CYBERSEC 2024 臺灣資安大會

企業必知：
適應新個資法下的資安挑戰與機遇

蕭奕弘

2024年5月16日

簡　歷

現職

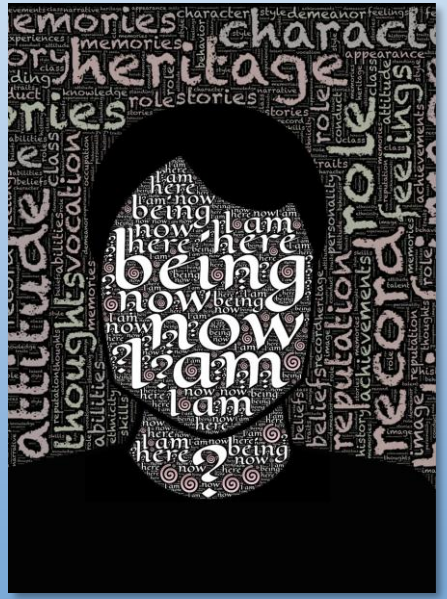
蕭奕弘法律事務所主持律師
台大國企系兼任副教授級實務教師
台北律師公會刑事法委員會主任委員

經歷

- 台北地檢署檢察官
  重大金融專庭、刑事庭公訴檢察官
  電腦及智慧財產犯罪專組偵查檢察官
- 司法院資訊處法官、嘉義地院法官

學歷

- 成功大學法律系博士班在學
- 中央電機系、電機所
- 台大科際整合法律學研究所
- 台大資訊網路與多媒體研究所博士班肄業
- 華盛頓大學法學碩士



個資保護的過去

- 99年，電腦處理個人資料保護法修正為「個人資料保護法」，於101年施行
  - 涵蓋所有公務、非公務機關
  - 要求要有「適當安全措施、安全維護計畫」
  - 有行政檢查、行政裁罰
  - 有團體訴訟、民事損害賠償
- 但施行後
  - 行政檢查、行政裁罰少、能罰的金額也少（20萬元）
  - 團體訴訟、民事求償少
  - 除了金融機構、上市櫃公司以外，對個資保護的重視程度不高
- 相較於GDPR
  - 全球營業總額的百分之4，或2000萬歐元
- 相較於洗錢防制
  - 50萬元以上、1000萬元以下罰鍰

British Airways因個資外洩後續調查裁罰2000萬英鎊

- 裁罰時間：2020年10月16日
- 處罰國家：英國
- 處罰機構：Information Commissioner（ICO）
- 處罰原因：欠缺技術上或組織上的安全措施，以維護資訊安全
  - 英國航空公司British Airways表示ba.com網站跟APP遭到駭客入侵15日(2018/8/21-9/5)，影響的交易達38萬筆，可能外洩的個資包括個人及交易資料(姓名、帳單地址、電子郵件及信用卡號)，但不包括旅遊細節及護照號碼。

個資法第27條：安全措施與維護計畫

(第1項)非公務機關保有個人資料檔案者，應採行**適當之安全措施**，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

(第2項)中央目的事業主管機關得指定非公務機關訂定個人資料檔案**安全維護計畫**或業務終止後個人資料處理方法。

(第3項)前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。

個資法施行細則第12條：適當的安全措施

- **技術上**及**組織上**之措施。
- **得**包括下列事項，並**以與所欲達成之個人資料保護目的間，具有適當比例為原則**：
  - 一、配置管理之人員及相當資源
  - 二、界定個人資料之範圍。
  - 三、個人資料之風險評估及管理機制。
  - 四、事故之預防、通報及應變機制。
  - 五、個人資料蒐集、處理及利用之內部管理程序。
  - 六、資料安全管理及人員管理。
  - 七、認知宣導及教育訓練。
  - 八、設備安全管理。
  - 九、資料安全稽核機制。
  - 十、使用紀錄、軌跡資料及證據保存。
  - 十一、個人資料安全維護之整體持續改善。

