝通計畫，包括：對於媒體之應對計畫。

2.準備事故應變之必要資源，包括：

(1)應變所需要系統，包括：系統主機、資通安全設備等。

(2)應變所需之外部人員，包括：技術、法律、鑑識以及事故處理相關的資源，應於平時即建立相關關係或建立相關委託合約關係。

(3)通知消費者管道，例如：發送大量郵件、簡訊、電話通知等

---

[12] A list of Visa-approved CISP Incident Response Assessors (QIRA) can be found at：

http://usa.visa.com/download/merchants/cisp_qualified_cisp_incident_response_assessors_list.pdf

[13] Visa, Master 等發卡組織均要求 72 小時內提出事故處理計畫

方式及技術細節，應考量事先規劃並簽約。

3.事故應變程序

電子商務業者於平時應建立事故的應變程序或管理計畫，包括：

(1)事故應變之啟動條件與時機。

(2)召集事故應變小組(包括：外部專業人士)。

(3)內部人員任務分工。

(4)標準資訊作業程序，例如：隔離主機、網站公告方式及消費者通知等。

4.事故應變程序演練

電子商務業者應於計畫建立後以及定期進行計畫之演練，如演練結果與原計畫之目標不符合或有其他須修正計畫之因素，應於演練後進行計畫之修正。

(三)事故應變相關資訊蒐集

電子商務業者應定期至政府機構或金融組織、國際安全組織等機構、網站及其他專家論壇蒐集事故應變相關之資訊，例如：

1.165 防詐騙專線網站提供之詐騙資訊、趨勢及統計資訊(https://www.165.gov.tw/index.aspx)。

2.VISA、Master 組織所訂定之事故應變說明。

3.其他國際或國內安全機構提供之案例及預警說明等。

電子商務業者可以藉由前述之資料蒐集進行應變提早準備，以有效因應或通知消費者注意。

陸、事中應變措施實施指引

一、事中應變措施的目的與重點

在資料洩漏事故產生後，進入事中應變階段，本階段措施實施的目的最主要在於控制事故，避免事故擴大及降低事故的衝擊。實施的重點主要在做出緊急應變、進行回應及通報。

二、個資外洩事故類型

電子商務業者於面對消費者資料或交易資料外洩之事故，通常可分為以下幾種狀態：

(一)內部發現

1.業者本身發現其資料外洩，例如：發生系統故障、內部人員發現錯誤寄送郵件、或檔案遺失等由內部發現之資料外洩。

2.業者發現系統執行出現異常、系統遭異常存取紀錄或發現資料錯誤等現象。

(二)外部發現

1.消費者通知發現其資料外洩，例如：於網站上可見、或其他方式發現且與電子商務業者相關。

2.消費者進線客服說明自己的個人資料遭利用於其他目的或錯誤使用(例如：將消費者的資料誤傳至其他人帳號)。

3.消費者通知或其他管道(例如：165 反詐騙專線或其他主管機關)通知電子商務業者，消費者之個人資料或交易資料遭詐騙集團使用進行詐騙。

4.消費者或其他金融機構告知消費者之交易資料(例如：信用卡卡號)遭外洩、冒用等。

依據國際組織調查的發現，67%的資料外洩受害者，是由外部通知，分析統計詳如圖 30 所示。

資料來源： Mediant 調查報告 2014

圖30 個資外洩之事故類型統計

三、個資外洩事故之處理

資料外洩處理框架與步驟，詳如圖 31 所示。

資料來源： 本計畫整理

圖31 資料外洩處理框架與步驟示意圖

有關事故的處理，基本上可以歸類為如下：

(一)發現階段(Informed/discovered)

自事故發生或電子商務業者知悉開始，事故可能由內部發現或外部通知，因此事故(例如：入侵或外洩)實際發生時間可能與電子商務業者知悉之時間不同。

在調查確認是否為電子商務業者本身產生之外洩確認前，事故僅能視為「疑似事故」。於此階段須確認所掌握之訊息，作為下一階段進行調查、確認項目。

(二)調查、確認階段(Investigtion/Confirmation)

於事故發生後，電子商務業者需開始進行調查，調查並確認疑似事故是否為本身所導致；或該等外洩資料是否由電子商務業者本身所擁有，因此調查確認階段可能的結果可以分為三個主要類型判定：

1.本組織所為

電子商務業者確認該等資料係為本身所擁有或保存，例如：由內部發現，或經過資料比對，多筆資料均與本組織之資料相符，電子商務業者肯定此外洩事故為本身所為。

電子商務也可以依據目前掌握疑似外洩的資料欄位、數量與該疑似資料外洩事故的發生時間，並與進一步與內部交易處理的資料流進行比對，判斷資料外洩的可能之作業或位置。

2.非本組織所為

電子商務掌握重要資訊確認該外洩資料不可能為本組織所為，例如：通報之個資外洩內容與本組織所擁有之資料不同；或該等資料與本公司不符合(如網站出現的資料)。

3.無法判定

外部通報的事故，有許多的狀況因為通知者所提供的資訊不能肯定為本公司;或僅有單一個案,未能肯定為本組織所為；或經過調查本組織未能確認重要判定證據。

但由於電子商務業者面對消費族群或媒體壓力，通常於此階段如判定為「無法判定」狀態，仍須進一步進行可能性的判定，以協助決定下一階段的處理執行方式。通常以百分比方式決定其可能性，本指引並將協助於後續章節提供判定之建議方式，例如：在判定 70%以上為本組織所為的可能時，就會啟動開始積極處理消費者安撫的作業(雖然尚未正式承認或認定為本組織所為)。

另外於調查、確認階段,如果調查判定的結果為「本組織」，電子商務業者應確認以下項目：

(1)可能外洩原因，不一定可於短時間內判定。

(2)外洩事故可能發生的時間。

(3)可能外洩的資料範圍(欄位、資料內容)。

(4)可能外洩筆數。

(5)信用卡號碼(應依據信用卡組織要求確認信用卡卡別等資訊)。

(6)其他資料外洩重要相關資訊。

(三)緊急處理階段(Prompt Actions)

