如何推動校園資安防護

國家衛生研究院 資訊中心

莊育秀 主任

111年11月30日

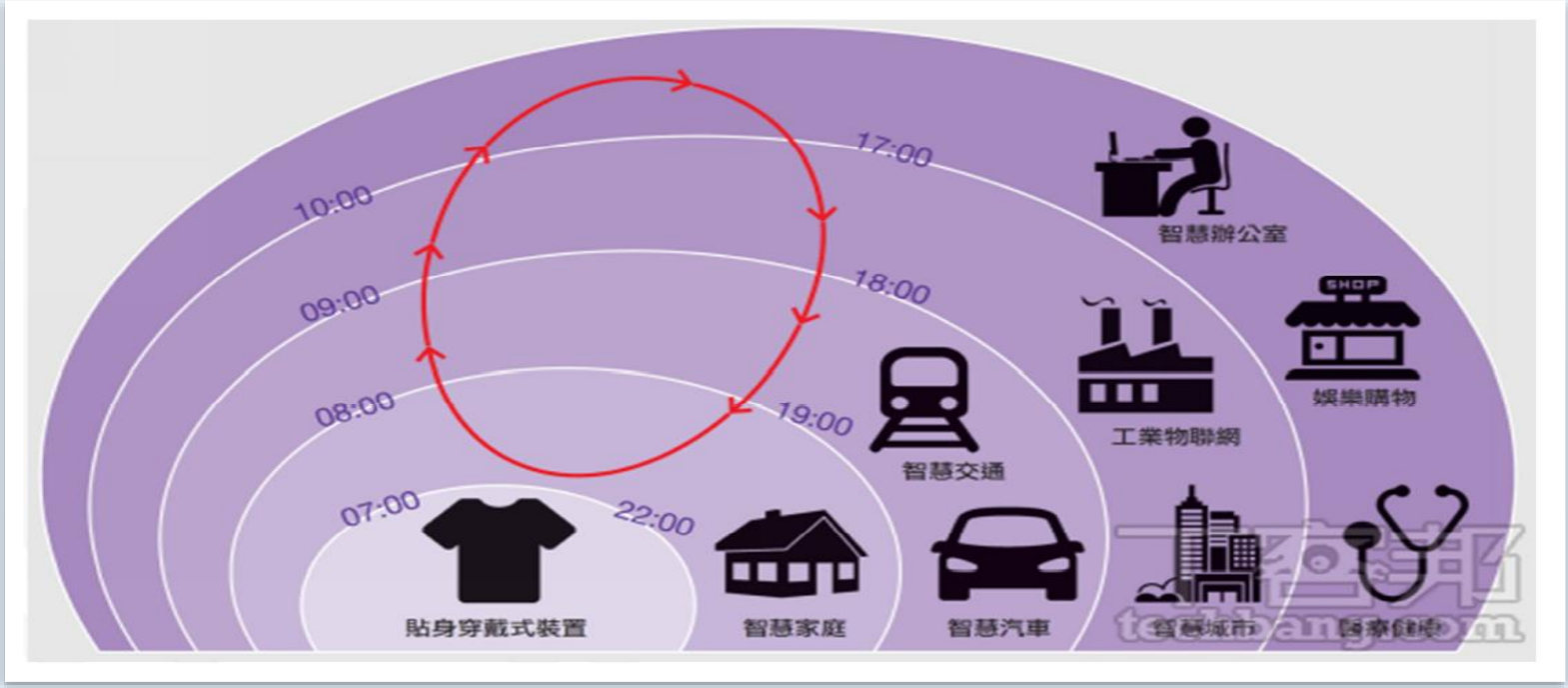
大綱

前言	資安與個資事件的趨勢
題一	校園資安現況與推動重點
題二	資安與高教深耕
題三	結合保護個資的資通安全防護的推動
最終	結語

大綱

前言	資安與個資事件的趨勢
題一	校園資安現況與推動重點
題二	資安與高教深耕
題三	結合保護個資的資通安全防護的推動
最終	結語

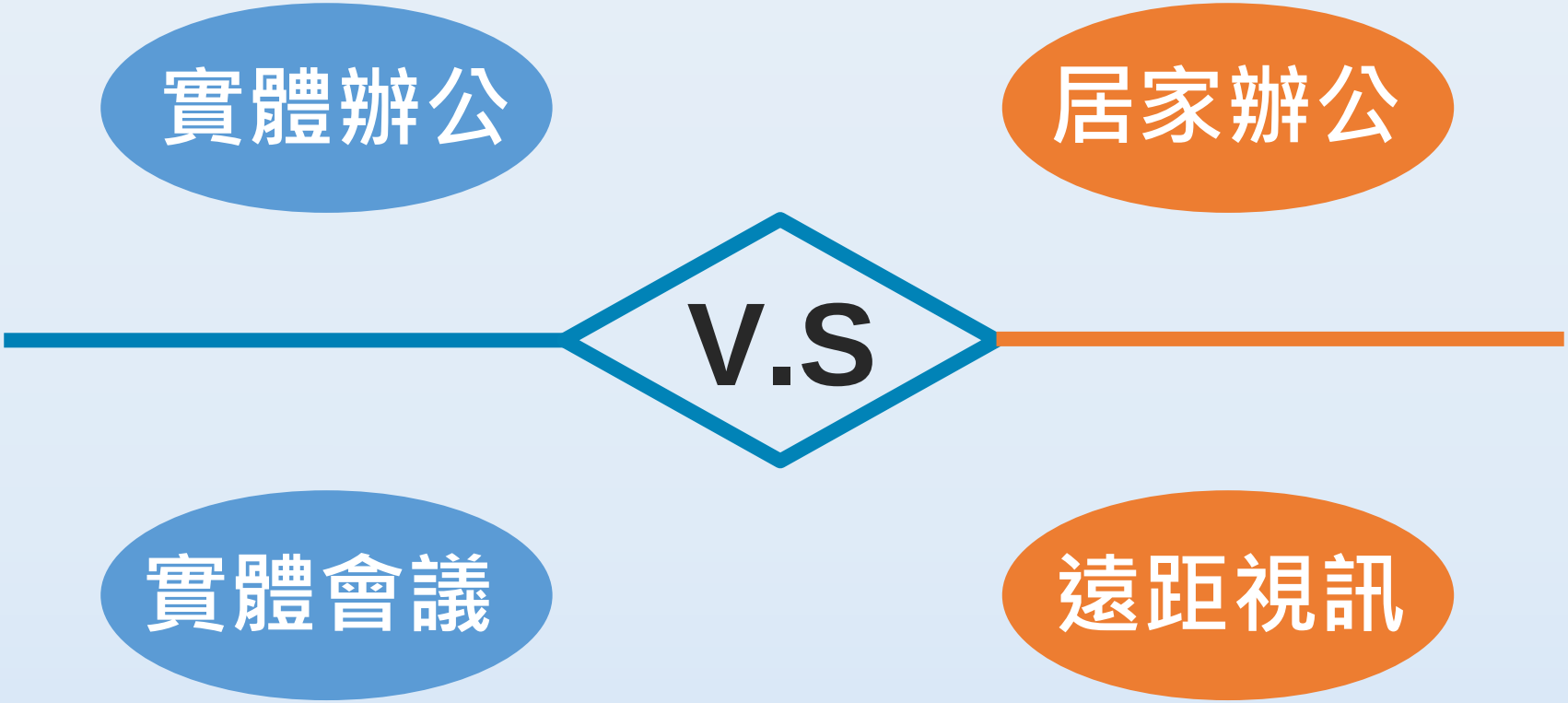
智慧生活的日常



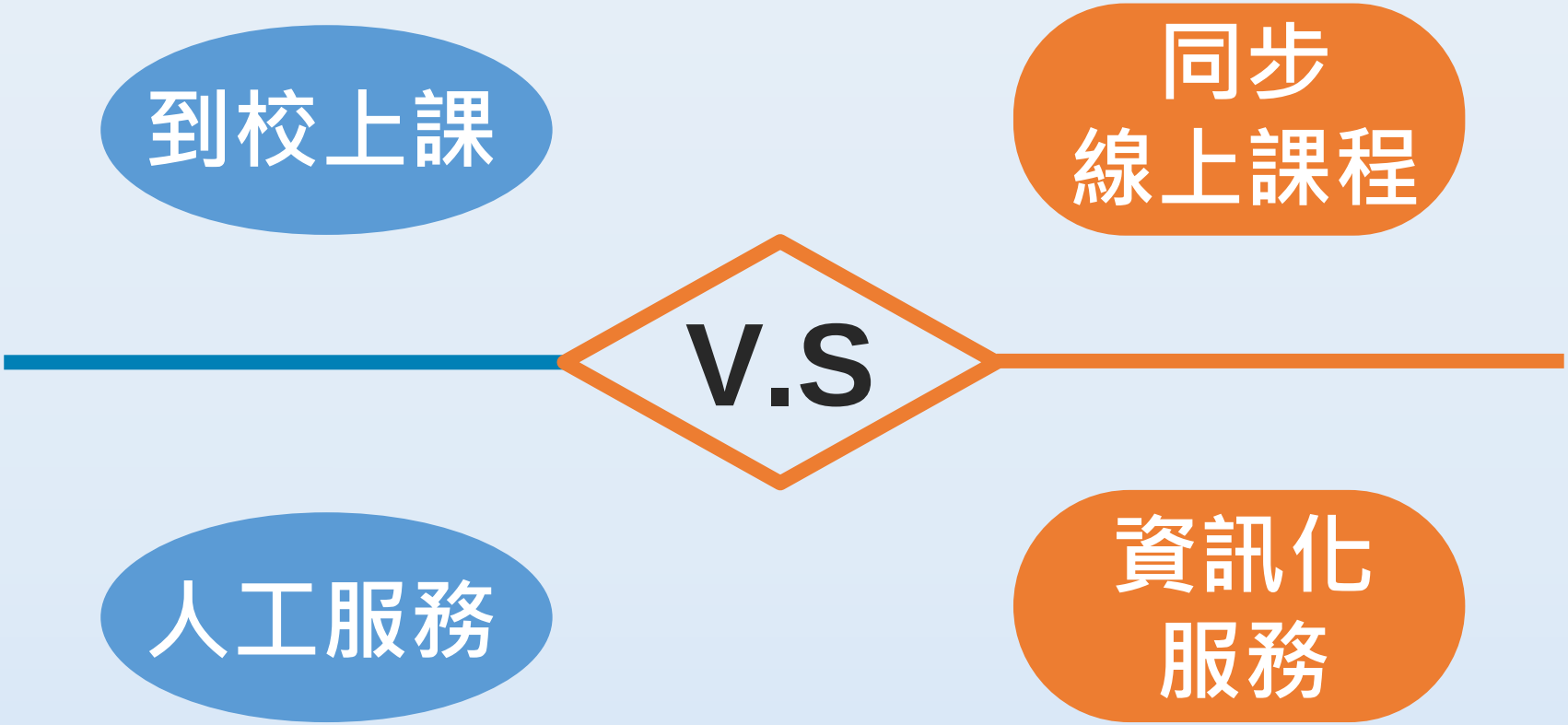
資料來源：痞客邦

- 資安即國安
- 資安防護人人有責
- 只有資安到位，數位轉型效果才能確保
- 開門７件事：柴 (網路)、米(手機、平板、電腦)、油(google)、鹽 (Line)、醬 (Twitter)、醋 (PTT、Dcard)、茶(Meta(FB) 、youtube、Netflix)…

您可接受的優先選擇?



您可接受的優先選擇?



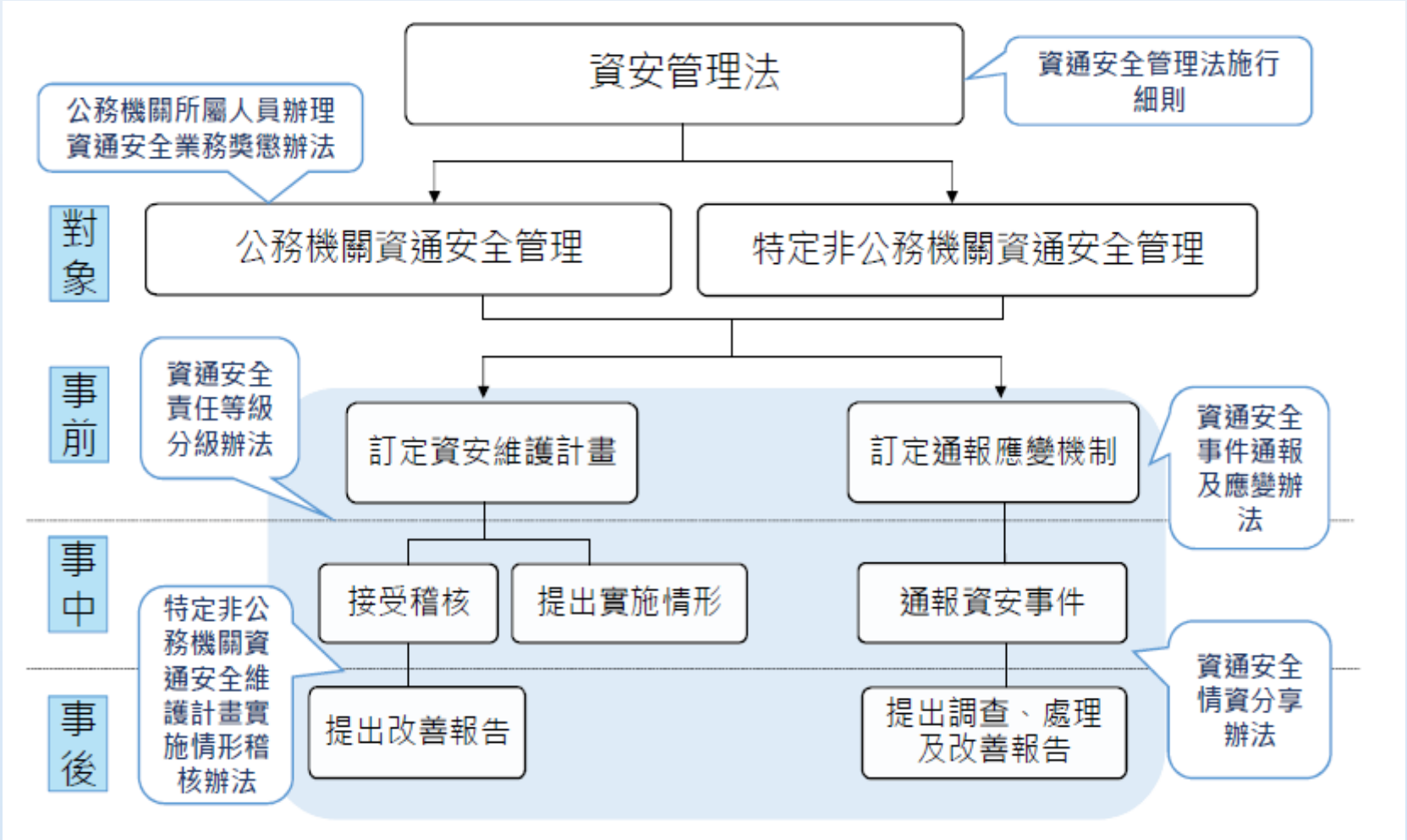
您不能接受的選擇?

公路中斷 V.S 網路中斷

您知道與資訊網路相關的法規嗎?

