經濟部產業發展署
Industrial Development Administration, MOEA

# 個資保護看過來
# 資安防護DO IT RIGHT

## 製造業及技術服務業個人資料檔案安全維護管理辦法懶人包

2026年

# 製造業面臨資安挑戰

## 常見的資安事故原因

內　部

外　部

攻擊

### 硬體設備老舊

容易導致軟體無法更新，產生系統漏洞

### 軟體未更新

軟體久未更新可能無法因應新的病毒或攻擊手法

### 員工資安意識不足

誤開釣魚信件的機率提高，且可能意外洩漏企業機密與客戶資訊

### 駭客攻擊

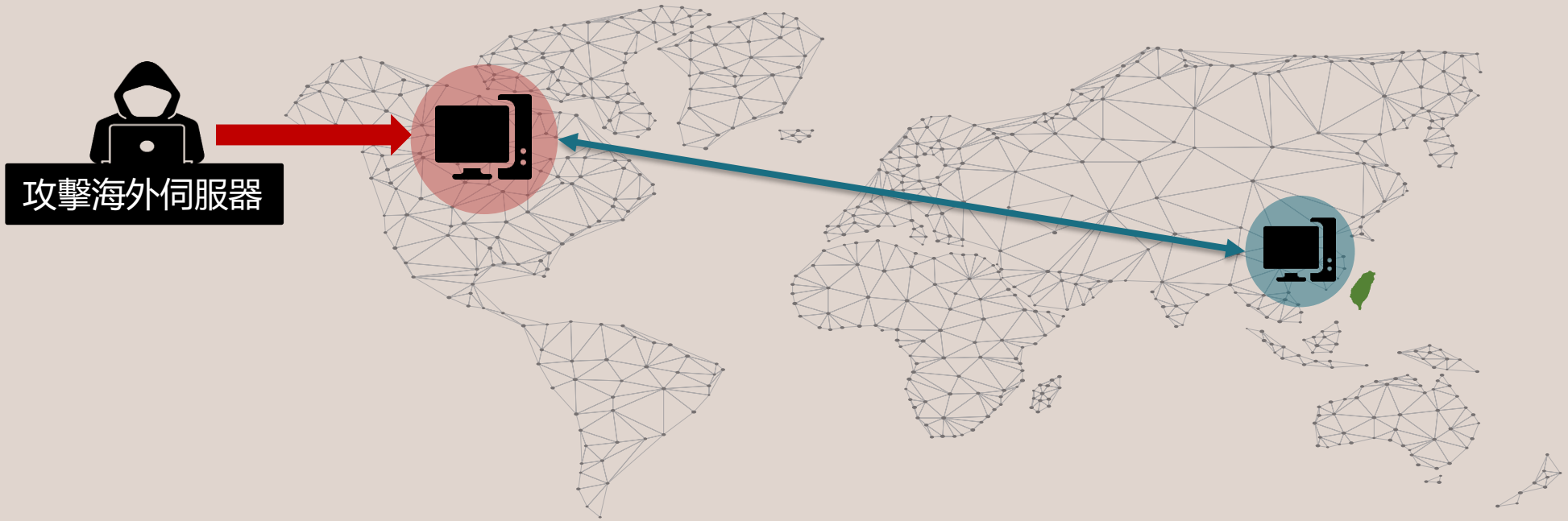
利用系統漏洞或是弱點駭入公司內網，並開始攻擊或勒索



經濟部產業發展署
Industrial Development Administration, MOEA

# 境外資安事故
# 是近年製造業面臨的重要挑戰

近年來世界各地伺服器多遭受駭客攻擊，我國製造業業者於海外之伺服器亦有受攻擊之風險。由於網路無遠弗屆，並不會受到地理因素區隔，因此當國外的子（分）公司之資料庫受攻擊，也可能影響到位於我國的公司。