如果判定該事故為電子商務業者本身所為，或無法明確證據判定是本身所為，但有極高的可能性是本身所為，應進行緊急處理作業，本階段作業包括以下作業：

1.控制階段

於判斷需要進行相關處置後，應進行控制及減少損失之處置，可能包含後續事後調查(或提起後續法律行動)而須要進行更深入調查，緊急處理階段的控制，惟必須注意不會破壞重要證據。控制階段應注意及辦理事項包括：

(1)立即由應變小組啟動緊急應變程序。

(2)進行證據的保全以利後續調查，決定是否要求外部學者或經TAF(台灣認證基金會)認證核可之數位鑑識實驗室進入協助處理，並避免證據破壞。

(3)與管理或法務單位討論是否需要進行數位鑑識，以確保後續之法律之效力。

(4)記錄下所有緊急處理實施的相關動作以供後續階段使用。

(5)通知相關利害關係者。

(6)如涉及信用卡部分外洩事故，通知相關收單銀行或信用卡組織。

(7)進行後續回應階段之準備，包括：彙整目前已知之調查結果以及準備相關回應之內容。

2.注意事項

(1)不要存取或變更被入侵之主機(例如：登入該主機、變更密碼、或以 Root 或 Administrator 身分登入)。

(2)除非必須，儘可能不要使用該被入侵之主機，以保全所有證據。

(3)避免將疑似被入侵的主機關機(以避免破壞證據)，如要防止資料繼續洩漏應進行將該主機隔離即可，例如：透過拔掉硬體網路線或自 Hub/Switch 端將該主機網路拔除即可。如果有數位鑑識的需求及必要，為保全相關入侵或惡意攻擊的證據，

應考慮保持線路連結直到採證作業完畢。(有關進一步鑑識相關步驟，請參考法務部頒訂之「行政院及所屬機關數位證據保全標準作業程序」)

(4)保存所有可能 Logs(例如：資通安全設備紀錄、網站、資料庫、防火牆等紀錄)

(四)初步回應階段(Responses)

第一階段之發現階段，按照前述分析可以分為內部發現或外部通知：

1.內部發現

由內部發現的事故開始到須要回應給客戶或主管機關階段的時間壓力較低，所以可在緊急處置完成後，於下一階段之事故後處理進行回應。

2.外部通知

(1)由於由消費者通知之事故，當事人因為已經被詐騙或擔心其資料被誤用，其心理有許多的憤怒及恐懼，因此應儘速回應。

(2)由主管機關或政府單位通報者，政府機關會設定期限要求單位儘速通報，電子商務業者應於其規定時間依據規定方法進行後續回應。

目前內政部警政署刑事警察局已設有 165 專線受理民眾通報網路詐騙案件，刑事局除針對民眾報案進行偵察之外，並將每週接獲民眾通報累計達 10 件以上之網路零售業者，移送經濟部商業司依個人資料保護法查處，除依據個資法相關規定，函請業者限期提出改善措施，同時亦透過相關資安輔導計畫，派員進行實地訪查，以協助業者改善資安問題。

(五)回應方式

1.針對民眾及媒體之回應

(1)統一回應窗口，並要求內部其他人員不應針對此部分進行對外之發言。

(2)需安排固定後續對應之窗口，避免轉換不同人員進行回應。

(3)回應前應內部討論，包括：溝通之策略、內容以及須揭露的細節，如有媒體涉入，應由指定之媒體對應窗口進行溝通，對應媒體必要時應準備相關文字稿件。

(4)溝通方式原則上以指派人員拜訪或電話為主，若使用信件、訊息或電子郵件等文字方式回應，則應審慎考量是否容易造成錯誤解讀或曲解。

2.通報主管機關

有關通報主管機關部分，應注意如發生相關外洩事件應依據個資法對主管機關(經濟部商業司)進行通報，目前也設置 EC-CERT 電子商務資安服務中心，電子商務業者如發生事故可以向該單位通報並請求協助，該單位並且備有「行政檢查之業者自評表」供電子商務業者自我評估是否已依據個人資料保護法進行安全保護管理。

另外，部分電子商務業者可能已經建立個人資料管理系統包括 BS10012、TPIPAS 或 ISO29100 等管理系統，於管理系統中已建立安全事故通報流程者，也可以進一步參照已建立的管理作業流程進行對於主管機關及消費者的通報或通知。

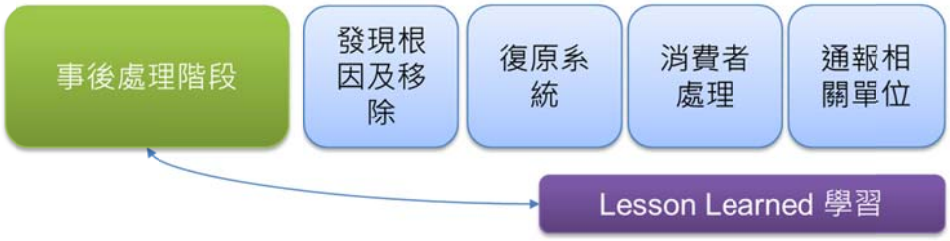
柒、事後處理實施指引

一、事後處理措施之目的與重點

事後處理措施實施的目的在於能發現根因、移除並恢復系統的正常運作。實施的重點在於系統恢復與遵循法律的要求，並積極處理消費者的溝通與損害補償作業。

二、整體事後處理作業說明

電子商務業者在事故中進行應變後，進入事故後階段應進行以下工作項目，本指引將調查確認、緊急應變部分分類為事故中應變，較屬於緊急的狀況處理及控制作業。事故後階段屬於較長時間的處置階段，重點在於發現根因、復原系統以及作出對於消費者的後續溝通及處理，以下為事故後處理階段應進行的事項，詳如圖 32 所示。



