數位發展部資通安全署
Administration for Cyber Security, moda

資安現況(資安六法與個資法)與未來趨勢

資通安全署

112年3月

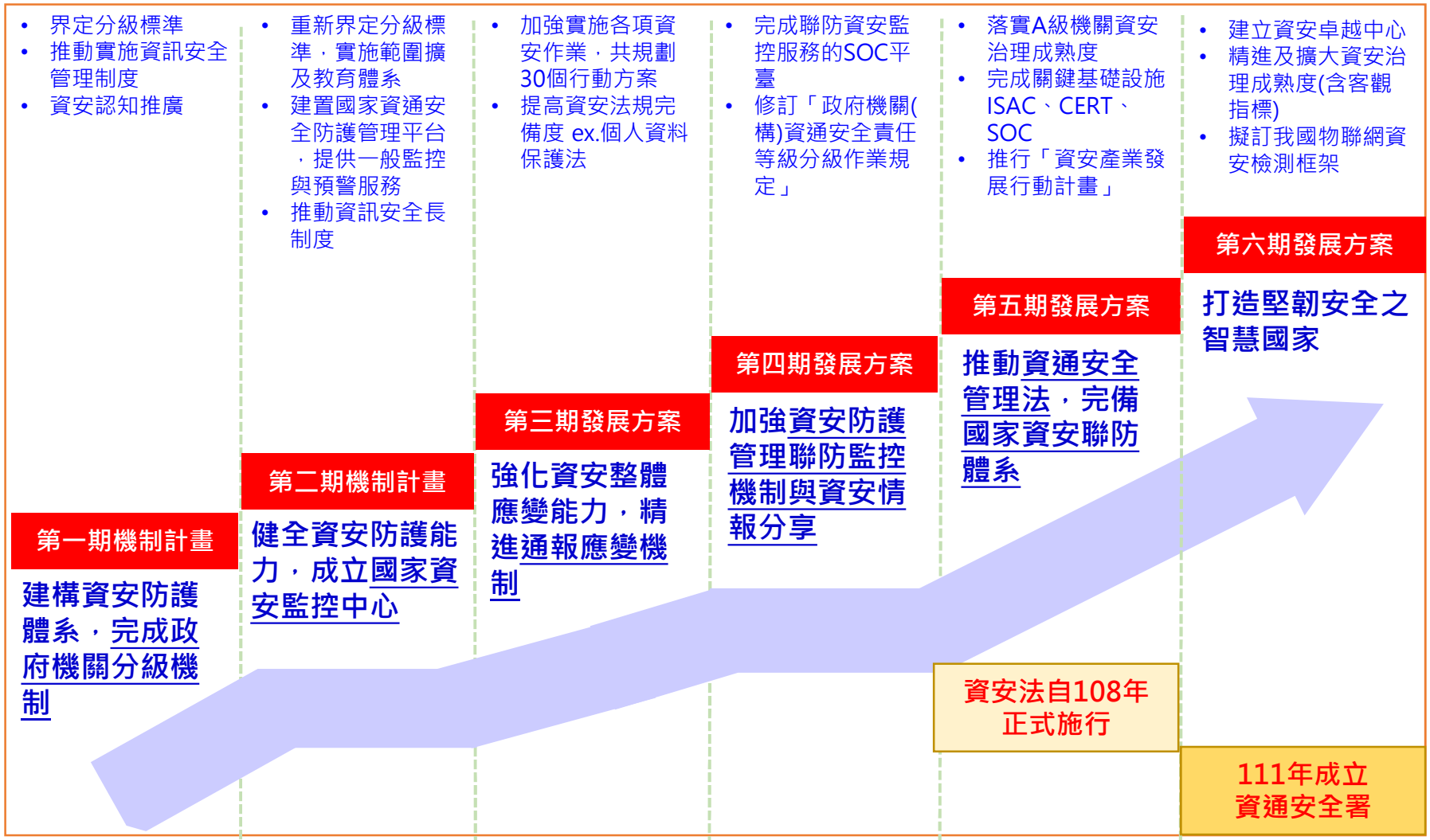
大綱

數位發展部資通安全署
Administration for Cyber Security, moda

- 資安法規範重點介紹
- 個資保護管理
- 資安威脅趨勢與防護建議
- 案例分享
- 結論與建議

資安法規範重點介紹

我國資安推動進程

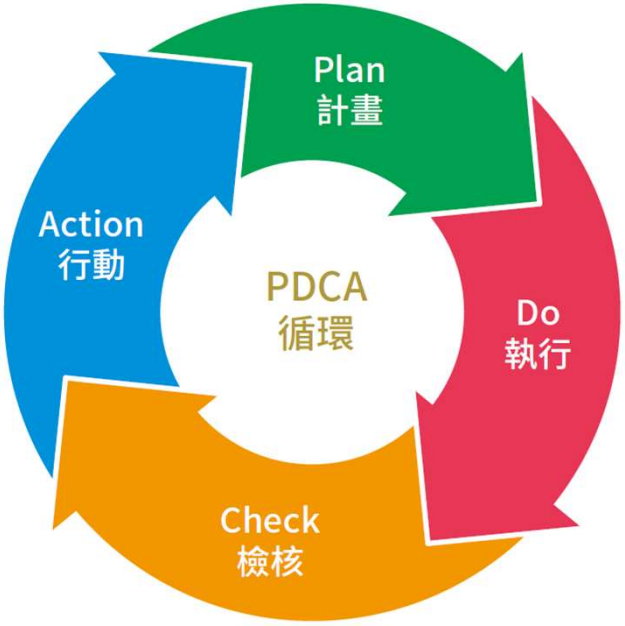

界定分級標準
推動實施資訊安全管理制度
資安認知推廣
第一期機制計畫
建構資安防護體系，完成政府機關分級機制
2001 - 2004
重新界定分級標準，實施範圍擴及教育體系
建置國家資通安全防護管理平台，提供一般監控與預警服務
推動資訊安全長制度
第二期機制計畫
健全資安防護能力，成立國家資安監控中心
2005 - 2008
加強實施各項資安作業，共規劃30個行動方案
提高資安法規完備度 ex.個人資料保護法
第三期發展方案
強化資安整體應變能力，精進通報應變機制
2009 - 2012
完成聯防資安監控服務的SOC平臺
修訂「政府機關(構)資通安全責任等級分級作業規定」
第四期發展方案
加強資安防護管理聯防監控機制與資安情報分享
2013 - 2016
落實A級機關資安治理成熟度
完成關鍵基礎設施ISAC、CERT、SOC
推行「資安產業發展行動計畫」
第五期發展方案
推動資通安全管理法，完備國家資安聯防體系
資安法自108年正式施行
2017 - 2020
建立資安卓越中心
精進及擴大資安治理成熟度(含客觀指標)
擬訂我國物聯網資安檢測框架
第六期發展方案
打造堅韌安全之智慧國家
111年成立資通安全署
2021 - 2024

資安法施行後之變革


適用範圍面
納管對象擴大
特定非公務
機關
資安管理
規定位階提
升為法令
維護計畫、
專職(責)人力
資安法
明定資通
安全推動事項
及情資分享
明定應辦
事項及控制
措施
規範面
管理面
政策及整合面
技術面