1. 著作權法(87.01.21/111.06.15-對教育相關，主文共117條)
2. 刑法-妨害電腦使用罪專章(92.06.25，相關條文共6條)
3. 兒童及少年福利與權益保障法(100.11.30，有46、46-1條)
4. 個人資料保護法(104.12.30，主文共56條)
5. 資通安全管理法(107.06.06，主文共23條)
6. 數位通訊傳播服務法....(研議中)

資通安全管理法之架構(共23條;細則13條)



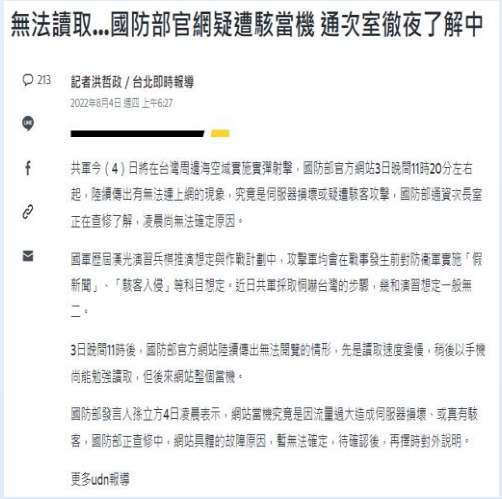
資安與個資事件(1)


110年政府機關重大資安事件通報
項次 通報時間 通報機關 事件說明 事件根因
1 110/1/25 教育體系 網站遭外部使用者不當存取方式，下載約1.3萬筆個人資料。 人為疏失
2 110/2/3 地方政府 廠商於活動網站發布採購資訊時，誤放連結使民眾資料外洩。 人為疏失
3 110/2/24 司法體系 資料庫服務中斷，超過可容忍中斷時間。 設備問題
4 110/3/26 教育體系 承辦人未將敏感資料進行遮罩即將包含個資資料上傳至網站。 人為疏失
5 110/3/26 教育體系 承辦人未將敏感資料進行遮罩即將包含個資資料上傳至網站。 人為疏失
6 110/4/16 教育體系 網站存在程式漏洞遭外部使用者不當利用，下載約650筆個人資料。 人為疏失
7 110/4/22 教育體系 來自國外異常連線以AP管理者帳號登入網頁，惟該職員休假中，疑似因弱密碼導致入侵。 人為疏失
8 110/5/10 中央機關 涉及CI維運系統服務中斷。 設備問題
9 110/6/4 教育體系 因線上報名程式漏洞導致部份個資外洩 人為疏失
10 110/8/25 教育體系 線上表單權限設定不當導致學生填報 人為疏失
11 110/9/6 教育體系 線上表單權限設定不當導致填報 人為疏失
今年至今尚無入侵事件，多為人為疏失造成個資外洩，已要求加強 資料的保護
HITCON 2021
WORK FROM HOME
HACK INTO HOME


109年政府機
項次 通報時間 通報機關
1 109/2/19 教育體系
2 109/5/13 地方政府
3 109/7/17 中央機關
4 109/8/8 地方政府
5 109/9/2 中央機關
6 109/9/3 醫療體系
7 109/9/10 中央機關
8 109/10/14 教育體系
9 109/11/1 中央機關
因人員操作不慎，誤將民眾個人資料夾帶於電子郵件寄出。
系統不當變更，致包含民眾個資之敏感資料外洩，估計約有51筆資料遭異常存取。
調整資訊服務採購契約範本，讓機關據以要求廠商負起資安責任
要求機關原則禁止遠端存取，並應在網站建置時就導入資安概念
27

資安與個資事件(2) - 近期遭駭網站

高雄市環保局網站網頁遭置換



國防部、外交部當機

7-11多家商店電視牆遭駭

▲裴洛西訪台，今（3）日上午台鐵新左營車站螢幕牆有白底紅字的醒目字。（圖／翻攝自王浩宇臉書）

左營台鐵車站電視牆遭駭

南投竹山網站網頁遭置換

臺灣大學網頁遭置換

民視直播遭駭

Wiseasy 支付終端遭駭

資安與個資事件(3)

誰偷了你個資？ 2300萬筆戶政資料疑遭駭PO網販售

王皓宇 羅士朋
2022年11月14日 週一 下午11:27

有賣家在網路上販售2300萬筆台灣民眾個資，引發關注，政府要如何把關，才能避免個資外洩事件一再發生？台灣資安人才不足，有網路安全公司與台科大合作，推出資安課程，揭開次世代防火牆供學生實戰，希望能填滿資安人才缺口。

圖／TVBS

後疫情時代，在家工作或遠工作邊度假已經成為常態，更成為近期另類遠距工作全球新趨勢，然而WFH大多使用自己的個人裝置，網路安全公司觀察到潛在的資安風險。

網路安全公司總經理尤專生：「網路的接上點就變多，你有可能在家裡，在咖啡廳或者你是從海外，透過雲端連線開一個視訊會議，從中就傳送了很多機密的文件，"零信任"主要就是因為疫情，在家工作以後，我們產出了一個資安的政策。」

零信任指的是一種IT安全方法，假設受信任的網路周邊並不存在，也會先行驗證每一筆網路交易，再放行，依循的是永不信任，一律驗證的原則，目的是要防止數據洩露得逞的策略計劃。

資安與個資事件(5)

新聞

北市衛生局遭駭一案調查公布，298萬個資被竊，10多個公部門與企業網站也遇害

對於去年8月發生的北市衛生局個資遭竊一案，法務部調查局於1月2日公布調查結果，駭客共竊取298萬筆北市民個資，且遭竊時間是在發現的一年之前，同時還調查出臺灣還有10多個公部門與企業網站也遭入侵。

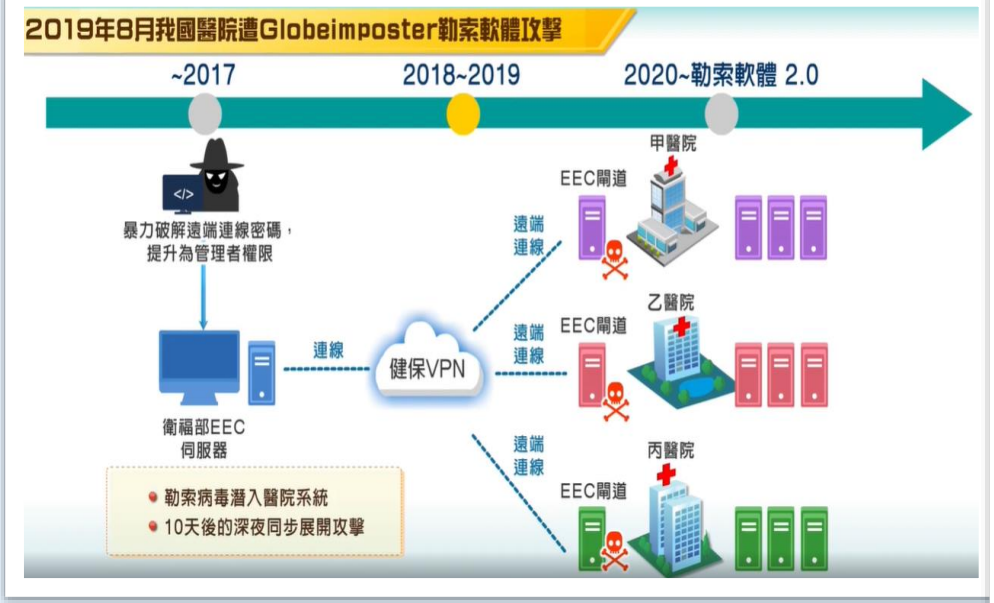
文/ 羅正漢 | 2019-01-03 發表

去年8月發生的臺北市政府衛生局個資外洩案，法務部調查局於今年1月2日，正式對外公布調查結果，共有約298萬的市民資料被駭客竊取，而調查的相關跡證中，也顯示臺灣有10多個政府機關、公立醫院、大學與企業網站被入侵。

同時，臺北市衛生局也在同一日，發出公衛系統個資外洩的公告，說明了調查局的調查結果，確認不當存取來源IP是在境外，遭不當存取資料

資料來源:iThome

資安與個資事件(4) - 主機管理很重要



衛福部所屬醫院多間醫院遇駭(透過健保VPN)

仁寶、研華、廣達等資料遭竊、勒索

公告日期	公告公司	發生事件公司	公告標題	相關報導
3月20日	宏碁	宏碁	說明媒體報導（報導內容:宏碁電腦遭駭客入侵勒索14億，公司緊急通報資訊保護機關處理）	宏碁傳出遭勒索軟體REvil攻擊，駭客索討5千萬美元贖金
4月6日	日月光投控	Asteelflash Group	代子公司環旭電子公告其控股子公司Asteelflash Group 網路安全事件	Asteelflash Group遭REvil勒索軟體攻擊，日月光集團公告說明環旭電子營運不受影響
4月22日	廣達電腦	廣達電腦	說明媒體報導（報導內容:廣達遭駭客攻擊）	廣達傳遭勒索軟體REvil攻擊，歹徒要脅蘋果購回外洩產品資料
5月26日	威剛科技	威剛科技	威剛針對部分資通系統遭病毒攻擊事件說明	記憶體大廠威剛科技公告部分資通系統遭病毒攻擊
6月3日	翔名科技	翔名科技	本公司部分資通系統遭到病毒攻擊事件說明	上櫃電子零組件翔名發布資安事件公告，部分資通訊系統遭病毒攻擊
8月6日	技嘉科技	技嘉科技	公告本公司遭受駭客攻擊	技嘉科技傳出遭勒索軟體攻擊，該公司公告部分伺服器遭網路攻擊
8月30日	關中	Grand Home Holdings INC.	代子公司Grand Home Holdings INC.公告遭受駭客網路攻擊	烤肉爐零售遭勒索軟體攻擊，上櫃貿易百貨業關中公告子公司遭駭
10月18日	帝寶工業	帝寶工業	說明本公司部分工廠廠區伺服器遭受病毒攻擊及影響	上市車燈大廠帝寶遭遇資安事件，臺灣廠區部分伺服器受影響
10月19日	宏碁	宏碁	說明媒體報導（報導內容:宏碁證實不到一周二度遭駭，強調在台客戶資料未外洩）	日前宏碁印度分公司與臺灣總公司遭攻擊，該公司發布重大訊息證實
10月27日	中鴻鋼鐵	中鴻鋼鐵	說明本公司輔助性伺服器遭受病毒攻擊及影響	鋼鐵大廠中鴻備份系統遭到病毒攻擊，駭客留下勒索訊息
10月29日	日勝生	日勝生	說明本公司及子公司部分資訊系統遭受駭客網路攻擊	上市營建公司日勝生遭網路攻擊，部分資訊系統受影響
11月1日	矽格	矽格	公告本公司網路安全事件	上市半導體封測矽格遭網路攻擊，受影響生產機臺仍在逐步恢復中
11月2日	京站實業	京站實業	說明本公司部分資訊系統遭受駭客網路攻擊	京站公告遭駭客網路攻擊，日勝生集團接連發布資安事件重大訊息
11月9日	雙美生物科技	雙美生物科技	說明本公司部分資訊系統遭受駭客網路攻擊	上櫃生技醫療雙美發布資安事件公告，部分資訊系統遭受駭客攻擊
12月20日	東元電機	東元電機	說明本公司部份資訊系統遭受駭客網路攻擊	東元與旗下東捷資訊遭駭客網路攻擊，部分資訊系統受影響
12月20日	東捷資訊	東捷資訊	說明本公司部分資訊系統遭受駭客網路攻擊	東元與旗下東捷資訊遭駭客網路攻擊，部分資訊系統受影響

資料來源：臺灣證券交易所，iThome整理，2022年2月

110年多家企業（資安事件）

資安與個資事件(6)

資料來源:iThome

資安與個資事件(7)

大考中心遭駭 2千考生個資外洩

2021-06-02 00:20 聯合報 / 記者潘乃欣／台北報導

+ 教育部

讚 24 分享 分享

為讓考生適應一一一學年新型學測試題，大考中心將於今年七月廿八到卅日舉辦試辦考試，開放高二生報名參加。未料昨傳出有兩千名考生報名資料遭駭，教育部證實此事，並說已送司法調查，也將請大考中心檢討並追究相關人員責任，同時強化資通安全防護，避免類此事件再次發生。

大考中心表示，大考中心因應試辦考試設立報名系統，今年四月一日上線，四月十二日開始報名，四月十五日就發現有不明人士透過不當手段，進入試辦考試觸及考生報名資料，約二千筆。

教育部表示，該系統發生少部分學生報名資料遭不明人士瀏覽，大考中心向教育部通報當下，教育部即依資通安全事件通報及應變辦法，要求大考中心緊急應變與損害復原，將損害降到最低。

(資料來源:聯合新聞網，https://udn.com/news/story/6925/5501972)

學生個資外洩 校方如何處理?

中正E報 Follow

Nov 6, 2020 · 3 min read

【記者 張雅涵、劉子君 / 中正大學報導】

一封電子郵件 學生個資全洩漏

國立中正大學通識中心在10月12號上午，誤將一份含有大量學生資料的檔案寄給報名講座的學生，其中包含104至108學年度，總共8495筆的入學學生姓名、生日、身分證字號……等重要個人資料，而校方卻在一天之後才向學生寄出道歉信，並請收到外洩資料的220位學生將郵件刪除。許多學生認為校方的處理態度與方式都不夠積極，令人無法接受。

國立中正大學學生：「當下知道這件事情的時候覺得蠻錯愕的，因為很誇張，這件事情沒有人想到會發生。」

國立中正大學學生：「感覺他們（校方）就知道他們錯，但是沒有做出相對應的處理。」

(資料來源:中正E報，https://pse.is/3gs7sk)

銀行業的資安迷思-第一銀行ATM盜領事件

一、臺灣ATM使用封閉網路，所以比較安全

二、 XP即使終止延伸支援，在封閉網路也安全

三、銀行資安稽核做得好，防駭能力一定好

四、臺灣人不懂怎麼駭入ATM，就比較安全

(資料來源:iThome)

資安的趨勢類型(1)

政府機關資安威脅情勢-2019~2021

一、個人資料外洩威脅持續存在

二、勒索軟體攻擊風險激增

三、IoT 與行動式設備資安弱點威脅升高

四、APT 鎖定式攻擊竊取機敏資料

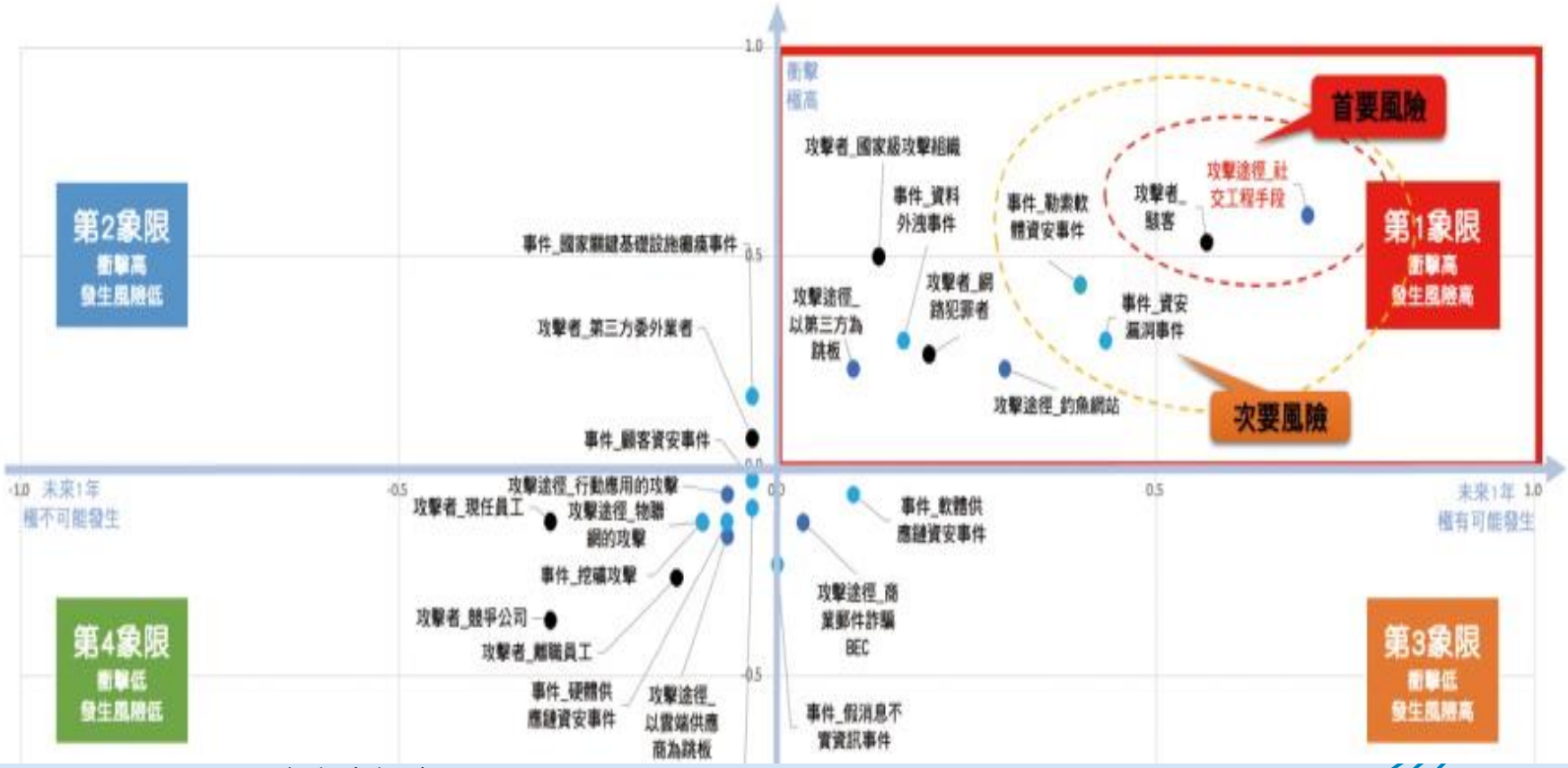
五、資通系統委外供應鏈遭駭

(資料來源:行政院2019、2021年國家資通安全情勢報告)

資安的趨勢類型(3-1)