# 境外資安事故亦常涉及個資外洩

近年案例

**1 我國人受僱於我國公司之境外分公司**

例如：我國人民直接受僱於我國製造業A公司之國外分公司B公司，當駭客攻擊B公司時就可能影響我國籍員工個資

**2 企業併購後未依區域整合員工資料**

例如：我國製造業C公司併購國外D公司及D公司之台灣分公司，但台灣分公司的員工資料仍在D公司的海外資料庫

**3 國內外公司網域未妥善區隔**

例如：我國製造業E公司併購國外F公司後，將國內及國外網域整合，F公司可以在海外接觸到E公司資料

# 資安事故造成莫大損害

**形象商譽受損**

資安事故涉及資料外洩將嚴重損害企業品牌形象及客戶信任，長期將影響企業的市場地位

**經濟財務損失**

駭客可能會勒索業者支付龐大贖金，不付的話可能會造成業務上嚴重損失。即使支付，駭客也可能拒絕回復資料。

**個資外洩受罰**

資料庫中可能包括客戶及員工個資，個資外洩將被中央目的事業主關機關依個資法裁罰。

# 公司資料庫包含客戶及員工個人資料，除了採取足夠的資安防護，也應遵循個資相關規範

《個人資料保護法》

《個人資料保護法施行細則》

《製造業及技術服務業個人資料檔案安全維護管理辦法》

# 《個人資料保護法》

**法規宗旨**

- 蒐集、處理或利用個資時應遵守《個資法》規定，保護當事人個資

**規範對象**

- 只要有蒐集、處理、利用個資，不管是自然人還是法人，都要遵守個資法!

**違法後果**

**未採取適當個資安全維護措施，中央目的事業主管機關或直轄市、縣（市）政府可要求業者限期改正並裁罰2萬~200萬元；若屆期未改正，仍可要求業者限期改正並按次處罰15萬~1,500萬元喔!**

# 製造業及技術服務業
# 個人資料檔案安全維護管理辦法

## 法規宗旨

- 《個資法》要求**製造業及技術服務業者**應依本安維辦法訂定「個資安全維護計畫」，並依循採取適當安全維護措施

## 規範對象

- 消費者個資筆數達5,000筆以上之製造業及技術服務業業者

個人資料保護法第51條之1
「製造業及技術服務業個人資料檔案安全維護管理辦法」第2條

# 個資保護重要基礎觀念

## 個人資料的定義

可識別個人身分的資料。例如姓名、指紋、生日、身分證字號、聯絡方式等

## 當事人的定義

個人資料之本人

## 必須做好安全維護措施

採取適當安全維護措施防止個資被竊取、洩漏、竄改、毀損或滅失等個資事故

## 必須合目的使用

個資法§19、 §20規定，蒐集個資須合法，且後續之處理利用須符合原始蒐集目的

## 必須告知當事人

個資法§8規定，公務機關或非公務機關向當事人蒐集個資時，應明確告知其名稱、目的、當事人權利等事項

## 當事人的權利

個資法§3規定，當事人可以查詢、要求製給複製本、補充或更正、停止蒐集處理利用、請求刪除

# 個資保護工作

## 平時維護

- 訂定個資檔案安維計畫
- 配置個資管理人員
- 界定個資範圍
- 建立風險評估管理機制
- 建立事故通報應變機制
- 建立個資內部管理程序
- 資安防護
- 定期員工教育訓練
- 保存使用紀錄、軌跡資料及證據
- 做好委外監督