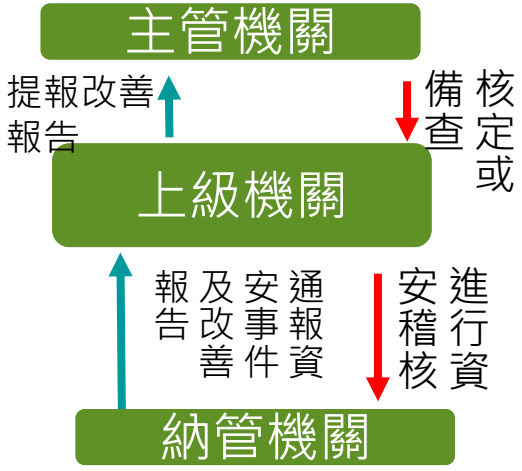
資通安全管理思考架構

資通安全管理思考架構：PDCA



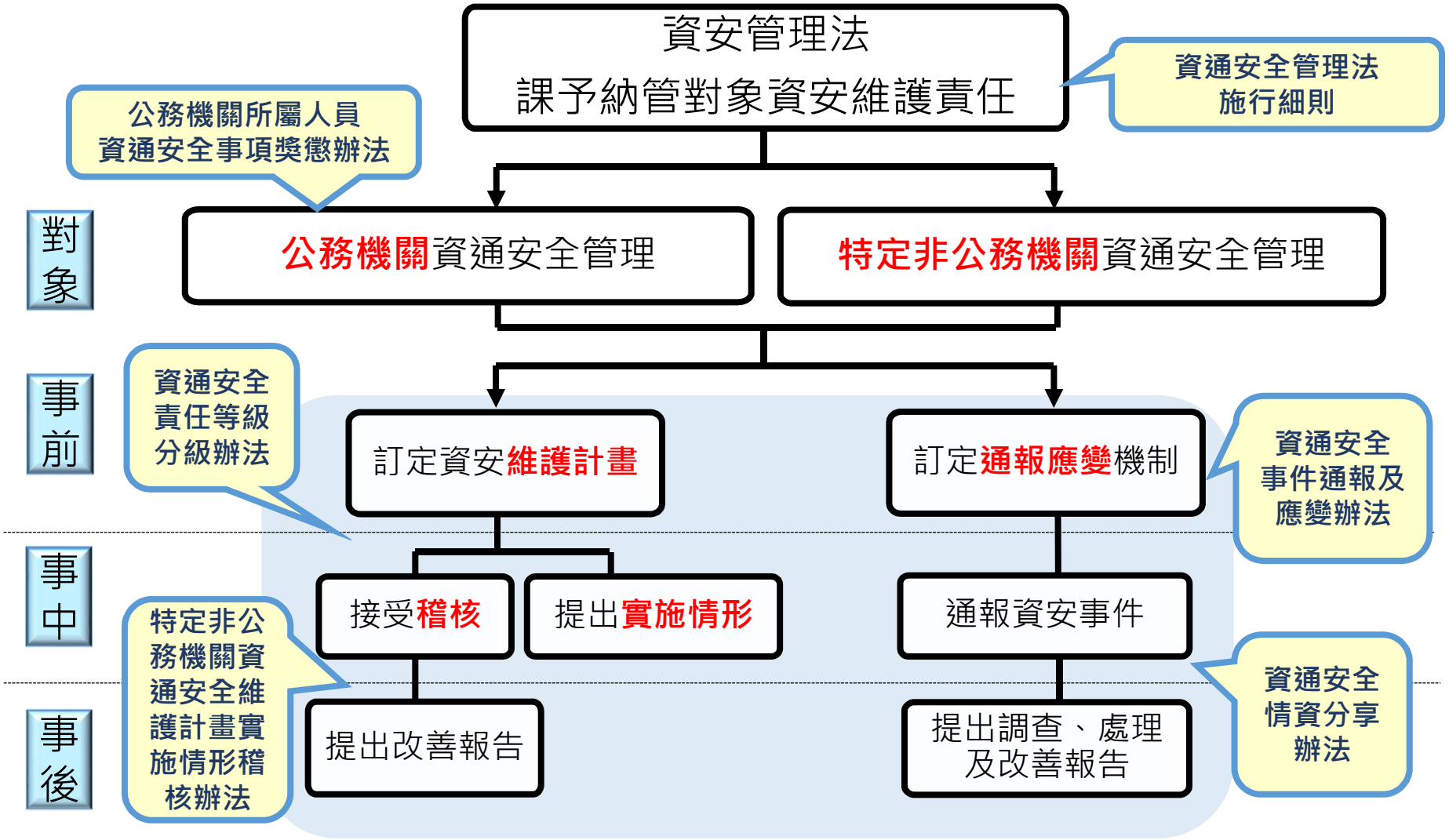
資通安全維護計畫(P+D)

稽核及改善報告(C+A)



- 訂定及實施資安稽核計畫
- 訂定資安事件通報及應變機制

資安管理法及各子法架構



資安法VS個資法之立法目的

個人資料保護法

- 規範目的：個人資料保護與合理利用之衡平
- 規範對象：持有個資之公務機關及非公務機關
- 措施：
  - 訂定個人資料安全維護計畫
  - 個資外洩通報(依情節由各目的事業主管機關裁罰)
- 罰則：刑罰、行政罰

資通安全管理法

- 規範目的：資安管理規範，以降低風險
- 規範對象：公務機關及特定非公務機關
- 措施：訂定資通安全維護計畫、資安事件通報(無罰則)→目的在於聯防協處，以再次預防資安事件
- 罰則：針對逾期未改善則處以行政罰

資安法納管情形

數位發展部資通安全署
Administration for Cyber Security, moda

- 立法目的：為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益。
- 規範對象：以對人民生活、經濟活動及公眾或國家安全有重大影響者為納管對象。

公務機關

- 中央與地方機關(構)
- 公法人

(不包括軍事機關及情報機關)

特定非公務機關

- 關鍵基礎設施提供者
- 公營事業
- 政府捐助之財團法人

重點工作_訂定資通安全維護計畫

數位發展部資通安全署
Administration for Cyber Security, moda

- 近年來教育體系發生多起重大資安事件，根因分析顯示各校資通安全維護計畫施行範圍未涵蓋全校
- 各校資通安全維護計畫適用範圍應涵蓋全校(各系、院、所教學單位及各行政單位)，並注意下列事項

資安長之配置

宜指派**主任秘書以上人員**兼任。

資安推動組織

宜由**資通安全長**召集全校各單位主管或副主管組成，**每年至少召開會議1次**。

資通系統盤點

盤點範圍應包含**全校各單位**。

內部資安稽核

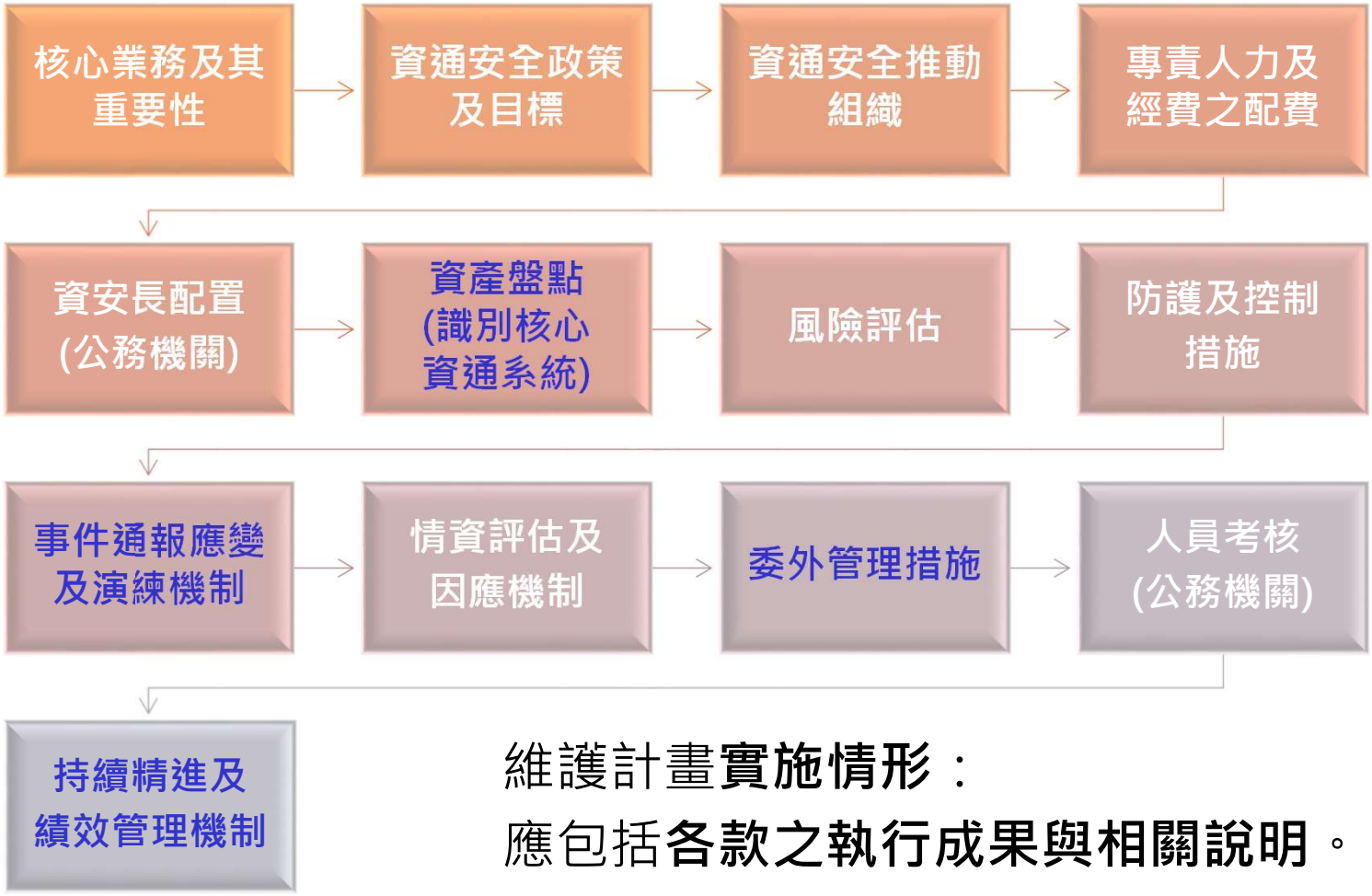
稽核範圍應包含**全校各單位**。

參考教育部110年12月30日臺教資(四)字第1100179797號函及國立大專校院資通安全維護作業指引

重點工作_訂定資通安全維護計畫

數位發展部資通安全署
Administration for Cyber Security, moda

- 基於風險管理之基礎，包含下列內容：



維護計畫**實施情形**：

應包括**各款之執行成果與相關說明**。

重點工作_落實資通系統及資訊之盤點

數位發展部資通安全署
Administration for Cyber Security, moda

- 各校建議依資安法相關規定，辦理下列安全防護及控制措施：
  - 落實**全校資通系統及資訊資產設備之盤點**，其盤點範圍至少包含：

資通系統盤點

■**行政、教學單位**自行或委外開發之資通系統。
■**學校採購及公務使用之物聯網設備**(如網路印表機、網路攝影機、門禁設備、環控系統、無線網路基地台/無線路由器等)。

