經濟部

資安防護參考指引推廣說明會

指導單位：經濟部商業司
主辦單位：資策會資安科技研究所
中華民國無店面零售商業同業公會

中華民國 106 年 8 月 30 日

資安防護參考指引推廣說明會

※時間：106 年 8 月 30 日 13:30~16:30

※地點：集思台大會議中心 洛克廳（台北市羅斯福路四段 85 號 B1）

※議程：

時間	內容	講者
13:30 ~ 14:00	來賓報到	
14:00 ~ 14:10	主席致詞	
14:10 ~ 14:50	電商業者反詐騙宣導方式成效分析及「解除分期付款」詐騙案防制建議	刑事警察局 165 反詐騙諮詢專線 黃泰詠偵查員
14:50 ~ 15:30	電子商務個資外洩資安防護參考指引說明	資策會 李彥震顧問
15:30 ~ 15:40	中場休息	
15:40 ~ 16:20	扮演柯南－如何留下駭客進攻足跡	奧盛網路營銷 李嘉峻資安經理
16:20 ~ 17:00	看對醫生找對方法－談資安診斷 3 步驟	Deloitte 勤業眾信 陳威棋協理

電子商務業者反詐騙宣導方式成效分析
—兼論「解除分期付款」詐騙案防制建議

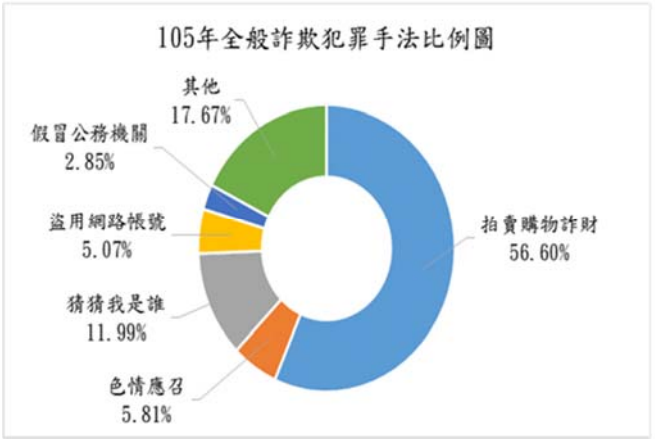
報告單位：內政部警政署刑事警察局
106年8月30日

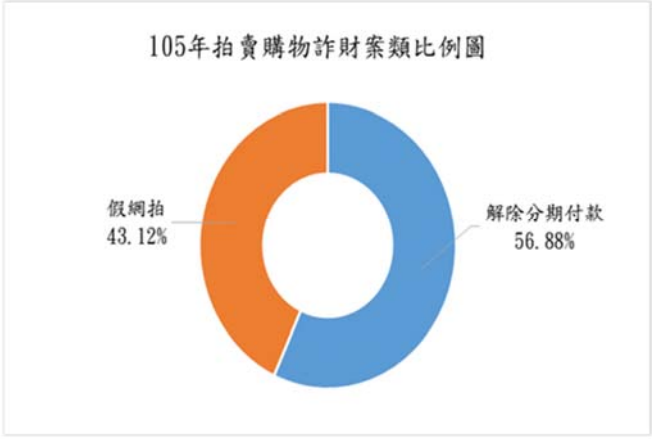
大綱

- 壹、前言
- 貳、現況分析
- 參、建議事項及效益評估
- 肆、結語

壹、前言

165反詐騙諮詢專線統計去（105）年拍賣（購物）詐財案類占全般詐欺案件之56.6%，該案類其中又以「解除分期付款」比例最高（占56.88%，如下圖），故以下僅就各電子商務業者之反詐騙宣導方式進行彙整及評估，提供各業者自我檢測，適時選擇較佳之宣導方式，期能有效提醒消費者。

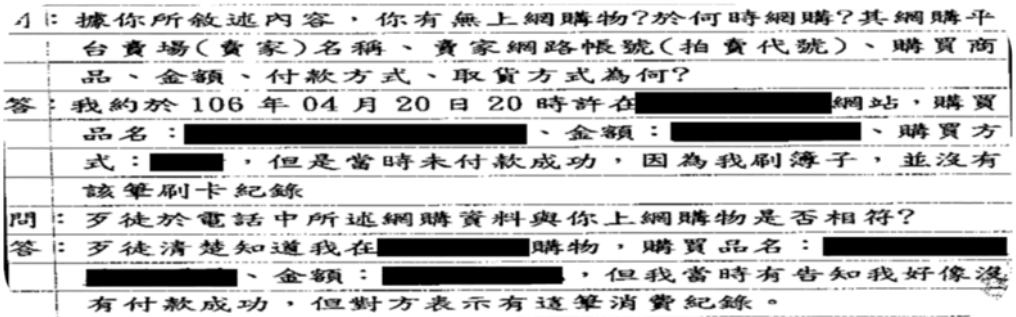




貳、現況分析

一、現況問題

165反詐騙諮詢專線統計去年全國受理「解除分期付款」詐欺案，單一電子商務業者被害案件發生數逾100件者計件18家，其中逾500件者達6家。經查被害人調查筆錄，被害人均稱接獲客服人員來電，因內部作業人員疏失誤設定成批發商、團購或分期付款，如要變更設定須前往自動櫃員機（ATM）解除，俟被害人聽從指示前往操作後方驚覺受騙。依被害人所言，歹徒明確掌握其所購買之商品、金額、付款方式以及連絡電話，故研判歹徒先行取得各拍賣購物平臺消費者資料後，再施以詐術詐騙被害人（如下圖）。



問：據你所敘述內容，你有無上網購物？於何時網購？其網購平台賣場（賣家）名稱、賣家網路帳號（拍賣代號）、購買商品、金額、付款方式、取貨方式為何？

答：我約於106年04月20日20時許在[redacted]網站，購買品名：[redacted]、金額：[redacted]、購買方式：[redacted]，但是當時未付款成功，因為我刷簿子，並沒有該筆刷卡紀錄

問：歹徒於電話中所述網購資料與你上網購物是否相符？

答：歹徒清楚知道我在[redacted]購物，購買品名：[redacted]、金額：[redacted]，但我當時有告知我好像沒有付款成功，但對方表示有這筆消費紀錄。

貳、現況分析

二、分析問題

(一)業者網路資訊安全恐有漏洞，疑個資外洩情形嚴重：業者雖增加網站資安維護成本，惟作業系統（瀏覽器）的漏洞、程序撰寫的錯誤或管理人員的疏忽，以及民眾所使用的個人電腦或智慧型手機未能即時更新或遭植後門程式，均為資料外洩因素，資安維護需持續強化。

(二)歹徒隨機挑選攻擊目標，業者因應時間不足：歹徒以隨機方式對不特定網路賣場資安漏洞實施攻擊並竊取個資，業者經常以個案看待且因應時間短暫，失去防範未然之先機。

(三)物流管道多樣，從業人員素質參差不齊，疑個資外洩原因之一：因現今物流管道多樣且競爭，而勞力密集之工作型態使從業人員素質參差，於貨品配送過程中可能故意或過失致使民眾個資外洩。

(四)民眾欠缺防詐意識：以某電子商務業者為例，本局曾隨機抽訪於106年2月20日至3月5日期間之被害人計82名，有效回應者20名，其中有13名(占65%)曾接獲該電商登或寄發之反詐騙宣導訊息，有7名(占35%)未收到宣導資訊。而於前述13名中，有6名於受騙前即有接獲訊息，究其原因，被害人表示多因歹徒能夠詳述其所購買物品之時間、金額及配送方式等，使渠等誤信以確為客服人員而前往操作ATM；亦或雖曾接獲反詐騙相關訊息，惟渠並未留意，致接獲電話時仍遭詐騙，顯見仍有不少民眾欠缺防詐意識。

參、建議事項及成效評估

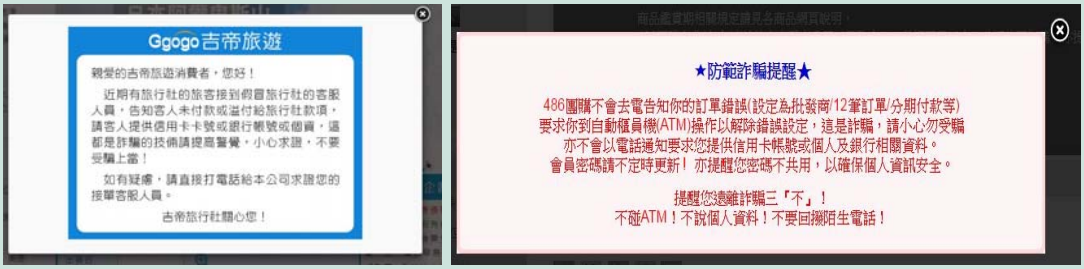
參、建議事項

一、蒐集各業者宣導方式（建議電子商務業者防制詐欺作為自評表）

建議項目		自評內容	
		符合	未符合
官方網頁首頁及會員登入處	官方網頁明顯處加註反詐騙警語		
	設置全版面彈跳視窗		
	網頁標明客服專線及客服時間		
	設置反詐騙宣導專頁		
	會員登入處加註反詐騙警語		
	結帳後，以彈跳視窗顯示提醒標語		
其他措施	針對會員發送反詐騙提醒簡訊		
	發送反詐騙會員通知信或電子報		
	貨品包裝（紙箱）印製反詐騙宣導警語		
	適時發布新聞（澄清）稿		
	延長客服時間至22時		
	錄製防詐騙客服語音置於第一層選單		
	利用手機APP推播功能提醒消費者		
	利用其他平臺推送反詐宣導（LINE、FB）		
	採用到店取貨方式，顧客無須留手機		
	個資隱蔽(於商品出貨後移除消費者手機聯繫資料或隱蔽聯繫方式)		
	將顧客訂單「手機」資訊另外置放儲存		

參、建議事項

一、蒐集各業者宣導方式

1	官方網頁明顯處加註反詐騙警語	
2	設置全版面彈跳視窗（宣導漫畫取代文字）	

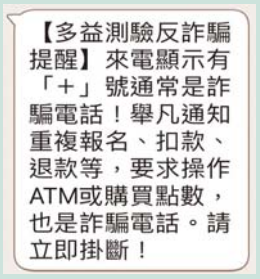
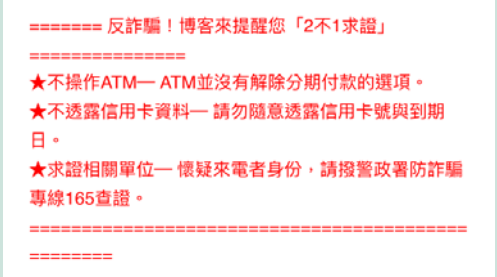
參、建議事項