## 個資事故發生時

- 採取應變補救措施(如緊急處理勒索軟體)
- 通報主管機關
- 通知當事人

## 個資事故發生後

- 改善個資安全措施
- 改善蒐集處理利用方式
- 將改善措施更新至安維計畫

個資法施行細則第12條

「製造業及技術服務業個人資料檔案安全維護管理辦法」導入手冊12頁以下

# 配置適當管理人員與資源

平時維護 | 個資事故發生時 | 個資事故發生後

**公司高層人員**

例如總經理、代表人

須為有權力決定之人

＋

**有管理及維護個資能力的人員**

至少一名


個人資料保護法施行細則第12條第2項第1款

「製造業及技術服務業個人資料檔案安全維護管理辦法」第3條

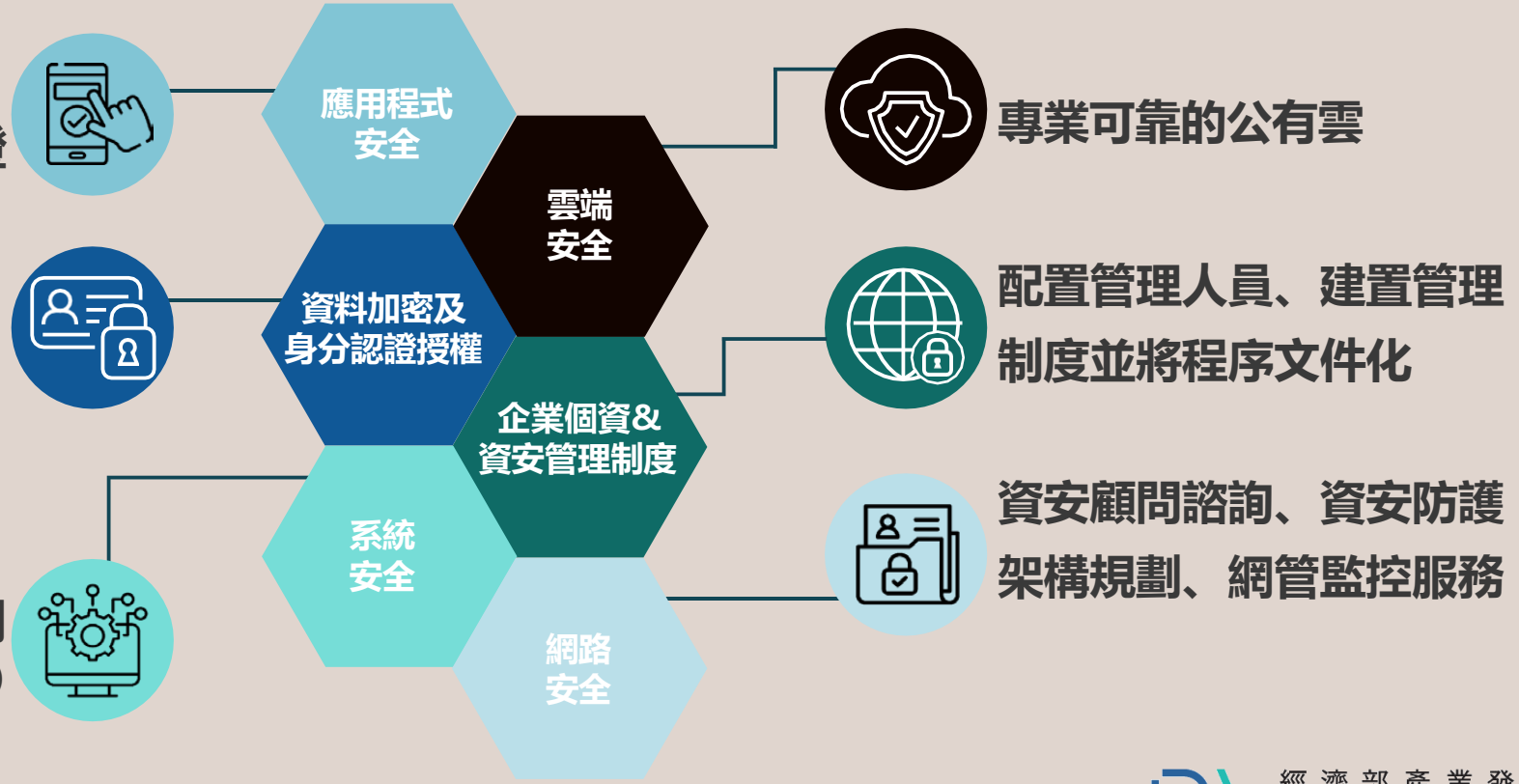
# 常見資安防護措施

**平時維護** | 個資事故發生時 | 個資事故發生後

原始碼檢測、
App資安認證

SSL憑證、
資料庫加密、
多因子認證

定期資安檢測
(含網站弱掃、系統主機弱掃)