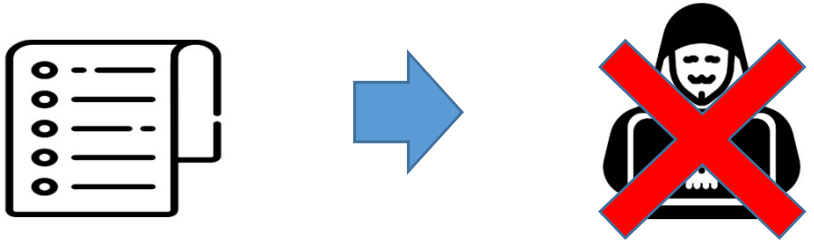
  - 盤點結果及異動情形應提報資安長知悉
  - 可參考資通安全責任等級分級辦法附表九「資通系統防護需求分級」之分級原則，訂定較客觀及量化之衡量指標(普中高)，據以分級

重點工作_執行風險評估及控制措施

數位發展部資通安全署
Administration for Cyber Security, moda

- 學校可由國家資通安全研究院(組改前行政院資安會報技術服務中心)或臺灣學術網路危機處理中心等其他管道接收資安情資(如：軟體弱點通報、惡意中繼站清單)，並針對接獲之情資，進行分類評估及因應措施 (如：弱點修補更新、封鎖惡意中繼站IP)

接收軟體弱點通報　盤點掌握　弱點修補/強化防護

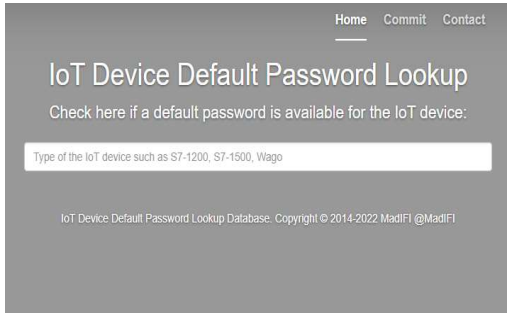


接收惡意中繼站清單　封鎖惡意中繼站IP

重點工作_執行風險評估及控制措施

- 各校建議依資安法相關規定，辦理下列安全防護及控制措施(續)：
  - 落實**全校資通安全風險評估**、資通安全防護及控制措施。
    - **不得使用弱密碼及廠商預設密碼**，並符合規範之**密碼複雜度要求**。
    - 依業務需求設定適當網路**存取限制**。

曝露在外網且使用廠商預設密碼 (Google等網站能輕易查找) 的IoT設備，幾乎等同沒有存取限制。



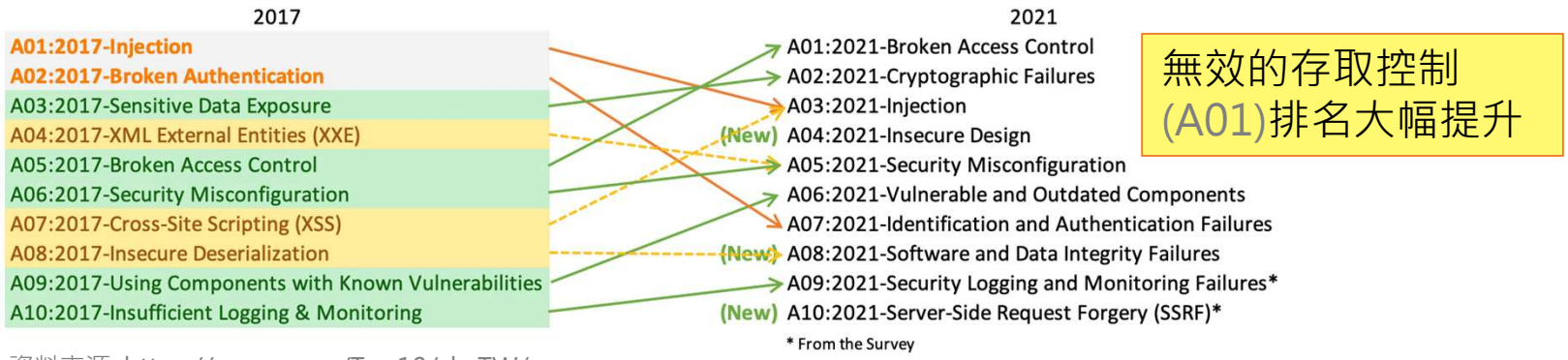
GCB密碼原則

1. **通行碼長度8碼以上**
2. **通行碼複雜度應包含英文大寫小寫、特殊符號或數字3種以上**

重點工作_執行風險評估及控制措施

數位發展部資通安全署
Administration for Cyber Security, moda

- 各校建議依資安法相關規定，辦理下列安全防護及控制措施(續)：
  - 資通系統避免軟體常見漏洞(如Injection、XSS等OWASP Top 10安全弱點)，落實漏洞修復並定期更新。



無效的存取控制(A01)排名大幅提升

資料來源: https://owasp.org/Top10/zh_TW/

個資保護管理

國際個資相關規範

1.OECD隱私保護及個人資料之國際傳遞指導方針(1980)

2.APEC隱私保護綱領(1998)

3.國際標準ISO 22307金融服務-隱私衝擊分析(2008)

4.英國標準BS 10012資料保護-個資管理系統規格(2009)

5.NIST SP 800-122(2010)

6.ISO/IEC29100資訊科技-安全技術-隱私框架(2011)

7.ISO 29191 (2014)

8.歐盟的GDPR(2018)

個人資料保護法立法過程

數位發展部資通安全署
Administration for Cyber Security, moda

民國84年8月11日

「電腦處理個人資料保護法」通過

民國99年5月26日

總統公布修正名稱與全文

民國104年12月15日

修正修文於104年12月15日立法院三讀通過

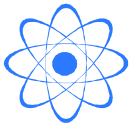
84年 | 99年 | 101年 | 104年 | 105年

民國99年4月27日

立法院三讀通過修正草案名稱修正為「個人資料保護法」

民國101年10月1日

除第6、54條條文施行日期，由行政院定之外，其餘條文定自101年10月1日施行



民國105年3月15日

修正版個資法開始施行

個人資料定義

個人資料的定義

個人資料

自然人之姓名、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、[病歷、醫療、基因、性生活、健康檢查、犯罪前科]、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料

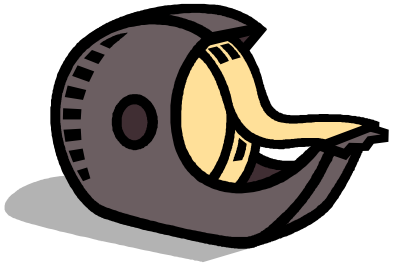
特種個資

病歷、醫療、基因、性生活、健康檢查及犯罪前科

電子資料定義

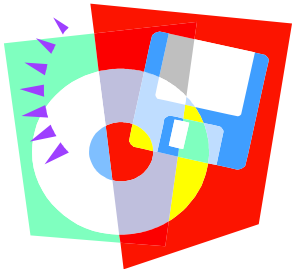
- 以電磁方式或數位型態以表現其文字、聲音、影像及圖片等傳遞訊息表示意義者之資料
- 依其存在的形式可分為
  - 電子檔案資料形式
  - 資料庫資料形式

(資料來源：電子資料保護參考指引)



- 電子資料
  - 指電腦可處理之文字或非文字資料，且符合檔案法與相關法令規定等

(資料來源：文書及檔案管理電腦化作業規範)



電子資料定義

個資與電子資料的生命週期類似

機敏資料主要包括個資與國家機密

要注意違反個資法的罰則

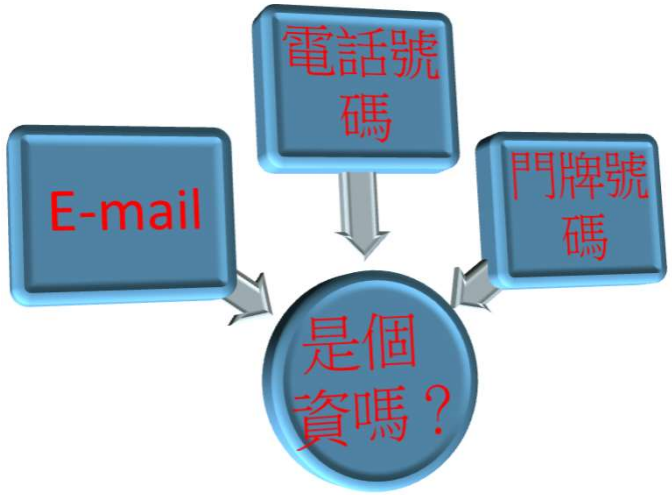
電子資料是個資存在的一種型式

要確認機敏資料受到適當的保護

電子資料與個資會因為被盜取產生危害，並使機關與保管者受罰

對個資認定迷失的澄清

- E-mail是個資嗎？
- 電話號碼是個資嗎？
- 門牌號碼是個資嗎？
- 含有個人資料的電子文件與紙本都受個資法規範



個資外洩的案例

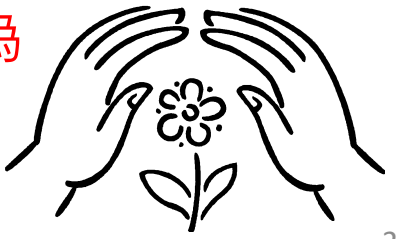
數位發展部資通安全署
Administration for Cyber Security, moda