一、蒐集各業者宣導方式

3	會員登入處加註反詐騙警語	 
4	結帳後，以彈跳視窗顯示提醒標語	 

參、建議事項

一、蒐集各業者宣導方式

5	針對會員發送反詐騙提醒簡訊	親愛的可樂旅遊消費者，您好，近期偶有詐騙集團假冒可樂旅遊客服人員，來電告知您「訂單錯誤」（例如：謊稱為「可樂網」人員、訂單變「團購客戶」、重複訂購、信用卡重複扣款、設定分期付款等），並要求您至自動櫃員機（ATM）操作（甚至只是查餘額），以解除錯誤設定。詐騙集團人員來電號碼開頭均有「+」號，請提高警覺，切勿受騙！如對訂單有疑義，請連繫您的接單客服人員，或撥165反詐騙專線諮詢，謝謝。可樂旅遊開心您 106年4月14日。此為系統傳送，請勿直接回覆。 → 親愛的可樂旅遊會員您好近期偶有詐騙集團假冒可樂旅遊同仁來電以各種擬真手法進行詐騙，提醒您，本公司不會以電話要求提供信用卡資料或要求至ATM轉帳或查詢餘額等，若遇上述可疑狀況，請即撥打本公司您的報名客服人員求證或撥165反詐欺專線。「請特別留意下班後或假日的可疑來電，提高警覺，切勿受騙」…可樂旅遊開心您 
6	發送反詐騙會員通知信或電子報	 

參、建議事項

一、蒐集各業者宣導方式

7	貨品包裝（紙箱）印製反詐騙宣導警語	 
8	適時發布新聞（澄清）稿	 

參、建議事項

一、蒐集各業者宣導方式

9	清楚標明客服方式（延長客服至22時）（客服語音反詐宣導）	
10	利用其他平臺推送反詐宣導（LINE、FB）	  

參、策進作為

一、蒐集各業者宣導方式

11	**採用到店取貨方式，無須留手機 個資隱蔽(於商品出貨後移除消費者手機聯繫資料或隱蔽聯繫方式)**	

個人資料保護法第十二條（0990427 全文修正）

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。

立法理由二、按當事人之個人資料遭受違法侵害，往往無法得知，致不能提起救濟或請求損害賠償，爰規定公務機關或非公務機關所蒐集之個人資料被竊取、洩漏、竄改或遭其他方式之侵害時，應立即查明事實，以適當方式（例如：人數不多者，得以電話、信函方式通知；人數眾多者，得以公告請當事人上網或電話查詢等），迅速通知當事人，讓其知曉。

參、建議事項

二、成效分析（擇2電商進行效益評估）

本局觀察去年至今年上半年A業者被害發生數趨勢，去年1月及4月份曾有200餘件之高峰，之後略趨穩定，直至本年1月再度發生100餘件、3月份發生近300件，顯示該賣場客戶資料隨時仍有遭歹徒竊取之可能。

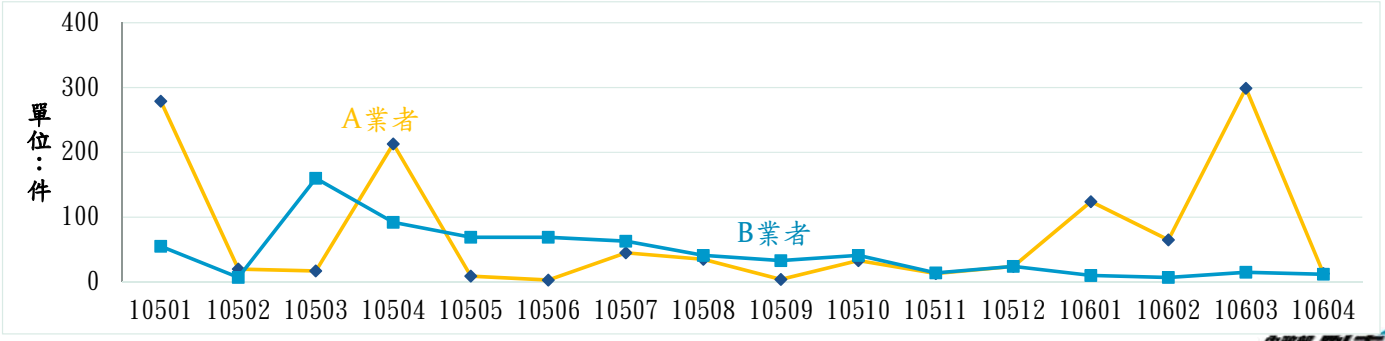
今年3月自發現該賣場詐騙被害案件數有急遽升高趨勢，即與業者保持聯繫，惟經於官方網頁放置反詐騙文宣及發送21萬封會員通知信後，被害發生數仍未下降。究其原因，疑電子商務業者寄送電子報或會員通知信過於頻繁，民眾多將上開信件直接移至垃圾信件區，甚至直接封鎖來自電商業者之信件，致使未能充分發揮提醒功能，效果不彰。

為遏止被害案件數發生並強化民眾防詐意識，本局於3月18日發布新聞稿並接受媒體採訪；再於3月22日邀集相關單位及業者共同研商因應對策，提供本局參考建議事項，請業者補強現行宣導措施不足處；另業者亦於3月23日啟用新版購物網頁，民眾於加入會員或使用到店取貨服務，均無須提供手機號碼，迄今觀察相關因應對策已漸收成效，惟後續效果仍為觀察重點。

參、建議事項

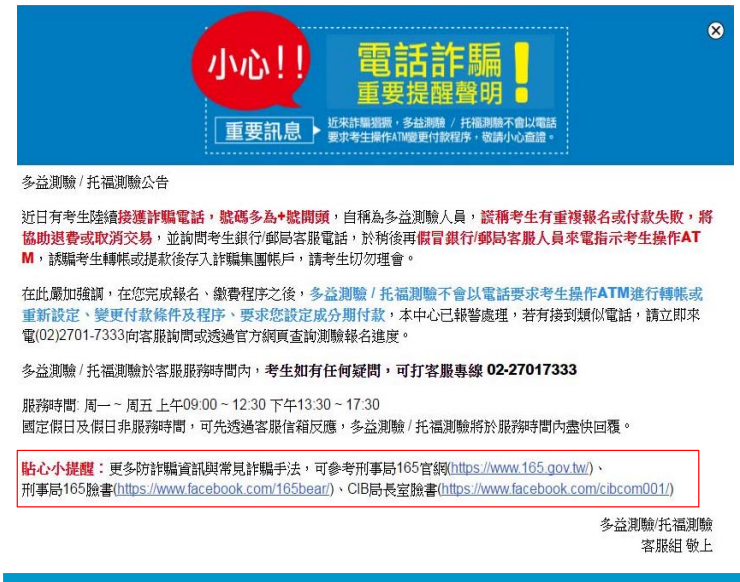
二、成效分析

觀察同區間電子商務業者B被害發生數趨勢，去年3月曾達160件之高峰，4月仍近百件惟5月之後持續降低，迄今每月案件被害發生數趨零星，與A業者相比較為平穩。自本局去年發現該賣場「解除分期付款」詐欺案類有升高趨勢，即與業者密切保持聯繫，提供即時數據供該業者參考。而該業者亦依據所提供之資料，針對網站同時進行「強化帳號安全機制」、「強化交易安全機制」、「防詐宣導」以及「資安聯防」4大面向之改善。



參、建議事項

二、成效分析（提供多元化宣導管道）


小心!! 電話詐騙 重要提醒聲明！

重要訊息 近來詐騙猖獗，多益測驗 / 托福測驗不會以電話要求考生操作ATM變更付款程序，敬請小心查證。

多益測驗 / 托福測驗公告

近日有考生陸續接獲詐騙電話，號碼多為+號開頭，自稱為多益測驗人員，謊稱考生有重複報名或付款失敗，將協助退費或取消交易，並詢問考生銀行/郵局客服電話，於稍後再假冒銀行/郵局客服人員來電指示考生操作ATM，誘騙考生轉帳或提款後存入詐騙集團帳戶，請考生切勿理會。

在此嚴加強調，在您完成報名、繳費程序之後，多益測驗 / 托福測驗不會以電話要求考生操作ATM進行轉帳或重新設定、變更付款條件及程序、要求您設定成分期付款，本中心已報警處理，若有接到類似電話，請立即來電(02)2701-7333向客服詢問或透過官方網頁查詢測驗報名進度。

多益測驗 / 托福測驗於客服服務時間內，考生如有任何疑問，可打客服專線 02-27017333

服務時間: 周一 ~ 周五 上午09:00 ~ 12:30 下午13:30 ~ 17:30
國定假日及假日非服務時間，可先透過客服信箱反應，多益測驗 / 托福測驗將於服務時間內盡快回覆。

貼心小提醒：更多防詐騙資訊與常見詐騙手法，可參考刑事局165官網(https://www.165.gov.tw/)、刑事局165臉書(https://www.facebook.com/165bear/)、CIB局長室臉書(https://www.facebook.com/cibcom001/)

多益測驗/托福測驗
客服組 敬上


謹防詐騙

進入165防詐騙網站>>

若您接到 +開頭的電話就算顯示是我們的電話請務必小心是詐騙集團來電。詐騙集團經常都在下班後來電，若有疑問請 立即撥打 165防詐騙專線尋求幫助！

客服不會跟您要求您的個人資料、如:信用卡卡號、密碼、存摺帳號，也不會要求您去ATM做任何取消或更改的動作。

刑事警察局

接到來電這樣說：
→內部作業疏失，誤將您先前的訂單設成分期付款（批發商、團購）……
→請您提供常用之銀行或郵局金融卡背面的客服電話……
→要求操作ATM解除設定，時間過晚上12點就會開始扣款……

上面這些都是詐騙集團常用的話術，千萬別去操作ATM！

實場名稱	被害件數
EZ訂（電影票券）	22
雄獅旅行社	15
明洞國際	13
DEVILCASE	11
HITO本舖、Q小舖	10

統計日期：106年7月24日至106年7月30日

民眾通報高風險賣場（平臺）

165官網：搜尋「警政署165反詐騙」　165APP：iTunes Store或Google Play搜尋「165反詐騙」
165 LINE：@tw165　165臉書：搜尋「165反詐騙宣導」，有刑事Bear才是官方版

二、成效分析（懶人包宣導方式）

肆、結語

電子商務
個資外洩資安防護
參考指引說明

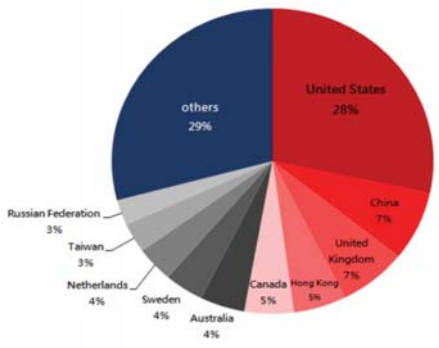
資策會 資安科技研究所
李彥震
20170830

固若金湯 - 為何資料仍舊遭竊？

- 資安事件持續頻傳
  - 技術挑戰?
  - 管理挑戰?
  - 組織設計/職能不足挑戰?