資料來源：本計畫整理

圖32 事後處理實施指引示意圖

(一)發現根因與移除(Eradication)

如電子商務業者發生外洩之事故，應於事故應變階段盡可能發現真實根因，但應變階段往往無法於短時間內發現外洩之主因，只能緊急將主機或系統做緊急的隔離以控制外洩。於事故後，由於處理的時間較為充裕，應儘速進行根因調查並進行移除。

電子商務業者如無法自行進行根因的判定，應委由外部技術或鑑識專家進行根因判定。

(二)復原系統(Recovery)

應於相關根因查證完畢並移除後進行系統之復原作業。系統復原除應進行系統的恢復，並應進行相關防禦措施並積極預防事故再次發生。

(三)消費者處理(Consumer issue handling)

消費者端因個人資料外洩，產生包括個資法法律問題、對於受害者的損害賠償問題等。消費者因電子商務業者資料外洩，引發後續資料被盜用、詐騙、偽冒等可能風險，因此於事故中及事故後電子商務業者均應妥善處理消費者之事務。

消費者處理涉及與消費者之溝通與補償、賠償等議題，電子商務事故應變小組應設立專門人員進行相關事宜，並避免因後續不當處理引發更大的商譽損失或賠償等。本指引將於後續章節提供消費者溝通與處理之細部作法。

(四)通報相關單位

依據個人資料保護法，於組織發生資料外洩事故時應通知當事人，如有需要應通報主管機關。

另個資外洩如涉及外部惡意攻擊或內部蓄意之行為，電子商務業者應於緊急處理階段向轄區警察局或165反詐騙專線等政府單位通報，以確保組織本身之法律及安全問題。

(五)自事故中學習

電子商務業者，應於事故發生及處理完畢後，進行對於資料外洩事故之檢討，並依據事故發生的根因、處理方式、消費者處理方式以及相關後續反應做出事後檢討，依據相關作業懲處失職或發生錯誤之人員。

檢討之結果應作成相關紀錄，並依列出問題提出改善計畫，避免相同或類似事故再次發生。

三、消費者溝通及處理方式

對於資料的外洩，由於相關系統的問題、弱點問題以及內部管理、技術問題，電子商務業者非常難避免，遇到類似的狀況或問題。因此對於資料外洩問題，應該積極做好準備。以下提供相關消費者處理之溝通及處理方式

(一)溝通計畫(Communication Plan)

溝通計畫應針對消費者、媒體、主管機關、主要夥伴或利害關係者分別訂之，計畫內容應包括：溝通的策略、方式、管道以及主要應對之人員。其中尤其以消費者之人數眾多，如何有效的指派分工將更為重要。溝通計畫可於事前備妥並於事故應變階段中進行調整或建立。

(二)處理原則

對消費者溝通之處理原則，必須精確而且快速，並考量下列處理角度：

1.設身處地思考消費者的心境及壓力

由於消費者面對個資外洩事故後面對詐騙、盜刷信用卡、或其他因為個人資料外洩後可能有的不良後果，因此電子商務業者於進行消費者溝通時，應設身處地以消費者目前的心境及壓力、急迫感覺作為建立溝通及後續處理的基礎。

2.組織授權人員提前進行事故反應與處理範圍。

3.資料外洩事故之成因往往複雜且需耗費時間進行調查，但消費者之壓力與媒體壓力有其急迫性，電子商務業者之商譽與業務

亦可能因為時間的拖延而惡化。

再者，事故後續的處理由於涉及的個體相當多且溝通、處理的步驟繁瑣需費時長久。因此電子商務業者應考慮授權事故應變小組或權責人員得於事故原因查清、確認前進行部分的處理，例如：先進行消費者溝通、協調或其他名單清查、準備作業等工作。

4.提供時間表

由於事故根因的調查耗費時間，因此電子商務業者在溝通時,如未能於消費者、媒體預期的時間內提出正確之調查說明，應主動提供相關預估時間表，以安撫相關消費者情緒及建立媒體的信任關係。若不提供時間表，往往造成媒體或消費者透過其他管道以及方式進行其他的調查或訊息探詢，反而容易造成電子商務業者更多的困擾，並可能衍生其他消息外洩或臆測問題。

5.溝通須注意相關事證、情況可能隨時會有變化

與消費者或媒體溝通時，由於資料外洩事故之調查可能因時間而有不同，例如：受害者的數量，外洩的資料欄位乃至於外洩的管道、技術細節等，因此電子商務業者應儘量以「截至目前調查結果..」,「依據目前證據判定...」等方式進行於事故期間的溝通，避免過於武斷或確認的言詞。

(三)開放、誠實及透明原則

1.透明的處理原則

電子商務業者於事故處理階段，應秉持透明之原則，誠實至上，避免過度的掩蓋事實(例如：內部員工外洩或遭糾舉掩蓋事實之風險)透明公開的處理方式，可以進一步的安撫客戶及取

得溝通間的信任基礎。

2.不要過於絕對的判定

由於資料外洩的成因、後果、數量、程度等均極為複雜，因此電子商務應避免絕對的判定，以避免因判定的錯誤造成其他的事故或造成更大的消費者或媒體輿論的攻擊。

3.避免誤導消費者

對於消費者可能因事故產生的不良後果，電子商務業者不應為降低外部壓力或減少後續之賠償等因素，藉由揭露資訊的方式或於溝通過程誤導消費者，例如：誤導消費者本次外洩事故之資料，將不足以被詐騙集團利用...等言詞。

4.別嘗試隱藏關鍵事證

由於關鍵的事證往往是後續事故處理，或消費者後續可能危害處理或預防的重要資訊，例如：外洩事故中隱瞞根因為駭客攻擊，或隱瞞已被惡意攻擊者勒索等重要事證以避免影響後續業務發展，但這些關鍵事證的隱瞞將誤導消費者或誤導相關處理者、執法者對於事故的應變。

