數聯資安

台南應用科技大學
TAINAN UNIVERSITY OF TECHNOLOGY

個人資料保護管理審查會議
主官管個人資料保護宣導

數聯資安 資安顧問 王信何

==========

CISA, CISM, PMP, NSPA
ISO/IEC 27001 LA, BS 10012 LA, ISO 20000 LA
ISO 29100 LA, ISO 9001 LA, OHSAS 18001LA

遠傳電信 關係企業

Agenda

- 資訊安全威脅
- 個人資料保護法認知
- 個資案例

Agenda

- ☑資訊安全威脅
- ☐個人資料保護法認知
- ☐個資案例

資安發展趨勢

資料來源：World Economic Forum(WEF)

世界經濟論壇(WEF)在2020年全球風險報告中指出2020全球風險矩陣：

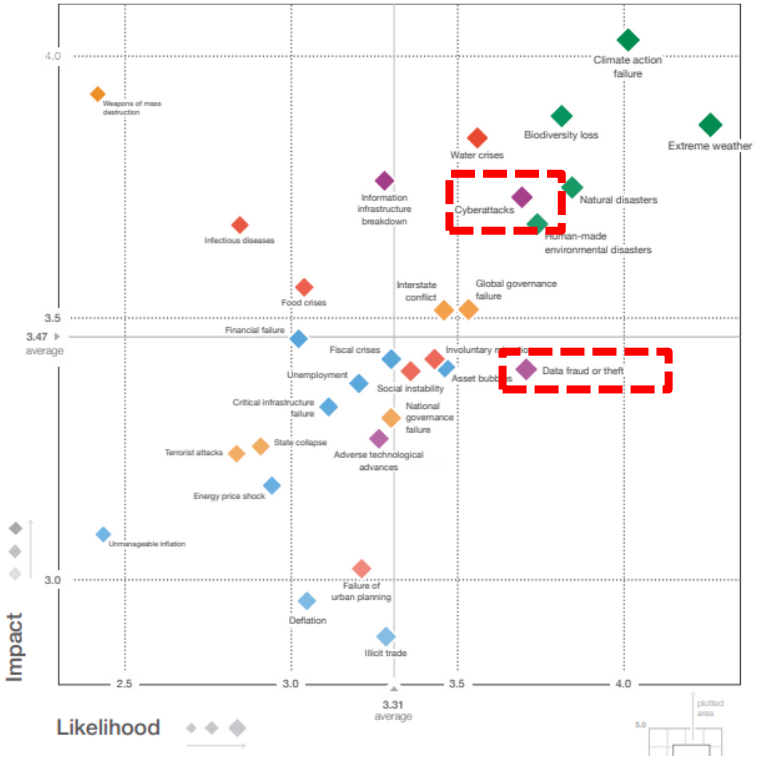
Top 10 risks in terms of **Likelihood**

1. Extreme weather
2. Climate action failure
3. Natural disasters
4. Biodiversity loss
5. Human-made environmental disasters
6. Data fraud or theft
7. Cyberattacks
8. Water crises
9. Global governance failure
10. Asset bubbles

Top 10 risks in terms of **Impact**

1. Climate action failure
2. Weapons of mass destruction
3. Biodiversity loss
4. Extreme weather
5. Water crises
6. Information infrastructure breakdown
7. Natural disasters
8. Cyberattacks
9. Human-made environmental disasters
10. Infectious diseases

Figure II: The Global Risks Landscape 2020



2020年資安趨勢10大預測

資料來源：iThome

2020年資安趨勢10大預測

今年資安趨勢與往年最大不同在於，出現5G世代下的資安挑戰，隨著越來越多國家開始提供5G行動網路，勢必會帶來更多連網裝置的應用，以及更快的連網速度，但相對也帶來更多風險，面對新的一年，哪些資安威脅是需關注：

趨勢1】管理不周導致資料外流事件頻傳，企業、雲端業者、政府均應強化管理

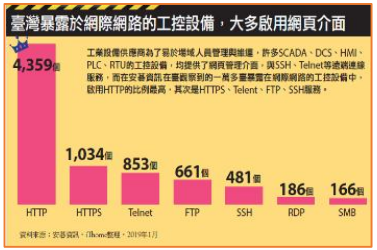
目的：取得個人資料、金融資訊(信用卡...)、商業或業務祕密 → 進行詐騙、廣告、盜領、盜刷、商業利益...