政府與學校企業資安風險圖（未來一年）

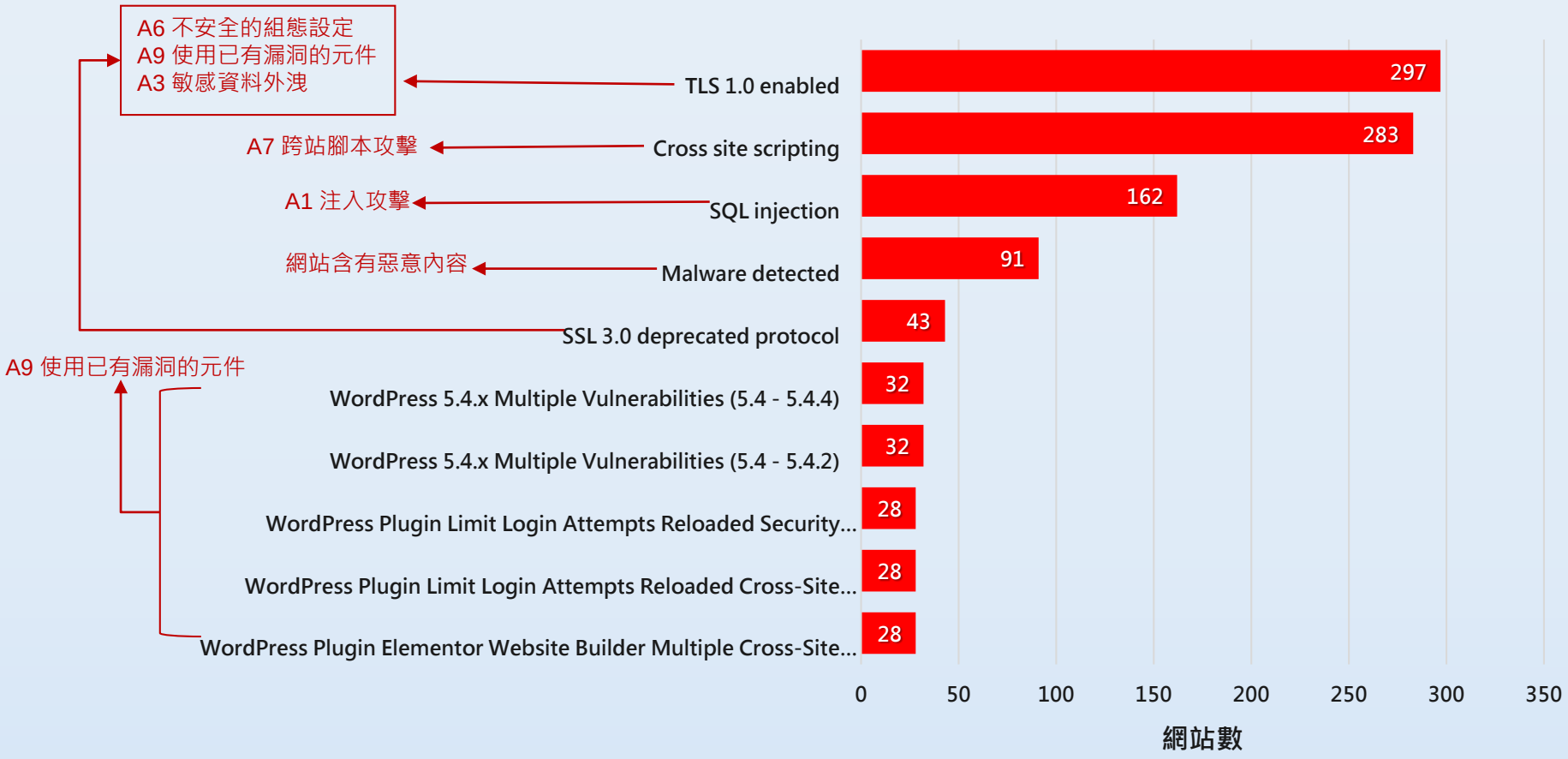
政府機關和學校今年兩大首要風險是社交工程手段和駭客的威脅，又以社交工程手段的衝擊最大，未來一年也最可能發生，這是今年突然崛起得特別留意的風險。其次，資安漏洞事件和勒索軟體資安事件則是今年次要風險



資料來源：iThome 2022 資安大調查

教育網站Top 10高風險弱點

統計期間:110/01/01-110/08/11



資料來源:DNS、學校網頁向上集中計畫

資安的趨勢類型(2)

醫療業的五大資安缺口

一. 健保 VPN：勒索病毒入侵與擴散

二. 端點設備：Windows 檔案共享、遠端桌面服務

三. 伺服器主機/OT 設備：作業系統老舊無法更新、防毒無法支援等等

四. 內部網路：容易破解的密碼

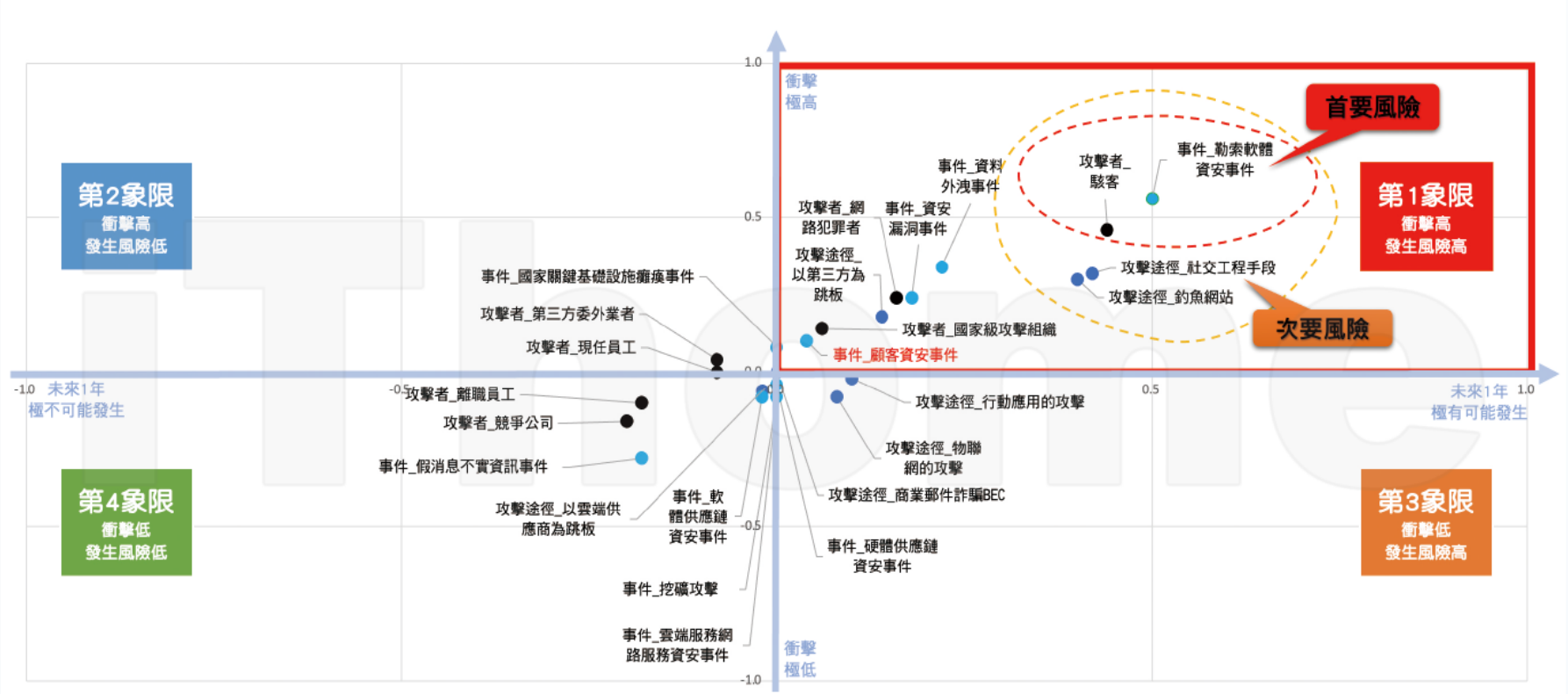
五. 護理推車：資料傳輸安全、週邊設備如 USB、藍芽等存取控制

(資料來源:資安人)

資安的趨勢類型(3-2)

醫療業企業資安風險圖（未來一年）

勒索軟體資安事件和駭客是醫療業者在 2022 年要面對的兩大首要風險，又以勒索軟體資安事件的衝擊最大，未來一年也最可能發生。其次，社交工程手段和釣魚網站威脅也是醫療業得留意的次要風險。顧客資安事件是醫院今年突然竄起的風險，不得不防



企業資安風險圖製作說明：

在iThome 2022年CIO暨資安大調查中，由企業自評各資安項目的兩項指標，一項是該項目對企業帶來的衝擊程度（衝擊極高和衝擊極低），另一項是這個項目未來1年的發生風險（極可能發生與極不可能發生），再換算成不同程度的量化數據來製圖。垂直軸是該項目對企業的衝擊，位置越往上代表衝擊越大，水平軸是企業未來1 年發生該項目的風險，位置越右，代表可能性越大。紅色文字的項目為今年發生風險明顯提高者。【問卷說明】大調查執行期間從2022年7月1日到29日，對臺灣大型企業、歷屆CIO大調查企業、政府機關和大學的IT與資安主管，進行線上問卷，有效問卷416家，其中61.9%填答者為企業資安最高主管

資料來源：2022 iThome CIO大調查，2022年8月

資安的趨勢類型(3) - 資安威脅面

一、硬體環境安全

- 防天然災害
- 防止毀損
- 保全防竊

二、軟體及系統安全

- 防止駭客入侵
- 防中電腦病毒
- 弱點、漏洞

三、資料庫安全

- 防天然災害
- 防止資料毀損(含被加密)
- 防止被竊取

四、人員安全

- 防竊取
- 防止誤刪(公視紀錄影片、學習歷程)
- 誤點社交信件

資安的趨勢類型(4) - 資安威脅層次

一、影響維運層次(表像面)

- ●網頁的置換竄改
- ●分散式阻斷攻擊(DDoS)
- ●惡意軟體-病毒和蠕蟲
- ●DNS 通道

二、造成資料外洩損失層次(實質面)

- ●網路釣魚、社交工程
- ●中間人攻擊
- ●SQL 注入攻擊
- ●零時差攻擊
- ●惡意軟體-間諜軟體、勒索軟體
- ●進階持續性滲透攻擊（***Advanced Persistent Threats, APT***）

資安的趨勢類型(5) - 資安防護措施

- **定期資安檢測(網站弱掃、系統弱掃、原始碼檢測、App認證、API檢測)。**
- **防勒索之儲存備份機制。**
- **建立資安憑證加密(SSL憑證)機制。**
- **建立網路管理監控服務。**
- MDR(Managed Detection and Response)、EDR(Endpoint Detection and Response)威脅偵測服務。
- 建立F/W、WAF、防毒軟體、DDoS流量清洗、IPS、IDS等防護設施。
- 檢視校園網路運作及資通安全防護兼顧的架構，以取得網速與資安的平衡。
- 導入全機關的資安輔導諮詢。

大綱

前言	資安與個資事件的趨勢
壹	校園資安現況與推動重點
貳	資安與高教深耕
參	結合保護個資的資通安全防護的推動
肆	結語

校園資安推動現況（1）

- 期待所核予之資安責任等級(A、B、C、D、E)愈低愈好。
- 推動組織未能涵蓋校內系所及行政單位主管。
- 所制定的ISMS範圍仍以資訊單位的機房或負責系統為主。
- 對資通系統的清查未能全面落實，對應之安全分級的評估亦未確實，以等級(普、中、高)愈低愈好。
- 對所業管之資訊系統相關防護作為要求不對稱，如備份週期需求短而RPO&RTO的設定時間長、投入開發成本高而安全等級為”普”。

校園資安推動現況（2）

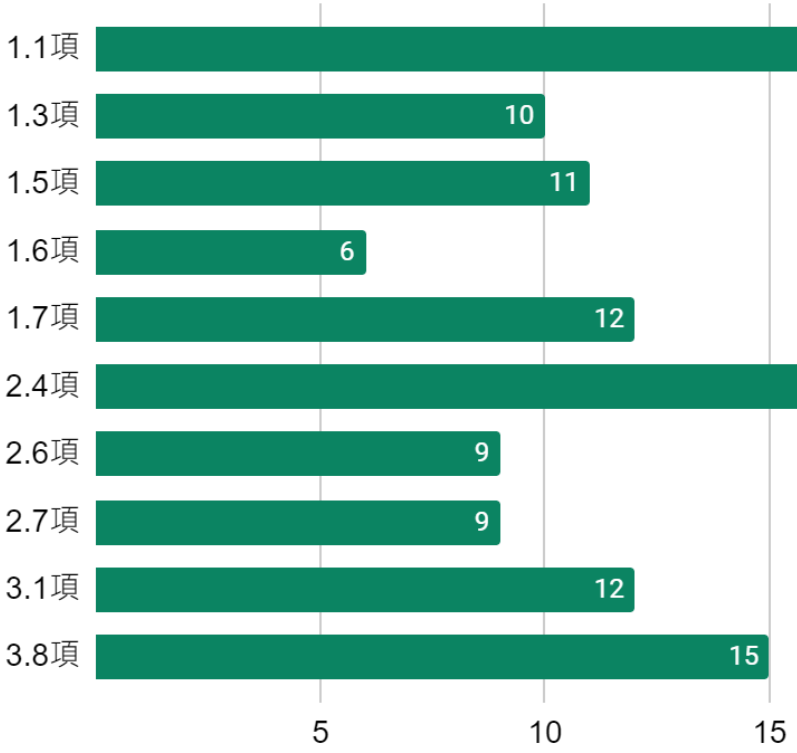
- 對核心系統僅象徵性的以學校網站為主，對全校性之學籍、選課等校務系統皆未納入。
- 業務持續演練過程僅做最低度的還原情境模擬。
- 員工的資安認知教育訓練僅限行政人員。
- 對資訊服務委外合約未納入資安相關規範，也未確認承商是否具備資安防護能力。
- 系統之資安防護措施未對應編列經費。
- 業務相關人員普遍認為資安是技術性問題。

資通安全實地稽核項目檢核表

資通安全責任等級分級辦法
附表十

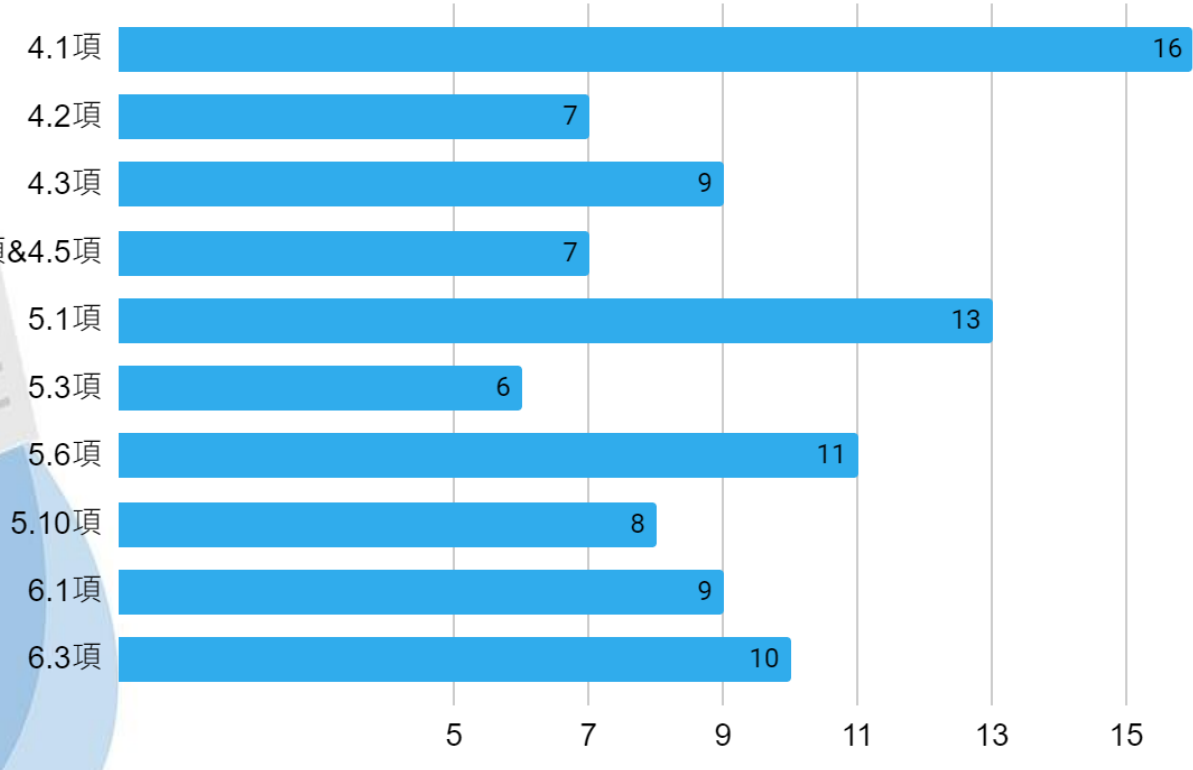
26/108	29/108	53/108	77
策略面	管理面	技術面	防護基準
1.核心業務及其重要性 2.資通安全政策及推動組織 3.資安專責人力及經費配置	4.資訊及資通系統盤點及風險評估 5.資通系統或服務委外辦理之管理 6.資安維護計畫與實施情形	7.資通安全防護及控制措施 8.資通系統發展及維護安全 9.資通安全事件通報應變	存取控制、稽核可歸責性、營運持續計畫、識別鑑別、系統與服務獲得、通訊保護、系統與資訊完整性