- 美國國稅局於2015年5月26日的新聞稿發佈證實超過10萬人的**所得稅申報書與收入資料**遭駭客竊取
- eBay在2015年3月初發生**用戶資料遭駭客竊取**的事故，由於遭竊的數量不易估計，可能衍生的災情慘重且影響深遠
- 2014年11月日本警視廳發現Sun Techno公司的代理伺服器有非法取得的網路購物網站的**506萬筆個資**。其中包括樂天、Line與Amazon的用戶

這些外洩的個資都是以電子資料的型式被駭

電子資料保護的方式

- 避免
  - 透過安全控制措施，阻止相關威脅的發生
  - 例如：將電子資料進行實體隔離，阻絕來自網路的安全威脅
- 偵測
  - 無法避免相關威脅的發生，但透過安全控制措施的偵測，可以在威脅發生時發現，進一步採取對應的處理程序
  - 具有嚇阻與事後補救的作用
  - 例如：啟動資料庫稽核機制，記錄存取行為



電子資料保護的措施

- 直接防護
  - 對電子資料或資料庫資料加密，限制存取
  - 對電子資料或資料庫資料進行備份
- 間接防護
  - 通訊加密：電子郵件傳遞過程中加密，保護附件電子資料
  - 加強網站應用程式：避免電子資料或資料庫資料從網站系統中擷取、竄改或刪除

重點宣導_防疫所蒐集個人資料管理

- 個人資料蒐集之特定目的消失後，如無保留之必要，**應主動將個人資料予以刪除**
- 機關除防疫相關系統，亦應注意**紙本、個人電腦及雲端空間**儲存之個人資料
- 如有透過**電子郵件**傳遞資料情形，亦應檢視電子郵件之資料留存情形
- 本院已就該等電子資料安全管理機制納入**資通安全稽核**檢核項目內
- 機關建置及維護資通系統，**仍應依資安法相關規定辦理**各項管理措施，如系統盤點、防護需求評估，**符合對應之防護基準措施**；並納入機關整體資安防護，適時稽核確認措施落實情形

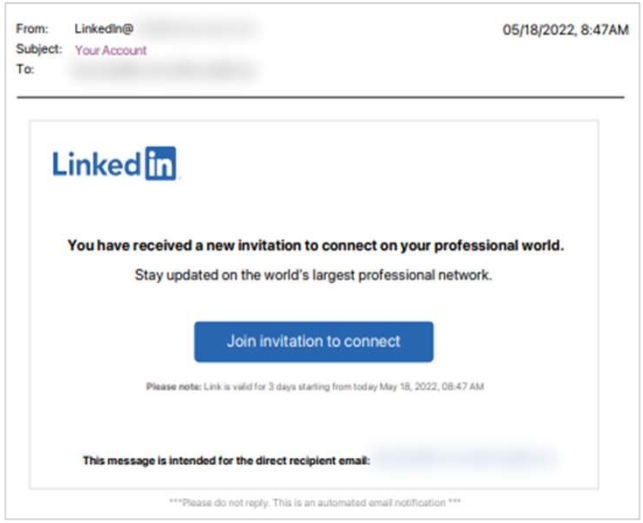
資安威脅趨勢與防護建議

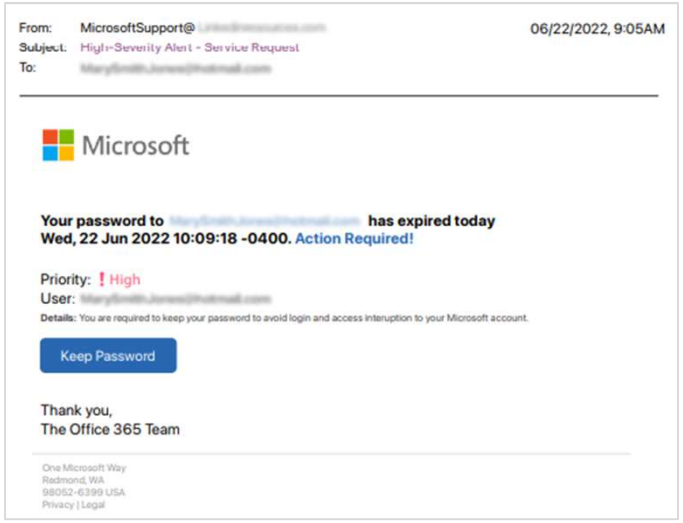
全球資通安全威脅趨勢

- 綜整111年全球資安威脅報告，由網際攻擊狙殺鍊(Cyber Kill Chain)歸納資安威脅趨勢，可分為六大類

社交工程手法層出不窮

- 據統計，社交工程電子郵件攻擊占比第一為釣魚攻擊(Phishing)，包含一般引誘性郵件與魚叉式攻擊，其次為各式詐騙電子郵件(Scam)
  - 資安廠商Abnormal Security111年H2報告指出，共計超過265個大眾熟悉品牌常遭利用於釣魚攻擊，其中以社群網路登入與微軟相關產品最常被偽冒，以騙取個人機敏資訊
  - 資安廠商Trellix指出111年美國選舉之惡意電子郵件大幅增加，駭客藉選舉之際，透過釣魚攻擊騙取選舉工作人員帳號密碼





進階持續性攻擊竊取機敏資料

- 進階持續性攻擊(APT)為駭客集團鎖定特定組織或國家，精心策劃結合多種攻擊手法，包括：社群平台、手機、Office文件及各式產品漏洞，持續而隱匿地逐步滲透，藉此竊取機敏資料
  - 111年9月，微軟揭露北韓駭客組織Zinc利用LinkedIn平台建立招募員工假檔案，鎖定英、美及印度國籍之工程師，要求求職者以WhatsApp通訊，透過手機通訊管道遞送已被植入後門之惡意檔案
  - 111年9月， 資安廠商DuskRise指出俄羅斯駭客組織APT28利用PowerPoint簡報檔案散布惡意軟體Graphite，針對歐盟、東歐國家政府部門與國防單位進行攻擊
  - 111年9月，資安廠商Recorded Future指出中國駭客組織利用Sophos防火牆產品漏洞(CVE-2022-1040)與微軟Office文件漏洞(CVE-2022-30190)，針對西藏社區組織與個人發動攻擊

遠端程式碼執行漏洞仍頻繁

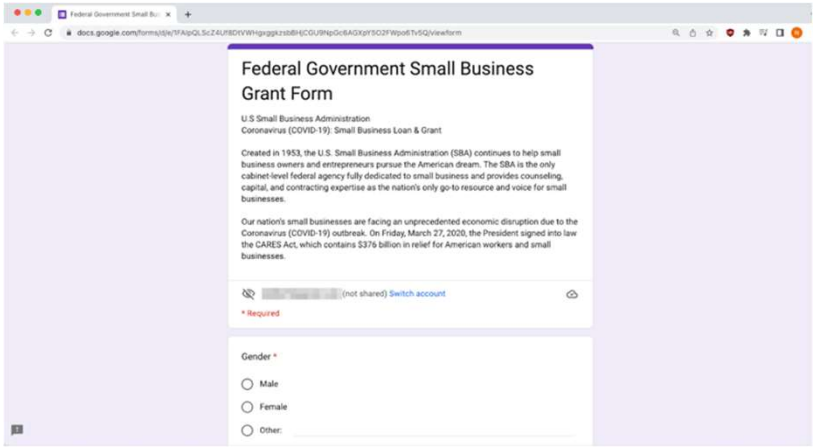
- 參考近年美國網路安全及基礎設施安全局(CISA)漏洞報告與資安廠商INFOSEC發布之111年最危險漏洞資訊
  - 駭客最愛利用漏洞主要為遠端程式碼執行或提權等權限控管缺陷
  - 另商用軟體Exchange伺服器產品等重大漏洞也屢被利用

CISA公布之10大常用漏洞				
漏洞代號	CVE編號	CVSS分數	漏洞類型	APT攻擊常用
Log4Shell	CVE-2021-44228	10(Critical)	RCE	V
N/A	CVE-2021-40539	9.8(Critical)	RCE	V
ProxyShell	CVE-2021-34523	9.8(Critical)	Elevation of privilege	
	CVE-2021-34473	9.8(Critical)	RCE	
	CVE-2021-31207	7.2(HIGH)	Security feature bypass	
ProxyLogon	CVE-2021-27065	7.8(HIGH)	RCE	V
	CVE-2021-26858	7.8(HIGH)	RCE	V
	CVE-2021-26857	7.8(HIGH)	RCE	
	CVE-2021-26855	7.8(HIGH)	RCE	
N/A	CVE-2021-26084	9.8(Critical)	Arbitrary code execution	