趨勢2】連網裝置資安標準開始成形，企業應重視網路分析、偵測與反應

物聯網裝置盛行，使得駭客鎖定這種應用發動攻擊。由於涉及的領域相當廣泛，無論是金融、公共服務、製造業，零售業，乃至於能源設施和醫療，都有採用這種應用。開發這些裝置的業者，要如何增加安全性，成為物聯網資安發展的重點

資料來源：iThome

2020年資安趨勢10大預測(續)



趨勢3】工控環境正面臨真實發生的資安威脅，勒索軟體來勢洶洶

在萬物聯網、大數據與AI等技術的潮流下，智慧製造、智慧醫療已成臺灣政府積極推動的政策，以促進為國內產業智慧化轉型升級，然而，所面對的操作科技（OT）資安威脅持續受到關注，仍是2020年的焦點

趨勢4】資安法適用範圍擴及關鍵基礎設施，個資法為了因應GDPR將修法

法遵議題是組織單位賴以生存的基本，2020年臺灣組織和企業面對重要的法遵要求，對內有資通安全管理法適用、個人資料保護法的再修訂，對外受影響的法遵規範

趨勢5】資安產品驗證蔚為風潮，隱私保護有賴ISO 27701整合ISMS

資訊安全管理不再只是單純服務流程的驗證，包括軟、硬體產品和整個供應鏈安全，都已經是政府和企業無法忽視重要趨勢，ISO 27701是2020年最重要的隱私管理標準

資料來源：iThome

2020年資安趨勢10大預測(續)

趨勢6】AI冒用身分的攻擊現身，對於新興辨識技術的採用更顯迫切

趁機取得使用者帳密的網路釣魚，近年更是發生大量帳密外洩事件，以及弱密碼，與預設密碼等各式帳密安全問題，而在2020年，還有一個新興的身分安全威脅趨勢值得注意，那就是以AI技術所進行的深度偽造與詐騙，稱為Deepfake

趨勢7】攻擊型態趨於多元，供應鏈防護需涵蓋VPN網路與外部服務

IT人常用的工具軟體被駭客攻陷、VPN漏洞讓供應鏈有弱點、網站使用的外部服務遭濫用，駭客置入惡意程式，綜觀這些發生的供應鏈攻擊事件，企業若要做好相關的防護，必須思考各種形式委外服務的依賴

趨勢8】IT服務供應商成勒索軟體新目標，針對委外業者攻擊，間接影響企業

愈來愈多的勒索軟體攻擊行動，鎖定管理服務供應商或第三方服務供應商，因為只要發動一次攻擊，就能要脅到許多受害者

資料來源：iThome

2020年資安趨勢10大預測(續)