2017上半年度全球前10區域占全球攻擊總次數比例

排名	區域	全球總攻擊次數占比%
1	United States	28%
2	China	7%
3	United Kingdom	7%
4	Hong Kong	5%
5	Canada	5%
6	Australia	4%
7	Sweden	4%
8	Netherlands	4%
9	Taiwan	3%
10	Russian Federation	3%



資料外洩主要管道說明

- 伺服器端遭駭客入侵將資料外洩
  - 任何對外之伺服器均有可能遭駭客入侵，目標可能是應用程式、掛載之服務或作業系統之漏洞遭利用或設定疏忽所造成
- 擁有權限之使用者端電腦遭惡意程式感染或駭客入侵
- 擁有權限可存取敏感性資料之使用者端電腦遭感染或駭客入侵，導致敏感性資料遭外洩

駭客入侵或惡意程式感染之主要管道

- 人為的疏失造成
  - 設定或管理疏失
  - 下載及執行被偽裝的程式或檔案
- 駭客入侵
  - 大多利用系統漏洞或設定疏失
    - 作業系統漏洞 / 服務漏洞(FTP、Http 、 DNS 、 Mail / 網站漏洞 / 應用軟體漏洞...等路徑)
  - 若漏洞被駭客發現早於系統修補時間
    - 零時差攻擊

資安管理需注意之問題

- 檢視所有對外主機
  - 是否有對外伺服器疏忽？(電話通信主機/CCTV/測試機...)
  - 重要伺服器均放置DMZ ，其設定允許協定及方向
  - 帳密管理
    - 共同
    - 密碼設定太簡單
  - 遠端存取管理
  - Log 稽核
- 委外管理
- 異常能否查覺

參考指引與資安基本查核表(1/2)

- **經濟部商業司制訂個資外洩資安防護參考指引與資安基本查核表，作為網路零售業者檢視平臺及營運管理的資安基礎能力之參考**
- 參考指引與查核表屬非強制性要求
  - 透過鼓勵方式引導網路零售業者自主管理，取代立法之強制規範
  - 協助業者解決資安問題，以確保臺灣網路零售業環境的安全
- EC-CERT電子商務資安服務中心提供咨詢服務，是網路零售業者可以利用的資源

參考指引與資安基本查核表(2/2)

依據參考指引之內容濃縮成資安基本查核表，控制措施分為人員、作業、技術及設備等四大類，共四十項控制措施

人員	5項控制措施
技術	10項控制措施
作業	20項控制措施
設備	5項控制措施

參考指引與資安基本查核表整體架構圖

資安基本查核表-作業執行方式

業者預防性自主管理

作業管理

業主依據資安基本查核表之要求，
執行自評作業。

諮　詢

EC-CERT以電話/email進行顧問諮詢，
協助解決資安問題

顧問服務

重大資安問題資安顧問團隊，提供
實地現場服務，協助解決資安問題。

網站自行下載

中華民國無店面零售商業同業公會
網址：http://cnra.org.tw/
EC-CERT電子商務資安服務中心
網址：http://ec-cert.org.tw/

Email索取

中華民國無店面零售商業同業公會
塗家興　組長
nemos@cnra.org.tw

服務電話：(02) 2701-0411　塗家興　組長

資安基本查核表內容重點說明

人員　5項控制措施

項次	建議控制措施
1	指定專人負責資安及個資保護政策、計畫與管理之工作事項，訂定相關程序文件。
2	檢查同仁存取關鍵服務、客戶資訊，客戶要求的內容已納入安全管理責任並正式授權。
3	每年至少執行一次公司員工資訊安全及個資保護認知宣導訓練。
4	每年應對公司個資專責人員及資安人員至少執行一次資訊安全及個資保護教育訓練。
5	員工和廠商在被允許存取資訊或設施之前，均應簽署機密性或保密協議

資安基本查核表內容重點說明

作業 20項控制措施(1/2)

項次	建議控制措施
6	依據營運要求，訂定「個人資料保護管理」、「資訊安全政策」、「個人資料檔案安全維護計畫」及「業務終止後個人資料處理方法」等管理程序文件及管制措施並定期審查檢討。
7	客戶之個人資料及客戶交易檔案，每年至少執行一次清查工作並定期審查維護。
8	建立帳號管理，包含帳號權限之申請、開通、停用及刪除並定期清查帳號權限，不得有共用帳號之行為。
9	硬體設備、應用軟體及系統軟體等之最高權限帳號應列冊保管；最高權限帳號使用時須先取得權責主管同意，並保留稽核及審查紀錄。
10	超過所規定之預期閒置時間或使用期限，系統應自動將使用者登出。
11	資訊系統管理者應保存可識別存取來源的稽核軌跡，並定期審查使用者帳號活動，若發現帳號不正常使用時，應回報管理者及主管。
12	避免使用未經授權之電腦程式，及其他可能涉及侵害智慧財產權之行為。
13	建立並遵循電子郵件使用安全管理作業之規定。
14	建立並遵循使用者通行碼管理之作業規定
15	個人電腦及主機應有即時掃描及攔阻病毒之防毒軟體，並隨時更新病毒程式碼。

資安基本查核表內容重點說明

作業 20項控制措施(2/2)

項次	建議控制措施
16	定期進行設備、系統元件、資料庫系統及軟體漏洞修補。
17	建立並遵循媒體及可攜式儲存媒體使用安全管理作業規定。
18	資訊系統及設備僅開啟必要之網路、服務、程式及通道，使用者僅能存取已被授權使用之網路服務、程式及通道。
19	使用遠端連線應使用強度足夠之加密通訊協定，不得將通行碼紀錄於工具軟體內。
20	資訊系統、個人資料、重要資料(資料庫)及軟體應定期備份，並定期執行回復測試。
21	確立與營運所在地之警察機關、主管機關及EC-cert等相關機構之聯絡體制、資安事件管理文件及紀錄留存。
22	服務或設備委外時，應事先明確訂定作業目標、範圍及雙方權力義務。
23	確定委外廠商之各項安全措施可以符合資料安全及個人資訊保護等法令法規。
24	委託契約內容應包含資訊處理方式、安全政策保護及個人資料保護相關事項之管理及檢核。
25	定期稽核及審查責任範圍內的資訊設施與安全政策、標準及其他任何安全要求的遵循性，並保留相關紀錄。

資安基本查核表內容重點說明

技術　10項控制措施

項次	建議控制措施
26	機敏性資訊傳輸過程得採取資訊加密保護措施，資料傳送以業務所需之最少資料為原則。
27	採取具備資訊隱密性功能與識別、確認對方端末設備及防止儲存資料外洩等資料保護措施。
28	明訂網際網路作業相關管理辦法、作業規範及網路系統安全政策，並定期檢視修訂。
29	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，並遵循防火牆安全管理程序規定。
30	至少每年實施1次弱點掃描，並完成缺失改善。
31	應避免採用已停止弱點修補或更新之系統軟體與應用軟體。若一定要採用，則應採用其他配套防護措施。
32	應管制個資檔案透過輸出入裝置、通訊軟體、系統操作複製至網頁、網路檔案或列印等方式傳輸，並應留存相關紀錄軌跡與數位證據。
33	限制外部網路存取功能，同時外部網路可以存取的機器設備應維持在最少的數量並定期審查檢討。
34	建立存取控制(即帳號權限管理)機制功能，加強對不當資料檔案及存取之檢查。
35	應確認資訊系統開發設計中已納入必要的安全控管機能。

資安基本查核表內容重點說明

設備　5項控制措施

項次	建議控制措施
36	應建立公司資訊設備清冊並定期盤點及檢討資訊設備的安全防護機制。
37	識別所有資訊資產之擁有者，並指派維護資訊資產責任。
38	所有主機及設備在接入網路前，應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。
39	通訊網路及伺服器放置處應有門禁管制；非授權人員進出應填寫進出登記，並由內部人員陪同與監督；進出登記紀錄應定期審查，如有異常應適當處置。
40	訂定各類設備、應用軟體系統、儲存媒體之使用、報廢及轉移作業之管理規範。

持續改善電子商務營運環境安全

瞭解組織的網路及網站

日常操作維運

設施配備技術

發現及修補網路與網站及管理的漏洞

測試與確認網路與網站及管理的安全強度(如社交工程/滲透測試)

電商資安管理關鍵作為

- 組營階層董事會(董監事)需扮演必要角色
  - 資安改善成效應列入經營決策議程
  - 資安納入企業經營風險管理
  - 資安預算
- 全面落實且持續的資安管理風險評估
- 與資安風險共存、在威脅攻擊下存活
  - 事前、事中、事後之運作管理能力
- 資安管理是全組織體投入的對抗，通報反應是決勝的關鍵
- 保障消費者權益、保護組織得以持續營運

資安與風險控管重點

- 隱私保護與資料去識別化
  - 尊重用戶隱私
  - 確保以用戶為中心
  - 全程的保護
  - 須對資料進行適度之加密或匿名處理
- 系統開發安全
  - 採用安全系統發展生命週期SSDLC 方法，進行程式開發流程調整
  - 從系統發展生命週期全面強化安全控制措施
  - 委外開發廠商測試品質及驗收標準

資安與風險控管重點

- 委外服務關係管理
  - 定義資安與個人資料保護的角色與責任，管理責任明確化
  - 資料保護與使用需求、存取控制
  - 保密協議、審核與稽查
  - 事故通知

資安與風險控管重點

- 服務與產品安全評估
  - 基礎設施安全
    - 資訊環境架構安全
    - 資訊系統弱點掃描
    - 資訊系統配置安全
    - 網路活動檢視
  - 產品服務
    - 程式碼安全檢測
    - APP安全檢測
    - 行動APP安全檢測

建構資安管理營運

- 安全、預警、持續的
  - 事前安全性(準備與營運)
    - 全面性風險評估，以風險導向建立資安控制措施
    - 資訊安全技術檢測 / 系統安全開發生命週期 / APP應用安全檢測 / 資訊安全委外策略運用 / 資料保護與生命週期管理
  - 事中預警性(監測與應變)
    - 資訊安全外部威脅情報 / 日誌蒐集與監控 / 使用者行為監控與分析 / 網路活動監控
  - 事後持續性(持續與回復)
    - 營運持續管理 / 資訊安全危機管理 / 證據保全機制 / 改善活動

練好防禦基本功-立足數位經濟時代

- 「這種事情不會發生在我身上」-- 不去面對問題，就不會有解決問題的能力。
- 最基本的資安觀念-資訊安全要有策略，正確投資才能產生效益。
  - 了解個資及交易資料之維護範疇
  - 避免儲存過多客戶資訊
  - 修補伺服器的弱點或漏洞；取消系統不必要的服務，這些修改都不需要專業人士來做，只要透過教育訓練要求即可達到效果。(不需要額外的投資)
  - 教育訓練員工，如何安全處理電子郵件的附件及使用網際網路與社群軟體，降低受威脅攻擊的機會。

敬請指導

肆、結語

「解除分期付款」案類被害案件數多寡，常取決於歹徒是否容易取得民眾消費資料（業者對於後臺資安維護的重視程度）；另一方面被害人常因歹徒能夠詳述其所購買物品之時間、金額及配送方式等，使渠等誤信確為客服人員而匯款受騙，亦或雖曾接獲反詐騙相關訊息，惟未留意致接獲電話時仍遭詐，顯示民眾防詐意識仍甚薄弱，尚有強化空間。

未來為能機先預防詐騙案件發生，茲彙整上開自評表及範例，提供各電子商務業者參考，其各業者能適時參酌建議事項調整宣導作為，以最有效的宣導方式喚醒全民反詐意識俾利減低遭詐騙之風險。