5.聚焦且簡潔

溝通的內容應該包括：消費者、媒體所關心之議題，例如：事故根因、影響範圍、後續處理等主要議題，但須注意於溝通過程應聚焦且簡潔，避免離題、擴散或模糊事故的焦點。

(四)勇於負責

1.主動承擔責任

事故的處理中，電子商務業者的態度往往影響消費者情緒的安撫，不負責的態度將加深消費者的憤怒，並成為被攻擊的

主題。被迫負責往往造成後續攻擊力道的持續，因為消費者或媒體預期電子商務業者會迫於更大壓力而擔負更多責任。因此主動、積極於早期階段就能說明責任的承擔可以獲得較好的溝通結果。

2.別以受害者姿態博取同情

電子商務業者應避免以本身也是事故的受害者之姿態應對，例如：說明係受駭客之攻擊或受到內部員工誤用等藉口，由於安全防護、管理本來就是業者本身所需肩負的責任，受害之姿並無法達到卸責之效果，反而易形成推諉責任之形象。

3.表示歉意

由於消費者的積累情緒，如果電子商務業者未能對於事故進行抱歉，消費者會感到業者未對已造成的傷害或錯誤感到悔意或承認錯誤，因此適度的表達歉意，也是溝通中相當重要的態度與步驟。

(五)個資法遵循

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。」

因此電子商務業者應依據本規定，在資料洩漏事故發生後，於查明洩漏之原因後以適當方式通知消費者。

其中通知之方式與內容應遵循個資法施行細則第 22 條之規定：

1.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。

2.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。

因此電子商務業者可以以各種方式通知消費者，但內容必須注意包括消費者資料被侵害的事實與以採取之因應措施，並建議留下相關通知之紀錄，以利後續主管機關之查核及相關通知紀錄證明。

捌、附件

一、附件 1：電子商務業者個資外洩資安防護查核表(事前資安強化)

表7　電子商務業者個資外洩資安防護查核表(事前資安強化)

電子商務業者個資外洩資安防護查核表(事前資安強化)									
事前防禦措施			強化安全	事中、事後	降低動機、風險	提高知覺	基本	加強	檢核結果說明
A 網路安全架構強化									
	1	是否建立網路安全架構，於電子商務網站服務網段(主機區)建立防火牆或路由器設備，區隔外網區、DMZ 區以及內網區。	V				V		
	2	是否於主機區所有之對外連線區域建立 DMZ 區，以避免內網區直接對外連線或外網區可以直接進入內網區。	V				V		
	3	是否於辦公作業區，依據職務相關之連線需求與安全等級需求進行區隔，並控制相關區域對於主機區之連線能力及各區間的路由能力，以強化安網路架構安全。	V					V	
	4	是否限制辦公室區域，除主機管理、系統程式更新、資料庫管理等連線作業外，應儘量避免對於主機區域之直接連線，相關客服及業務單位之連線，應盡可能由外部透過防火牆控制方式進行連線，以避免惡意攻擊者進入辦公區後實施對主機區域的攻擊。	V					V	

電子商務業者個資外洩資安防護查核表(事前資安強化)									
事前防禦措施			強化安全	事中、事後	降低動機、風險	提高知覺	基本	加強	檢核結果說明
	5	主要資料存放設備例如：資料庫及重要檔案伺服器是否僅存放於內網區。	V				V		
	6	是否僅將有必要對外(Internet)連線之設備置放於 DMZ 區，非必要對外連線之設備，是否僅置放於內網區。	V				V		
	7	是否限制內網區之主機，不得直接連線至外網區，外網區之連線，不得直接進入內網區。	V				V		
	8	是否禁止於主機區主要資料存放區使用無線網路，以避免遭惡意攻擊者利用。	V				V		
	9	主機區內(如 DMZ 區、內網區)，是否依據區域內主機之功能、安全要求不同進行網路之區隔並限制必要之互相連線，以避免不同安全需求之主機於遭受攻擊後不影響其他區域主機。	V					V	
上述措施另可參考經濟部商業司電子商務交易安全規範(網路平台)V3.0 版—規範要求 4.1，或電子商務資訊安全機制與管理規範檢核表之 A1。									
B 網路安全管理									
	1	是否建立維持網路架構圖(Network Diagram)，並維持最新。網路架構圖中應包括所有的對外連線、網路區隔、安全設備及主要之網路服務主機及主要資料儲存設備。		V			V		

電子商務業者個資外洩資安防護查核表(事前資安強化)									
事前防禦措施			強化安全	事中、事後	降低動機、風險	提高知覺	基本	加強	檢核結果說明
	2	是否建立網路安全政策，強化對於使用無線網路安全之要求，包括：不得於主機區使用無線網路以及所有無線網路連線均須以防火牆或其他路由設備與辦公區網路區隔並限制僅允許核准之必要連線。	V				V		
	3	是否僅使用安全之網路協定(Protocol)，如須使用不安全之網路協定，應有相對應的安全保護措施。	V				V		
	4	是否僅於業務所必須(BusinessNeeds)開放網路連線，所有網路之連線限制，均應包括對於服務(Service)、協定(Protocol)、連接埠(Port)以及網路位址(IP)之限制。	V				V		
	5	是否限制及管控所有進出 DMZ 區之網路流量，包括：限制非必要之辦公區域進入內網區。	V				V		
	6	是否限制管控所有進入內網區之網路流量，由內網區及主要資料儲存區域對外之流量應僅限制為業務所必須。	V				V		
	7	消費者之資料或交易資料於公眾網路傳輸，是否僅以安全、加密之網路連線進行傳輸。	V				V		
	8	是否設置網路入侵預防設備以避免網路之入侵攻擊，並定期更新其偵測入侵所需之必要資訊。	V					V	
上述措施另可參考經濟部商業司電子商務交易安全規範(網路平台)V3.0 版—規範要求 4、(供應商)—規範要求 5.1、(物流商)—規範要求 6，或電子商務資訊安全機制與管理規範檢核表之 A4。									