趨勢9】NCC要求所有電信業者，5G資安要做到Security By Design

國家通訊傳播委員會委員孫雅麗表示，5G網路將成為國家重要的關鍵基礎設施，要求所有電信業者，在打造5G網路的同時，就必須納入資安管理的概念

趨勢10】培育學校生根有成，資安人才與產業接軌是關鍵

儘管臺灣目前學校資安人才培育有成，該如何讓人才順利和產業接軌，並透過政府仍在規畫中的資安研訓院，持續提高人才培訓能量，才是生生不息的關鍵

資料來源：iThome

Agenda

- ☐資訊安全威脅
- ☑個人資料保護法認知
- ☐個資案例

我國個人資料保護法發展沿革

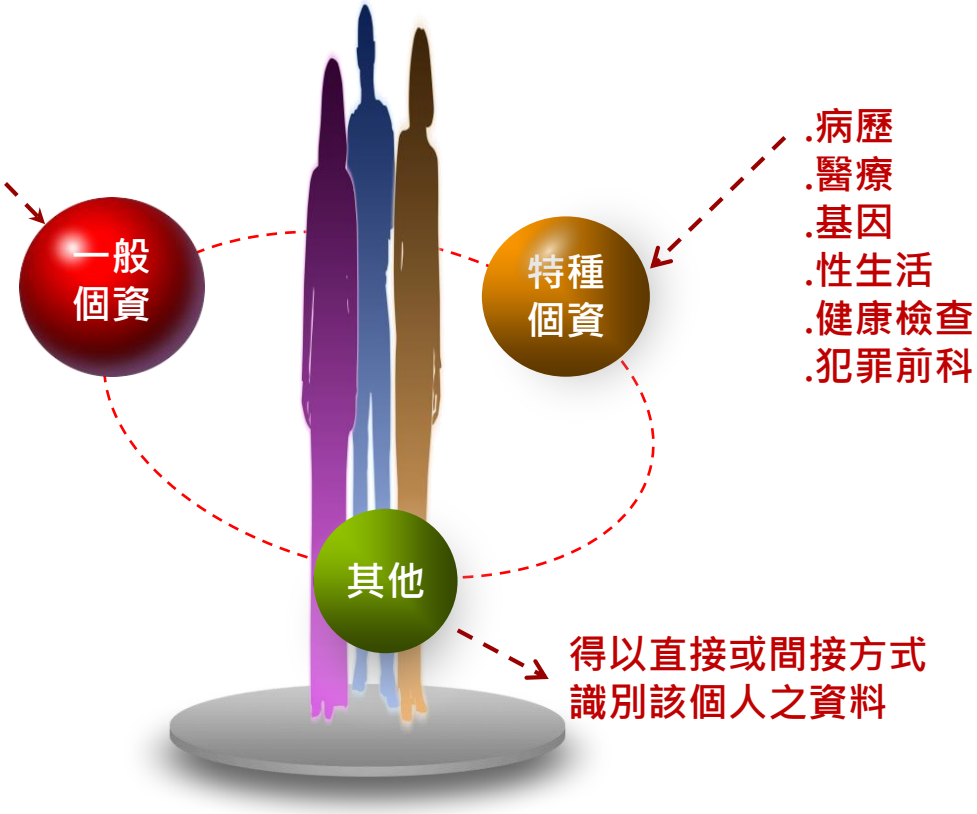
個人資料保護法之法律主政機關

我國個人資料保護法架構圖

個資法所稱之個人資料

自然人

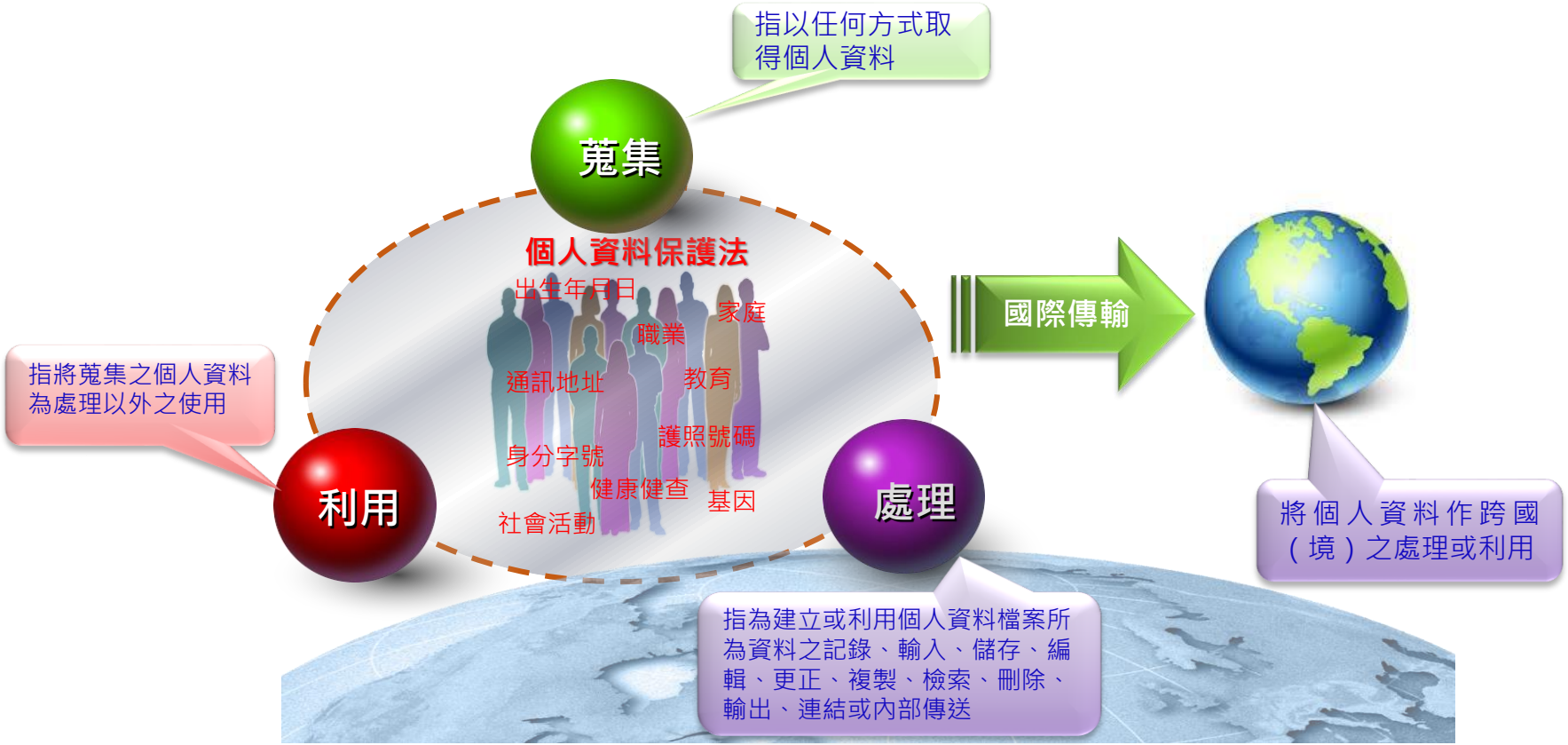
.姓名
.出生年月日
.國民身分證
統一編號
.護照號碼
.特徵
.指紋
.婚姻
.家庭
.教育
.職業
.聯絡方式
.財務情況
.社會活動