策略面



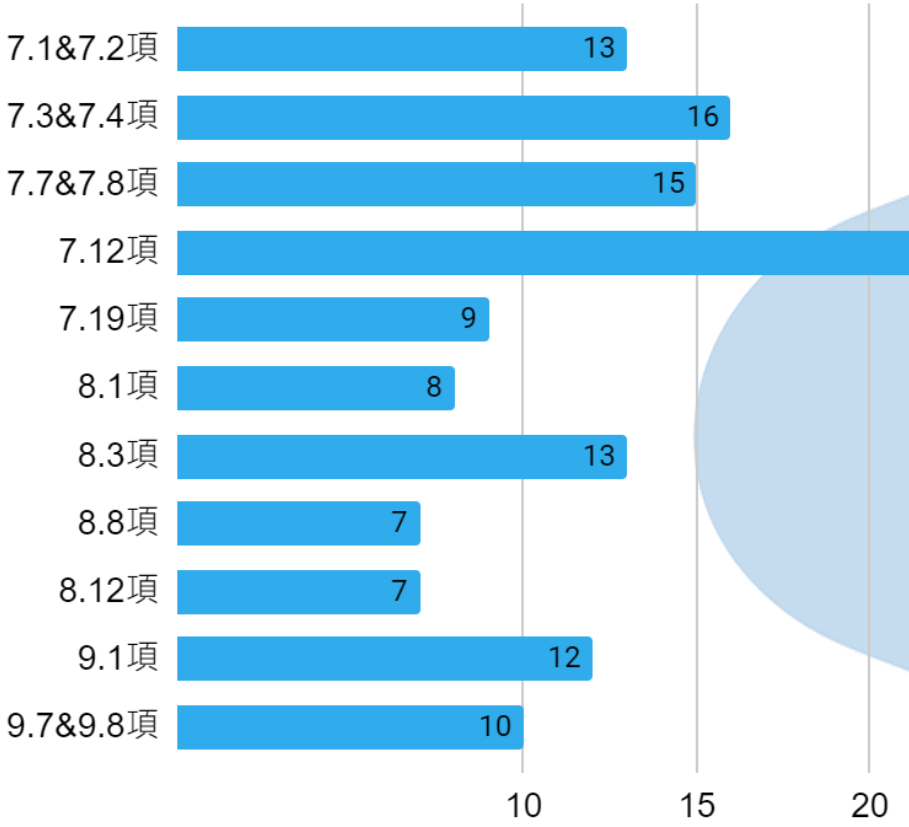
資料來源:教育機構資安驗證中心

管理面



資料來源:教育機構資安驗證中心

技術面



資料來源:教育機構資安驗證中心

法遵事項及行政院重要政策

一、行政院秘書長109年12月18日函送公務機關使用資通訊產品原則：(院臺護長字第1090201804A號)

- **公務用之資通訊產品**(包含軟體、硬體、服務)**不得使用大陸廠牌**，已使用或採購者應列冊管理，**不得與公務環境介接**，且應**於110年12月31日前完成汰換**。

二、行政院111年8月資安警戒專案相關會議指示：

- 針對**傳播影像或聲音**，供**不特定人士**直接收視或收聽之情形，皆不可使用大陸廠牌軟體、硬體及服務。
- 非屬前述傳播類型之危害國家資安產品，亦須列冊管理，控管資安風險，請各機關透過**委外契約**及**場地租借使用規定**來推動辦理。

教育部第二方稽核關注事項

- **法遵落實**情形 **(策略面、管理面、技術面)**
  - 資通安全維護計畫
  - 依機關資通安全責任等級之應辦事項。
  - 依資通系統防護需求等級之控制措施。

    (按合適之系統抽樣原則，建議關注中級以上或含個資等機敏資訊者)
- **大陸廠牌資通訊產品**之盤點及**汰換**作為(含**出租場域**) **(管理面)**
- 全機關**物聯網**(IoT)**設備**之**盤點**及風險管理措施 **(管理面)**
- **委外安全**管理規範 **(管理面)**
- **安全系統開發程序**(SSDLC) **(技術面)**
- **「原則禁止、例外允許」遠端維護**資通系統之管理作法 **(技術面)**
- **社交工程防範 (技術面)**

宣導事項(1/3)

- 本部已於110年12月30日函送**國立大專校院資通安全維護作業指引**，請**務必落實**辦理，包含下列事項：

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

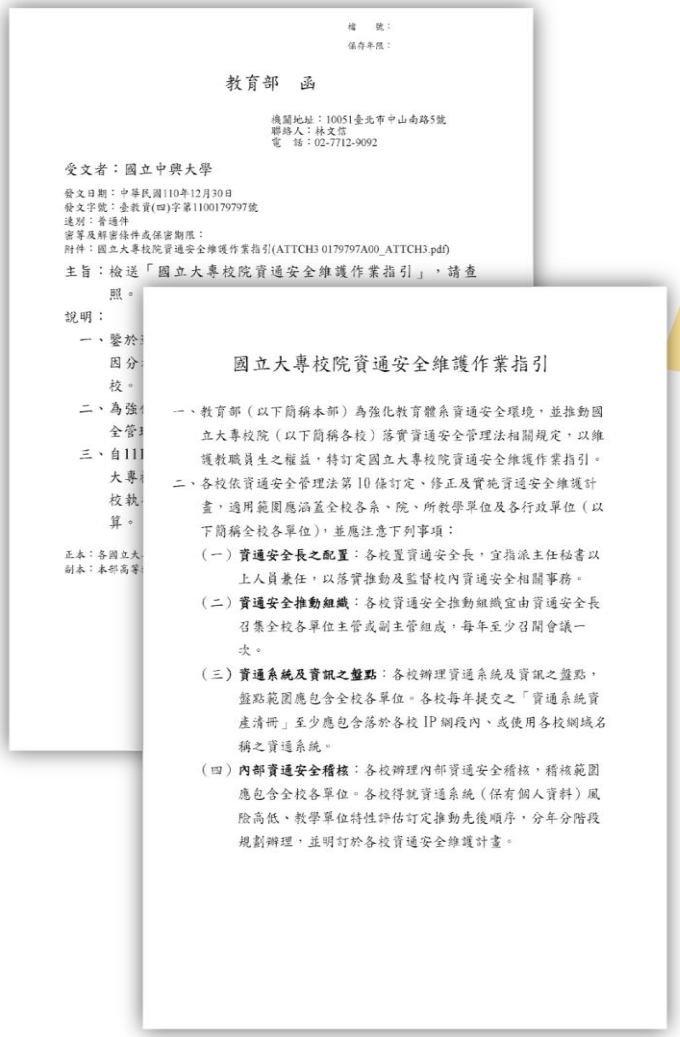
宜由**資通安全長**召集全校各單位主管或副主管組成，**每年至少召開會議1次**

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**



檔　號：
保存年限：

教育部　函

機關地址：10051臺北市中山南路5號
聯絡人：林文哲
電　話：02-7712-9092

受文者：國立中興大學

發文日期：中華民國110年12月30日
發文字號：臺教資(四)字第1100179797號
速別：普通件
密等及解密條件或保密期限：
附件：國立大專校院資通安全維護作業指引(ATTCH3 0179797A00_ATTCH3.pdf)

主旨：檢送「國立大專校院資通安全維護作業指引」，請查照。

說明：

一、鑒於

因分

校。

二、為強

全管

三、自11

大專

校執

算。

正本：各國立大

副本：本部高等

國立大專校院資通安全維護作業指引

一、教育部（以下簡稱本部）為強化教育體系資通安全環境，並推動國立大專校院（以下簡稱各校）落實資通安全管理法相關規定，以維護教職員生之權益，特訂定國立大專校院資通安全維護作業指引。

二、各校依資通安全管理法第10條訂定、修正及實施資通安全維護計畫，適用範圍應涵蓋全校各系、院、所教學單位及各行政單位（以下簡稱全校各單位），並應注意下列事項：

（一）**資通安全長之配置**：各校置資通安全長，宜指派主任秘書以上人員兼任，以落實推動及監督校內資通安全相關事務。

（二）**資通安全推動組織**：各校資通安全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，每年至少召開會議一次。

（三）**資通系統及資訊之盤點**：各校辦理資通系統及資訊之盤點，盤點範圍應包含全校各單位。各校每年提交之「資通系統資產清冊」至少應包含落於各校 IP 網段內、或使用各校網域名稱之資通系統。

（四）**內部資通安全稽核**：各校辦理內部資通安全稽核，稽核範圍應包含全校各單位。各校得就資通系統（保有個人資料）風險高低、教學單位特性評估訂定推動先後順序，分年分階段規劃辦理，並明訂於各校資通安全維護計畫。

國立大專校院資通安全維護作業指引(臺教資(四)字第1100179797號)

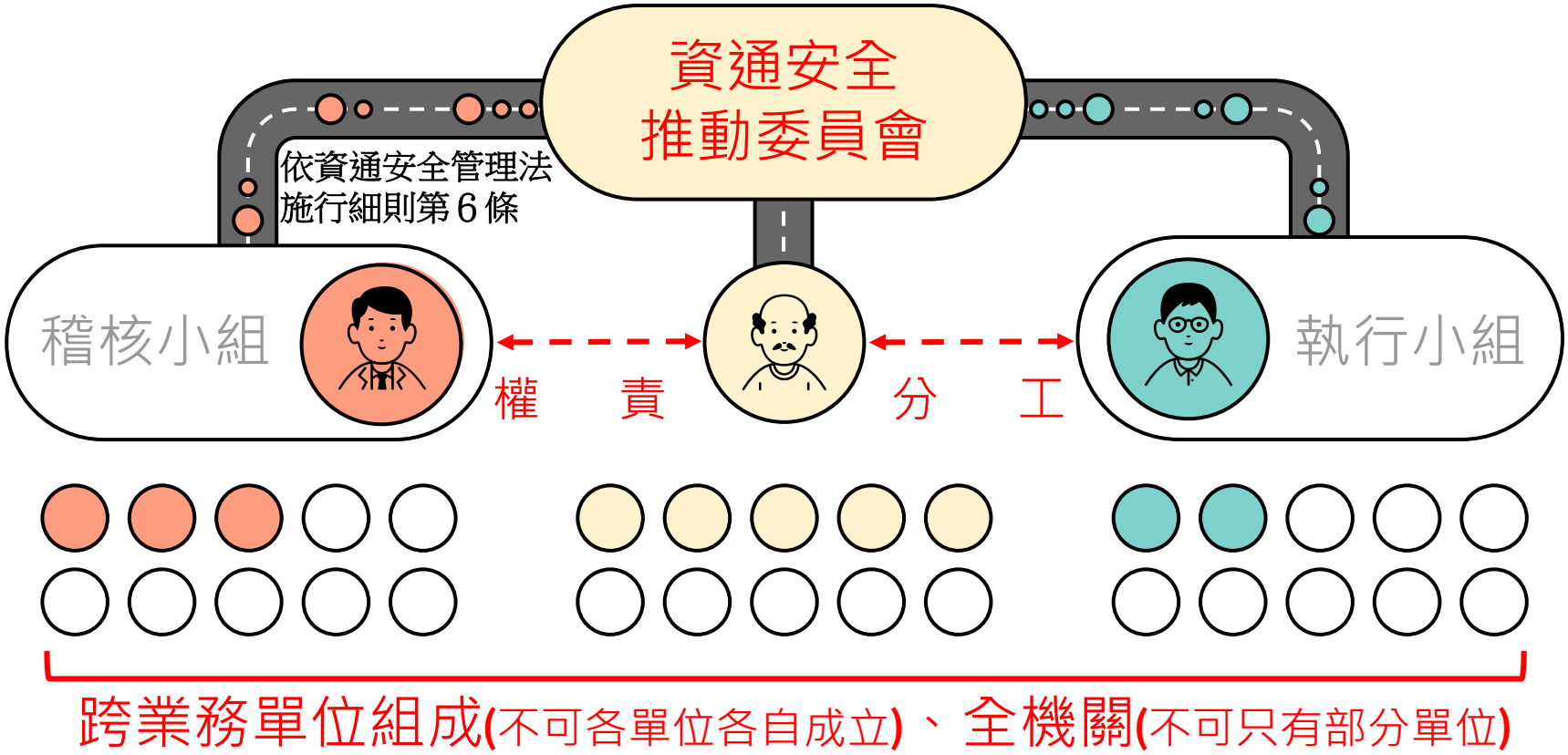
各校依資通安全管理法第10條訂定、修正及實施資通安全維護計畫，適用範圍應涵蓋全校各系、院、所教學單位及各行政單位，並應注意下列事項：

（一）資通安全長之配置

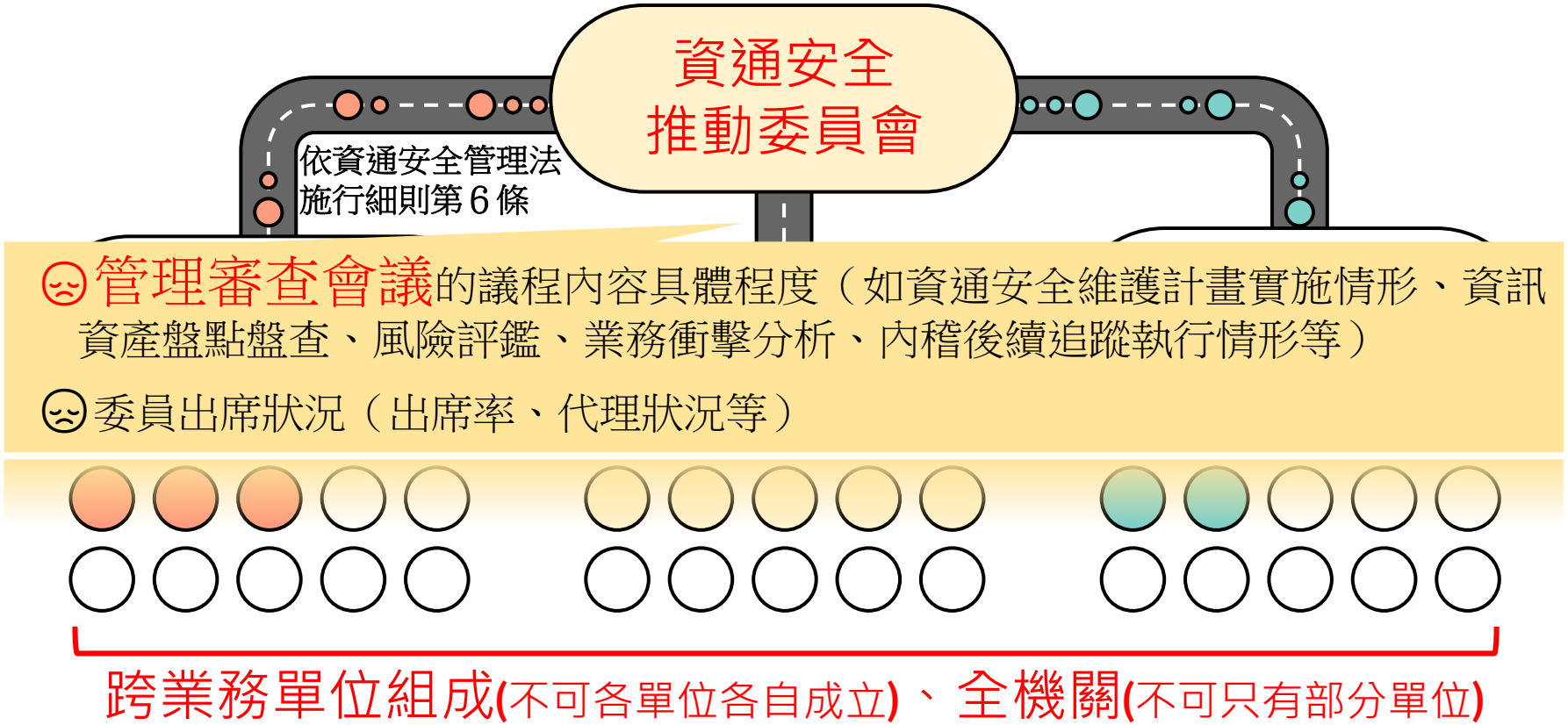
（二）資通安全推動組織

（三）資通系統及資訊之盤點

（四）內部資通安全稽核



2.4 成立**資通安全推動組織**，負責推動、協調監督及審查資通安全管理事項，推動組織層級之適切性，且**業務單位是否積極參與**。



2.4 成立**資通安全推動組織**，負責推動、協調監督及審查資通安全管理事項，推動組織層級之適切性，且**業務單位是否積極參與**。

宣導事項(2/3)