Microsoft Exchange Server相關漏洞

雲端服務平台遭駭客濫用

- 雲端服務平台可幫助企業組織快速部署提高效率，但也遭駭客利用以掩飾惡意行為
  - 趨勢科技「2022 Midyear Cybersecurity Report」報告[7]指出，現今駭客常使用雲服務進行隱匿通訊(Cloud Tunneling)，除減少建置永久性網路基礎架構之需求，也不需特意掩蔽真實來源IP位址
    - Cloudflare, Google Cloud Platform, AWS, 微軟Azure, 阿里雲, 騰訊雲等
  - 駭客利用合法雲服務網域(Domain)建置釣魚頁面，以規避偵測
    - 因應疫情，駭客濫用Google表單並搭配釣魚電子郵件，蒐集受駭者個人資料[1]
    - 駭客濫用AWS建置與託管釣魚網站頁面，以騙取個人帳密



駭客濫用Google表單蒐集個資

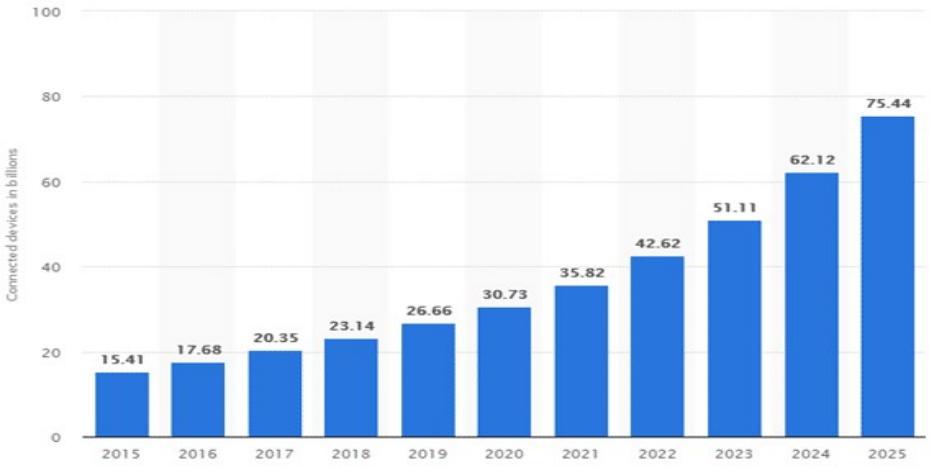
駭客持續破壞供應鏈安全

- 供應鏈風險對全球組織影響漸增，供應鏈安全落差使駭客鎖定監控較不嚴謹之設備或供應商，做為入侵管道
  - ISACA「全球供應鏈安全差距」調查報告[8]顯示，全球25%組織在過去1年內皆曾遭受供應鏈攻擊
  - 111年1月，身分驗證及存取管理業者Okta之第三方廠商Sitel工程師筆電遭駭[9] [16]，導致Okta客戶資料外洩，包含Nvidia與三星等，並使微軟遭駭客入侵
  - 111年2月，台灣金融業曾遭軟體供應鏈攻擊[10]，利用金融業常用證券軟體管理介面漏洞入侵，並安裝後門程式意圖竊取資料

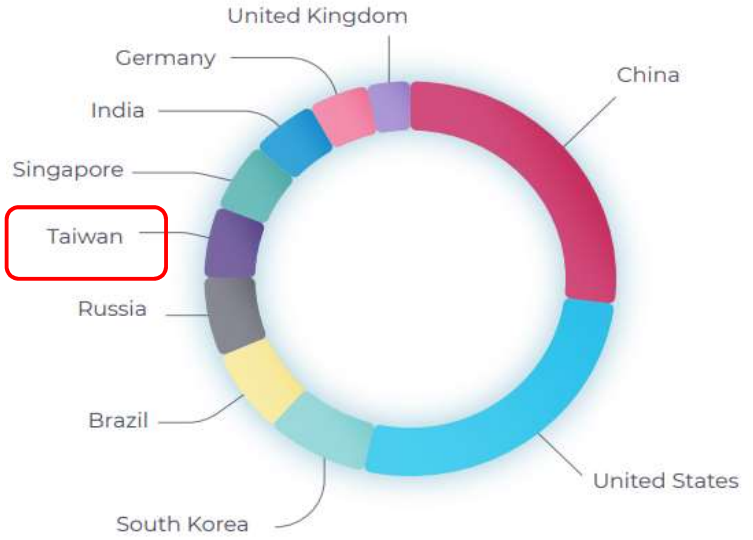
最擔憂會影響組織之供應鏈風險		
1	勒索軟體	73%
2	供應商資安落實程度不佳	66%
3	軟體漏洞	65%
4	第三方儲存	61%
5	第三方供應商可存取到資訊系統	55%

萬物聯網受駭風險倍增

- 因物聯網設備普及，多數物聯網裝置缺乏有效控管，長期遭駭客入侵利用於各種攻擊，如DDoS攻擊與殭屍網路
  - IOT Business News [18]指出111年物聯網主要威脅包括：
    - 殭屍網路與惡意物聯網設備
    - 弱密碼與身分驗證機制不足
  - Nozomi Networks Labs[11]在111年上半年OT/IOT安全報告中指出，駭客最常透過SSH與Telnet協定存取安全性不足之物聯網設備



IOT設備成長趨勢

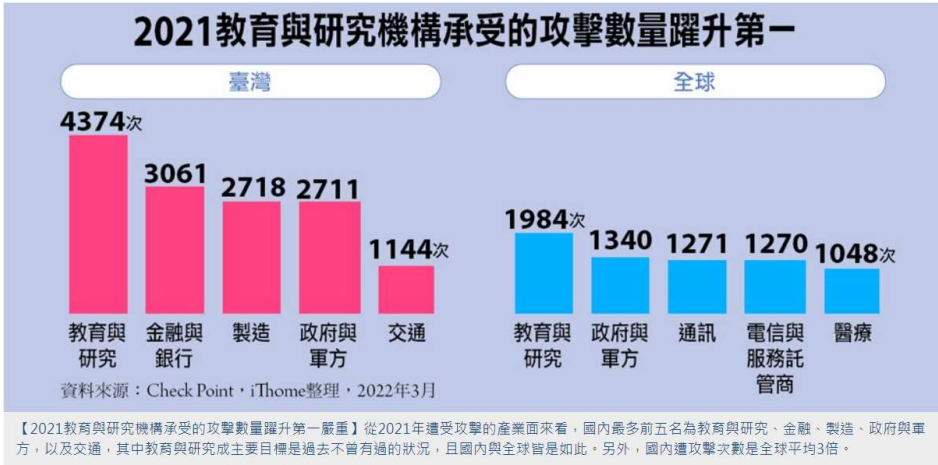


駭客利用受感染IoT設備發起網路攻擊之主要國家

教育體系資安威脅

- 依據資安業者統計 (Check Point 110年全球威脅趨勢回顧報告)：

  - 臺灣每週平均遭受攻擊次數，依產業別，以教育與研究機構最多(4,374次)
  - 全球亦同(教育與研究機構最多)，且比前一年度增長75%



【2021教育與研究機構承受的攻擊數量躍升第一嚴重】從2021年遭受攻擊的產業面來看，國內最多前五名為教育與研究、金融、製造、政府與軍方，以及交通，其中教育與研究成主要目標是過去不曾有過的狀況，且國內與全球皆是如此。另外，國內遭攻擊次數是全球平均3倍。

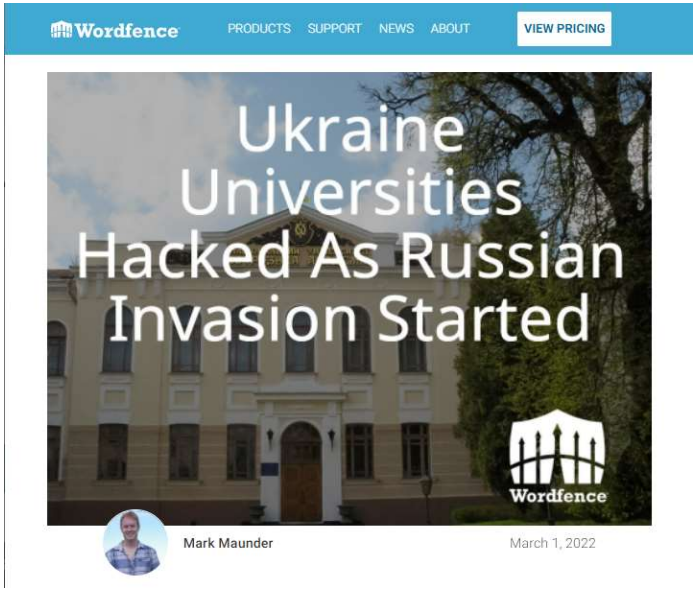
資料來源: iThome 111/3/16 報導，
https://www.ithome.com.tw/news/149919

教育體系資安威脅

- 國家/地區間發生衝突時，教育機構經常首當其衝。
  - 俄烏戰爭爆發後，至少30所烏克蘭大學網站遭到駭客入侵，包含網頁被惡置換(插旗)情形。

Date	Notifier	H	M	R	L	Domain	OS
2022/03/10	theMx0nday	H	M			vstup.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M			consulting.vbs.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M			db.lib.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M			events.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M			gw.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M			handbook.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M			hrampfo.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M			igsu.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M			iirns.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M			incgc.oa.edu.ua	FreeBSD