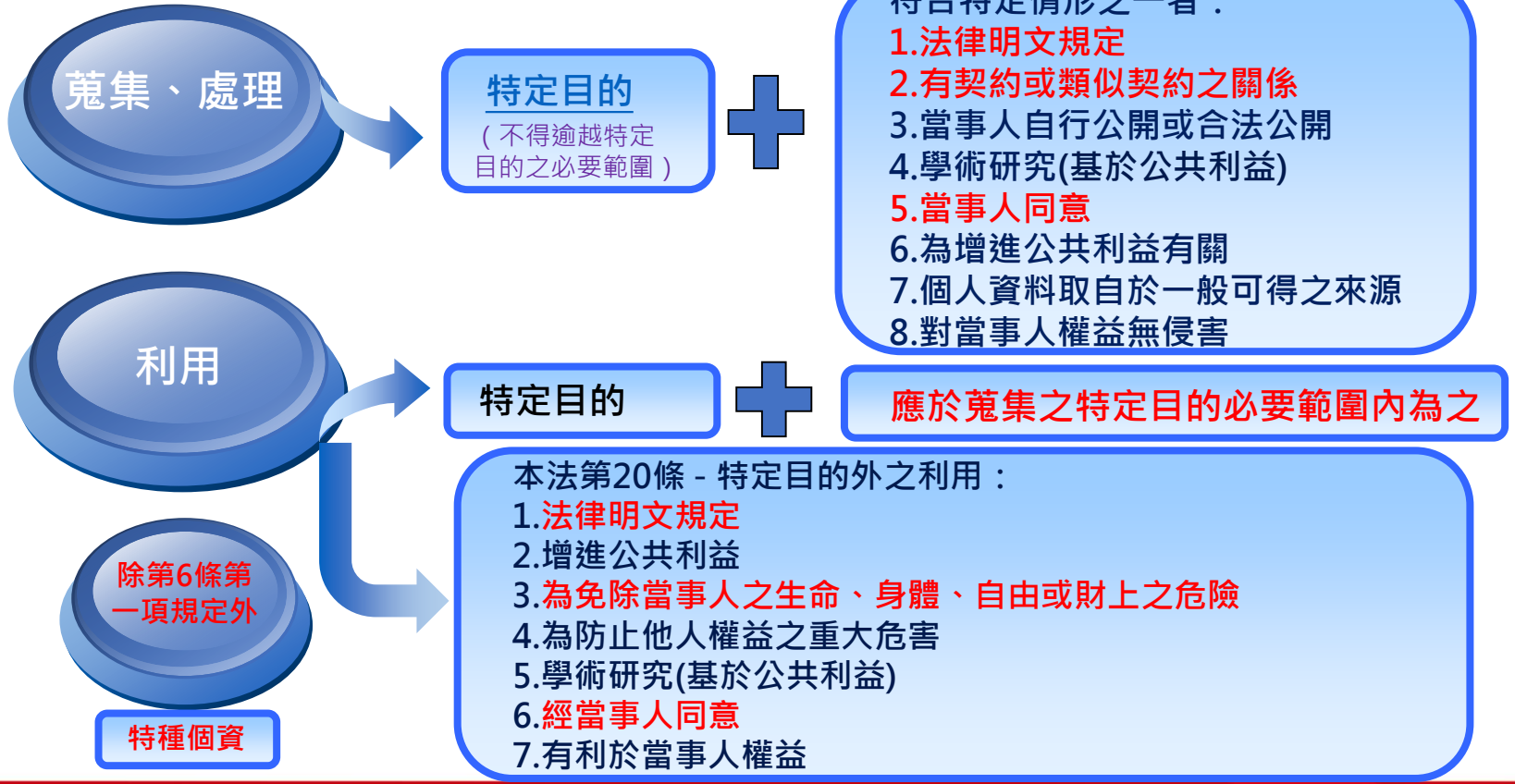
.病歷
.醫療
.基因
.性生活
.健康檢查
.犯罪前科

得以直接或間接方式
識別該個人之資料

個資法所指行為定義


指以任何方式取得個人資料
蒐集
個人資料保護法
出生年月日
家庭
職業
通訊地址
教育
護照號碼
身分字號
健康健查
基因
社會活動
國際傳輸
指將蒐集之個人資料為處理以外之使用
利用
處理
將個人資料作跨國（境）之處理或利用
指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送

蒐集、處理與利用個資之規範(非公務機關)



直接蒐集告知事項

第8條 公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：

應告知事項	得免為告知之況情
一、公務機關或非公務機關名稱	一、依法律規定得免告知
二、蒐集之目的	二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要
三、個人資料之類別	三、告知將妨害公務機關執行法定職務
四、個人資料利用之期間、地區、對象及方式	四、告知將妨害第三人之重大利益
五、當事人依第三條規定得行使之權利及方式	五、當事人明知應告知之內容
六、當事人得自由選擇提供個人資料時不提供將對其權益之影響	六、個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響

個資法施行細則明訂安全維護事項

個資法 11 項安全維護措施

安全維護措施	實施重點	實施面向
1. 配置管理的人員及相當資源	指派專人或成立個資因應小組，有專人負責推動個資因應措施，並有適當的資源來支持。	管理面
2. 界定個人資料的範圍	盤點內部所有的個人資料，確定該保留的個資、定義個資管理的權責。	管理面／技術面
3. 個人資料的風險評估與管理機制	評估個人資料的價值與風險，依據風險擬定個資管理機制與應變措施。	管理面
4. 事故的預防、通報及應變機制	依個資的風險建立事故預防、通報及應變機制，確保可提早預防個資侵害事件，或於侵害事件發生時可立即因應，降低損害。	管理面／技術面

個資法施行細則明訂安全維護事項

5. 個人資料蒐集、處理及利用的內部管理程序	依個人資料的蒐集、處理或利用的規定，擬定內部作業管理流程。	管理面
6. 資料安全管理及人員管理	擬定資料分級、安全管理機制，以及人員存取資料的權限管理。	管理面
7. 認知宣導及教育訓練	宣導個資法，提升個資意識，並定期舉行教育訓練。	管理面
8. 設備安全管理	針對資訊設備或與個資處理有關的設備，擬定管理制度，落實管控措施。	技術面
9. 資料安全稽核機制	擬定資料安全稽核機制，落實個資管理制度，持續找出問題。	技術面
10. 使用紀錄、軌跡資料及證據保存	保存日後可用來舉證，證明已善盡管理義務的各種記錄、證據、軌跡資料等。	技術面
11. 個人資料安全維護的整體持續改善	定期持續檢討，找出問題，不斷改善，落實個資管理制度。	管理面