- 資安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**)。

資通系統盤點

- 各校每年提交之「**資通系統資產清冊**」**至少應包含**落於**各校IP網段內**、或使用**各校網域名稱**之資通系統。

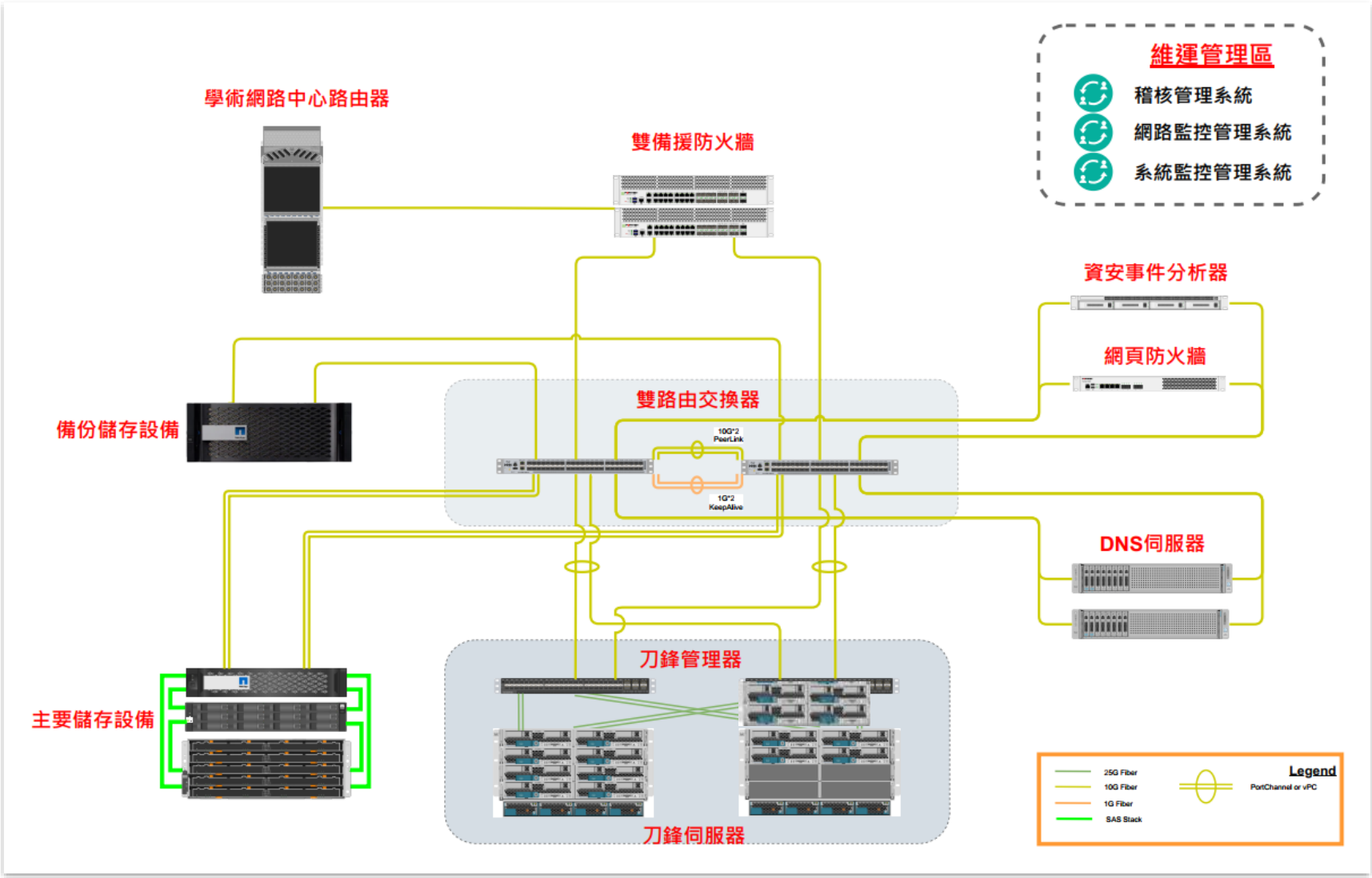
內部資安稽核

- 各校得就資通系統(保有個人資料)風險高低、教學單位特性**評估訂定推動先後順序**，**分年分階段**規劃辦理，並**明訂於**各校資通安全**維護計畫**。

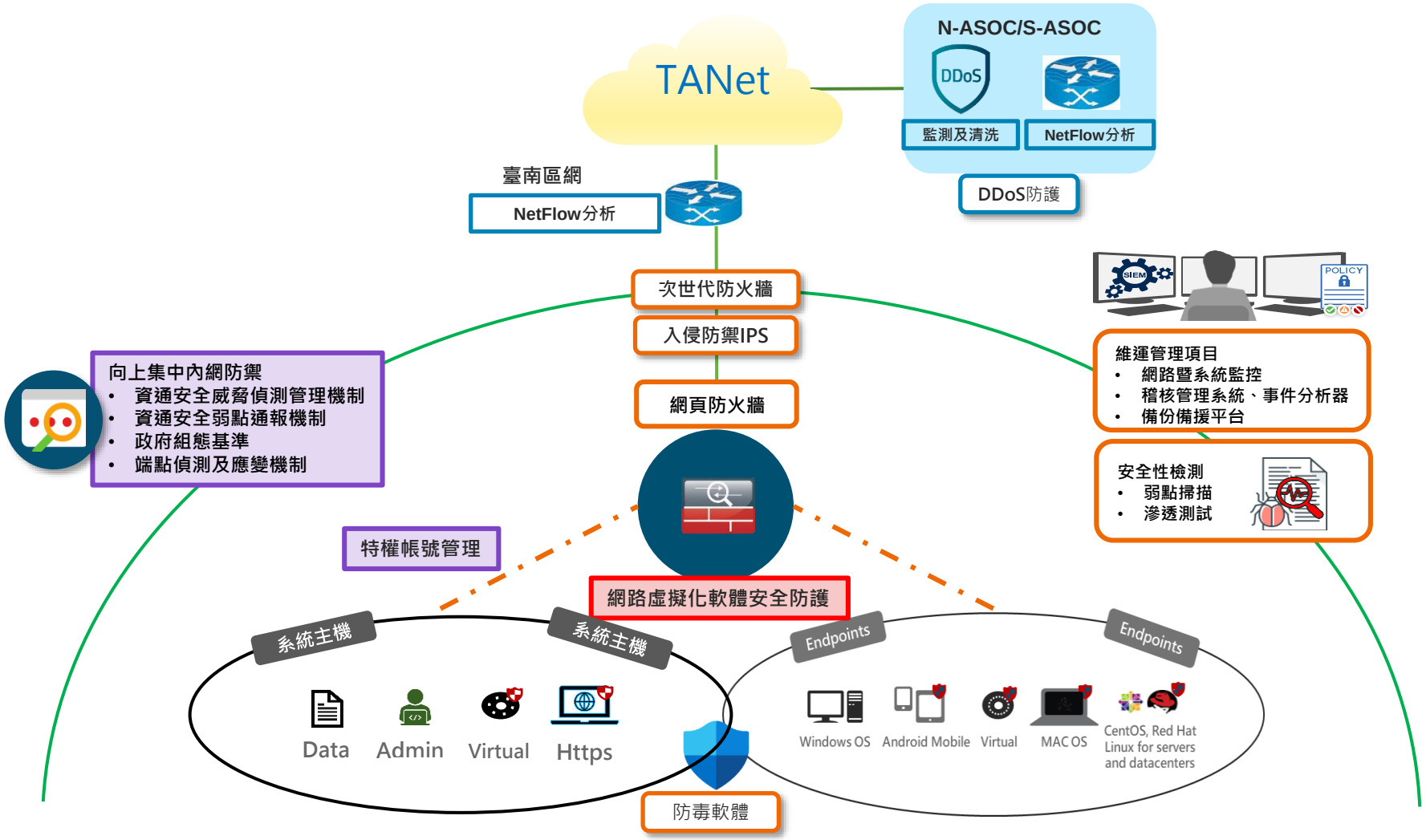
宣導事項(3/3)

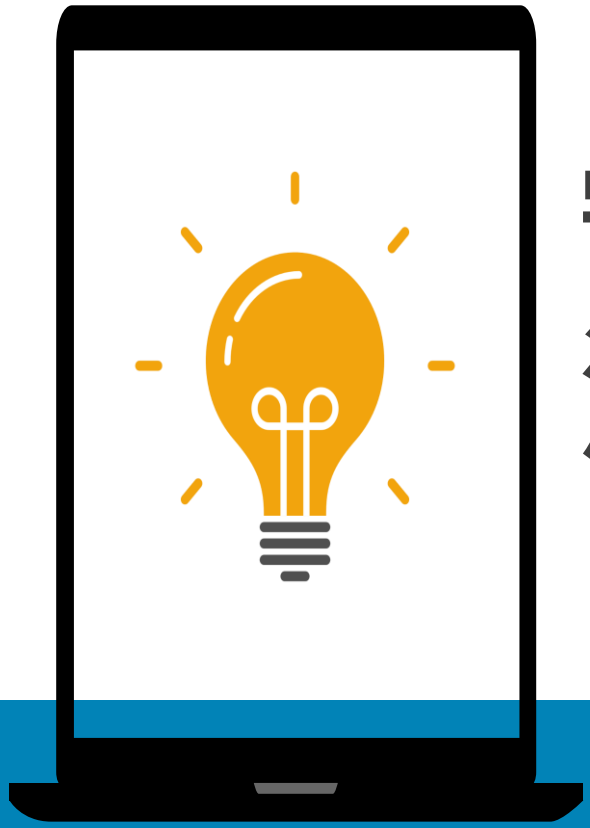
- 本部已於110年9月8日函送**各級學校使用資通系統或服務蒐集及使用個人資料注意事項**，請**務必落實**辦理。

校園資安統整運作環境 (示意架構)



校園統整網路及資安防禦(示意圖)





學校Web網站
注意事項

資通系統的資安與個資(1-1)

~~網站維護更新~~

- **學校與網站維護廠商之維護約簽訂：**簽訂內容務必思考學校自身需求
  - 弱掃及風險修補
  - 憑證安裝之協助
  - 網站功能異常與修改
  - 學校其他需求
- **弱掃風險修正：**網站/系統弱掃報告中，不符標準且法規規定不可存在的風險必需改善
- **定期檢視主機內容：**
  - 檢查是否有異常程式運轉
  - 密碼複雜度之維持與定期更新

資通系統的資安與個資(1-2)

~~使用HTTPS連線~~

◆**SSL 憑證申請：**

注意憑證到期日，建議到期前一個月就要申請新憑證

◆**網站 HTTPS**：學校任何對外網頁，皆需使用 HTTPS 進行連線

- 將 HTTP 連線強制導向至 HTTPS
- 使用有效憑證(注意瀏覽器網址列所顯示是”鎖頭”或”不安全”符號)
- 只使用 TLS1.2 以上 protocols

資通系統的資安與個資(1-3)

~~檢視網站內容~~

- **勿放置機敏資料：**

  請檢視網頁所有資訊，如有個資請遮罩處理或移除下架

- **注意外部連結有效性：**

  請留意放置連結是否失效，如已失效請移除，以免該連結導向異常網站

資通系統的資安與個資(2-1)

電子郵件的資安(社交工程)

1. 盜取由官方信箱主機(如HiNet)發出釣魚信。
2. 示例

(資料來源:openfind網站，https://www.openfind.com.tw/taiwan/markettrend_detail.php?news_id=24696)

資通系統的資安與個資(2-2)

電子郵件的資安(社交工程)

1. 連往釣魚網站的圖片偽裝成附檔掩人耳目。
2. 示例

(資料來源:openfind網站，https://www.openfind.com.tw/taiwan/markettrend_detail.php?news_id=24696)

資通系統的資安與個資(2-3)

電子郵件的資安(社交工程)

1. **免費雲端儲存空間被濫用，成為檢查機制死角。**
2. **示例**

(資料來源:openfind網站，https://www.openfind.com.tw/taiwan/markettrend_detail.php?news_id=24696)

資通系統的資安與個資(2-4)

電子郵件的資安(社交工程)

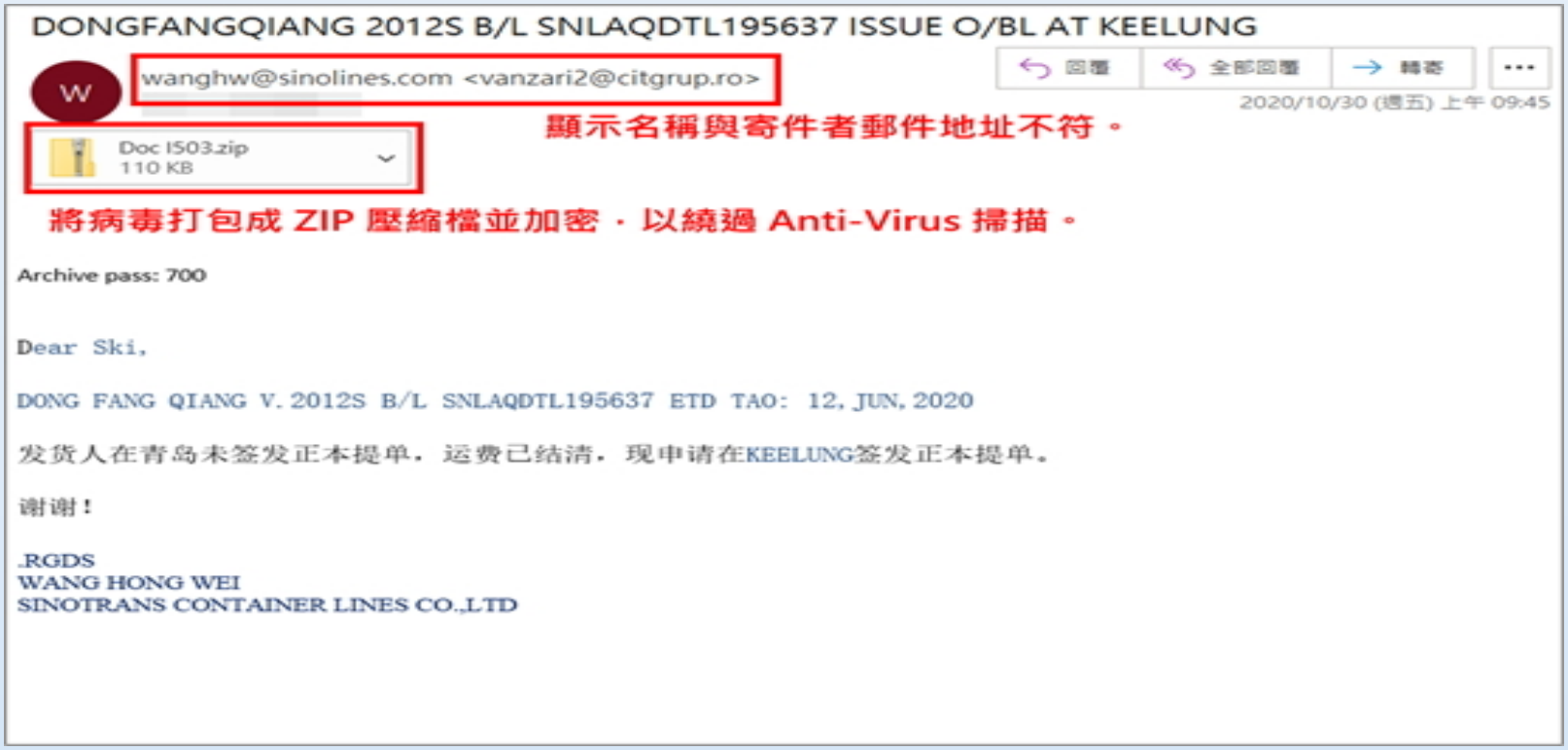
1. 植入有木馬病毒的 **Office** 文件。
2. 示例

(資料來源:openfind網站，https://www.openfind.com.tw/taiwan/markettrend_detail.php?news_id=24696)

資通系統的資安與個資(2-5)

電子郵件的資安(社交工程)

1. 將病毒檔置於加密壓縮檔中，以繞過檢查機制。
2. 示例



(資料來源:openfind網站，https://www.openfind.com.tw/taiwan/markettrend_detail.php?news_id=24696)

資通系統的資安與個資(2-6)

電子郵件的資安-因應方案

1. **詐騙信特徵分析** — 分析詐騙(Business Email Compromise, BEC)信件特徵，目前可由郵件系統端直接攔截。
2. **示例**