扮演柯南-如何留下駭客的足跡

@Titan Lee

Agenda

扮演柯南-如何留下駭客的足跡

1.人是誰殺的？
2.柯南需要甚麼
3.所以...? 我該怎麼辦？
4.記錄檔儲存及備份
5.Q&A

人是誰殺的？

人是誰殺的？

在這議題開始前
我想問.....？

人是誰殺的？

ETNEWS > 社會 > 社會　　2017年08月16日 03:27

社會　社會焦點　保障人權

切車？貨車剎不住撞爛Lexus　行車紀錄器1分「還原打臉」

【手刀點擊】天天抽500杯咖啡　厭世暑氣秒退散！

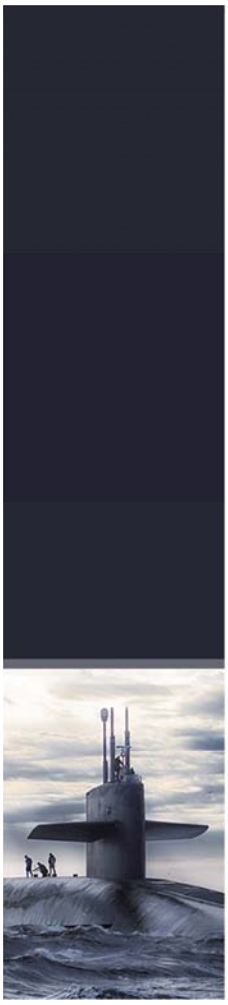
5,427 讚　ETNEWS新聞雲　說這專頁讚　337 萬 按讚次數

人是誰殺的？

人是誰殺的？

車上已經裝行車紀錄器
電腦也該裝一個？

柯南需要甚麼？

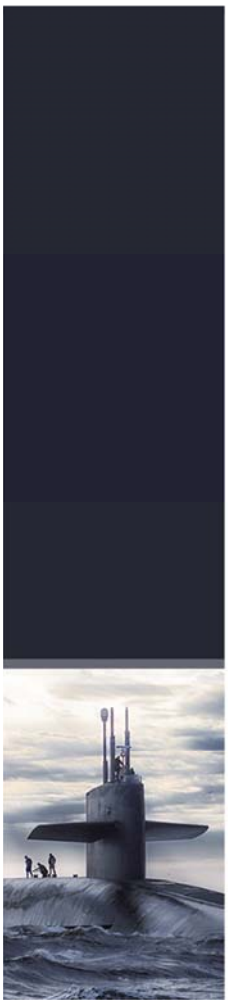


柯南需要甚麼？

記錄檔(Log)的重要性

原本在個資法細責第五條說明：「軌跡資料」係指個人資料在蒐集、處理、利用過程中，所產生非屬於原蒐集個資本體之衍生資訊（Log Files），包括（但不限於）資料存取人之代號、存取時間、使用設備代號、網路位址（IP）、經過之網路路徑...等，可用於比對、查證資料存取之適當性。從用戶端到對外服務的網站、從外部防火牆、入侵偵測系統到內部網路節點、從應用系統、網站、電子郵件服務、上網記錄到即時通訊等，甚至是語音電話系統。

幾乎是所有企業營運過程中的環節都可以產生所謂的稽核軌跡與記錄。



柯南需要甚麼？

記錄檔記錄類型分類

方向	說明
營運流程	針對員工的資料檔案申請、簽核及核准之資料儲存授權行為紀錄 ex: 簽呈
應用系統	員工透過自家系統存取客戶或其他個人資料之使用行為紀錄 ex:客戶管理系統/訂單物流系統
資料庫	程式或管理人員直接進行資料操作和存取之使用紀錄 ex: DBA登入資料庫紀錄
作業系統	系統管理人員值系統上相關操作 ex : windows event log
網路環境	係指存取網路還進相關設備紀錄 ex:防火牆紀錄/IPS紀錄/netflow/流量紀錄.....
實體環境	機房進出入紀錄/監視系統 (CCTV)/員工門禁紀錄

請問被覆蓋的檔案 如何救援??

0

資料庫 office

zhongcetw 8 年前 · 62457 瀏覽

我們的經理，不幸的將9月的 *.mdb 檔，用7月的覆蓋掉了，請問救的回來嗎??
不是刪除喔，是用程式匯入覆蓋~ @@

回答 9 討論 邀請回答 追蹤 檢舉

登入發表討論

9 個回答

舊至新 新至舊 最高Like數

32

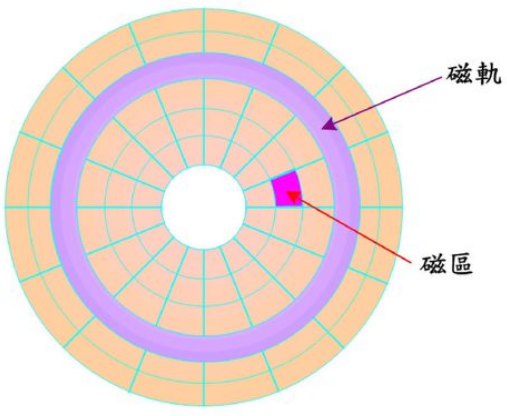
jamesjan
iT邦高手 1 級 · 8 年前

最佳解答

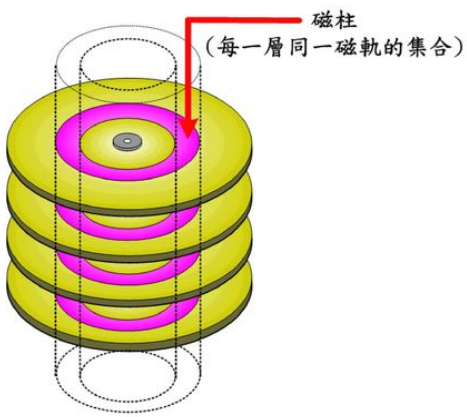
應該無解了 >.<
因為以匯入的方式，是直接取代掉原來的程式，ACCESS是不會幫您做備份處理的
在修改程式之前沒有先做備份嗎？這是 Common sence
不過我想經過這次教訓，下次就會先做備份了 XD

柯南需要甚麼？

硬碟的容量及資料儲存格式



磁軌與磁區



磁柱示意圖

所以...? 我該怎麼辦？？

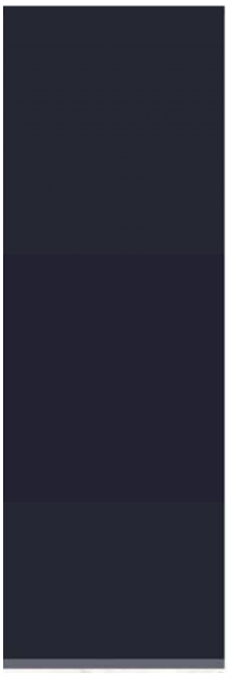
所以...? 我該怎麼辦？？

收好收滿！

不在乎多收多少

只在乎曾經收過

所以...? 我該怎麼辦? ?



所以...? 我該怎麼辦? ?