資料來源: http://www.zone-h.org/archive



資料來源: https://reurl.cc/anlZV7

案例分享

新冠疫情社交工程攻擊案例

- 駭客利用國人關注新冠肺炎議題，以提供紓困福利為由，架設偽冒衛福部與相關政府域名釣魚網站，散布釣魚郵件與手機惡意應用程式，對政府機關與一般民眾無差別發動攻擊，進行個人資料與網路銀行詐騙

防護建議

- 注意郵件來源之正確性，勿開啟不明來源之郵件與連結
- 確認政府相關域名之正確性，勿隨意提供機敏資訊

偽冒機關帳號散布惡意電郵案例

- 駭客利用政府機關電子郵件伺服器未設定寄件者原則架構(SPF)，大規模偽冒政府機關人員電子郵件帳號，發送大量惡意勒索電子郵件進行社交工程攻擊
  - 111年9月偵測發現，遭駭客偽冒之政府機關，共計87個政府機關、117機關域名未完善SPF設定

防護建議

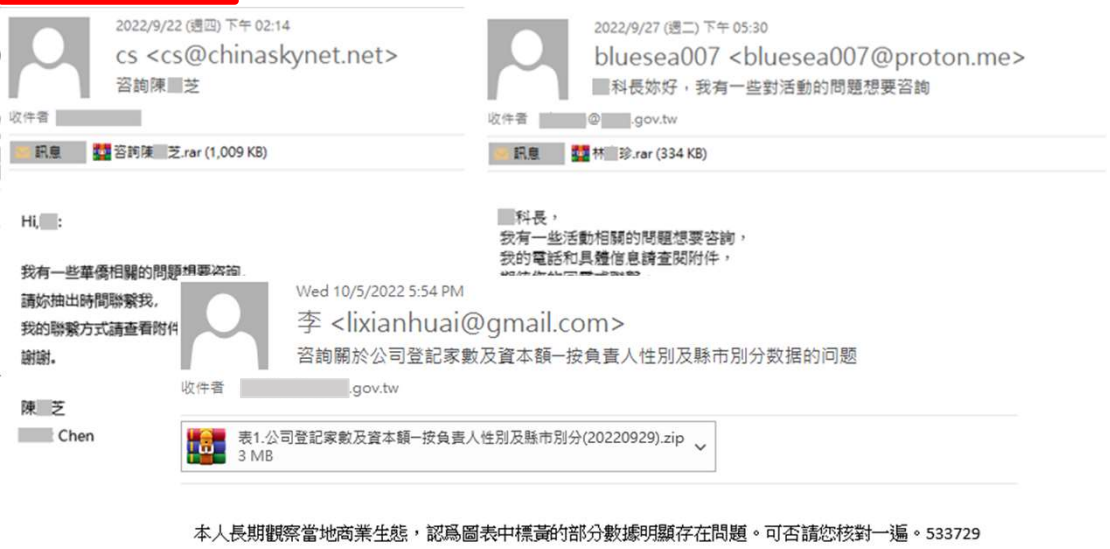
- 建議可參考寄件者原則架構(SPF)設定，完善郵件安全防護，避免機關電子郵件帳號遭偽冒利用

進階持續性攻擊郵件案例(1/2)

- 除新冠肺炎議題相關攻擊外，組織型駭客針對政府機關業務負責窗口，以業務諮詢相關問題為主旨，搭配惡意附檔，發動魚叉式社交工程攻擊

新冠議題

業務諮詢



防護建議

- 注意郵件來源之正確性，勿開啟不明來源之郵件與連結
- 確認電子郵件附檔屬性或檔名後才點擊檔案，提高警覺

進階持續性攻擊郵件案例(2/2)

- 組織型駭客偽冒技服中心，於郵件中安插技服中心圖示並使用「資安審查」等郵件主旨，針對台灣企業發起魚叉式社交工程釣魚郵件攻擊

防護建議

- 注意郵件來源之正確性，勿開啟不明來源之郵件與連結
- 如感覺有異請先洽技服中心查證，可以利用通報網站或技服信箱進行情資分享

產品漏洞威脅案例

- 網通設備產品一向為駭客鎖定之攻擊目標，111年初F5之BIG-IP產品發現重大安全漏洞(CVE-2022-1388)，可透過iControl REST身分鑑別漏洞存取BIG-IP系統，並遠端執行任意程式碼
- 經異常連線行為偵測，發現某機關疑似受駭，經鑑識調查後，發現駭客利用BIG-IP漏洞入侵該設備以放置後門程式與駭客工具，意圖遠端操控並進行內部橫向擴散

防護建議

- 儘速下載對應版本之更新檔，並將管理頁面功能更新至最新版本
- 若版本因已停止支援而未釋出修補程式，建議升級至仍有支援且已推出修補程式之版本
- 若無法更新至最新版本，請採出官方所建議之緩解措施

雲端服務中繼站威脅案例

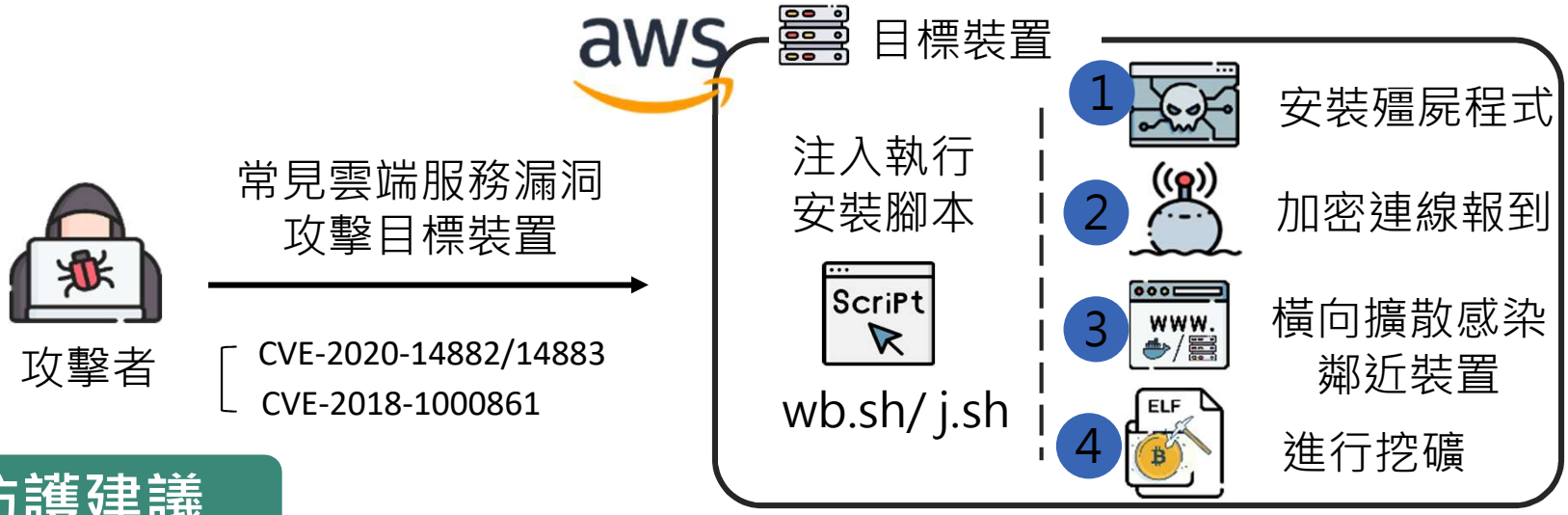
- 110年偵測多起進階持續性郵件攻擊，駭客使用紅隊演練工具產製Cobalt Strike後門程式，搭配Cloudflare、AWS、騰訊雲等服務建置中繼站，竊取資料與命令控制

防護建議

- 提升機關內部同仁資安意識，請留意相關電子郵件，注意郵件來源之正確性，勿開啟不明來源信件之附檔以防遭植入惡意程式
- 建議針對雲端服務之存取行為建立控管機制，並定期檢視網路可疑連線，避免造成資安漏洞。

雲端服務遭攻擊利用案例

- 111年技服中心蜜罐偵測Kinsing殭屍網路針對雲端服務之攻擊，駭客企圖利用WebLogic與Jenkins漏洞，感染雲端裝置後對內部進行擴散，並用以挖取門羅幣