個資法損害賠償規定

民事賠償
每筆500~20000
回復名譽

求償有效期
知情2年
不知情自損害發生時起5年

刑事責任
5年以下有期徒刑併科NT1百萬以下(意圖營利或不法利益)

行政罰則
違反個資行為規範罰5萬~50萬
個人資料維護不當、未善盡告知責任、不履行個人權益

代表人、管理人除能證明已盡防止義務者外，應並受同一額度罰鍰

不知行動裝置資安威脅

- 當Android賦予智慧型手機使用者可自由從非官方市集安裝軟體時，也為惡意程式作者敞開了大門
- 電腦駭客已轉移戰場，從**電腦轉移到智慧手機**或是平板等移動裝置

網路安全威脅研究報告-Symantec

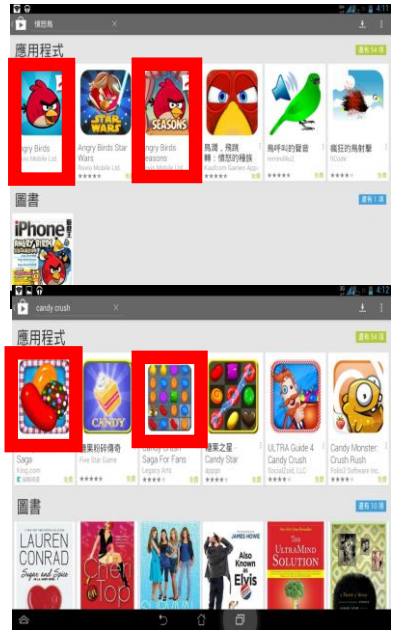
不知行動裝置資安威脅

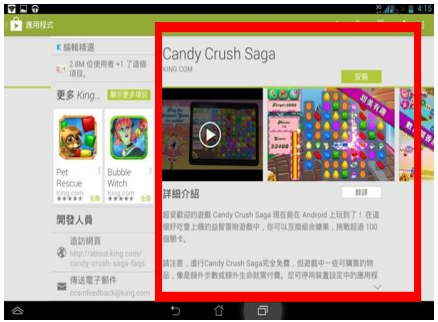
- 賽門鐵克的「諾頓報告」顯示有多數的成人不知道行動裝置也有資訊安全軟體，突顯出**行動裝置危機意識的缺乏不足**
- 未來無此安全意識將持續成長，為何呢？
  - 行動裝置使用**無安全意識**，使用者的**教育不足**
  - 使用智慧型手機的人，**未意識**到需要安裝**資訊安全**軟體
  - 行動裝置的**使用者數量成長快速**，使用者多半較不熟悉數位生活，對於相關的安全意識更是不足

APP權限你給多少?