事先作業 **-Windows** 篇

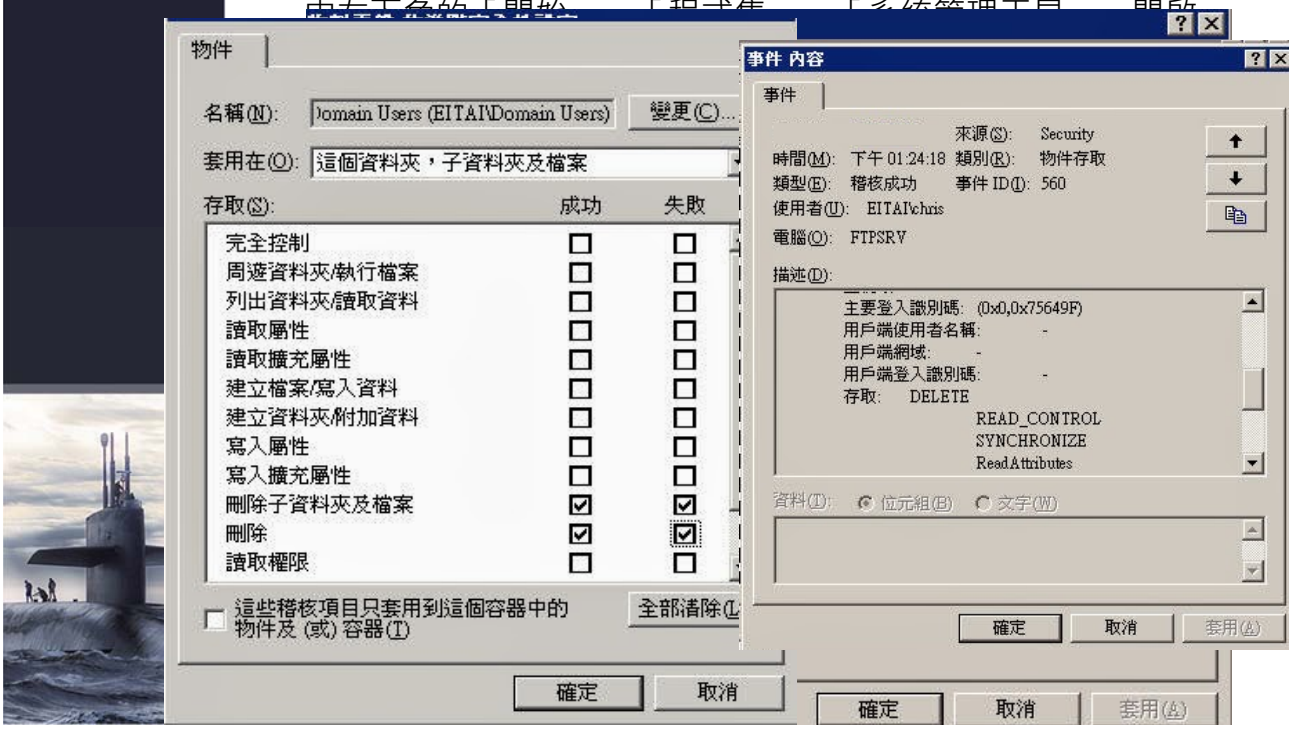
1.建議事先開啟檔案稽核

2.完整的登入事件

3.把Log增大

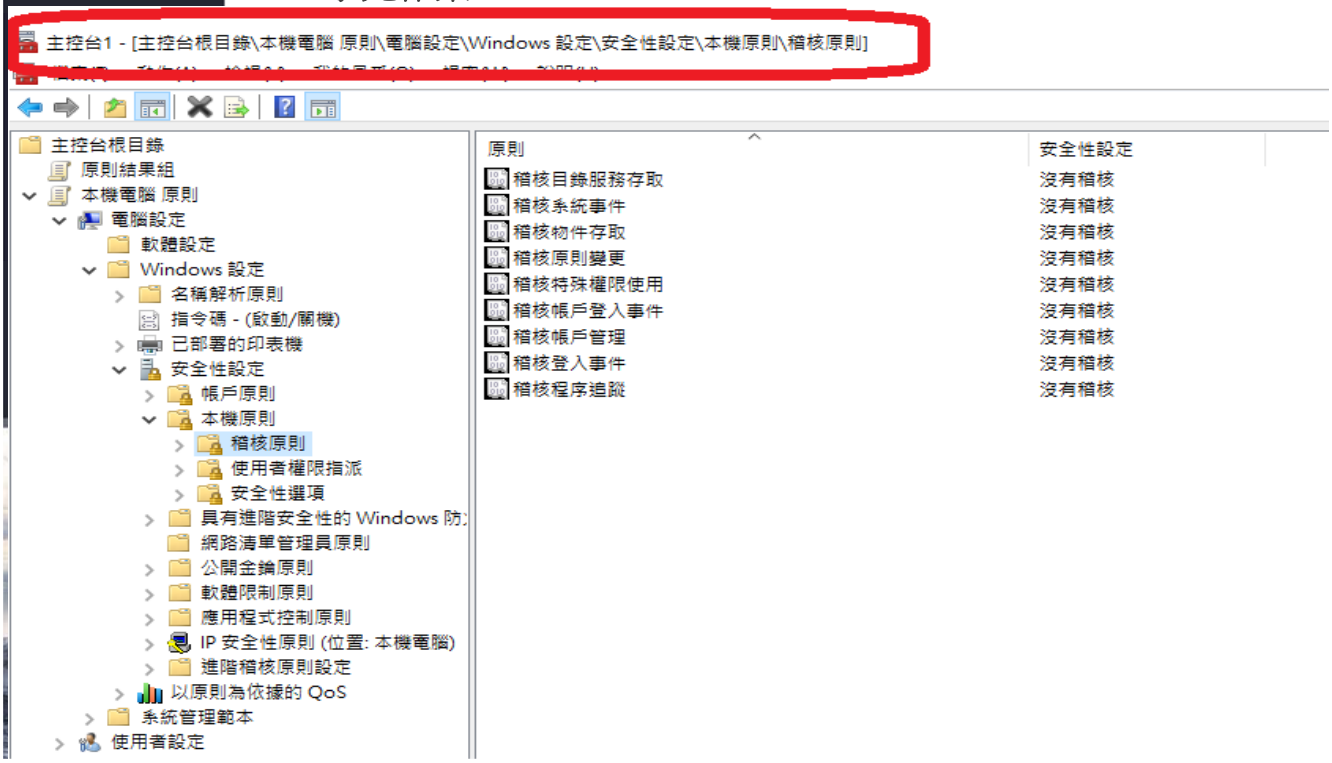
所以...? 我該怎麼辦? ?

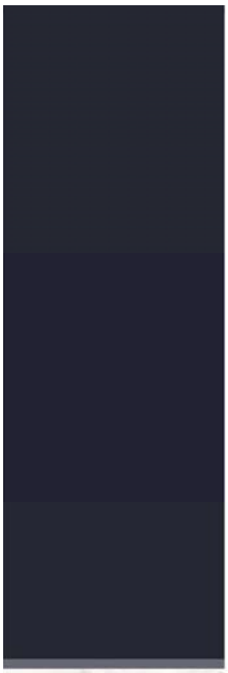
事先作業 - **Windows** 篇 -開啟檔案稽核



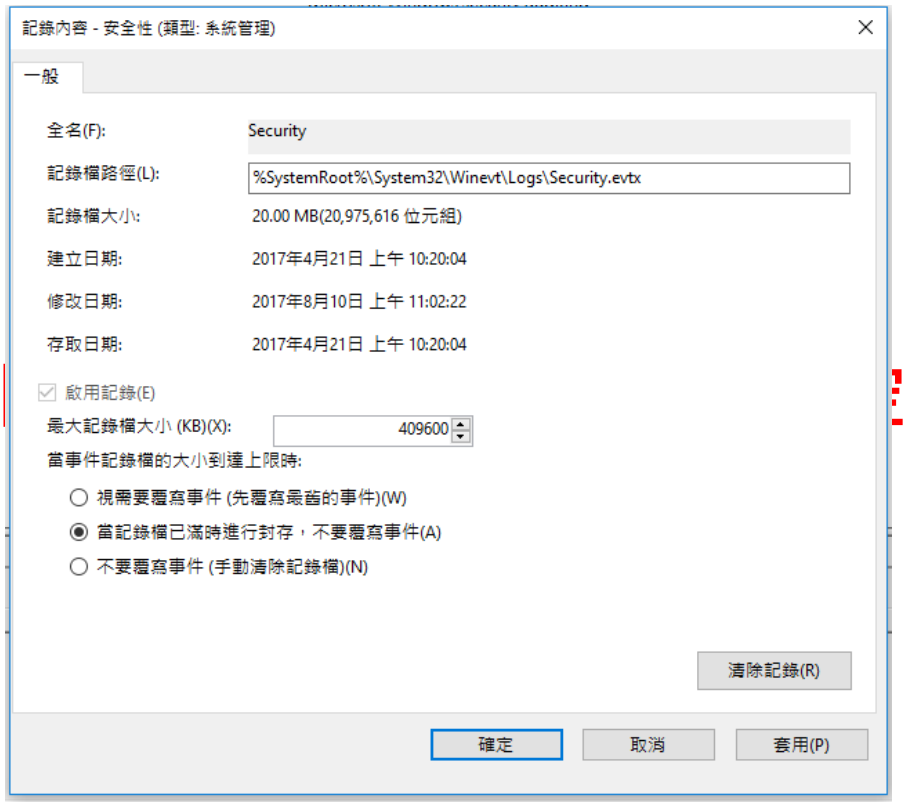
所以...? 我該怎麼辦? ?

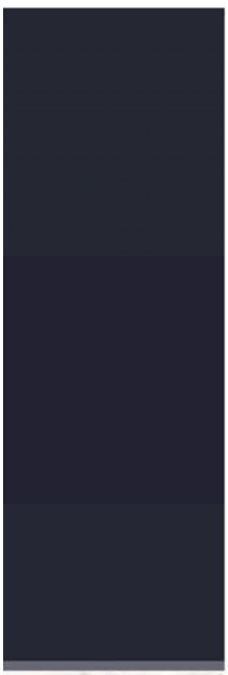
事先作業 **-Windows** 篇 –完整登入





所以...? 我該怎麼辦? ?





所以...? 我該怎麼辦? ?

Windows 篇 – 結論

服用前：請注意自己的硬碟空間

設定	企業桌上型電腦	企業膝上型電腦	高安全桌上型電腦	高安全膝上型電腦
稽核帳戶登入事件	成功	成功	成功，失敗	成功，失敗
稽核帳戶管理	成功	成功	成功，失敗	成功，失敗
Log大小	**請依照硬碟比例**	**請依照硬碟比例**	**請依照硬碟比例**	**請依照硬碟比例**
稽核登入事件	成功	成功	成功，失敗	成功，失敗
稽核物件存取	沒有稽核	沒有稽核	失敗	失敗
稽核原則變更	成功	成功	成功	成功
稽核特殊權限使用	沒有稽核	沒有稽核	成功，失敗	成功，失敗
稽核開啟檔案	刪除	刪除	刪除/寫入	刪除/寫入
稽核系統事件	**成功**	**成功**	**成功**	**成功**

所以...? 我該怎麼辦? ?

Event log 分析

Event Log ID		
Windows 2003 事件ID	Windows 2008 事件ID	說明
517	4612	所有稽核日誌清除事件
528	4624	成功登入『除了 3、8 以外的』
529	4625	登入失敗嘗試以不明的使用者名稱，或已知使用者名稱與錯誤密碼登入
530	4626	登入失敗使用者帳戶嘗試於允許的時間之外登入
531	4627	登入失敗嘗試使用已停用的帳戶登入
535	4631	登入失敗特定帳戶的密碼已過期
538	4634	使用者的登出程序已完成
539	4635	登入失敗嘗試登入時帳戶已鎖定
540	4636	成功由網路登入『登入類型：3、8』
624	4720	使用者帳戶已建立『可確認新增哪一個帳號』
627	4723	使用者密碼已變更
630	4726	使用者帳戶已刪除
636	4732	已將成員加入本機群組『可確認加入哪一個群組』

所以...? 我該怎麼辦? ?

Event log 分析

記錄事件 528、540 時，事件日誌中也會列出登入類型下表說明每一種登入類型

類型	登入標題	說明
2	互動	使用者已登入這部電腦
3	網路	使用者或電腦從網路登入這部電腦
4	批次	批次登入類型是批次伺服器所使用，其中程序可代表使用者執行，而無須使用者的直接介入
5	服務	服務已由 [服務控制管理員] 啟動
7	解除鎖定	此工作站已解除鎖定
8	NetworkCleartext	使用者從網路登入這部電腦使用者的密碼以非雜湊格式傳遞給驗證封裝內建的驗證在傳送所有雜湊認證通過網路之前會先進行封裝認證不會以純文字形式 (又稱為明文，cleartext) 周遊網路
9	NewCredentials	呼叫者複製其目前的權杖，並指定輸出連線的新認證新的登入工作階段擁有相同的本機識別，但對其他網路連線使用不同的認證
10	RemoteInteractive	使用者使用 [終端機服務] 或 [遠端桌面] 從遠端登入這部電腦
11	CachedInteractive	使用本機電腦上 Cache 登入網域帳號，未與 AD 進行認證

所以...? 我該怎麼辦？？

事先作業 –Linux 或 UNIX 篇

1. History指令顯示時間記錄
2. chattr +a
3. SELinux

所以...? 我該怎麼辦?？

事先作業 –Linux 或 UNIX 篇 -History指令顯示時間記錄

```
echo "HISTFILESIZE=2000" >> /etc/bashrc && echo "HISTSIZE=200
0" >> /etc/bashrc && echo 'HISTTIMEFORMAT="%Y%m%d %T "'>
> /etc/bashrc && export HISTTIMEFORMAT
```

```
HISTFILESIZE=2000 <== 存起來的檔案之指令的最大紀錄筆數。
HISTSIZE=2000 <== 目前環境下，可記錄的歷史命令最大筆數。
```

所以...? 我該怎麼辦??

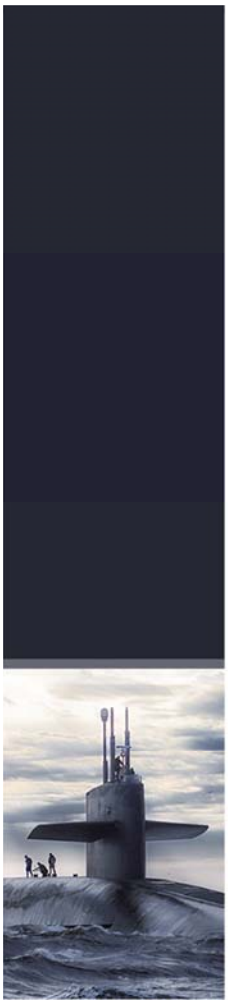
事先作業 –Linux 或 UNIX 篇 -chattr +a

請注意：『僅適合已經對 Linux 系統很有概念的朋友』來設定， 對於新手來說，建議你直接使用系統的預設值就好了，免得到最後登錄檔無法寫入

```
[root@test.rtm ~]# chattr +a /var/log/admin.log
[root@test.rtm ~]# lsattr /var/log/admin.log
```

如果將一個檔案以 chattr 設定 i 這個屬性時，那麼該檔案連 root 都不能殺掉！而且也不能新增資料，嗯！真安全！但是，如此一來登錄檔的功能豈不是也就消失了？ 因為沒有辦法寫入呀！所以囉，我們要使用的是 a 這個屬性！你的登錄檔如果設定了這個屬性的話，那麼他將只能被增加，而不能被刪除！嗯！ 這個項目就非常的符合我們登錄檔的需求啦！因此，你可以這樣的增加你的登錄檔的隱藏屬性。

記錄檔儲存及備份



記錄檔儲存及備份

儲存的方式為何？

File base還是DB base？

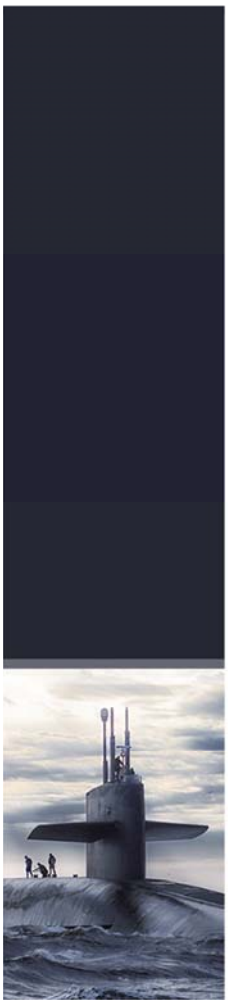
考慮包括可儲存容量為多少？用什麼方法存？

儲存的安全性如何？是否採用加密？有沒有數位簽章？

如何證明具有法律證據力？

儲存在storage內的log是否可以修改?