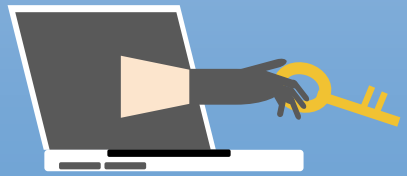
未來，個資保護的資安議題，會比過去受到更大的重視

- 在**過去**，個資法第48條規定，違反第27條第2項「未採行適當安全措施」或第3項「未制定安全維護計畫」，效果是：
  - 限期改正
  - 屆期不改正，按次連續處罰2萬以上20萬以下罰鍰
- 先限期改正，才能該開始處罰，而且裁罰金額低，至多20萬元。
- 除了金融法規將個資保護納入內控制度一環，屬於金檢範圍及金融法規裁罰範圍外，其他公司未必重視。
- 消費者對個資保護的意識尚未抬頭，個資外洩的民事訴訟求償少，企業沒有投入的動機。
- 行政檢查也少。

在個資外洩愈來愈多常見的情況下，個資法再次修正

- 2024-03-30：被駭客盯上！**7高中**校務系統遭駭、個資外洩 教育部公布學校名單
- 2024-03-26：華航今年又被駭！**上百萬筆**客戶個資流出 全被放上暗網出售
- 2024-03-06：車主個資外洩！北市**民營停車場**網站遭駭 緊急張貼公告
- 2024-01-04：近**500筆**雇主個資遭外洩 移工續聘居留整合服務系統驚現資安漏洞
- 2023-11-28：個資外洩被罰 **上海商銀**為十年來第3案、金管會匯整四大問題
- 2023-11-21：**雄獅**遭網路攻擊個資外洩 籲旅客當心詐騙
- 2023-02-25：**微風百貨90萬**會員個資遭駭 經濟部喊查：未改善將開罰
- 2023-02-09：**iRent 40萬筆**個資外洩！公總認定有疏失 開罰20萬限期改正

……



新個資法的資安挑戰與機遇

新個資法改為直接處罰並加重裁罰金額

2023.05.31修正公布個資法第48條

修正前(§48 ④)	修正後(§48 Ⅱ、Ⅲ)	說明
非公務機關未採行適當安全措施，或未訂定個資安全維護計畫或業務終止後個資處理方法： (先)限期改正 (再)按次處2萬~20萬罰鍰	非公務機關未採行適當安全措施，或未訂定個資安全維護計畫或業務終止後個資處理方法： **(先)處200萬以下罰鍰+限期改正；情節重大者：處15萬~1,500萬** (再)按次處15萬~1,500萬	1. **不宜於限期改正而屆期未改正始予處罰**，改採裁處罰鍰並命限期改正之處分。 2. 又為加強督促違反上開義務之行為人儘速改善個人資料保護措施，就屆期未改正者，**加重處罰額度**。

個資法第48條第2、3項

（第2項）非公務機關違反**第二十七條第一項**或**未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法**者，由中央目的事業主管機關或直轄市、縣（市）政府處**新臺幣二萬元以上二百萬元以下罰鍰**，並令其限期改正，屆期未改正者，按次處新臺幣十五萬元以上一千五百萬元以下罰鍰。

（第3項）非公務機關違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法，其**情節重大**者，由中央目的事業主管機關或直轄市、縣（市）政府處**新臺幣十五萬元以上一千五百萬元以下罰鍰**，並令其限期改正，屆期未改正者，按次處罰。

上市櫃公司重大訊息的發布

臺灣證券交易所股份有限公司對有價證券上市公司重大訊息之查證暨公開處理程序§4 I 第26點：

「發生災難、集體抗議、罷工、環境污染、**資通安全事件**或其他重大情事，致有下列情事之一者：

(一)**造成公司重大損害或影響者**；

(二)經有關機關命令停工、停業、歇業、廢止或撤銷污染相關許可證者；

(三)單一事件罰鍰金額累計達新台幣壹佰萬元以上者；

(四)金融控股公司或屬金融監督管理委員會組織法第二條所稱之銀行、證券、期貨及保險業之上市公司，經主管機關廢止其許可或因違反金融控股公司法、銀行法、保險法、票券金融管理法、證券暨期貨等相關法令經主管機關處分。但處分種類為糾正或限期改善，且對公司財務或業務無重大影響者，不在此限。」