Android系統APP安全

確認官網 → 詳讀介紹評論 → 安裝授權審視 → 留意開發者的其他APP





LINE通訊軟體安全設定

取消自動加入好友功能 取消允許被加入好友選項	隱私設定中取消公開ID	如無使用個人電腦登入LINE，應取消允許自其他裝置登入

LINE通訊軟體安全設定

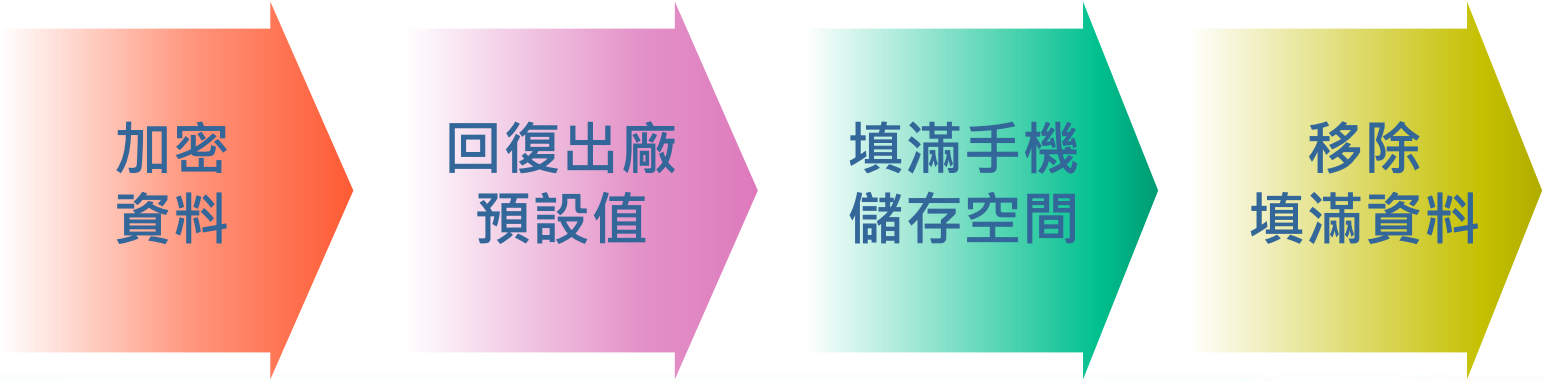
- LINE為強化帳號安全，電腦登入LINE和LINE Store帳號時，手機版立即通知。若收到不明裝置登入提醒，如何處理?

1.強制將對方登出

2.更改電子郵件帳號密碼

行動裝置出售或丟棄前

- 保障個人隱私的方法：
  - 先透過設定中的安全選項將手機加密，再回復出廠預設值
  - 回復Android出廠預設值後，以無害的影片或照片檔填滿手機儲存空間，讓這些資料能夠覆蓋原來的檔案空間，再移除一次



行動裝置資安保護措施_資料保護

資料加密與備份	● 資料定期備份(使用雲端備份時要留意資料的敏感性) ● 行動裝置儲存的資料重要資料可考量安裝加密軟體防護
遠端定位與資料刪除	● 建議使用內建行動裝置追蹤功能或額外安裝可遠端定位並進行資料清除功能之APP
報廢行動裝置資料處理	● 行動裝置於報廢不用時，應完整清除所有資料，並回復為出廠設定
設定行動裝置密碼自動鎖定功能	● 為避免未經授權的人藉機使用行動裝置，建議應設定自動上鎖。

Agenda

- ☐資訊安全威脅
- ☐個人資料保護法認知
- ☑個資案例

指揮中心發布實聯制指引

- 指揮中心今日發布新冠肺炎實聯制措施指引，要求各營業場所或集會活動所蒐集的民眾個資，不可用於疫調之外的其他目的，最多存放28天就要主動刪除銷毀，且刪除的紀錄也須保存，以供後續政府監督稽核使用

資料來源：iThome

勒索軟體攻擊案例

企業 勒索病毒風暴??	醫院 勒索病毒加密??	政府機關 勒索病毒攻擊??

勒索軟體攻擊案例

- 加油站遭到駭客鎖定台灣中油從5月4日傳出受到勒索軟體攻擊，使得部分付款服務被迫停用

首頁 > 新聞與公告 > 本部新聞

→ 本部新聞

2020-05-04 15:01 台灣中油公司

台灣中油加油站因遭受惡意程式攻擊資訊系統異常 加油站暫時僅使用現金及信用卡交易

點閱數：686

台灣中油公司因遭受惡意程式攻擊，感染勒索病毒，目前加油站加油部分受影響者為無法使用捷利卡、中油PAY等相關作業，請消費者加油先使用現金及信用卡，其餘生產和供應並未受到影響。

台灣中油指出，資訊系統今天出現操作異常，目前資訊單位已緊急處理中，儘速排除障礙；消費者大部分使用的現金及信用卡交易不受影響，唯牽涉台灣中油內部系統的相關作業如捷利卡、中油PAY等暫停使用，請消費者改用現金或信用卡支付。

資料來源：iThome

「臉書」不當分享8700萬名用戶個資

- 社群媒體龍頭「臉書」不當分享8700萬名用戶個資，去年遭到美國當局調查。華爾街日報報導，美國聯邦貿易委員會已經批准跟臉書的和解協議，並罰款臉書50億美元，約合台幣1550億