電子商務業者個資外洩資安防護查核表(事前資安強化)									
事前防禦措施			強化安全	事中、事後	降低動機、風險	提高知覺	基本	加強	檢核結果說明
C 系統及設備安全管理									
	1	是否維持主機及系統、設備之清冊，盤點包括各系統、主機、設備之功能、設置位置、網路相關資訊及已實施之安全管理機制。		V			V		
	2	是否停止使用軟體供應廠商已停止安全支援服務或更新之軟體(例如：WindowsXP, Windows 2000 Server)。	V				V		
	3	是否依據最佳實務(Best Practice)建立系統安全組態(Configuration Standard)，並依據安全組態進行系統管理，包括所有安全設備、主機以及相關應用系統。	V					V	
	4	所有主機及設備是否在接入網路前，變更供應商預設之帳號或通行碼，並移除非必要之所有帳號。	V				V		
	5	所有主機系統應是否安裝一個主要功能，以避免不同安全等級要求之應用系統安裝於同一主機，降低該主機之安全等級。	V					V	
	6	所有主機是否僅開放必要之服務(Service)、協定(Protocol)、連接埠(Port)。	V				V		
	7	所有主機是否已移除非必要之功能、服務(Serviceor Daemon)、介面、子系統或檔案系統。	V					V	
	8	是否對所有非本機登入(non-consolelogin)之管理權限活	V				V		

電子商務業者個資外洩資安防護查核表(事前資安強化)									
事前防禦措施			強化安全	事中、事後	降低動機、風險	提高知覺	基本	加強	檢核結果說明
		動(Administrative activities)進行安全管控包括使用安全或加密保護之連線方式，非本機登入僅限制使用安全之協定(例如：SSH,VPN,TLS)。							
上述措施另可參考經濟部商業司電子商務交易安全規範(網路平台)V3.0 版—規範要求 2、(供應商)—規範要求 2、(物流商)—規範要求2，或電子商務資訊安全機制與管理規範檢核表之A3.A6。									
D 保護消費者資料安全									
	D.1 消費者資料保護								
	1	是否僅依據電子商務交易之需求進行資料之蒐集，包括蒐集之數量、欄位。			V		V		
	2	是否避免蒐集高風險之資料欄位，例如：特種個資、財務資料、完整個人資料(Profile)等。			V		V		
	3	是否避免儲存非必要之交易資料，例如：信用卡卡號、銀行帳號等，如須蒐集應符合相關法律規定，並實施必要之安全防護。			V		V		
	D.2 資料安全								
	1	是否進行重要消費者個人資料或交易資料存放位置盤點，包括：資料庫、檔案伺服器、應用系統、備份、紀錄檔、報表及其他資料可能出現的地方，並做成資料盤		V			V		

電子商務業者個資外洩資安防護查核表(事前資安強化)									
事前防禦措施			強化安全	事中、事後	降低動機、風險	提高知覺	基本	加強	檢核結果說明
		點清冊。							
	2	是否依據盤點資料每年進行至少 2 次資料盤點，確保所有資料的數量、安全保護、存放位置均為正確且被安全保護。		V		V	V		
	3	是否使用技術工具，例如：以卡號或個資之掃描工具定期進行對營運環境進行技術清查作業，確保沒有未被清查或盤點的個人資料，並確保無大量資料留存於個人電腦。掃描之區域應包括各類主機、個人電腦、安全設備紀錄檔等。		V		V		V	
	4	重要備份檔案是否進行加密，並儘可能以離線方式儲存，避免遭受網路之攻擊。	V		V		V		
	5	是否訂定資料保存期限，並每季進行過期資料之安全刪除，包括：已備份之資料以及紙本資料。	V		V		V		
	D.3 資料加密								
	1	是否針對主要資料庫主機及資料存放區進行加密機制保護。	V		V			V	
	2	是否針對超過一定數量消費者個人資料或交易資料之檔案或報告、紙本等進行安全保護，電子檔案應進行加密，紙本應進行實體控管。			V		V		
	3	加密應使用符合業界水準之加密強度	V		V			V	

電子商務業者個資外洩資安防護查核表(事前資安強化)									
事前防禦措施			強化安全	事中、事後	降低動機、風險	提高知覺	基本	加強	檢核結果說明
		(3DES,RAS2048,AES128 以上或其他業界水準認定為安全等級之加密)。							
	4	是否進行資料加密之金鑰(key)於保存、使用、不被未授權置換。	V					V	
	5	是否備妥金鑰管制程序，進行定期金鑰之更換，或在金鑰遭破解或其他弱化金鑰強度時進行更換等。	V					V	
	6	如果系統同時使用明碼資料儲存及密碼資料儲存，是否區隔並避免交互參照破解加密之可能。	V		V		V		
	D.4 資料庫主機安全								
	1	是否針對所有存放消費者資料或交易資料之資料庫主機及檔案伺服器進行弱點掃描，並進行弱點補強確認未有系統弱點存在。	V			V	V		
	2	重要資料庫主機是否依據標準組態進行設定，並使用安全組態工具進行檢查。	V			V		V	
	D.5 存取控制								
	1	是否針對資料庫主機進行嚴格管控，重要資料庫主機應限制可以主機登入(Console Login)之權限。	V				V		
	2	是否對於系統程式使用之帳號進行管控，程式使用之帳號，應限制不得進行資料庫主機登入(Console Login)，或	V					V	