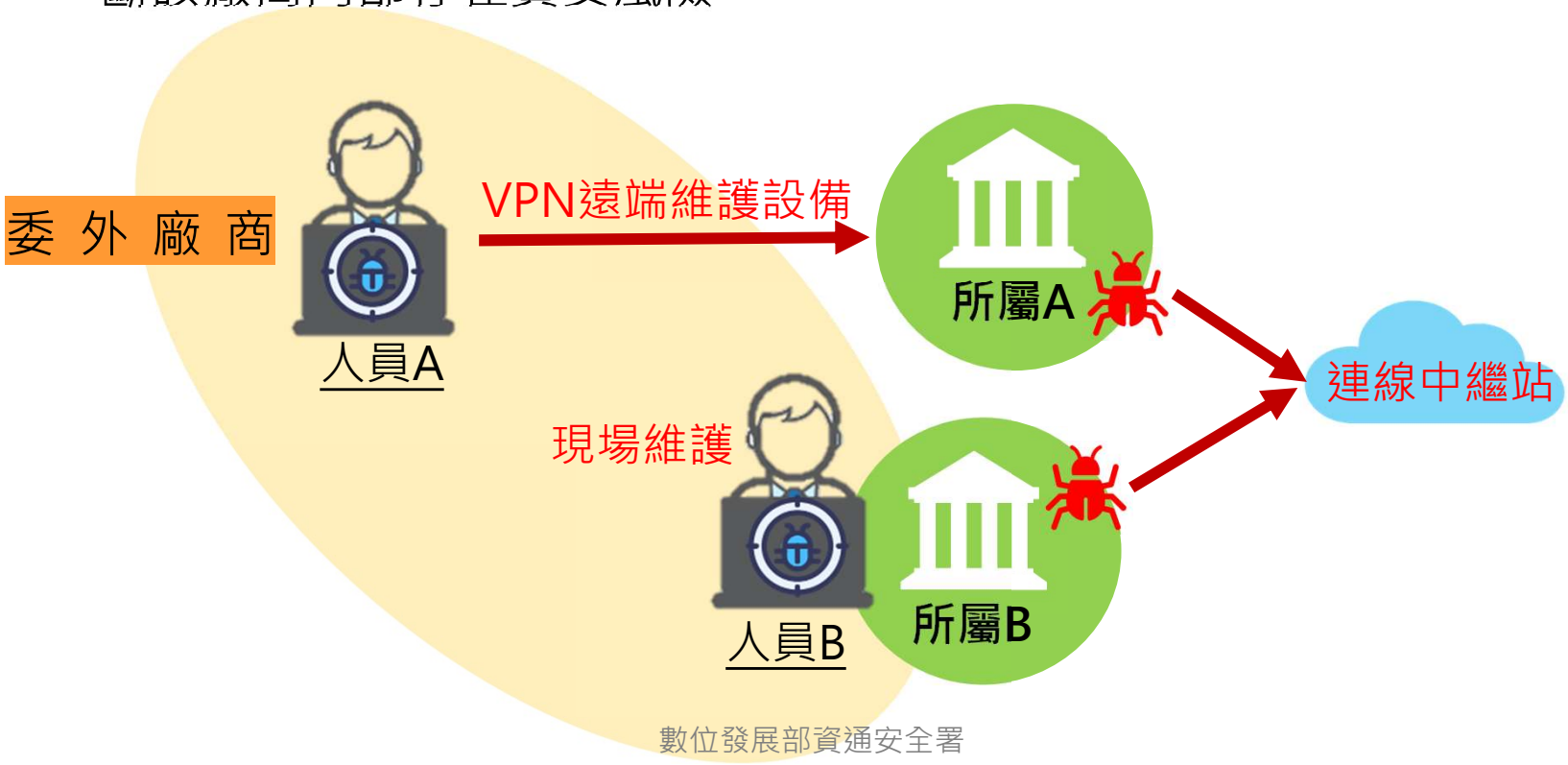


防護建議

- 以雲端平台建置對外服務之機關，應使用供應商最新公版容器建置服務，並定期更新軟體版本修補漏洞
- 建議針對雲端服務之存取行為建立控管機制，並定期檢視網路可疑連線，避免造成資安漏洞。

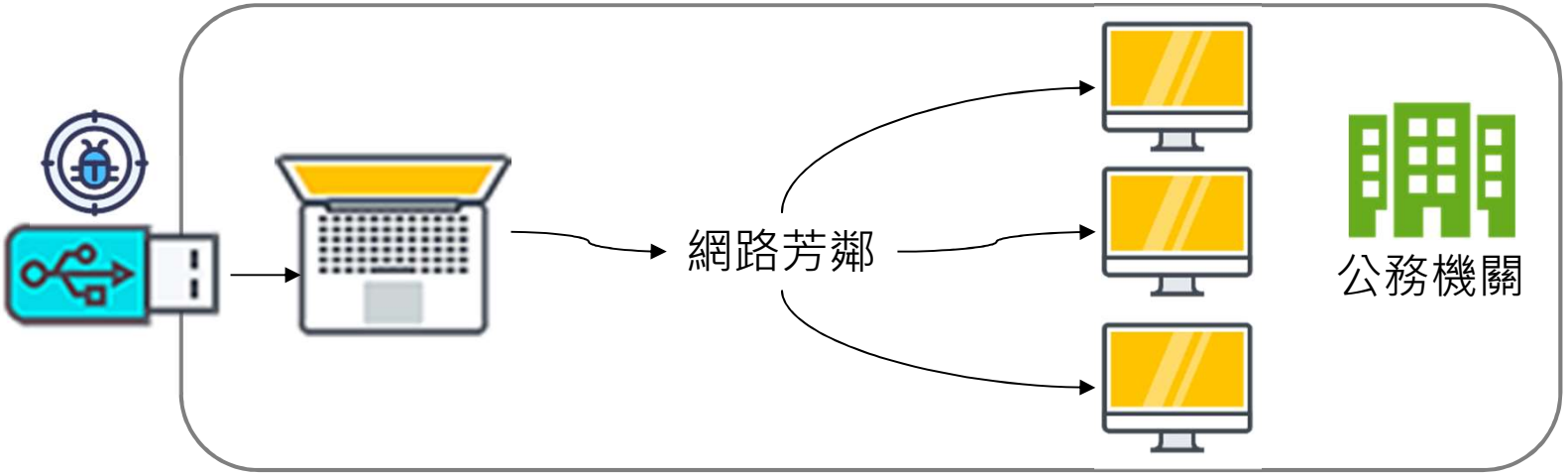
供應鏈攻擊-資訊廠商環境(1/3)

- 案例一：
  - 委外廠商人員電腦遭入侵植入惡意程式，廠商使用遭入侵之資訊設備維護機關資通系統，導致機關遭植入惡意程式
  - 委外廠商兩台電腦皆於相同資料夾路徑，發現相同的惡意程式，判斷該廠商內部存在資安風險



供應鏈攻擊-資訊廠商環境(2/3)

- 案例二：
  - 機關使用駐點廠商閒置電腦建置視訊環境，未先執行系統更新與安全檢測等作業，導致該電腦存在安全性漏洞遭利用，嘗試利用網路芳鄰協定對機關內部其他主機進行攻擊行為
- 案例三：
  - 廠商至機關進行電話交換機設定維護作業，將中毒USB插入機關提供之電腦並連網，連帶資訊設備中毒並嘗試利用網路芳鄰協定(Port 445)對其他主機進行可疑連線行為



供應鏈攻擊-資訊廠商環境(3/3)

防護建議

- 建議機關選任計畫委辦廠商時，依資通安全管理法與子法要求評估適當之受託者，並監督其資通安全維護情形
- 執行計畫時，機關應要求廠商建置環境之設備符合機關資安要求，並循正常流程管道申請使用機關設備，避免未經管制設備於機關環境中使用
- 作業執行前，機關或廠商應將作業系統與防毒軟體更新至最新版本，並持續更新修補漏洞，以降低遭外部入侵風險

物聯網裝置應用風險案例

- 案例一：
  - 111年8月，因美國聯邦眾議院議長裴洛西訪台行程一事，導致台灣攻擊事件頻傳，超商與車站電子看板等物聯網設備遭駭客入侵並置換內容[19]

- 案例二：
  - 111年9月，經偵測發現某機關設備有異常連線行為，進一步確認時發現該機關受駭設備為門禁系統，且存在身分驗證繞過漏洞，駭客透過該漏洞入侵設備，並安裝惡意程式

防護建議

- 管理介面應強化存取控制
- 盤點機關內部相關IT與OT資產並納入風險評估
- 可透過VANS系統定期檢視相關IT與OT設備漏洞並更新

資料外洩/人為疏失案例

- 機關委託廠商辦理競賽活動，並提供活動資訊，欄位包含姓名與行動電話號碼等，廠商工作人員為協助活動宣傳，將參與人員資訊上傳至個人公開網站，造成個資資料外洩

防護建議

- 建議機關選任計畫委辦廠商時，合約中應納入資通安全管理法與個資法相關要求，並監督廠商落實執行
- 資料放置於網站前，應審核確實公告內容含有個資之必要性，不得逾越特定目的之必要範圍
- 資料上傳至公開網站後，應重複確認公開之資訊內容適切性
- 活動結束後，應監督廠商完成資料或相關存取權限等，返還、移交、刪除或銷毀，以及資料自網站下架

勒索病毒/人員資安意識

- 案例一：
  - 機關人員使用公務電腦瀏覽網站，點擊下載與執行偽裝成微軟更新包之惡意程式，大陸影音網即遭植入勒索病毒，並透過網路芳鄰感染網路硬碟，致個人電腦與網路硬碟檔案資料遭加密
- 案例二：
  - 機關人員個人電腦之檔案遭加密，經查為同仁於上班時段瀏覽免費漫畫網站，點擊惡意連結，下載並執行檔案，導致個人電腦感染勒索病毒

防護建議

- 加強內部同仁資安觀念：公務電腦應僅供公務使用
- 軟體更新作業應配合機關政策，並勿下載未經授權軟體

資料維護/網站資料維護

- 機關維護之網站提供外部A單位連結，由於A單位之舊網域租用到期未續約，後由其他公司註冊為色情網站
- 因機關未即時接獲相關消息並更新連結資料，以致使用者點擊該連結時導向至色情網站