[特徵1] Reply-to 詐騙情境

[特徵2] 相似網址詐騙情境

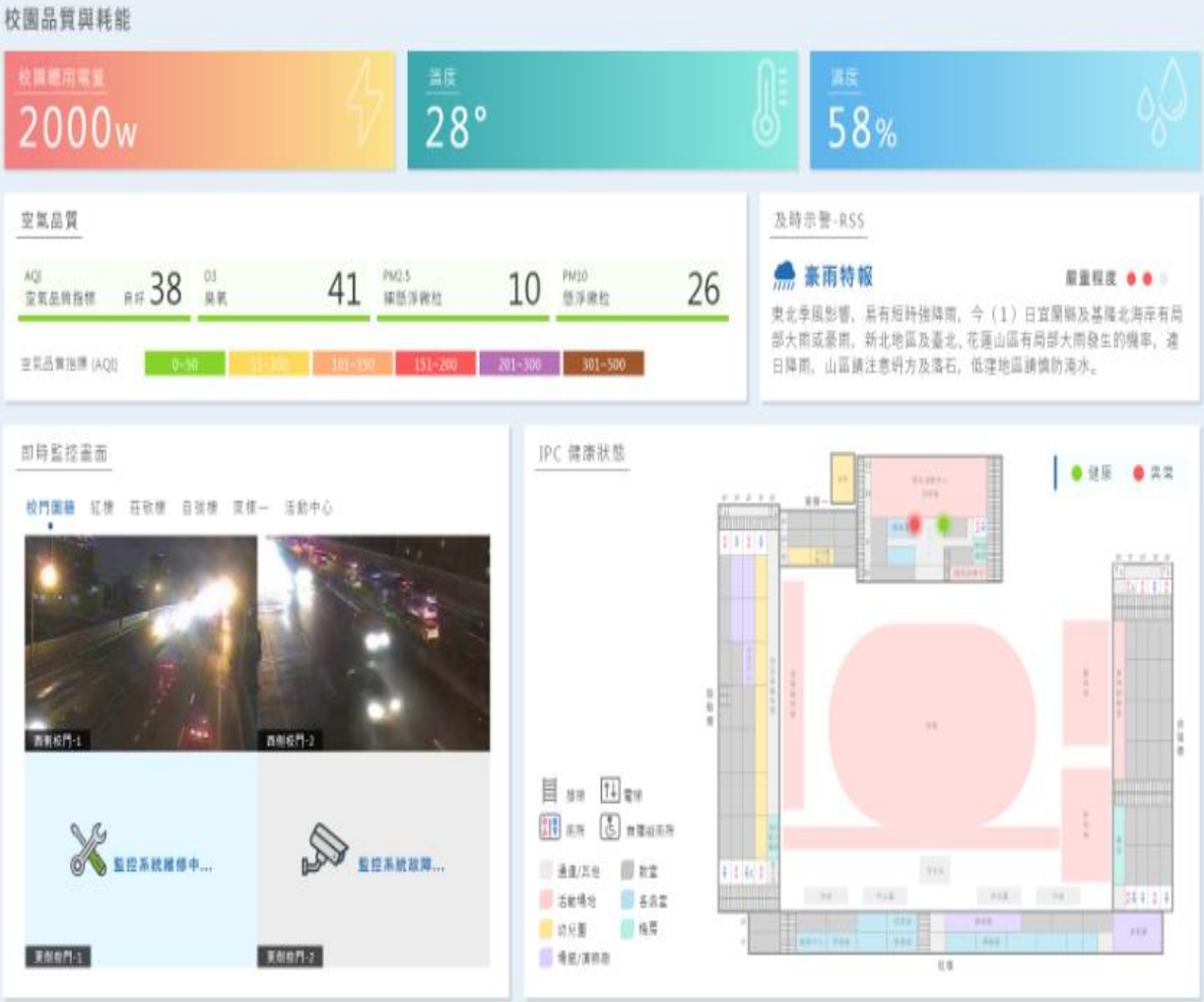
資通系統的資安與個資(2-7)

電子郵件的資安-因應方案

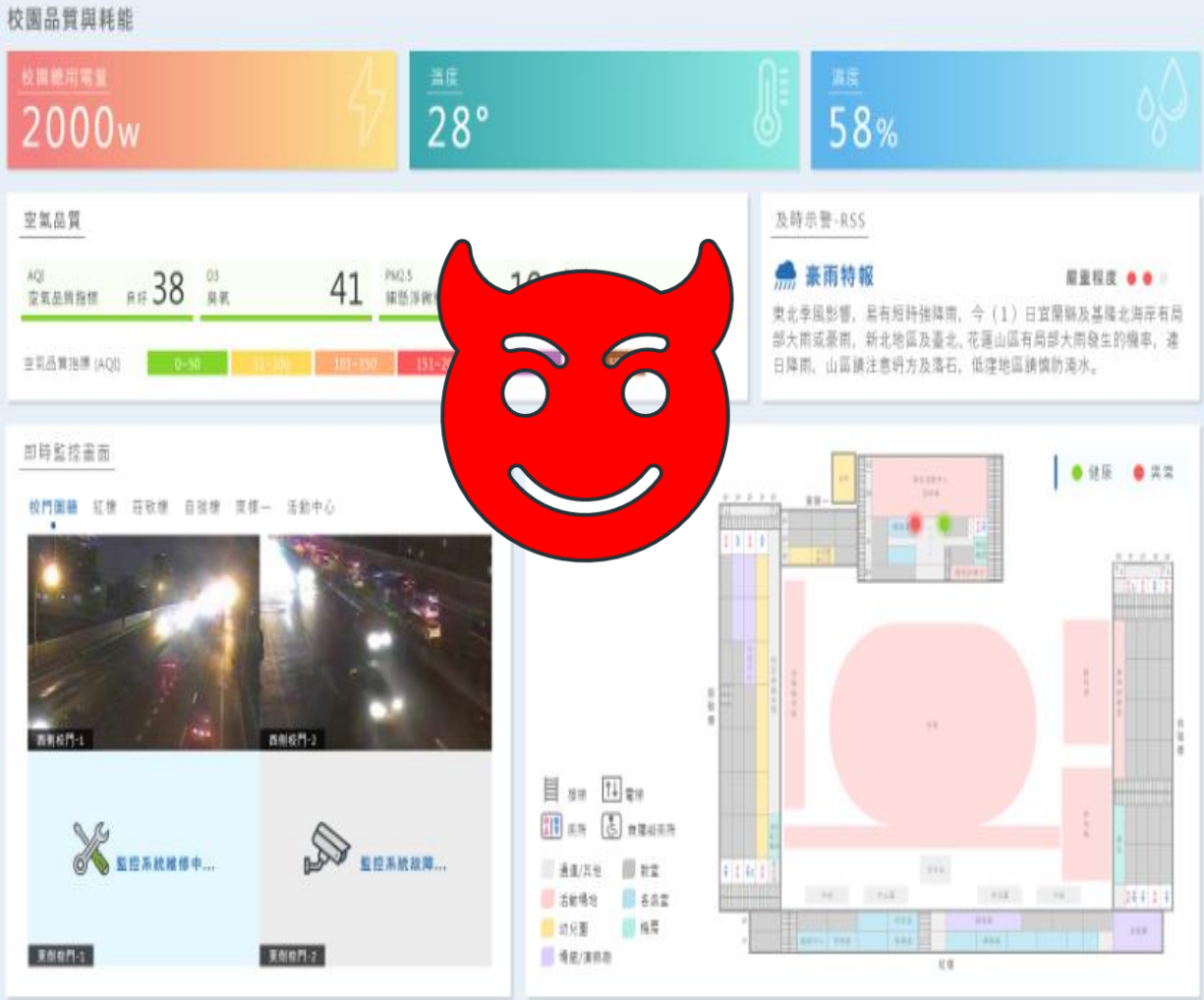
1. **動態惡意轉址警示**—杜絕時間差造成的進階社交工程攻擊及魚叉式郵件釣魚攻擊威脅。
2. **示例**

IoT物聯網安全(3-1)


智慧佈告欄


校園品質與耗能
2000w
28°
58%
空氣品質
AQI
38
O3
41
PM2.5
10
PM10
26
及時示警-RSS
豪雨特報
即時監控畫面
監控系統維修中...
監控系統故障...
IPC 健康狀態
健康
異常

想像一下學校的IoT被入侵…(3-2)



IoT被入侵，會怎麼樣？(3-3)

駭客要的是…

1. 綁架你的設備，讓你成為共犯 (Botnets)
2. 你的名譽、隱私
3. 你的資料
4. 你的錢
5. 利用你的設備收集資訊
6. 讓自己的駭客履歷更漂亮
7. …

OWASP IoT top 10(3-4)

https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10

1. 弱密碼 (Weak Guessable or Hardcoded Passwords)
2. 不安全的網路服務 (Insecure Network Services)
3. 不安全的生態界面 (Insecure Ecosystem Interfaces)
4. 不安全的更新機制 (Lack of Secure Update Mechanism)
5. 使用不安全的元件 (Use of Insecure Outdated Components)
6. 隱私防護不足 (Insufficient Privacy Protection)
7. 不安全的資料轉移和儲存 (Insecure Data Transfer and Storage)
8. 缺乏裝置設定 (Lack of Device Settings)
9. 不安全的預設 (Insecure Default Settings)
10. 缺少物理加固措施 (Lack of Physical Hardening)

四步驟保護IoT安全(3-5)

1. 產品的資安品質
   a. 購買設備前確認產品資安品質
   b. 是否有弱點被揭露？修補了嗎？
   c. 廠商更新維護品質如何？
2. 盤點與管理
3. 設定密碼
   a. 預設密碼一定要改掉！！！
   b. 密碼長度，至少8碼以上
   c. 密碼複雜度，至少含英數＋大小寫+符號
4. 定期更新軟體韌體

推動校園資安時應思考之觀點(1)

- 是否已掌握校園有那些資訊服務系統及資通訊設施?風險為何?
- 現有資訊服務系統及資通訊設施停止運作時，有其他因應替代方案可維持正常運作嗎?所面對的服務對象是否可接受？(評估對資訊化的依存度)
- 當業務相關系統被入侵破壞或竊取資料時，會有什麼損失或對組織衝擊？
- 當有資訊服務委外他人時，所訂定的契約要求是否將資安相關規範納入?否具備對應的資安防護驗測能力？

推動校園資安時應思考之觀點(2)

- 對所建構或維護之資通系統，是否充分評估資源投入、效能及效益、風險承受力的平衡。
- 學校是否會承接他單位委託有涉資訊相關的服務或計畫？委外於我時，所訂定的契約被要求的資安相關規範否已具備對應的資安防護能量？
- 學校是否有與相關單位或所屬機構建立密切資料交換的互連網?其資安責任等級是否較高或低?
- 是否能認為資通系統的資安防護作為僅需技術性的投入，無需有其他業務人員的參與？

醫療機構電子病歷製作及管理辦法
（110.12.8預告，預計111.7公告施行）

第3條 醫療機構實施電子病歷者，應建置電子病歷資訊系統（以下簡稱系統）....

第三條第一項系統，醫療機構得委託大專校院、依法登記或立案之法人、機構或團體（以下併稱受託機構）建置及管理之，並由醫療機構負本法及本辦法規定之責任。

前項醫療機構之委託，應訂定書面契約。但有下列情形之一者，得免訂定書面契約：

一、委託所屬醫療法人或其他法人之其他附設醫院。

二、委託所屬學校之其他附設醫院。

三、委託所屬機關設立之其他醫院。

第一項受託機構，應通過中央主管機關認可之資訊安全標準驗證，並有證明文件。

校園推動資安可運用之資源

- 教育學術資訊安全維運中心(A-SOC)-
  - 國立臺灣大學、國家高速網路與計算中心
- 教育機構資安驗證中心(ISCB)-
  - 國立中興大學
- 教育體系分散式阻斷攻擊(DDoS)流量清洗服務-
  - 國立臺灣大學
- 教育體系資安技術檢測服務中心-
  - 國立陽明交通大學
- 教育網站資安弱點掃描防護服務-
  - 國立成功大學
- 臺灣學術網路危機處理中心(TACERT)營運服務-
  - 國立中山大學
- 教育機構資安分享與分析中心(A-ISAC)-
  - 逢甲大學
- 教育體系資安職能訓練-
  - 國立政治大學

補充說明

- 資通安全管理法108年1月1日正式施行。
- 資安事件
  - 依「**資通安全通報及應變辦法**」進行資安通報。
  - 如發現所轄系統(網站)遭竄改，**10分鐘內上架「維護公告網頁」**。
  - 機關、學校因管理不當導致資通安全事件，將以**不遮蔽該機關、學校**方式作為教育體系**內部案例宣導**。
  - 發生重大資通安全事件之機關、學校，將辦理**專案實地稽核**。
- 獎懲
  - 公務機關：公務機關所屬人員資通安全事項獎懲辦法。
  - 非公務機關：臺灣學術網路管理規範。

大綱

前言	資安與個資事件的趨勢
題一	校園資安現況與推動重點
題二	資安與高教深耕
題三	結合保護個資的資通安全防護的推動
最終	結語

1.第二期規劃 - 主冊專章：資安強化

第二期規劃 - 主冊專章：資安強化

- **計劃說明:**

  為協助大學建立持續性與永續性的教研環境，不因資安事件受影響而中斷教學與研究，爰規劃**資安強化專章**，大學可**參照資通安全管理法及其子法要求，推動資通安全管理，以資通安全責任等級分級辦法就管理面、技術面及認知與訓練面**研提規劃推動之策略及擬定相關績效指標。

貳、高教深耕計畫(第二期112-116年)

第一部分
全面性提升大學品質及促進高教多元發展
（維護學生平等受教權）

第二部分
協助大學追求國際一流地位及發展研究中心
（強化國家國際競爭力）

資料來源：高等教育深耕計畫網站

2.計畫專章撰寫建議方向

壹、前言-近期資安攻擊事件

【8月2日】

DDoS攻擊總統府證實網站遭DDoS攻擊，疑與美國眾議院議長裴洛西訪臺有關

DDoS攻擊政府入口網站、外交部網站傳出因遭到DDoS攻擊而無法存取，外交部指出網站收到每分鐘多達850萬次請求

DDoS攻擊國防部、外交部，以及桃園國際機場的網站，疑似遭到DDoS攻擊

【8月3日】

內容置換7-11櫃臺後方數位看板的內容遭置換，刑事局調查指出是遭駭客入侵

內容置換臺鐵新左營車站電子看板疑遭駭客入侵，出現簡體中文恐嚇訊息

DDoS攻擊國防部8月3日網站遭到DDoS攻擊

假訊息自稱是APT27的駭客組織宣稱將對臺灣發動特別網路攻擊行動

假訊息中國媒體謊稱臺灣已殉職的空軍飛官開F16戰機投靠中國

分散式阻斷服務（DDoS）攻擊、內容置換（Deface），以及幾可亂真的假訊息等。

資料來源：iThome 2022-08-12 新聞

資通安全實地稽核項目

策略面 26/115

1.核心業務及其重要性

2.資通安全政策及推動組織

3.資安專責人力及經費配置

管理面 32/115

4.資訊及資通系統盤點及風險評估

5.資通系統或服務委外辦理之管理

6.資安維護計畫與實施情形

技術面 57/115

7.資通安全防護及控制措施

8.資通系統發展及維護安全

9.資通安全事件通報應變

資通系統防護基準(構面)

核心資通系統作業


資料備份、系統備援、
復原才迅速。
備份頻率長短，決定
資料復原時間點RPO
應訂定MTPD
最大可容忍中斷時間
業務持續運作演練，
系統復原時間RTO

貳、高教深耕計畫

申請資格：各公私立大專校院（含國防醫學院）皆可申請主冊計畫；專輔學校、宗教研修學院除外

額外爭取
資安專章
總經費1.5
億

資料來源：高等教育深耕計畫網站

貳、主冊專章：資安強化

為協助大學建立持續性與永續性的教研環境，不因資安事件受影響而中斷教學與研究，爰規劃**資安強化專章**，大學可**參照資通安全管理法及其子法要求，推動資通安全管理，以資通安全責任等級分級辦法就管理面、技術面及認知與訓練面**研提規劃推動之策略及擬定相關績效指標。

參、撰寫建議

- 參考數位發展部資通安全署「資通安全維護計畫範本」
- 訂定資安強化的各項指標(KPI)
- 建立相關參考文件(例如:程序書或表單)

參、撰寫建議-績效指標(1/2)

- **資安強化(績效指標)**提供參考之績效指標(A1~A4)

A1: 全校導入資訊安全管理系統（ISMS）

- K1.資通安全長之配置
- K2.資通安全推動組織
- K3.資通系統及資訊之盤點
- K4.資通安全風險評估
- K5.內部資通安全稽核及委外稽核
- K6.業務持續運作演練
- K7.資訊安全管理系統(ISMS)適用範圍

A2:強化學校人員資通安全認知與訓練

- K1.配置資通安全專職人員
- K2.提升資通安全專職人員資安職能
- K3.提升教職員資安意識

參、撰寫建議-績效指標(2/2)

- **資安強化(績效指標)**提供參考之績效指標(A1~A4)

A3:確保資通系統管理量能

- K1.資通系統集中化管理
- K2.適度降低資通系統數量

A4:落實管理危害國家資通安全產品

- K1.禁止公務使用大陸廠牌資通訊產品
- K2.限制出租場域使用大陸廠牌資通訊產品

參、撰寫建議-內容

- 計畫書內容

1.計畫推動策略(可就**全校導入資訊安全管理系統(ISMS)、強化學校人員資通安全認知與訓練、確保資通系統管理量能、落實管理危害國家資通安全產品**等面向**自行調整或增列**)