電子商務業者個資外洩資安防護查核表(事前資安強化)									
事前防禦措施			強化安全	事中、事後	降低動機、風險	提高知覺	基本	加強	檢核結果說明
		其他方式進行直接取用資料庫資料。							
	3	是否對所有重要主機、安全設備遠端登入應使用安全協定外，並使用雙因子認證以確保安全。	V					V	
	4	是否開啟資料庫稽核作業功能，確保所有個人、程式或其他系統對資料庫資料存取均被記錄。紀錄檔案應被妥善保存，避免資料庫管理者或有權限者可以進行異動。		V		V		V	
	5	是否限制主要資料存放區之存取權限，消費者資料及交易資料不得存放於無權限管控之共用資料區。	V				V		
	6	安全區域內的重要主機、安全設備應設置高強度通行碼，至少為 12 碼以上並包含複雜度，每 60 天更換通行碼，不得與前 5 次使用過之密碼相同。	V				V		
	7	鎖定系統或應用程式重複錯誤登入次數超過 5 次以上之帳號。	V				V		
	8	辦公區域中不使用之網路線及網路接口，應以安全設備控管其連線能力或以實體方式阻絕未授權之接入使用。	V					V	
D.6 資料傳輸安全									
	1	於公眾網路傳輸消費者個人資料或交易資料應使用高強度加密之傳輸機制(例如：SFTP,VPN,TLS 等)。	V					V	
	2	嚴禁使用一般傳輸、信息工具進行傳輸未保護的消費者	V				V		

電子商務業者個資外洩資安防護查核表(事前資安強化)									
事前防禦措施			強化安全	事中、事後	降低動機、風險	提高知覺	基本	加強	檢核結果說明
		個人資料或交易資料進行資料。							
	3	是否於傳輸帳號、通行碼均時使用高強度密碼進行加密或於安全協定、通道下傳送帳號、通行碼等識別資料。	V				V		
上述措施另可參考經濟部商業司電子商務交易安全規範(網路平台)V3.0 版—規範要求 3、(供應商)—規範要求 3、(物流商)—規範要求 3，或電子商務資訊安全機制與管理規範檢核表之 D1-D4。									
E 維護弱點管理計畫									
	E.1 防範病毒及惡意軟體								
	1	是否於所有可能遭受病毒或惡意軟體之主機系統(包括 Linux 或其他平台 OS 主機)安裝防毒軟體並定期更新。	V					V	
	2	是否確保所有安裝之防毒軟體具備偵測、移除及保護系統之功能，並可以因應所有已知之病毒、惡意軟體類型。	V				V		
	3	確保所有個人電腦安裝之防毒軟體不被使用者自行停止或移除，並且定期更新。	V				V		
	E.2 維持安全之系統或應用系統								
	1	是否定期針對網站使用之系統(System)，包括網站主機、資料庫、安全設備等)進行安全性弱點掃描，並針對掃描結果進行修正，如原廠尚未提供修正程式時，應進行補	V			V	V		

電子商務業者個資外洩資安防護查核表(事前資安強化)									
事前防禦措施			強化安全	事中、事後	降低動機、風險	提高知覺	基本	加強	檢核結果說明
		強措施或暫停使用該功能或元件。							
	2	是否定期針對重要對外主機(Public Facing)進行滲透測試(Penetration Test)，並依據滲透測試結果進行修正，如原廠尚未提供修正程式時，應進行補強措施或暫停使用該功能或元件。	V			V		V	
	3	所有原廠提供(Vendor Supplied)安全更新是否於最遲於發布後一個月內安裝更新。	V				V		
	4	對外服務之網站應用程式(Public Facing)，是否定期及於網站應用系統或軟體元件重大更新上線前，進行網站應用程式安全掃描(Application Security Scan)，並依據掃描結果，排除可能的安全弱點或漏洞。	V				V		
	5	對外服務之網站應用程式(Public Facing)，是否使用或安裝網路應用程式防火牆(Web Application Firewall)並定期更新其偵測防禦所需資訊，以有效防止針對網站應用程式之攻擊。	V					V	
	E.3 應用系統開發安全								
	1	是否依據標準或產業最佳實務進行系統開發作業(例如：OWASP, NIST 等)以確保系統開發之安全。	V				V		
	2	是否於應用系統上線前，移除測試或非必要之帳號，通行碼以及測試資料。	V				V		

電子商務業者個資外洩資安防護查核表(事前資安強化)									
事前防禦措施			強化安全	事中、事後	降低動機、風險	提高知覺	基本	加強	檢核結果說明
	3	是否於應用系統上線前進行源碼檢查(Code Review)，源碼檢查應至少能偵測使用網路應用程式主要的漏洞或安全弱點(例如：OWASP Web Application TOP10)。	V					V	
	4	是否進行應用系統開發人員之系統開發安全防護訓練，以確保系統人員具備安全系統開發之能力(Secure coding)。	V				V		
	5	是否區隔測試區與正式區之管理權限，如為同一人執行，應分別不同的帳號並使用不同的通行碼，以避免誤用或遭惡意攻擊利用。	V					V	
F 監控系統及交易									
	1	是否將所有安全紀錄(Log)對應到應被記錄監控的個人，不應僅記錄群組、共用帳號或其他無法識別實際使用者的代號。		V		V	V		
	2	是否建立以自動機制或其他方式記錄以下 Log		V		V	V		
		A.所有個人(非系統)對於消費者個人資料或交易資料之存取。							
		B.所有個人執行以管理者權限(Administrator 或 root)的所有活動，包括：以提升權限或最高權限執行程式。							
		C.對任何系統之稽核軌跡(Audit Trail)之存取動作。							

電子商務業者個資外洩資安防護查核表(事前資安強化)									
事前防禦措施			強化安全	事中、事後	降低動機、風險	提高知覺	基本	加強	檢核結果說明
		D.所有提升權限的動作。							
		E.任何對於具備系統 Root 或 Administrator 權限帳號的新增、修改、刪除動作。							
		F.啟動、暫停或停止稽核記錄機制(Audit Log)。							
		G.新增或移除系統元件動作。							
	3	是否設置避免管理人員或具備管理權限之其他人員對稽核紀錄進行任何變更，包括主機、設備內及集中蒐集之紀錄檔。		V			V		
	4	所有紀錄應至少保留至少一年。		V			V		
	5	所有稽核紀錄，包括位於 DMZ 區之主機及安全設備 Log 應存放於內網區，並嚴格限制存取，以避免遭受惡意攻擊者變造或抹除。	V	V				V	
	6	所有系統應進行同步校時，並應設定可靠之校時主機(TimeServer)。		V			V		
	7	應設置檔案變更管理監視機制(File Integrity Management)監控重要主機設備、安全設備之 Log，並在 Log 被未授權變更、刪除時預警通知管理人員。		V				V	
G 人員與環境安全									