專業可靠的公有雲

配置管理人員、建置管理制度並將程序文件化

資安顧問諮詢、資安防護架構規劃、網管監控服務

# 因應境外駭客攻擊應採取之防護措施

## 平時維護

### 防火牆入侵偵測/防禦系統（IDS/IPS）

- 在企業總部與國外子公司之間部署防火牆與具備自動化阻擋功能的IDS或IPS
- 即時偵測並封鎖異常流量

### 多因子驗證（MFA）

- 後臺管理介面、VPN或其他高敏感性系統，建議採用多因子驗證，提高攻擊門檻

## 個資事故發生時

### 網路分割（Network Segmentation）

- 確保公司內部與對外服務網段隔離，降低駭客入侵後向內部移動的風險

### 供應鏈安全評估

- 國外子公司若需依賴當地的雲端服務、硬體供應商，必須評估其安全管控機制
- 可在契約中加入明確的資安責任與個資法責任，確保第三方的資安品質

## 個資事故發生後

### 使用安全通道

- 與境外公司之間的資料傳輸盡量使用加密連線，避免資料在傳輸過程中被竊取或竄改

### 提升員工資安意識

- 針對釣魚郵件、深度偽造（Deep Fake）等攻擊手法，定期教育訓練
- 建立內部通報管道

# 委外監督

平時維護 | 個資事故發生時 | 個資事故發生後

**條　件**

委託第三人蒐集處理或利用個資時，應於委託契約或相關文件說明相關監督內容

**建議措施**

1. 請委外廠商繳交自評表
2. 稽核委外廠商

**未監督後果**

若沒有做好委外監督，當委外廠商發生個資外洩時，業主也需要負責!

個人資料保護法第4條意旨
個人資料保護法施行細則第8條

# 事故發生時應立即避免損害擴散

平時維護 | 個資事故發生時 | 個資事故發生後

**01 中斷網路連線**
立刻斷網避免災情擴大

**02 關機並拔插頭**
立刻持續按壓電源鍵或拔插頭，強迫電腦關機

**03 緊急宣導、清查**
立即宣導，提升警覺性。並通知所有同仁有狀況立即回報

**04 評估災情**
了解企業損失範圍與嚴重性、清查這些檔案是否有備份

**05 保存現場並尋求協助**
保存一臺受害主機，以便提供分析及調查

**06 系統重灌**
格式化、重灌系統，讓電腦回復成乾淨的原始狀態

**07 報 案**
向檢警報案，涉及個資外洩時通報主管機關並通知當事人



經濟部產業發展署
Industrial Development Administration, MOEA

# 個資事故須通報主管機關

平時維護 | **個資事故發生時** | 個資事故發生後

## 通報對象

**經濟部**

（或直轄縣市政府並副知經濟部）

## 通報方式

**填寫本安維辦法附表二**（請掃Qrcode下載）

**信箱：jjhuang@ida.gov.tw**

**電話：02-27541255#2427**

## 通報時間

**72小時內**

（自業者知道發生個資事故時起算）

第六條附表二

附表二　非公務機關個資外洩通報表

| 個人資料侵害事故通報與紀錄表 | | |
|---|---|---|
| 業者名稱<br>通報機關 | 通報時間：　年　月　日　時　分<br>通報人：　　簽名(蓋章)<br>職稱：<br>電話：<br>Email：<br>地址： | |
| 事件發生時間 | | |
| 事件發生種類 | □竊取<br>□洩漏<br>□竄改<br>□毀損<br>□滅失<br>□其他侵害事故 | 個資侵害之總筆數(大約)<br>□一般個資 _____筆<br>□特種個資 _____筆 |
| 發生原因及事件摘要 | | |
| 損害狀況 | | |
| 個資侵害可能結果 | | |
| 擬採取之因應措施 | | |
| 擬採通知當事人之時間及方式 | | |
| 是否於發現個資外洩後72小時通報 | □是　□否，理由 | |

掃描我下載

個人資料保護法施行細則第12條第2項第4款

「製造業及技術服務業個人資料檔案安全維護管理辦法」第6條

# 個資事故須通知當事人

平時維護 | 個資事故發生時 | 個資事故發生後

僅有反詐騙宣導
不符合個資法規範喔!

**通知內容02**
調查成因

**通知內容03**
事後修補措施

**OO公司員工個資外洩通知信**

0月0日星期O 00:01

寄件人：OO系統-ZZZ <zzz@OO.com.tw>
收件者：員工A-YYY <yyy@A.com.tw>；員工B-WWW <www@B.com.tw>；員工C-VVV <vvv@C.com.tw>
副本：OO系統-UUU <uuu@OO.com.tw>

親愛的同仁您好：
本公司於0月W日00時10分時，遭到不明駭客入侵，導致員工個資外洩。本公司先於0月W日00時01分時收到員工通報後，本公司立即採取以下措施：

1. 防堵所有可能的出入口，並尋找惡意程式，於0月W日00時50分時，找到木馬程式並刪除。本公司也立即更新系統，修改存取權限，請各位同仁配合以下列方式立即進行更新：.....
2. 本公司並立即調查事件成因，發現駭客是以.....
3. 本公司將進行以下系統修補，包含：(1) ○○○○ (2) ○○○○ (3) ○○○○
4. 本公司已向主管機關通報，並向165警方報警。
5. 若各位同仁有任何需要本公司協助之處，請聯繫資訊處個資專員○○○（電話：00-0000-0000）。本公司並將盡所能協助調查事故，並持續補修系統以建立更完善的系統資安。