購票平臺個資外洩客戶遭騙判決出爐

- 在2017年，有民眾提告EZ訂個資外洩，致使受害者遭騙25萬元，如今二審判決在2019年9月出爐，士林地方法院指出業者也應付起7成部分責任，最終裁定賠償18萬3,274元。這起判例，也將影響未來個資外洩事件的判決

員工誤點網釣信件，害64萬人個資外洩

- 美國奧勒岡州健保署年初遭**網釣攻擊**，造成64.5萬名居民個資外洩，該部門以郵件通知受影響的民眾

News Release

DHS | Oregon Department of Human Services

Date: June 18, 2019

Contact: Jake Sunderland, (503) 877-0170, Jake.Sunderland@state.or.us

Notices mailed to 645,000 clients possibly impacted by data breach

(Salem, Ore.) – The Oregon Department of Human Services is sending notices by mail to approximately 645,000 clients notifying them that their personal information was compromised during a previously announced January 2019 data breach.

It is not known if the compromised information, which includes personal health information, was viewed or used inappropriately.

資料來源：iThome

漏洞管理、資安措施不當 泰航950萬筆個資外洩

- 國泰航空2018年10月爆發系統遭駭、950萬名客戶個資外洩事件，上周香港隱私管理機關公布調查報告，揭露是兩個駭客組織行動結合國泰航空多項**資安措施不當**及**漏洞管理疏漏**的結果

示意圖（圖片來源：國泰航空）

銓敘部個資外洩通知

本部於108年6月22日接獲外部情資知悉國外網站揭露疑似本部所掌理之個人資料餘59萬筆，本部依個人資料保護法第12條及施行細則第22條規定通知當事人相關事項如下：

一、影響範圍：94年1月1日至101年6月30日間中央及地方機關公務人員送審人員歷史資料，實際影響人數為243,376筆，欄位包含身分證字號、姓名、服務機關、職務編號、職稱。

二、已採取因應措施：

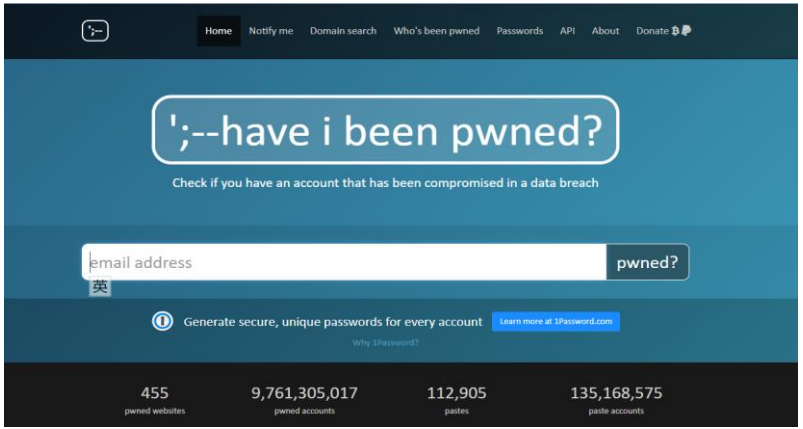
(一)依資通安全管理法向行政院國家資通安全會報技術服務中心進行資安事件通報。

(二)疑似外洩資料之資訊系統早已於104年3月下線，為求審慎，本部即刻對本案現行運作相關資通系統進行弱點檢測及重新檢視防護措施。

針對本事件，本部已協請行政院資通安全處協助進行根因調查及全機關全面性資通安全檢測，本部將確實檢討改進，並依資通安全管理法及個人資料保護法持續精進各項資通安全及個資保護相關作為。

如何查詢自己個資是否外洩

- 透過搜尋網站-關鍵字查詢(如姓名、身分證字號、電話號碼、E-mail...)
- 用電子郵件查詢 Have I Been Pwned https://haveibeenpwned.com/
- 用姓名及身分證末6碼查詢台灣抓漏小天使https://breach.tw/ (暫時關閉)



數聯資安

資訊安全與個資防護觀念必須是一種**習慣**與**文化**，而不能只是一種技術與專業

Thank You