電子商務業者個資外洩資安防護查核表(事前資安強化)									
事前防禦措施			強化安全	事中、事後	降低動機、風險	提高知覺	基本	加強	檢核結果說明
	G.1 人員安全								
	1	上述措施另可參考經濟部商業司電子商務交易安全規範(網路平台)V3.0 版—規範要求 1.4、(供應商)—規範要求 1.3、(物流商)—規範要求 1.3，或電子商務資訊安全機制與管理規範檢核表之 A1。							
	G.2 環境安全								
	1	是否強化實體安全，避免惡意攻擊者透過實體進入辦公區域竊取資訊、設備或安裝網路監聽設備、入侵設備等。							
	2	辦公區域中不使用之網路線及網路接口，是否以安全設備控管其連線能力或以實體方式阻絕端口以避免未授權之使用。							

資料來源： 本計畫整理

二、附件 2：電子商務業者個資外洩資安防護查核表(事中應變)

表8　電子商務業者個資外洩資安防護查核表(事中應變)

電子商務業者個資外洩資安防護查核表(事中應變)									
事中應變查檢表			作業目的	產出	需求資源	注意事項	執行人員	支援人員	檢核結果說明
A 調查/確認階段									
	A.1 調查階段- 查證是否資料為本組織外洩								
	情境說明		電子商務商家接獲客戶通報，其資料遭詐騙集團使用，詐騙集團並能說明其轉帳設定錯誤等方式誘騙，詐騙集團知悉之內容包括交易日期、姓名、購買物品內容等。						
	1	透過資料庫進行資料查詢，確認資料是否為本公司所有，包括通報內容之包含之欄位、日期、資料內容等。	確認是否為我方客戶，確認資料是否可能自我方流出。	回應前端業務，該筆資料是否為本組織所有。	客戶資料庫。	在系統未確認是否遭駭，建議盡可能不要使用系統管理權限登入查詢，儘量以一般之系統權限進入。			
	2	查詢通報項目過去之交易紀錄。	確認此一消費者過往交易過的紀錄，包括：金額、日期、品項等。	客戶交易歷史資料檔。	客戶資料庫。	在系統未確認是否遭駭，建議盡可能不要使用系統管理權限登入查			

電子商務業者個資外洩資安防護查核表(事中應變)									
事中應變查檢表			作業目的	產出	需求資源	注意事項	執行人員	支援人員	檢核結果說明
						詢，儘量以一般之系統權限進入。			
	3	依據通報內容進行交易日期查詢，並設定出可能資料外洩之日期，如無其他方式訂出可能外洩事故之熱區，則依據該通報的交易日期時間為中心點(D Day)，往前後三個月內為熱區(Hot Zone)[14]，往前六個月為溫區(Warm Zone)[15]。	訂出入侵或外洩可能的日期熱區以利後續調閱資料之可能窗口，以避免一次須調閱太多的事件，作為重點查詢之範圍。	事故發生可能熱區或溫區。	透過客戶交易查詢相關系統。	備註，由於用來詐騙的資料有其新鮮度的限制，過久的資料並無法有效進行詐騙，因此此熱區與溫區時間並非固定，係由實際之情境而定。			

[14]熱區(Hot Zone)：亦稱為災區。

[15]溫區(Warm Zone)：亦稱為警戒區。

電子商務業者個資外洩資安防護查核表(事中應變)									
事中應變查檢表			作業目的	產出	需求資源	注意事項	執行人員	支援人員	檢核結果說明
	4	調閱受害消費者於主機存放之資料於熱區時間內被存取的應用程式內存取紀錄、網站存取紀錄、資料庫存取紀錄，並比對此三紀錄於存取該筆紀錄的數量、時間是否吻合。	藉由比對網站、應用系統、資料庫 Log 判定是否可以找出外洩前可能的存取點(係來自網站、應用層，還是透過資料庫層)。	查詢系統記錄事故與外洩事顧是否關聯。	系統 Log 資料（包括 Web、AP、DB)三層。	儘可能使用另外存放的系統紀錄(例如：Log Server)，以避免進入個主機取用(需登入主機)。			
	5	調閱受害消費者存於主機以外地區存放之資料於熱區時間內被存取的紀錄。	查詢主機以外區域包含該筆資料之檔案或資料庫、備份等資料是否有在熱區時間內被存取的紀錄。	查詢是否有異常存取客戶資料檔案之跡象。	資料盤點清冊，確認所有有可能存放的位置及型態。	由於其他類型資料客戶能無單筆之資料存取紀錄，應查閱對於整個檔案的存取紀錄。			
	6	檢視熱區及溫區內系統異常通報紀錄，包括：防火牆、	先由出現異常狀況之紀錄查詢系統，記錄事故與外洩事顧是否關聯。	關聯性判定。	需求 Log 記錄、告警(Alert)紀錄及	儘可能使用另外存放的系統紀錄(例如：Log Server)，以避免進入個			

電子商務業者個資外洩資安防護查核表(事中應變)									
事中應變查檢表			作業目的	產出	需求資源	注意事項	執行人員	支援人員	檢核結果說明
		資料庫、網站主機等。			處理紀錄。	主機取用(需登入主機)。			
	7	檢視各段網路流量紀錄(例如：MRTG)，各主機之流量，比對熱區時間內，存放資料的主機是否出現較大的網路流量。	資料於入侵發生時會產出異常的網路存取量，尤其資料庫系統等，但此比對需依據該主機之流量以被單存化，如主機具備複雜功能，比對之可能性較小。	判定異常流量之紀錄，作為進一步深入比對之依據。	透過網管系統紀錄，MRTG 圖(各主機)。	如果組織未建立以主機為主的流量監控方式，則此方法將不會有效果。			
	8	依據前述 4-6 步驟，如果能限縮相關範圍(例如：發生在哪一層、哪一個檔案或更精確的時間)，依據該範圍進行後續步驟，如果未能發現，嘗試使用溫區時間進行相同測試。							