2.五年(112年至116年)總體目標

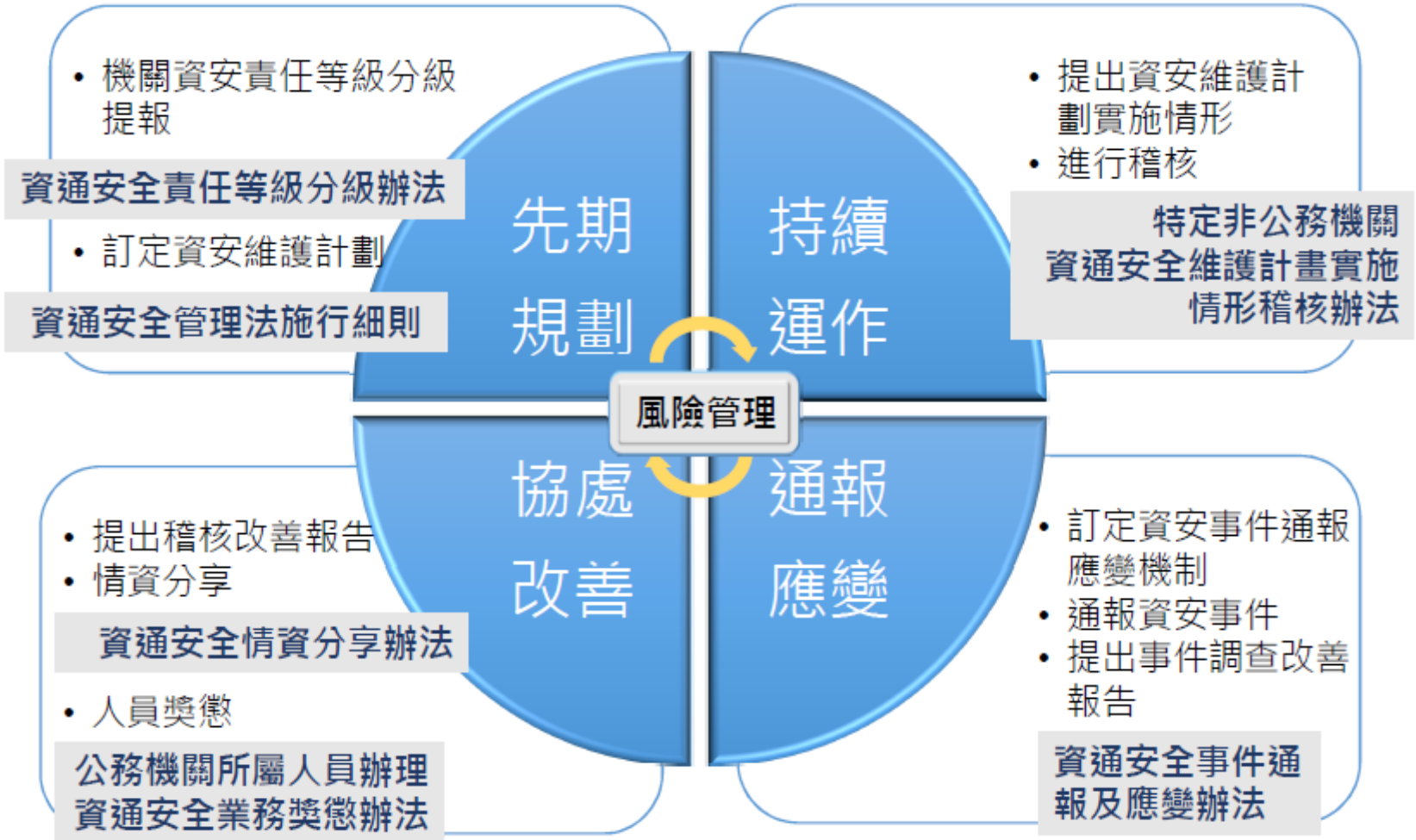
3.各年度(112年至116年)目標值

4.經費規劃

大綱

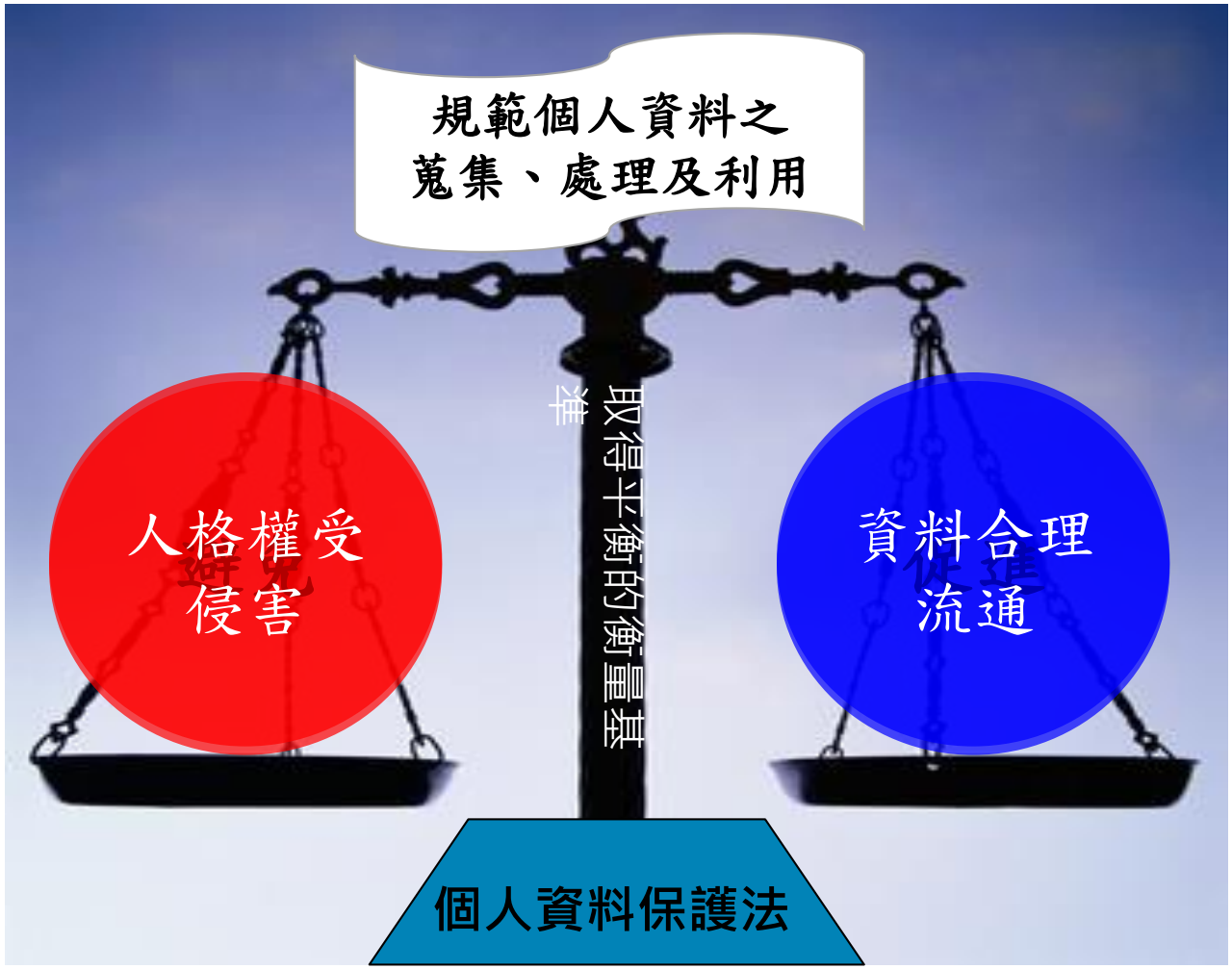
前言	資安與個資事件的趨勢
題一	校園資安現況與推動重點
題二	資安與高教深耕
題三	結合保護個資的資通安全防護的推動
最終	結語

資通安全管理法之體系


先期規劃
持續運作
協處改善
通報應變
風險管理
• 機關資安責任等級分級提報
資通安全責任等級分級辦法
• 訂定資安維護計劃
資通安全管理法施行細則
• 提出資安維護計劃實施情形
• 進行稽核
特定非公務機關資通安全維護計畫實施情形稽核辦法
• 提出稽核改善報告
• 情資分享
資通安全情資分享辦法
• 人員獎懲
公務機關所屬人員辦理資通安全業務獎懲辦法
• 訂定資安事件通報應變機制
• 通報資安事件
• 提出事件調查改善報告
資通安全事件通報及應變辦法

資通安全管理法之作業建議

個人資料保護法之立法目的(共56條;細則33條)



--個人資料蒐集與利用的基礎概念--

個資保護 ✚ **V.S** **隱私保障**

{111年8月12日大法官釋憲]

個人健康保險資料依法提供公務機關、學術研究機構從事醫療或衛生目的的統計分析與研究，是國家醫療與衛生政策形成非常關鍵且重要的基礎，但資訊隱私權的保障也是自由民主憲政秩序的核心價值，兩者兼籌並顧是所有大法官毫無懸念的共識

--個人資料蒐集與利用的關鍵概念--

目的 ＋ **必要**

基礎關係
(法律要件)