上市櫃公司重大訊息應發布事項

2024.01 證交所、櫃買中心發布「**重大訊息發布應注意事項參考問答集**」

「發生災難、集體抗議、罷工、環境污染、**資通安全事件**或其他重大情事，致有下列情事之一者：……」(重大訊息之查證暨公開處理程序§4 I 第26款)

● 問答集

「公司發生資通安全事件……，或公司之核心資通系統、官方網站等，**遭駭客攻擊或入侵**，致無法營運或正常提供服務，或**有個資、機密文件檔案資料外洩之情事**，**即屬造成公司重大損害或影響**，**公司即應依第 26 款發布重大訊息**。」

「公司之核心資通系統、官方網站等，遭入侵、破壞、竄改、刪除、加密、竊取、服務阻斷攻擊(DDoS)等，致無法營運或正常提供服務，或有個資、機密文件檔案資料外洩之情事等。」

行政檢查常態化

2023.03 行政院第38845次會議「**防止非公務機關個資外洩精進措施**」

事前	1. 各主管機關常設「個資行政檢查小組」，每年**例行性行政檢查**。 2. 金管會促請上市櫃公司取得適當個資保護管理或資安驗證。
事中	1. 精進案件通報流程及監督程序：**主管機關於知悉重大矚目案件後3日內進行行政調查**、10日內完成調查報告。 2. 數位部參與行政調查。
事後	1. 限期業者改正並提出**改正計畫**、個資§25處分。 2. 針對個資外洩高風險事業進行行政檢查。

什麼是行政檢查？

個人資料保護法第22條

（第1項）中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，**進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料**。

（第2項）中央目的事業主管機關或直轄市、縣（市）政府為前項檢查時，對於得沒入或可為證據之個人資料或其檔案，得扣留或複製之。對於應扣留或複製之物，得要求其所有人、持有人或保管人提出或交付；無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制為之。

（第3項）中央目的事業主管機關或直轄市、縣（市）政府為第一項檢查時，得**率同資訊、電信或法律**等專業人員共同為之。

（第4項）對於第一項及第二項之進入、檢查或處分，**非公務機關及其相關人員不得規避、妨礙或拒絕**。

（第5項）參與檢查之人員，因檢查而知悉他人資料者，負保密義務。

2023年中央目的事業主管機關辦理情形

- 財政部：包括菸酒事業、公益彩券、記帳士、記帳及報稅代理人、報關業、保稅倉庫及物流中心。
- 教育部：私校、短期補習班及體育團體等業者。
- 經濟部：行政檢查16家業者。
- 交通部：對曾發生重大矚目案件、保有消費者個人資料筆數超過一定數量或列入高風險事業等觀光產業、汽車運輸業及民用航空業者。
- 衛福部：檢查17家業者。
- 文化部：自行架設網路平台販售書籍之出版社及電影院。
- 數位部：通訊網路及通傳領域關鍵基礎設施、數位經濟相關產業類等業者。
- 金管會：原本的金融機構檢查，並進行證券商及期貨商個資檢查。

行政檢查成員與方向

- 檢查成員
  - 主管機關
  - 警政署
  - 國家資通安全研究院
  - 專家學者（資安、法律）
- 檢查重點
  - **適當安全措施**
  - **資料安全管理措施**

適當安全措施

Plan（計畫）

1. 配置管理之人員即相當資源
2. 界定個人資料之範圍
3. 個資資料之風險評估及管理機制
4. 事故之預防、通報及應變措施
5. 個人資料蒐集、處理及利用之內部管理程序