你願意花錢買NAS或storage專門存log嗎？



記錄檔儲存及備份

你家裝上了監視器
100%會抓到小偷嗎?

記錄檔儲存及備份

你家裝上了門鎖
100%不會遭小偷嗎?

Deloitte.

勤業眾信

看對醫生找對方法 - 談資安診斷3步驟

勤業眾信聯合會計師事務所 風險諮詢服務

大綱

1. 電子商務產業安全議題
2. 資安診斷3步驟
3. 問題與討論

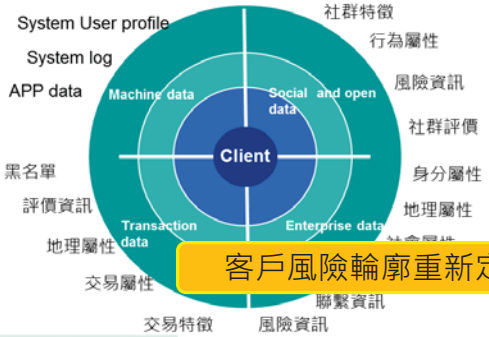
電子商務產業安全議題

安全消費的體驗將將影響用戶的消費意願

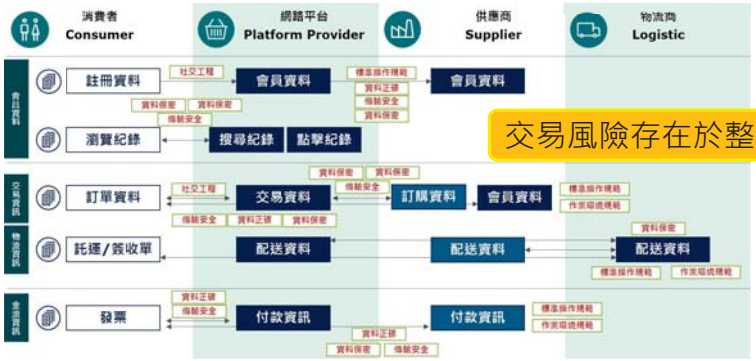
在電子商務追求口碑、精準、快速行銷的同時，「安全的消費」也將成為消費過程的一種體驗，並影響消費意願。

電子商務資訊安全與風險問題圍繞整個供應鏈及生態系

業務與交易風險樣態

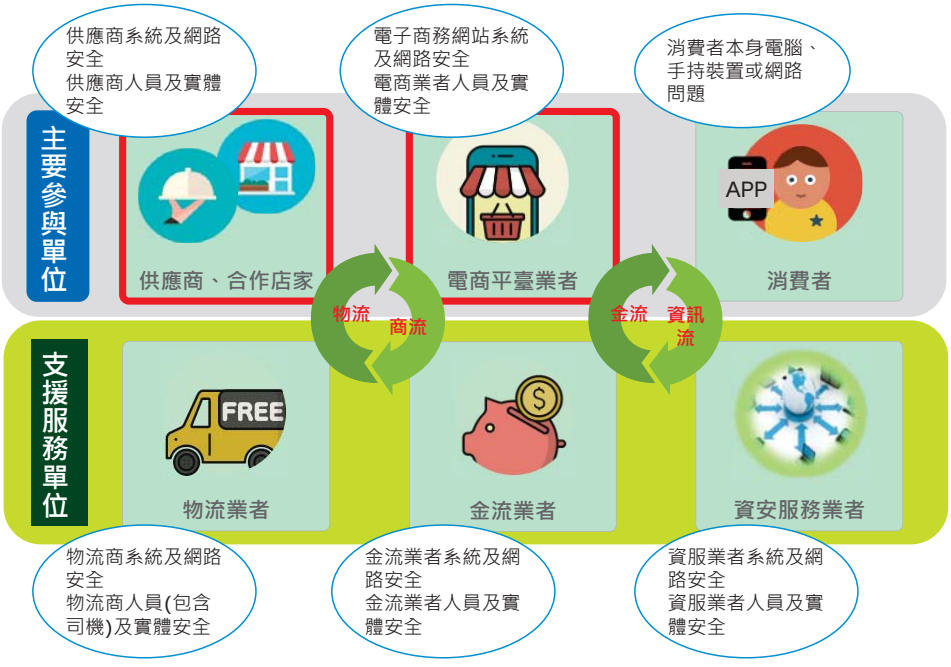


客戶風險輪廓重新定義



交易風險存在於整個生態系

電子商務產業安全議題



但是電子商務業者大有不同...

- **資訊來源太多元**：營運、維護/增值服務、產品開發與策略合作夥伴等。
- **使用單位太多元**：客戶、行銷、供應商、金流、相關策略合作夥伴等。
- **資料類型太多元**：結構化資料、非結構化資料與准結構化資料等。
- **生命週期太多樣**：中間有/無物流、有/無供應商、有/無金流等。
- **委外關係太複雜**：母子公司、公益往來、戰略合作、終止合作、安全保護等。
- **法令法規太繁瑣**：個人資料保護、委外安全管理、金融交易、跨境傳輸等。

目前國內既有電子商務資訊安全規範與參考資訊

- 網路平台 479項控管項目
- 供應商 158項控管項目
- 物流商 264項控管項目

電子商務交易安全規範（網路平台、供應商、物流商）(2012)

電子商務個資外洩資安防護參考 (2015)

- 事前、事中、事後之防禦及處理
- 事前70項
- 事中23項

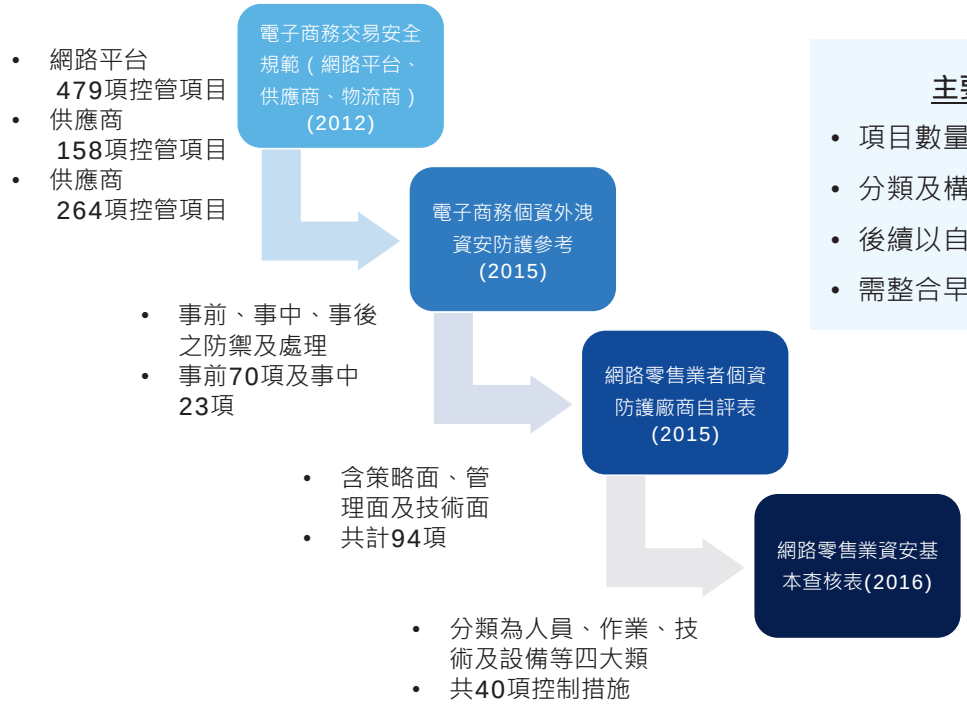
- 含策略面、管理面及技術面
- 共計94項

網路零售業者個資防護廠商自評表(2015)

網路零售業資安基本查核表 (2016)

- 分類為人員、作業、技術及設備等四大類
- 共40項控制措施

目前國內既有電子商務資訊安全規範與參考資訊(續)