防護建議

- 機關人員除定時檢視網站自身內容，亦應確保連結之正確性，避免導致民眾連結至錯誤之網站

設備管理不當/誤用報廢設備

- 某機關設備遭駭客暴力破解遠端桌面登入密碼進而植入惡意程式，由於該設備老舊並規劃報廢，故未進行處置
- 同仁誤使用該設備執行網路維護測試並連網，導致設備再次連線至駭客中繼站

防護建議

- 機關應訂定資訊設備報廢處理相關作業程序，並落實報廢設備管理規定，以避免待報廢設備衍生資安問題之疑慮
- 作業執行前，機關應確認設備已將作業系統與防毒軟體更新至最新版本，並持續更新修補漏洞，以降低遭外部入侵風險

弱密碼及身分驗證缺失(1/3)

數位發展部資通安全署
Administration for Cyber Security, moda

- 案例一
  - OO署委託A大學建置維運學生業務相關網站， A大學網站維運團隊於查看網站日誌紀錄(log)時，發現AP管理者帳號有來自陌生國外IP成功登入的紀錄，且疑似上百筆個資遭到非授權的存取
- 發生原因
  - AP管理者帳號存在弱密碼問題，且管理後臺並未限制存取來源。
  - 什麼樣的弱密碼？
    - 管理者帳號：[學校縮寫]+流水號，密碼：123456789
  - **帳密設定**功能頁面，遺漏將**管理者**納入**密碼複雜度限制**要求範圍

弱密碼及身分驗證缺失(2/3)

- 案例二
- 檢測發現
  - OO大學的人事業務相關系統，測試機曝露於外網，檢測作業時發現有弱密碼問題，且測試機疑似使用正式資料，導致可非授權取得上萬筆職員的個人資訊
- 風險說明
  - AP管理者帳號存在弱密碼問題，且管理後臺並未限制存取來源
  - 什麼樣的弱密碼？
    - 管理者帳號：admin，密碼：admin
    - 測試環境直接**使用正式資料**，且未有相關**配套保護**措施

弱密碼及身分驗證缺失(3/3)

防護建議

- 落實資通系統及其帳號權限(包含作業系統、應用系統、資料庫等各類帳號)的**盤點清查**，並加強**特權帳號之管理**
- 加強帳戶防護機制：
  - 資通系統使用密碼進行驗證時，應強制**最低密碼複雜度**
  - 密碼複雜度**規範對象**，應包含**所有具管理權限之帳號**
  - 密碼**複雜度檢查**程序，應被納入**所有密碼變更功能**
  - 建議啟用**多因子認證**，並減少管理者帳號數量。
- 機關宜訂定**密碼複雜度共通規範**，如禁止使用**與帳號名稱相同**、身分證字號、**學校/機關代碼**、易猜測之**弱密碼**、廠商預設密碼或其他公開資訊等

個資檔案未受適當保護(1/2)

- 案例一：調查局通知某2所公立高中將保有學生個人資料的檔案直接公開於學校官網，且未進行加密或遮蔽，並可透過Google搜尋引擎發現，可能洩漏上百筆個人資訊
- 案例二：OO高級中等學校收到民眾反映，可透過Google搜尋引擎發現學校具有上千筆個人資訊之相關Excel檔，查係該校學習登錄相關系統供轉存資料庫暫存使用。
- 發生原因：學校承辦人缺乏個資保護意識，針對敏感資訊安全處理亦未具有相關知能

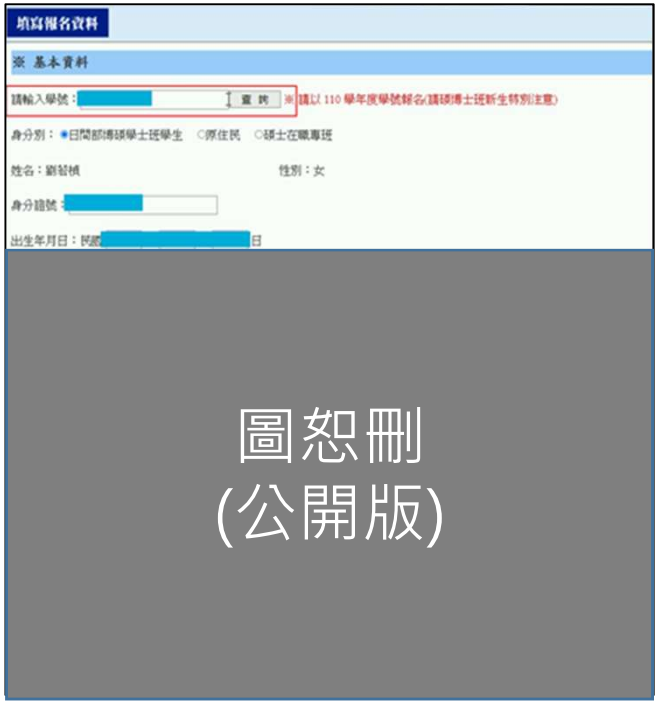
個資檔案未受適當保護(2/2)

防護建議

- 敏感性或機密資料應以加密方式進行儲存及傳輸
- 全面清查網站包含個資檔案，確認有無保留之必要，並針對需保留之部分，確認已實施存取控制或進行適當遮罩處理
- 網站更新或上傳檔案時應具備覆核機制，以確認內容應不包含敏感資訊(如個人資料、網站帳密等)。
- 強化個資檔案生命週期安全管理，落實重要個資檔案使用前之申請審核，及保存期限或業務終止後之確認刪除等管理措施
- 使用者寄送郵件時，應謹慎檢查收文者正確性

未落實SSDLC要求(1/2)

- 案例一：OO大學考試報名相關系統，經長官交辦因應疫情緊急開發上線，系統提供自動帶入申請人資料之便利功能，惟僅使用學號作為身分驗證條件，經學生通報問題後緊急下線，可能洩漏個人資訊
- 案例二： OO大學活動報名相關系統，因系統老舊遭駭客利用其元件漏洞上傳程式，取得系統執行權限後植入惡意程式，並連結學校Portal進而竊取教職員工個資
- 發生原因：學校承辦人缺乏個資保護意識，針對敏感資訊安全處理亦未具有相關知能



輸入任意學生學號後(為固定格式，學年度+系所代碼+流水號)，可顯示當事人之戶籍地址、電話、Email等資訊

未落實SSDLC要求(2/2)

防護建議

- 如因應業務需求緊急上線，仍應保留安全性檢測及弱點修補所需時間，避免因重大安全漏洞被利用，導致機關嚴重損失
- 盤點系統第三方元件使用情形，注意相關弱點情資通報(如國家資通安全研究院、TACERT之ANA情資)，並落實弱點修補或實施相當之風險管理措施
- 重要資料庫未最小授權
  - 機關應建立系統介接作業之權限審核機制
  - 重要資料庫應以最小權限原則進行存取授權，依介接系統之業務功能，提供所需資料表及資料欄位

重大變更管理失控

- D大學辦理學習歷程相關系統，該系統由D大學維運人員因應集中需求搬遷至OO機房，於O月O日因應更新重新開機，隨後發現因虛擬主機設定錯誤導致硬碟資料被還原，且因無相關備份，造成使用者資料遺失
- 發生原因
  - 備份機制失效：操作人員建立虛擬磁碟時**誤選「暫時性磁碟」選項**，致使系統重開機後磁碟資料被還原，且因備份系統不包含「暫時性磁碟」，故後續無法救回資料
  - 針對系統搬遷等重大變更過程及結果，缺乏驗證及複核機制

防護建議

- 落實資通系統變更管理
  - 針對系統重大變更之過程，應建立**多重驗證及複核**機制，並**訂定標準作業程序(SOP)**，據以執行並檢核應辦理事項
- 落實監控系統備份運作狀態，並定期辦理還原演練，確認備份有效性

結論與建議

結論與建議(1/2)

- 各校應加強內部宣導，提升人員郵件資安意識，持續強化郵件安全與相關防護
  1. 業務負責窗口，應謹慎留意可疑電子郵件，注意郵件來源正確性，防範駭客利用電子郵件進行攻擊
  2. 郵件伺服器管理，透過DNS系統設定寄件者原則架構(SPF)，避免機關電子郵件帳號遭偽冒，進行社交工程攻擊
- 持續提升學校人員個人資安與機敏資料保護意識
  1. 電腦應避免從事非校務用途，勿下載其他軟體造成資安風險
  2. 落實個資「認知宣導及教育訓練」，蒐集個人資料以最少必要資訊為原則，資料若需上傳至公開網站，則應重複確認資料存取設定與保存之妥適性

結論與建議(2/2)

- 各校應落實資訊作業委外安全管理，並責成委外廠商遵守資安管理措施：
  1. 建置系統時避免未經管制設備於機關環境中使用
  2. 遠端維護資通訊設備系統應採「原則禁止、例外允許」方式
  3. 如須開放遠端存取，原則以短天期為限，並建立異常連線行為管理機制，以確認時間與作業項目皆與實際情況相符
- 應強化資產盤點與漏洞修補，提升弱點防護能力，落實資安監控：
  1. 強化資產盤點與監控機制，即時掌握資通訊設備與相關資產分布
  2. 隨時關注資通訊設備漏洞更新情況與相關公告，並儘速完成漏洞修補作業

數位發展部資通安全署

Administration for Cyber Security, moda

資安是持續精進的風險管理