本公司再次向您致歉。

**常見通知方式**
Email、簡訊、網站公告等
(此以Email為例)

**通知內容01**
緊急應變與補救措施

**通知內容04**
通報主管機關及報警

**通知內容05**
協助當事人因應

個人資料保護法施行細則第12條第2項第4款
「製造業及技術服務業個人資料檔案安全維護管理辦法」第6條

# 事故後應改善防護措施

平時維護　　個資事故發生時　　**個資事故發生後**

**1 加強設備維護**

設備進場前務必進行惡意設備檢測、風險檢測，並定期更新硬體及系統

**2 更新管理制度/安維計畫**

重新檢視原本的管理制度/安維計畫，並將改善方式更新至新的管理制度/安維計畫

**3 提升員工資安意識**

定期舉辦員工教育訓練，使員工提升警覺心

# 其他常見QA

**Q1：未發生竊取或洩漏，即無違反規定嗎?**

A：不一定!

- 現行個資法第27條第1項規定，業者有安全保管所持有個資之責任，並非等到實際損害發生才違規。
- 竊取或洩漏只是「裁罰輕重」的參考，並非免責依據。

**Q2：只要採購防護軟硬體，就可以免責嗎?**

A：單純採購不能免責

- 單純採購軟硬體不足以主張免責。
- 個資與資訊之適當安全措施必須長期且持續投入。

# 其他常見QA

**Q3：會員遭釣魚詐騙，業者需要負責嗎?**

A：業者有法律上預防義務

- 預防義務：業者對於釣魚詐騙有採取預防、通報即應變之義務。
- 視同外洩：會員受騙，視同業者所保有的個資遭竊取。

**Q4：事後補救可以免責嗎?**

A：不行!

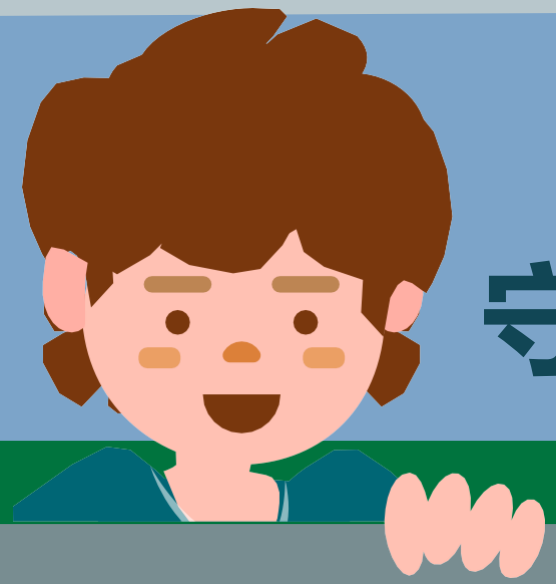
- 業者有「事前預防」並採取適當安維措施之義務，事後補救仍無法抵銷違法事實。

# 其他常見QA

**Q5：我們並非資安專業，能否免責?**

A：業者將訂單系統、主機系統或物流系統等蒐用個資功能委外處理，仍有委外監督義務

- 現行個資法第8條規定，業者委託他人蒐集、處理、利用個資時，必須適當監督。
- 建議可以於契約中明訂雙方權責與監督條款，定期查核廠商，並保留查核與改善紀錄。



# 守護資安 個資平安

**個資保護與資安防護關係密不可分， 必須落實資安措施，**
**才可以有效降低個資事故發生的風險！**



經濟部產業發展署
Industrial Development Administration, MOEA

# 其他參考資源

## 臺灣電腦網路危機處理暨協調中心（TWCERT）

數位發展部資通安全署指導下成立，協處企業資安事件通報、惡意檔案檢測服務等，提升業者資安認知及網路安全資安防護能量，業者可參加其會員成立資安聯盟。

網址：https://www.twcert.org.tw/tw/mp-1.html

## 內政部警政署165 全民防騙網

提供近期民眾遭遇詐騙之事件，並提供相關宣導資源

網址：https://165.npa.gov.tw/#/

## 製造業及技術服務業個人資料檔案安全維護辦法導入手冊

網址：
https://www.ida.gov.tw/ctlr?PRO=news.NewsView&id=21540&lang=0