主要趨勢

- 項目數量越來越少
- 分類及構面越來越簡單
- 後續以自檢表型式為主
- 需整合早期規劃資訊

資安診斷3步驟

資安診斷3步驟

科技資安風險掌握、控管落實確認及合適的委外廠商

政策、管理規範與作業程序

定期教育訓練與宣導認知

事前：安全性

透過風險導向資安檢測
防禦外在威脅

- 網路零售業資安基本查核
- 資訊架構檢視
- 主要資安設備建置與管理
- 系統安全開發要求
- 資訊安全委外要求運用
- 個資保護控管
- 定期資安體檢

事中：預警性

透過定期日誌分析
確認異常行為特徵

- 日誌留存與監控
- 使用者行為監控與分析
- 網路活動監控

事後：持續性

擁有復原及減小資
安事件所帶來衝擊
之能力

- 找到可靠的資安調查廠商
- 定期演練機制
- 數位證據保全機制

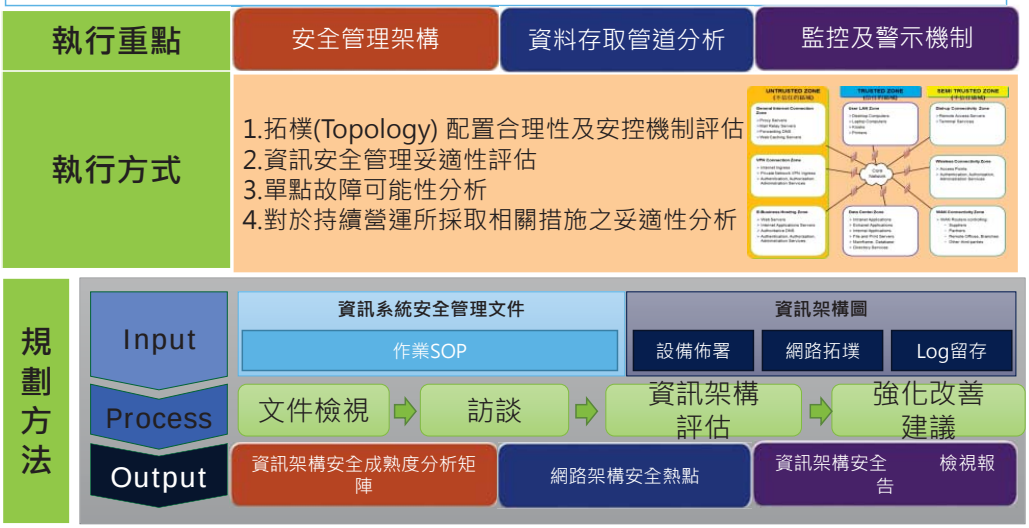
P. 11

資安診斷3步驟 - 事前：安全性

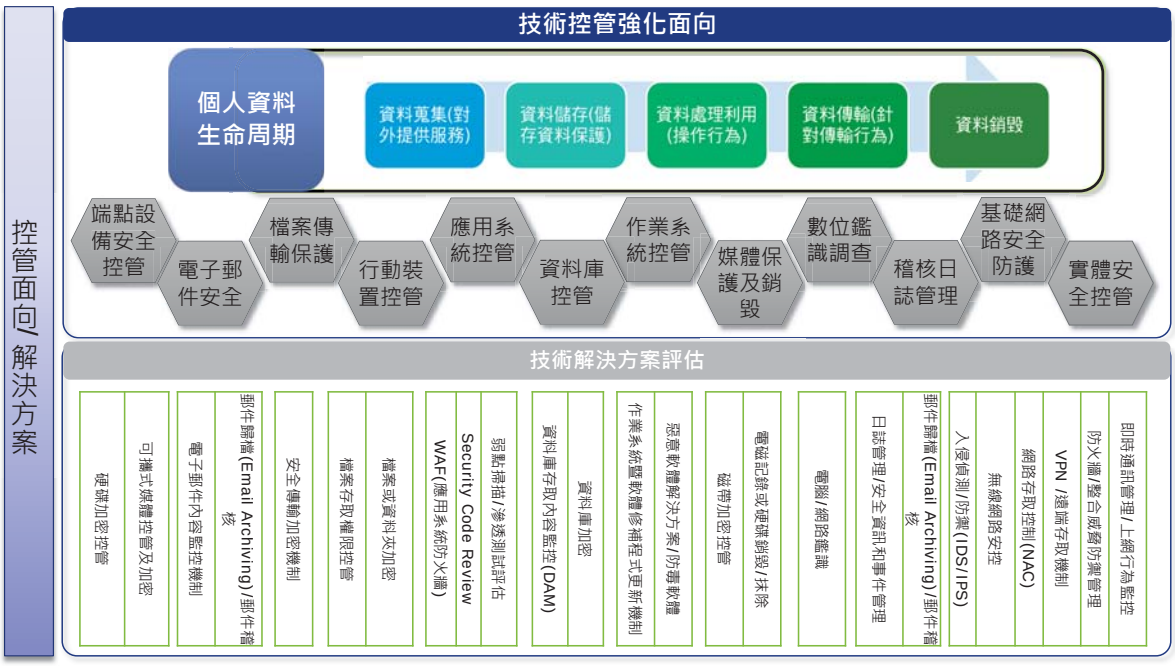
網路零售業資安基本查核

資訊架構檢視

評估各種流程或技術性的資訊架構安全控制，以衡量目前資安結構設計的有效性。除了訪談主機代管業者外，也會基於網路安全政策，網路架構圖，和目前的運行業務進行評估。

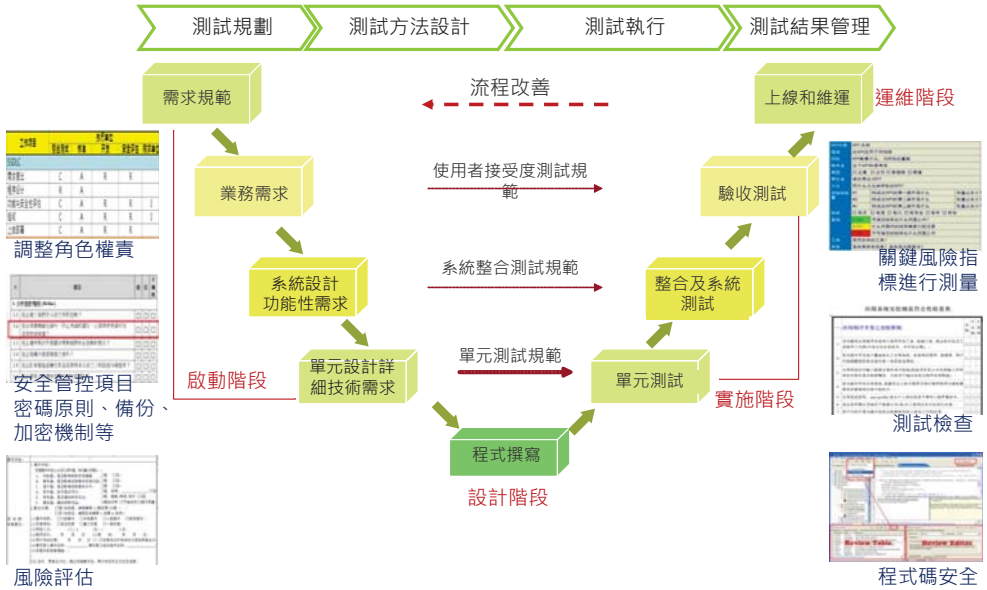


主要資安設備建置與管理

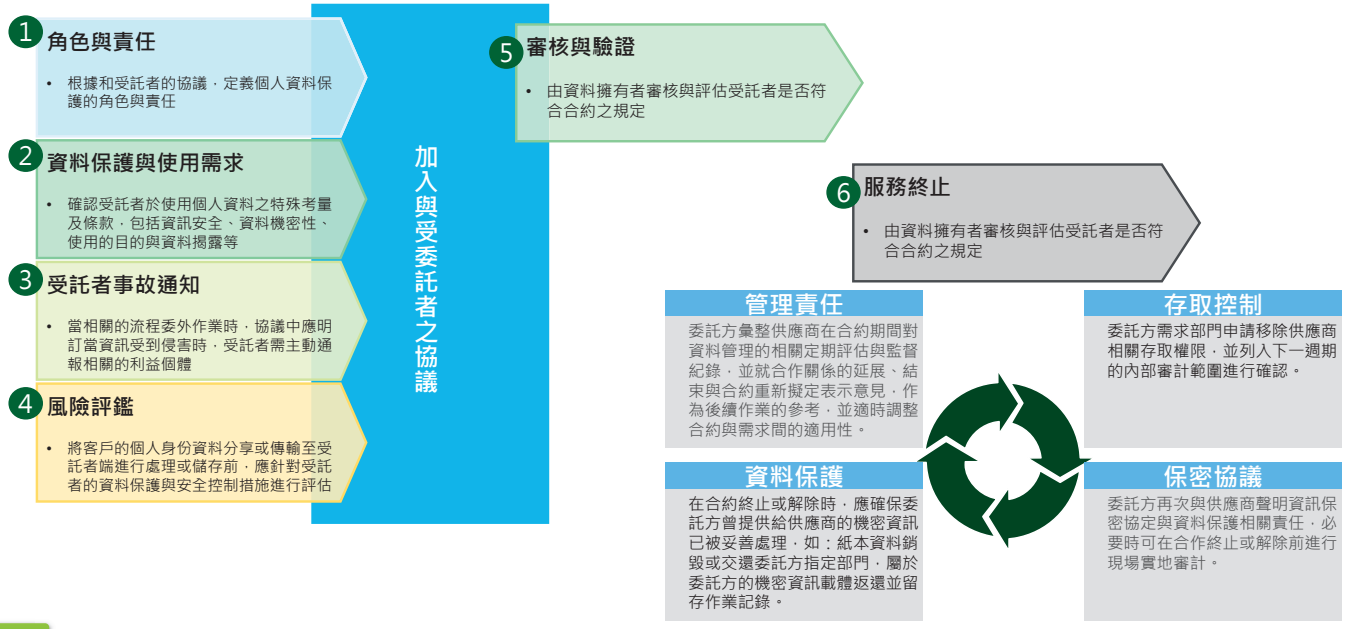


由系統開發生命週期角度強化安全控制措施

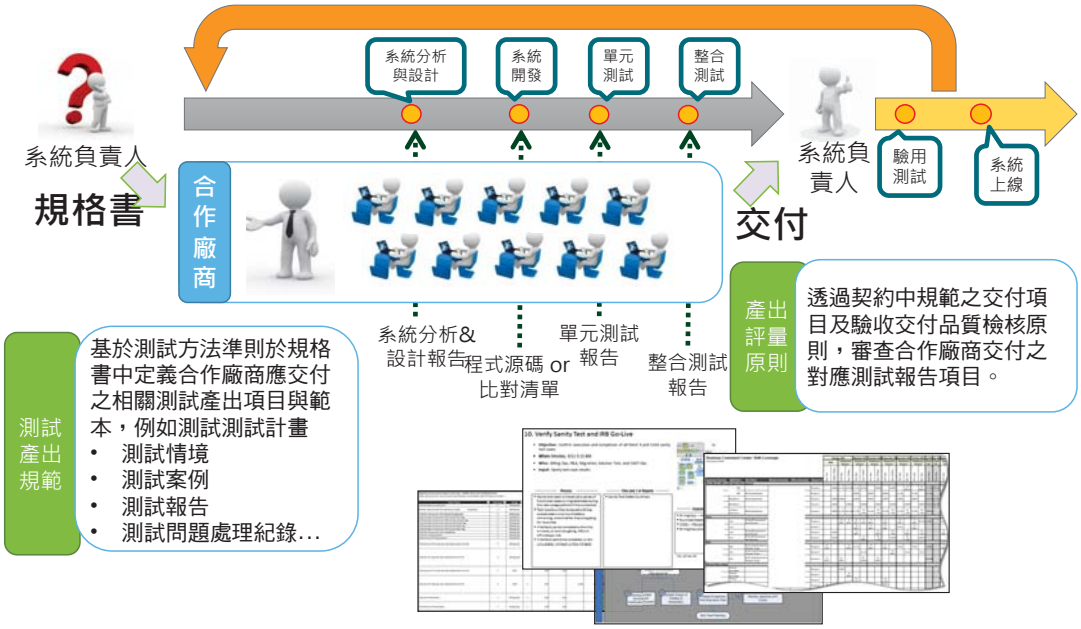
針對傳統應用程式開發流程，採用安全系統發展生命週期 SSDLC 方法，包含開發流程角色拆分、需求評估風險評估原則建立、原碼取存許可權拆分、上線維運移轉必要文件規範制定等環節，從系統發展生命週期全面強化安全控制措施。



資訊安全委外要求運用



資訊安全委外要求運用(續)



個資保護控管

資料庫保護及內容監控

- 資料庫資料存取之監控機制及規則
- 多重架構(如DB、AP、Web)間之點對點加密
- 高風險資料庫的存取人員、變更動作及時間之稽核軌跡紀錄開啟
- 資料庫用戶與管理者之存取控制，並定期稽核
- 資料遮蔽機制

資料存取權限控制

- 身份認證與識別管理
- 數位資料權限管理(DRM)

端點設備安全控管

- 端點防護政策
- 端點防護(End-point Security)防禦平臺：控管使用者的行為與周邊裝置，限制傳輸資料至可攜式裝置等行為。
- 筆記型電腦安全，包含：實體安全、硬碟磁區或檔案加密、雙因數認證、防毒軟體、修補程式更新與個人防火牆保護或端點安全機制
- 共用主機與可攜氏媒體存取控管