電子商務業者個資外洩資安防護查核表(事中應變)									
事中應變查檢表			作業目的	產出	需求資源	注意事項	執行人員	支援人員	檢核結果說明
	A.2 查詢可能攻擊的來源/入侵跡證								
	說明		判斷攻擊的來源/入侵跡證將可以協助商家產出可能的攻擊方式，並採取進一步的調查作業						
	1	依據前段判定定義的可能事故發生時間、熱區、溫區或判定後的限縮範圍進行進一步做可能攻擊的來源與入侵跡證及原因之判定。	找尋可能攻擊的來源與判定入侵跡證及原因。	判定說明報告。	由相關系統紀錄、設定檔找尋攻擊可能的來源及入侵的根因。				
B 緊急處理階段									
	1	確認/判定外洩發生原因或結果後回應。	回應告知客戶或單位。	初步回應說明。		回應應視實際狀況以及調查結果階段能掌握的內容為主，或於僅及處理階段完成後再進行回應。			
	B.1 控制階段								

電子商務業者個資外洩資安防護查核表(事中應變)									
事中應變查檢表			作業目的	產出	需求資源	注意事項	執行人員	支援人員	檢核結果說明
	1	進行必要之證據保存。	避免破壞後續所需之紀錄。	透過無破壞複製方式將主機之主要系統資料及組態進行複製。	可能需要外部專業人員及相關複製設備。	複製過程不應產生對系統狀態、紀錄相關的破壞。			
	2	於確認可能的外洩事件主機及應用系統、相關系統後，應做緊急控管、隔離之計畫。	為進行事故控制做準備。	產出事故控制、主機、服務隔離作業準備	主機架構、網路架構、資料庫列表等。				
	3	營運持續作業準備。	於開始處理相關作業前，由於針對網站、資料庫主機進行任何管制、處理作業時，將可能造成服務的中斷或其他影響，因此須於進行主機處理作業時進行營運持續作業評估，並依據評估做好相關準備。	營運持續計畫。	營運持續可能需求的主機、轉址、臨時架構資料庫等資源。	於拔除主機前，應備妥相關告知之網頁或轉址，如要以更換主機 IP 之方式，請注意如選用以更動 DNS 內指向 IP 可能須注意該 IP 實際生效時間。			

電子商務業者個資外洩資安防護查核表(事中應變)									
事中應變查檢表			作業目的	產出	需求資源	注意事項	執行人員	支援人員	檢核結果說明
	4	進行證據保全措施。	在進行主機事故根因調查及處理前進行證據之保全作業。	依據證據保全作業產出之備分或證據複製。	內部、外部技術人員、資安專家以及數位鑑識人員等。	須注意不當的證據保全措施將會影響證據的有效性，以及可能破壞證據的完整。			
	5	進行受入侵主機之隔離及控制作業。	依據前述之規劃之處理方式以及營運持續之準備進行主機之隔離與控制決議進行控管措施。		所有紀錄及系統設定、相關工具。	應依據指引中相關主機緊急處理應注意事項辦理。			
	6	紀錄所有緊急處理作業之內容。	緊急處理作業由於將於短時間內進行主機的各項調整、組態變更或針對應用系統做緊急的調整，因此必須記錄所有以執行步驟、細節以確保後續追蹤或系統恢復、還原時之參考依據。	緊急處理作業紀錄。		內容應包括時間、人員、作業動作、技術細節、執行原因、判定、Snapshot 或 Baseline 變更前之狀態、預期衝擊等內容。			
	7	通知利害相關者。	由於電子商務業務可能涉及上游、下游或合作廠商	相關單位通知清單。	組織通知人員。	應注意於通知相關單位時，利害相關者知悉			

電子商務業者個資外洩資安防護查核表(事中應變)									
事中應變查檢表			作業目的	產出	需求資源	注意事項	執行人員	支援人員	檢核結果說明
			等，應於進行緊急處理前通知相關單位。			外洩事故後是否會對外發言、外洩之問題。			
	8	準備消費者回應。	在緊急控制措施完成後，應開始準備相關的消費者回應作業，以進入事故後處理作業階段。		事故應變小組。				
C	初步回應階段								
	C.1 內部發現之事故								
	1	由內部發現的事故開始到需要回應給客戶或主管機關階段的時間壓力較低，所以可在緊急處置完成後，於下一階段之事故後處理進行回應。							
	C.2 外部發現之事故								
	1	建立回應窗口。	建立有效、一致的回應窗口，避免因回應之方式或說法產生額外問題。		事故應變小組以及指定之發言人員。				
	2	產出回應之內容。	建立一致、完整之回應內容，以統一對外之回應說法	回應內容	事故應變小組。	請參考本指引文件內之溝通建議，進行相關消			

電子商務業者個資外洩資安防護查核表(事中應變)									
事中應變查檢表			作業目的	產出	需求資源	注意事項	執行人員	支援人員	檢核結果說明
			及避免衍生其他枝節問題。			費者之溝通作業。			
	3	進行回應作業。	依據備妥回應的內容及窗口進行消費者回應作業，透過說明進行客戶之溝通及安撫。	回應作業結果紀錄	相關回應人員、紀錄回應結果所需之系統或機制。	如回應後消費者要求進一步的說明或要求，應由應變小組進行後續的應對方式進行作業修正等。			
	C.3 通知相關單位機關								
	1		達到法律、規定、產業規定或相關契約的告知義務。	通知結果紀錄	應於事前查明相關法律、規定產業規定及合約之事故通知要求。				

資料來源：本計畫整理