Do（執行）

6. 資料安全管理及人員訓練
7. 認知宣導及教育訓練
8. 設備安全管理

Action（行動）

11. 個人資料安全維護之整理持續改善

Check（查核）

9. 資料安全稽核機制
10. 使用紀錄、軌跡資料及證據保存

資安調查

- 使用者身分確認及保護機制
- 個人資料顯示之隱碼機制
- 網際網路傳輸安全加密機制
- 個人資料檔案與資料庫之存取控制及保護監控措施
- 防止外部網路入侵對策
- 非法或異常使用行為之監控及因應機制

行政裁罰實例（1/2）

有關蝦皮、誠品生活及旋轉拍賣涉及個資外洩事件 數位部查處說明(數位部數位產業署，2023/5/30)

- 有關蝦皮涉及個資外洩事件，經數位部多次要求業者完善個人資料保護，並提出相關佐證資料以為證明，該**公司在個資盤點上仍僅提供4筆盤點內容**，顯有缺漏，且在風險評估分析上，**對於風險值較高之流程未提供已採取矯正措施之佐證**。另外，對**委外廠商未落實稽核，未能提供完整的安全管控執行、稽核紀錄等具體佐證資料**，無法證實該公司對保有個資已採行適當之安全措施，因此依據個資法第48條第4款併第50條規定，處分業者併同其負責人罰鍰計**新臺幣20萬元**。

行政裁罰實例（2/2）

- 有關誠品生活案，經數位部產業署實地行政檢查，現場已發現在**帳號管理上執行未確實**，另要求事後提供之補充或佐證資料，該**公司個資盤點資料仍不完整**，且針對**委外廠商監督管理未落實執行**，因此依據個資法第48條第4款併第50條規定處分，業者併同其負責人罰鍰計**新臺幣10萬元**。

- 有關旋轉拍賣案，數位部說明該業者已經提出說明及佐證資料，且已依先前包含警政署等專家建議，**強化網站防詐警示、登入採用雙重驗證機制、並禁止用戶利用對話功能傳送未經驗證之網址連結**等，惟未提供針對**委外廠商整體制度稽核**，尚有待改進之處，將限期請業者再行補正。

個資資安事件的2種責任

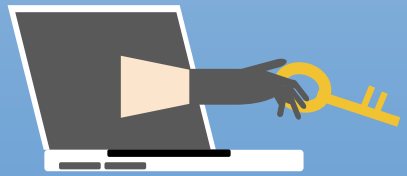
民事損害賠償 （個資法第29條第1項）	行政裁罰（個資法第48條第2、3項）
故意或過失	故意或過失
非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。	（第2項）非公務機關違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣二萬元以上二百萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處新臺幣十五萬元以上一千五百萬元以下罰鍰。 （第3項）非公務機關違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法，其情節重大者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣十五萬元以上一千五百萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處罰。

個資外洩的民事責任

個資法第29條第1項：非公務機關**違反本法規定**，致客戶資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。

但能證明有適當安全措施，不在此限。(無責任)

	責任類型	免責
公務機關	無過失的事變責任	除非損害是因天災、事變或其他不可抗力所致，才可以免責。
非公務機關	舉證責任倒置	由**被告來證明有適當安全措施**。



近年來的個資外洩損害賠償案例

序號	判決字號	案件代稱	宣判時間	外洩認定	賠償金額	備註提醒
1	臺灣高等法院112年度上字第656號判決	ＯＯ溫泉券	113.01.30	✓	2萬元（慰撫金）	單有個資保護、資安保戶等抽象政策規範，尚無法證明已有適當安全維護措施。
2	臺灣高等法院臺中分院111年度消上易字第3號判決	ＯＯ飯店案	112.07.19	✓	0元（僅請求財產上損害，經法院認定欠缺相當因果關係）	防詐騙警語、宣導≠適當安全維護措施
3	臺灣新北地方法院112年度重小字第3188號判決	ＯＯ客運訂票案	112.11.21	✓	5萬7,593元（財產上損害，原告與有過失）	● 被告防火牆為95年產品，遲未更新，經法院認定未盡適當安全維護措施。 ● 個資外洩 & 財產損害間相當因果關係：民訴277但書導置由被告舉反證推翻。