網路傳輸保護

- 以資料外洩防護(DLP)機制，針對對外流向採用內容監控與過濾
- 分析網路流量以偵測和保護任何違反資料保護政策之傳輸
- 採用相應的安全檔案傳輸工具與機制(如：HTTPS、 SFTP)

資料銷毀機制

- 包含敏感性資料之電子媒體與紙本的安全銷毀規範
- 稽核與監控委外的媒體銷毀

稽核軌跡與監控

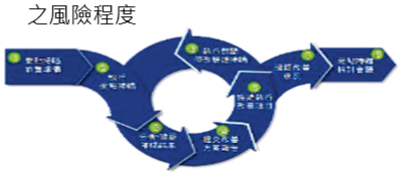
- 針對資料產生/取得、儲存、使用、共享、歸檔、銷毀等行為之相關活動紀錄，包含伺服器、防護設備與主機環境架構的稽核日誌。
- 針對異常行為進行有效追蹤及改善

定期資安體檢

基礎設施安全

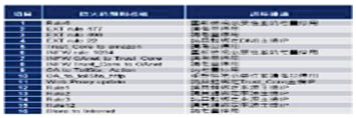
資訊系統弱點掃描

- 偵測重要資訊基礎建設可能的弱點與漏洞，強化較弱的環節，以降低整體之風險程度



資訊系統配置安全檢視

- 檢視伺服器(AD)有關「密碼設定原則」與「帳號鎖定原則」設定、防火牆、系統存取限制、辦公軟體及應用軟體等之更新設定及更新狀態。



網路與系統活動檢視

- 檢視公司對外網路活動，阻止惡意URL/間諜程式/傀儡網路 (botnet)/病毒及其他類惡意軟體的攻擊

產品安全評估

對外服務網站滲透測試

- 模擬駭客攻擊行為，進行對外網站的滲透測試

程式碼安全檢測

- 掃描對外網站的應用系統原始程式碼的安全問題，提供完整的檢驗分析報告及建議諮詢

APP安全檢測

- 針對客戶行動應用App 進行資訊安全檢測，檢測手法遵循多項國際與國內資安指引

資安診斷3步驟 - 事中：預警性

稽核軌跡與日誌留存

人

是誰在進行操作？

事

他做了哪些事情？

時

他什麼時候做的？

地

他在哪裡做的？

物

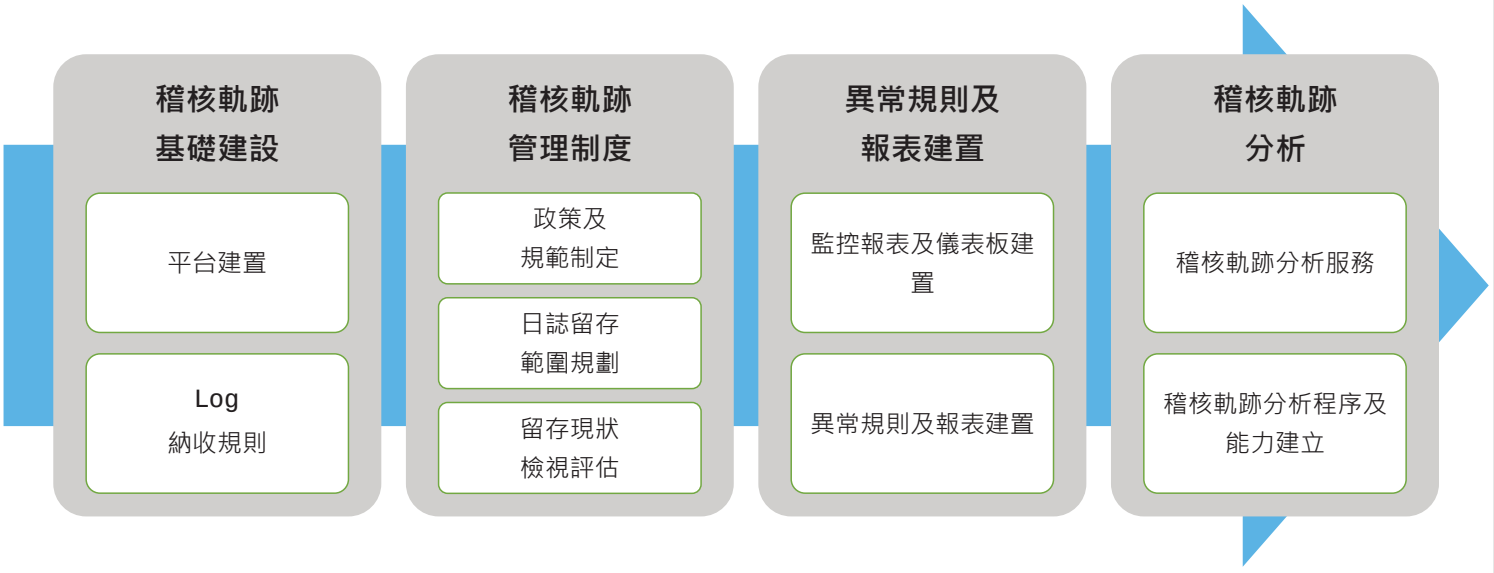
他碰到哪些資料？

建議應從資料外洩調查角度考量日誌留存及預警

序號	層面	領域	資安事件類型*			
			阻斷服務	惡意程式	非法存取	不當使用
1	Network & Physical Layer	Firewalls	Y	Y	Y	Y
		Web application firewall (WAF)	Y	Y	Y	
		Routers	Y	Y	Y	
		VPN Access Points			Y	Y
		Wireless Access Points		Y	Y	
		Intrusion Prevention System(IPS)	Y	Y	Y	
		Network Access Control			Y	
		Voice Network (PBX及Voicemail)			Y	Y
		Door security			Y	Y
		CCTV			Y	Y
2	Operating System & Platform Layer			Y	Y	Y
3	Application Layer			Y	Y	Y
4	Database Layer			Y	Y	Y
5	Other IT Related Areas of Interest	Antivirus		Y	Y	
		Data Leakage Protection(DLP)			Y	Y
		Email Auditing & Spam		Y	Y	Y
		Internet & Content Monitoring		Y	Y	Y
		Patch Management		Y	Y	
		User Authentication		Y	Y	
		Access Control			Y	Y
		Network Monitoring	Y	Y	Y	
		Log Management	Y	Y	Y	Y
		舉例	網站遭阻斷服務攻擊	電子公文遭植入木馬程式	1.官方網頁遭置換 2.猜測使用者帳密成功後進行存取	內部人員因職務之便，下載個資檔案至個人隨身硬碟並攜出

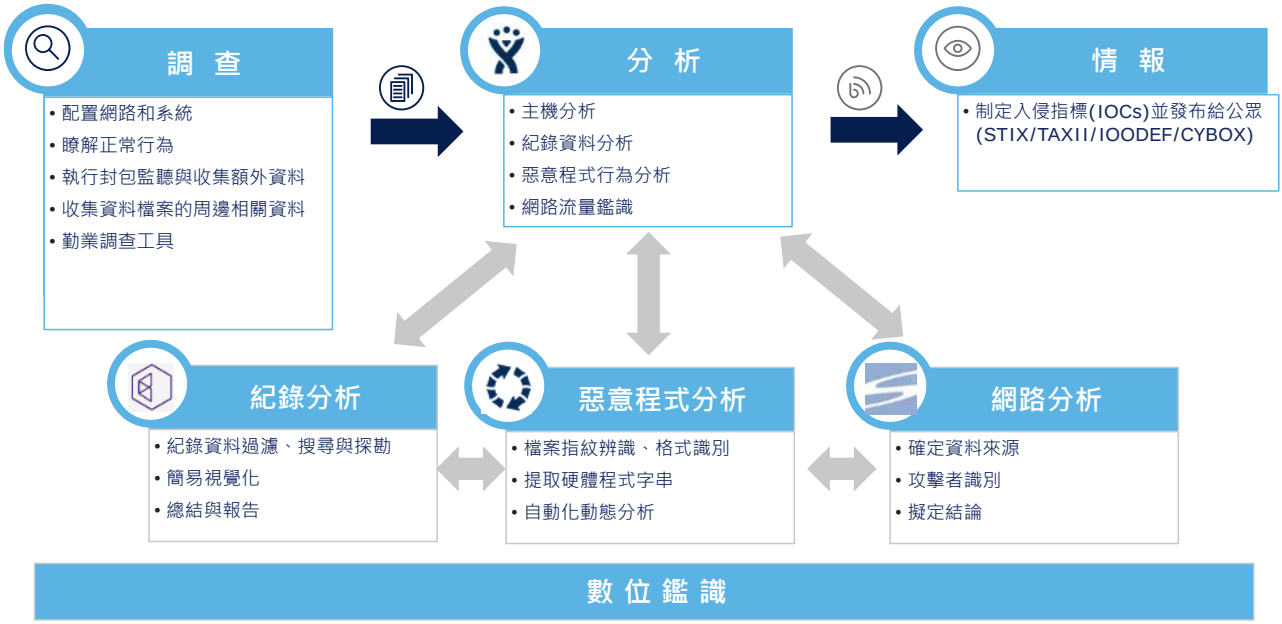
*資安事件類型：係為參考NIST「Computer Security Incident Handling Guide」文件中定義之4種資安事件類型。

稽核軌跡留存的下一步，異常行為分析、證據保全與數位鑑識

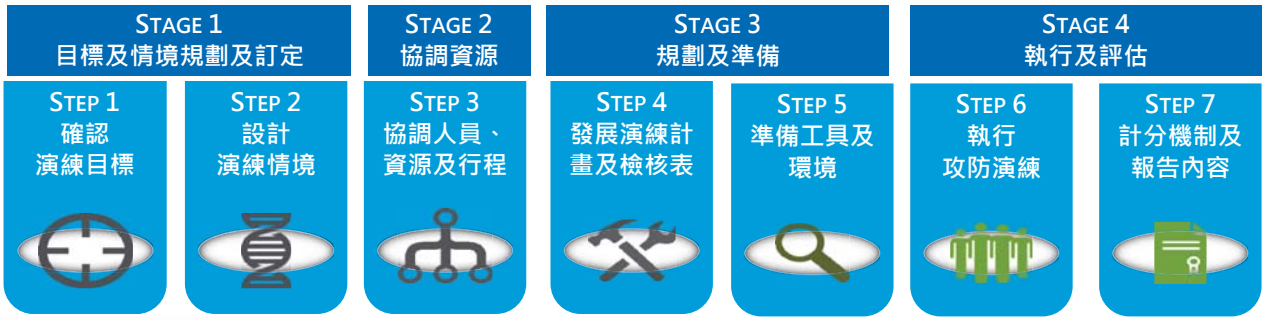


資安診斷3步驟 - 事中：持續性

找到合適的資安事件調查團隊協助



針對高風險業務活動，考量外部威脅情資，設計與實施攻防演練



建議針對演練目標確認、情境想定、資源及人力投入及動員、計畫擬定及通知、執行行程規劃、執行方式(程序/實際面)、風險處理對策、計分方式等須應進行通盤規劃及考量

演練角色

演練情境

Deloitte.

勤業眾信

中華民國
無店面零售商業同業公會

2016 年 3 月

加入我們

※本會簡介、章程及入會相關表格資料，敬請上網下載：http://www.cnra.org.tw/non-store.rar

※本會LINE ID：@tdb8291p

※本會FB無店面產業討論區