近年來的個資外洩損害賠償案例

序號	判決字號	案件代稱	宣判時間	外洩認定	賠償金額	備註提醒
4	臺灣臺北地方法院112年度訴字第2854號判決	ＯＯ電商網站案	113.04.12	X	公司部分0元；同案被告詐團取款車手賠59萬9,960元	● 以交易流程尚有產品業者、信用卡公司等，謂難合理排除原告個資自其他環節遭竊取或洩漏之可能性 ● 高風險賣場≠個資外洩 ● 網站防詐騙提醒->網站安全保護措施 ● 個資保護管理文件、內控作業手冊->安全維護義務 ● 公司個資演練報告複測結果低風險->資訊安全維護措施

近年來的個資外洩損害賠償案例

序號	判決字號	案件代稱	宣判時間	外洩認定	賠償金額	備註提醒
5	臺灣臺北地方法院111年度北簡字第16345號判決	ＯＯ零售商案	113.03.19	X	0元	●實體門市購物，購物資訊除被告公司外，尚有其他可能洩漏之原因及環節（如發卡銀行端、聯合信用中心端或其他可能） ●被告公司個人資料管理辦法、個人資料使用同意書、員工保密切結書、111年度個資保護教育訓練相關紀錄=適當安全維護措施 ●被告官方網站、Facebook粉絲專頁刊載反詐騙提醒訊息、普發防詐騙提醒簡訊予被告公司之會員=適當防詐措施

個資外洩的民事責任的四個思考點

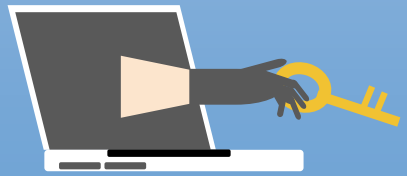
個資法§29 I：非公務機關**違反本法規定**，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。
但能證明其無故意或過失者，不在此限。

一、被害人遭不法蒐集、利用之個資是否來自該業者？

二、業者對被害人個資外洩遭不法利用是否具故意、過失？

三、被害人之財產損害與業者不法侵害隱私權行為，是否具相當因果關係？

四、被害人是否與有過失？被害人之非財產上損害？



（一）、被害人遭不法蒐集、利用之個資是否來自該業者？

原則　被害人需舉證個資自業者端外洩

【ＯＯ生活網案】北院112年度訴字2854號

- 「從系爭交易過程可知，原告於系爭平台上所留資料，除ＯＯ公司外，ＯＯ生物科技公司、ＯＯ銀行亦可知悉原告交易內容，是依本件原告主張，仍難合理排除原告個資自其他環節遭竊取或洩漏之可能性。」
- 經公告為高風險賣場？

【ＯＯ零售店案】北院111年度北簡字第16345號

- 「消費者在門市持卡消費之購物資訊，除被告公司外，尚有其他可能洩漏之原因及環節（如發卡銀行端、聯合信用中心端或其他可能），實難合理排除原告前開購物及消費資訊係自其他環節遭竊取或洩漏之可能性。」

（一）、被害人遭不法蒐集、利用之個資是否來自該業者？

觀察1：法院有用民訴§277但書減輕被害人舉證責任

【A溫泉酒店溫泉券案】高院112年度上字第656號

- 「系爭訂購系統為被上訴人所保有、建置及管理，上訴人所輸入之個資亦存放於該系統中，上訴人無從自行使用、管理，而有證據偏在情形」
- 詐騙集團精準行騙
- A公司函覆上訴人遭詐騙後寄發之存證信函：「本公司110年11月底接獲B公司通報後台偵測到異常IP…」
- 交通部觀光局監督通報紀錄表：「事件發生種類：竊取、個資侵害之總筆數（大約）資料庫外洩約5,423筆…」、「發生原因及事實摘要：…2.該飯店於110/11/16日接獲B公司通知票券系統資料被駭客入侵，相關購買紀錄恐遭竊取…」、「個資外洩可能結果：…另票券系統經由B公司提出電磁資料洩漏紀錄預估5,423筆，恐為不法利用之風險。」

(一)、被害人遭不法蒐集、利用之個資是否來自該業者？

觀察2：法院以平台高風險、是否只有平台可能存有個資來判斷

【英檢代理商個資外洩案】台北簡易庭107年北小字第266號民事判決

- 原告在被告公司網站報考測驗，留下個人資料。
- 詐騙集團佯裝被告公司員工，核對個資、報名場次、付費方式均正確。
- 165反詐騙專線在近似期間，受領類似統計高達47件。
- 被告公司陸續接獲1699名考生反應有冒用公司名義詐騙事件，公司因此委託資安公司檢視網站安全性。
- 詐騙集團除了知道個資基本資料外，也知道正確的報考序號、考試日期。

👉能夠同時掌握所有資訊的，只有被告公司；不會是其他人，如付款銀行。

(二)、業者對被害人個資外洩遭不法利用是否具故意、過失？

業者反證　**適當安全維護措施**：資安管理政策、反詐騙警語、資安演練報告…

【ＯＯ生活網站案】【鞋ＯＯ案】：個資保護及資安保護政策->舉證免責
【ＯＯ溫泉券案】均屬抽象之管理規範，非就系爭訂購系統所為之具體維護措施

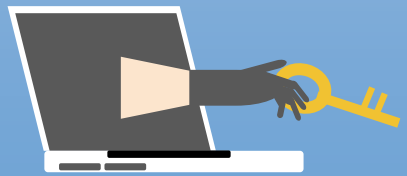
【ＯＯ生活網站案】【鞋ＯＯ案】
【台中ＯＯ飯店案】防詐騙警語等行為，充其量均屬提醒，與其有無善盡個資法第27條第1項之義務無涉

【ＯＯ客運訂票案】：民國95年的防火牆
【ＯＯ生活網站案】：演練專案複測結果與建議報告
【鞋ＯＯ案】：個人資料管理單位及適當組織、定期教育訓練、防火牆

（三）、被害人之財產損害與業者不法侵害隱私權行為，是否具相當因果關係？

欠缺相當因果關係
【ＯＯ溫泉券案】高院112年度上字第656號

上訴人之財產損失係因詐騙集團成員積極實施詐騙行為所致，
即被上訴人上開不法侵害上訴人隱私權、個資自主權之行為，在一般情形下，並不必然會發生上訴人受詐騙且受有財物損失之侵害結果，
此亦可由系爭陳情事件之監督通報紀錄表記載資料庫外洩約5423筆，然發生財損案件僅1筆足佐，
即被上訴人之過失行為與上訴人之財物損失結果間，難謂有相當因果關係



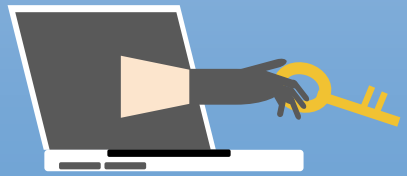
（三）、被害人之財產損害與業者不法侵害隱私權行為，是否具相當因果關係？

新發展？

民訴§277但書舉證責任倒置由業者舉證欠缺相當因果關係

【ＯＯ客運案】新北地院112年度重小字第3188號

- 宥於網際網絡科技浩瀚、參雜人為因素之變異而有高度舉證困難，倘責令被害人擔負完全之舉證責任實有不公；
- 被告對於個資被竊取或外洩風險之控制及分擔能力俱顯優於原告；
- 航空業者對旅客個資之維護義務，除建立在個人資料隱私權之保護外，亦有防免旅客個資外洩致影響飛航安全等重大風險實現。……。**是倘被告認無一般因果關係存在，自應由其提出確切反證證明。**
- 被告持有上開原告個人資料，未盡法定維護義務而有過失等情，業經認定如前，又不詳詐欺集團利用原告遭竊取、洩漏之個人資料對原告之隱私權施以不法侵害，致其財產受有損害情事，亦為被告所不爭，堪以認定。



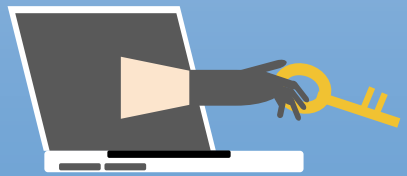
（四）、被害人是否與有過失？

【ＯＯ客運訂票案】原告過失程度3/10；被告賠償5萬7,593元(實際財損82,276元)

然衡以現今社會詐騙集團橫行，遭詐騙事件層出不窮，不惟電視新聞、報章媒體數年來均對此類事件多所報導及分析，政府及警政機關亦經常製作相關宣導影片，……，而本件原告於本案發生時，係已成年之國立大學學生，具有相當智識能力，竟疏未注意，欠缺對此社會常見詐騙犯罪類型相當之警覺性，亦即未有所察覺事件狀況可疑而為確認或撥打反詐騙專線等作為，逕聽從不詳之人指示在其網路銀行輸入所謂「密碼」，旋遭詐欺而生財產損害，故認原告就本件損害之發生與有過失，依法原告自應承擔其過失責任。

（四）、被害人之非財產上損害？

個資法第28條第3項：依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。



個資保護，該怎麼做？（1/3）

(一)法規要求

<table>
<tr><td>個資
§27 I</td><td colspan="2">非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。</td></tr>
<tr><td>施細
§12 II</td><td>一、配置管理之人員及相當資源。
二、界定個人資料之範圍。
三、個人資料之風險評估及管理機制。
四、事故之預防、通報及應變機制。
五、個人資料蒐集、處理及利用之內部管理程序。</td><td>六、資料安全管理及人員管理。
七、認知宣導及教育訓練。
八、設備安全管理。
九、資料安全稽核機制。
十、使用紀錄、軌跡資料及證據保存。
十一、個人資料安全維護之整體持續改善。</td></tr>
<tr><td colspan="3">ＯＯ業個人資料檔案安全維護管理辦法</td></tr>
</table>

個資保護，該怎麼做？ (2/3)

(二)具體作為

制度	訂定個資安全維護計畫、指定安全維護計畫專責人員
資料盤點	個資種類；蒐集、處理、利用目的；目的消失之刪除銷毀
人員管理	取用權限、儲存媒介物、保密義務、離職人員管理
資料安全管理措施	加密、備份、傳輸、防止外部網路入侵對策、非法或異常使用行為之監控及因應機制
認知宣導教育訓練	所屬人員、負責人及個資管理人員（每年至少一次）

個資保護，該怎麼做？（3/3）

(二)具體作為

事故機制	事故發生後應變措施（控制事故損害、通報）、通知當事人、矯正預防措施
設備安全管理措施	紙本文件保管措施、電子資料存放設備、環境進出管制、銷毀程序
資料安全稽核機制	出具定期稽核報告
記錄保存	個人資料之蒐集、處理或利用紀錄；自動化機器設備之軌跡資料；落實執行安全維護計畫之證據(至少5年)
整體持續改善機制	執行狀況、技術發展、法令修正或其他因素，檢視修改計畫

小結

- 個資保護要與公司制度、流程與文化等相結合。
- 過去，因為法規規範因素，個資、資安未必受到企業的重視。
- 在新個資法及相關配套上路後，企業如果沒有完成個資法遵，可能面臨高額的行政裁罰，以及來自消費者的損害賠償訴訟。
- 符合個資法遵要求，除了可以避免行政機關的裁罰外，也可以有效降低資安事件產生的風險。

感謝寶貴時間

albert.hsiao@idozone.com.tw