個人資料，無所不在

電信/網路
服務提供業者

帳單地址
電子郵件信箱
帳戶資料

開立帳戶資料
保單資料
貸款徵信資料
會員資料
周年慶抽獎券

銀行/證券/保險公司
百貨公司/大賣場

信用卡資料
客戶資料
宅配地址
教育程度

線上購物/ 網拍
社群網站

身分證號碼
結婚登記
報稅資料
駕照申請/換發

監理/ 戶政
財稅等政府單位

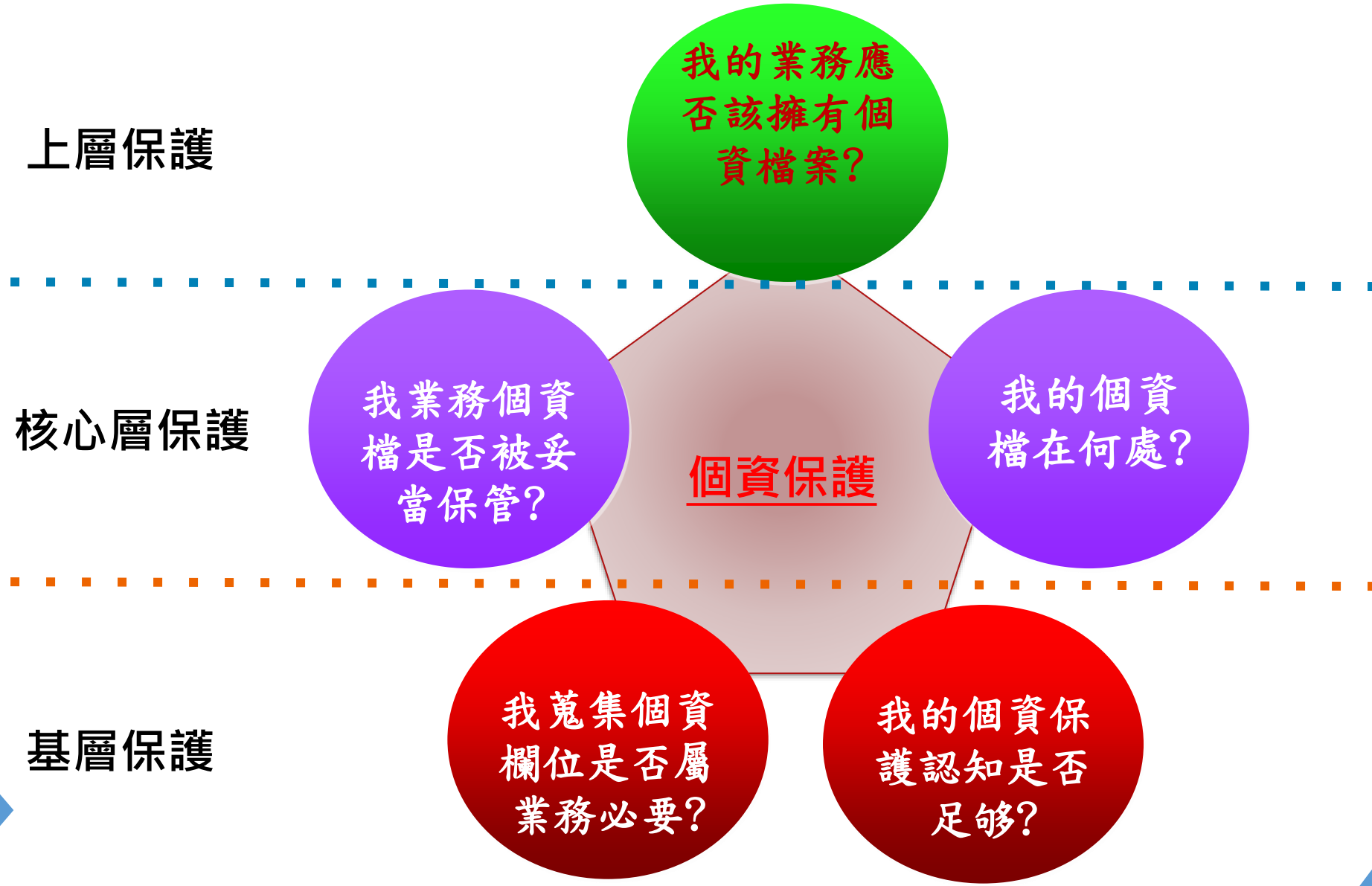
健檢報告
病歷資料
診斷書

醫院 / 診所
健康檢查中心

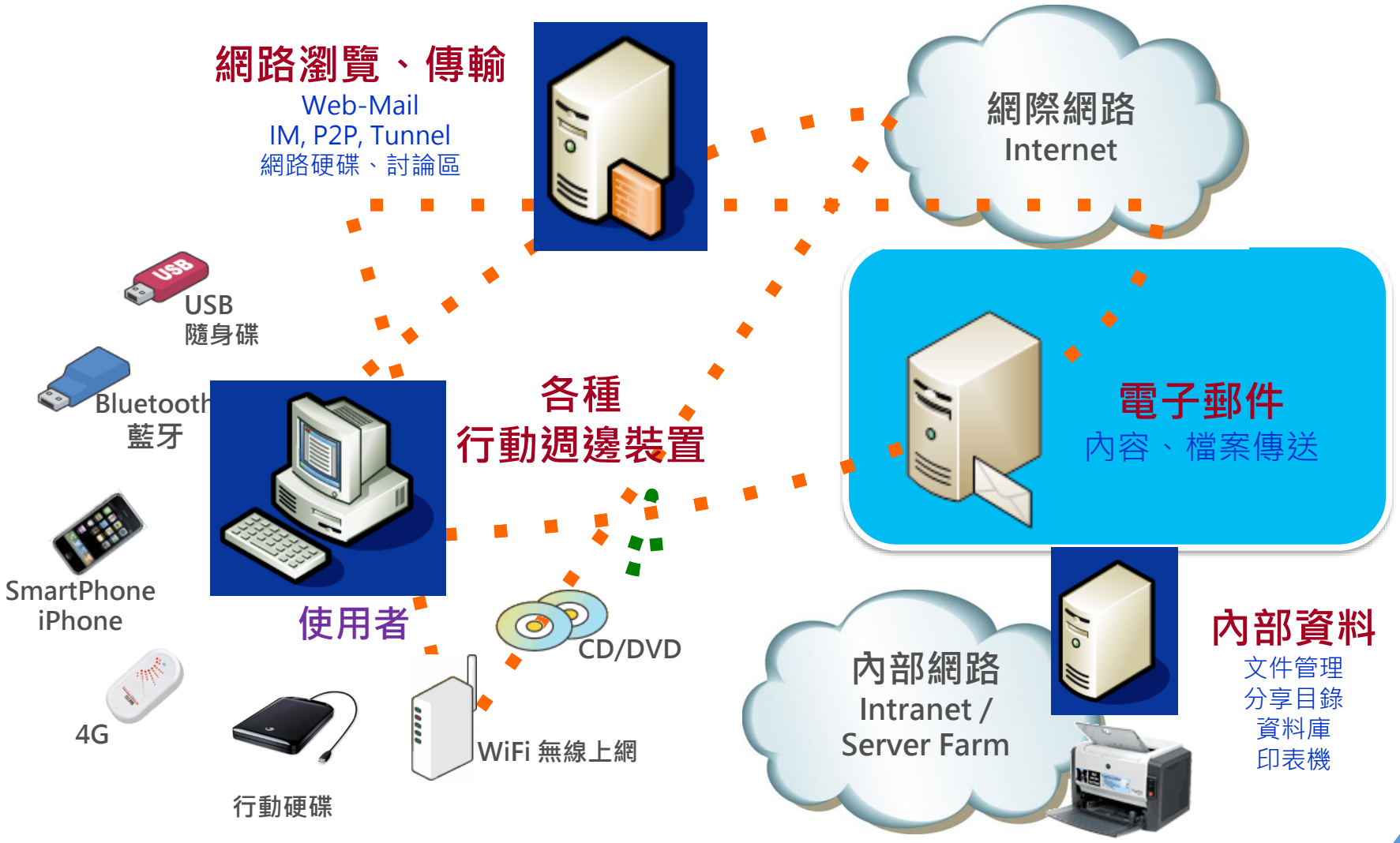
學籍資料
人事資料
註冊/報名資料
家長會聯絡

學校 / 補習班
社區活動中心

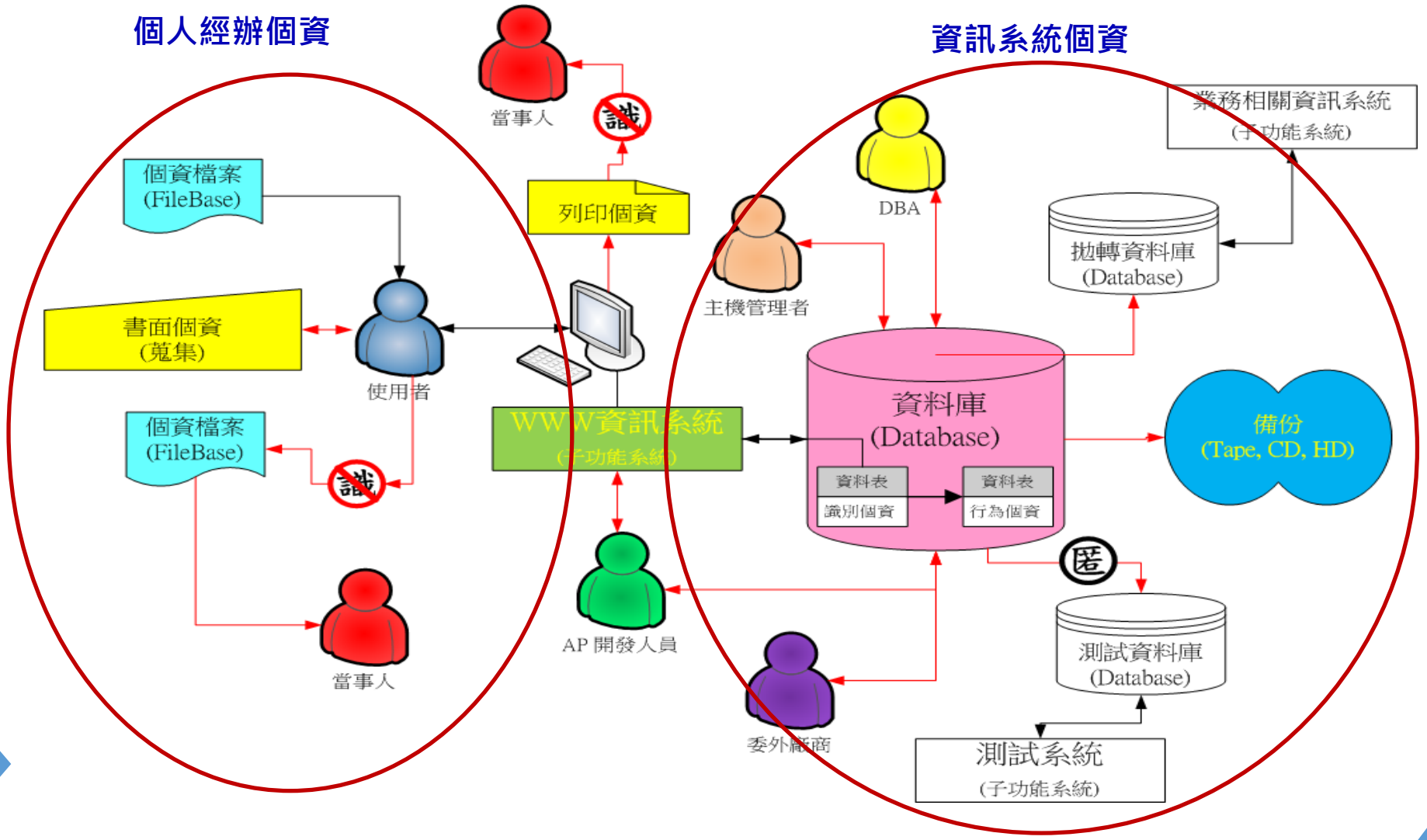
個資保護之五問


上層保護
核心層保護
基層保護
我的業務應否該擁有個資檔案?
我業務個資檔是否被妥當保管?
我的個資檔在何處?
個資保護
我蒐集個資欄位是否屬業務必要?
我的個資保護認知是否足夠?

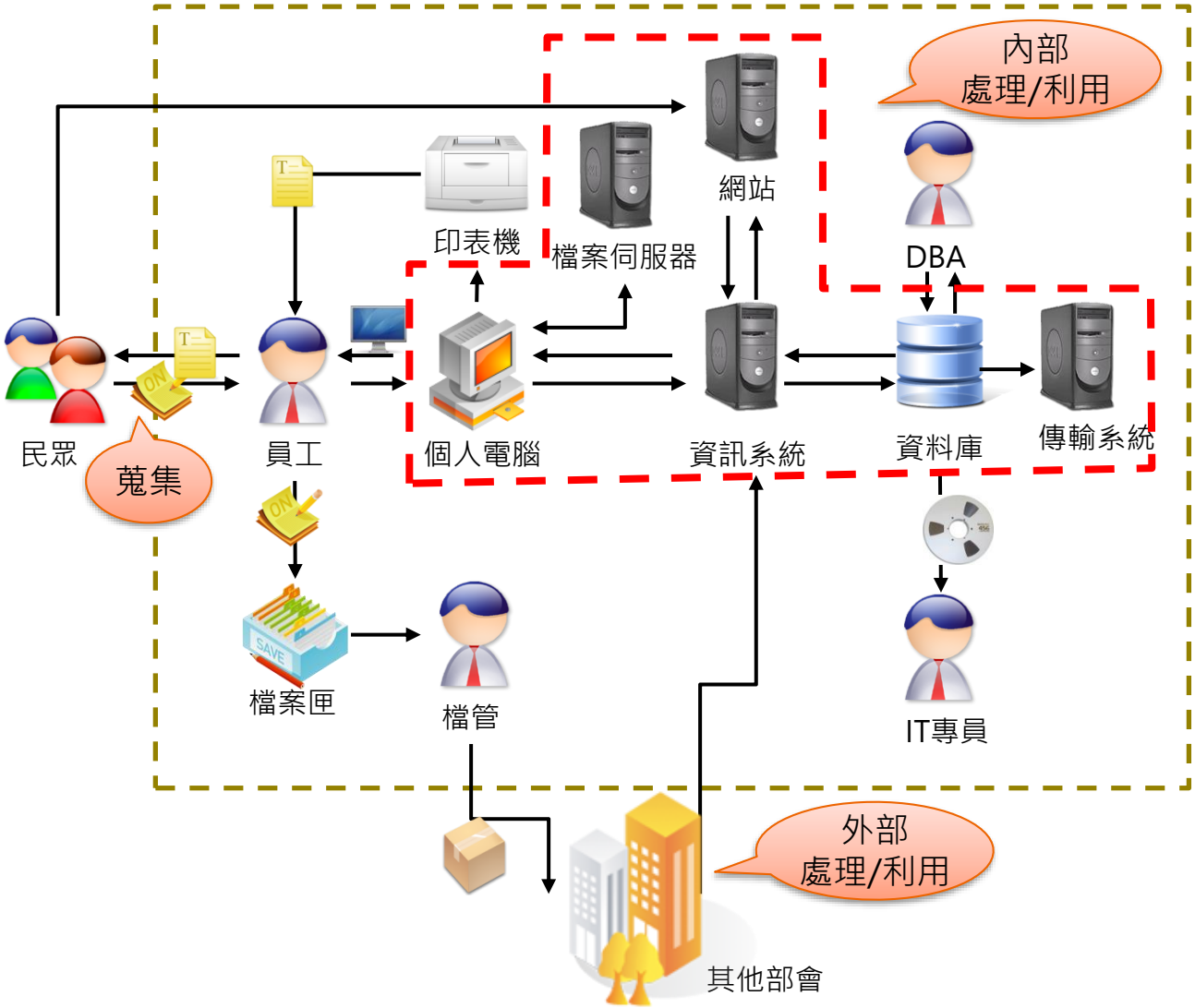
承辦人個人資料可能外洩管道風險



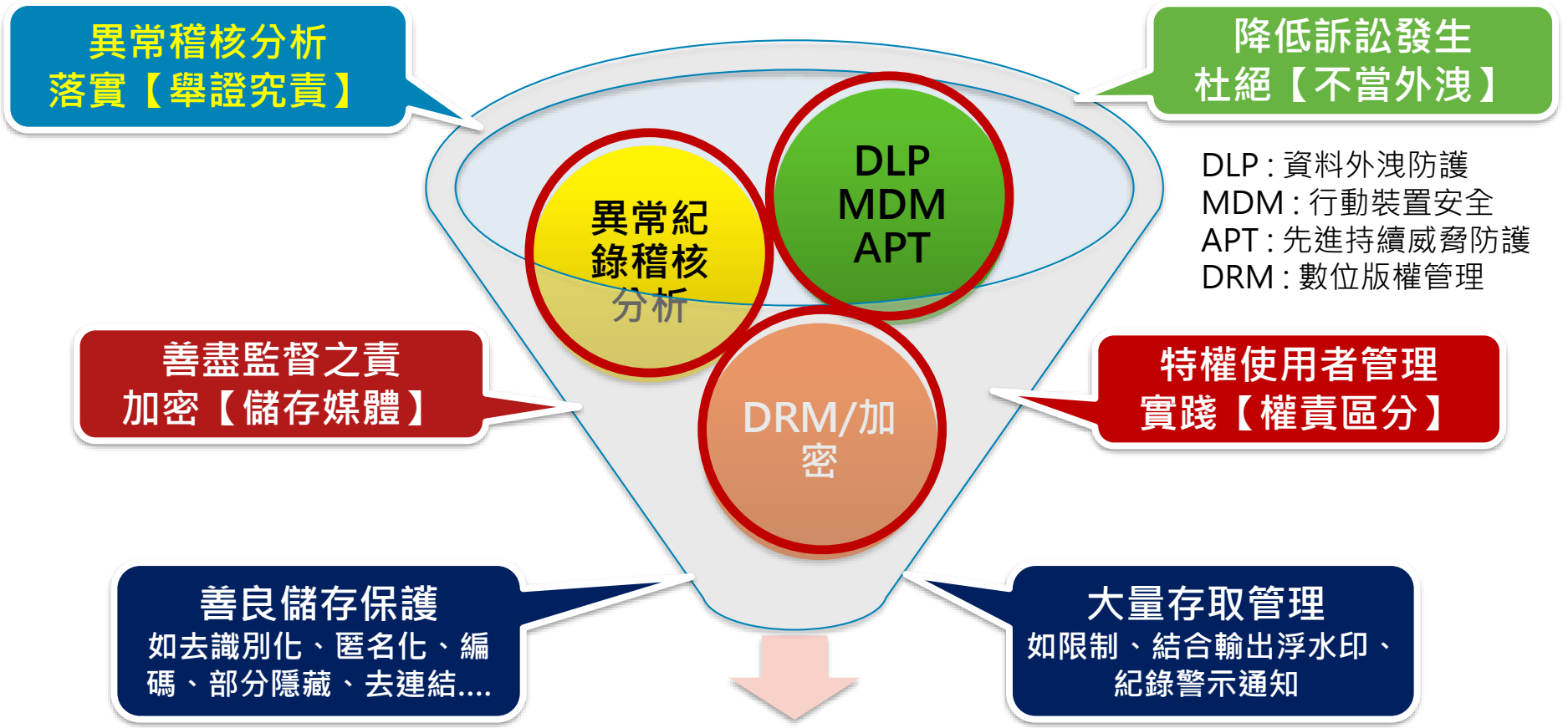
承辦人個人資料儲存位置



系統個人資料可能外洩管道風險



個資檔案安控的預防因應之道



預防損害發生

資料蒐集、處理、利用之自我檢查五步驟

步驟一：清點所有之個人資料

步驟二：清查蒐集個人資料之途徑與方式

步驟三：確認是否須履行告知義務並建立告知機制

步驟四：確認蒐集、處理、利用之特定目的

步驟五：檢視利用的範圍與方式

ISMS/PIMS規範導入事項比較

大綱

前言	資安與個資事件的趨勢
題一	校園資安現況與推動重點
題二	資安與高教深耕
題三	結合保護個資的資通安全防護的推動
最終	結語

推動資安建議(1)

資安長角色 ✚ 全信任

- 掌握學校重要資訊資產及核心系統的運作
- 檢視資安稽的落實及改善
- 定期審視資安團隊呈報的檢核結果
- 確保資安事件的通報順暢與
- 籌組具資安應變處理能力的團隊並演練

推動資安建議(2)

資安人員 ✚ 可信任

- 所規劃各項資安之事前、事中、事後工作皆有負責人員
- 訓練人人皆具備資安基礎認知，建立上網通行執照機制
- 確保具處理資安事件實務能力的行政及技術團隊，並定期進行模擬演練
- 建立資安工作的獎勵機制

推動資安建議(3)

資安運作環境 ＋ 零信任

- 隨時保持資安監測機制的正常、最佳運作
- 需有人力定期持續性的進行檢視、解讀所蒐集到的資安資訊
- 具備資安技術處置、諮詢的支援團隊
- 建立應變的處置能力
- 防護監控應內、外部兼顧，縱、橫向兼備
- 建立介於全信任及零信任，可信任之上網機制

結語-面對資安與個資保護應有作為

1. 個人資料保護及資通安全目前皆為法律規定，思考如何符合法遵，以善良管理之責。
2. 依個資法第27條規定，採行適當**安全措施**，訂定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，並指定**專人**辦理負責。(細則§12§25)
3. 依資通安全管理法之機構資安責任等級，提報資安維護計畫及實施情形(§17)，並建構資安推動組織及指派**專責人力**。
4. 認知相關標準：ISO27001、27700、CNS29100、29191
5. 定期辦理個資法教育訓練與宣導，提高員工個資保護意識。

結語

- 資通安全及個資保護是共生，且非僅是技術問題，需各單位人員協同參與才是落實有效防護及保護。
- 集中之資通系統係為減輕人力作業負荷、簡化管理工作，而非免責，故責任仍需由“**各單位負責**”，並在共同合作、分工的原則下進行相關管理維運。
- 將“資安防護與個資保護融入業務”，於規劃辦理各業務時應納入“資安防護與個資保護”的思維，方能提供符合安全法規規範之服務，同時需有成本及風險管理概念，並落實融入組織文化。
- 提供資通系統服務的便利性時應落實的資安防護及個資保護，以成就業務推動的「臨門一腳」。
- 科技始終來自人性，**資安則在挑戰、考驗人性**。

Q & A ?

Thank You!

參、撰寫建議-A1全校導入資訊安全管理系統(ISMS)

次要項目	KPI (可依需求自行另訂量化指標)	備註
K1.資通安全長之配置	學校置資通安全長，指派**主任秘書以上人員**兼任。	可參考「資通安全維護計畫書」範本，「伍、資通安全推動組織一、資通安全長」
K2.資通安全推動組織	學校資通安全推動組織由資通安全長召集全校各單位（包含行政單位及系所辦公室）主管或副主管組成，**每年至少召開會議1次**。	可參考「資通安全維護計畫書」範本，「伍、資通安全推動組織二、資通安全推動小組」
K7.資訊安全管理系統(ISMS)適用範圍	ISMS適用範圍至少**包含全校範圍**內之核心資通系統、保有個資或防護需求中等級以上之資通系統，及其相關網路與資訊機房活動。	可參考「資通安全維護計畫書」範本，「貳、適用範圍」

參、撰寫建議-A1全校導入資訊安全管理系統(ISMS)

次要項目	KPI (可依需求自行另訂量化指標)	備註
K3.資通系統及資訊之盤點	學校辦理資通系統及資訊之盤點，**盤點範圍包含全校各單位。** 1.資通系統資產清冊至少包含落於**各校IP網段內、或使用各校網域名稱**之資通系統。 2.**物聯網設備管理清冊**包含學校採購、公務使用之物聯網設備。	可參考「資通安全維護計畫書」範本，「柒、資訊及資通系統之盤點 一、資訊及資通系統盤點」
K4.資通安全風險評估	分析全校資訊資產及個人資料檔案可能面臨的風險，並**選取適當安控措施**。	可參考「資通安全維護計畫書」範本，「捌、資通安全風險評估」

參、撰寫建議-A1全校導入資訊安全管理系統(ISMS)

次要項目	KPI (可依需求自行另訂量化指標)	備註
K5.內部資通安全稽核及委外稽核	1.學校辦理**內部資通安全稽核**，稽核範圍包含全校各單位。 2.內部資通安全稽核結果需提報**管理審查**。 3.學校**定期稽核委外服務供應商**，以確保資訊作業委外安全。	可參考「資通安全維護計畫書」範本，「壹拾伍、資通安全維護計畫及實施情形之持續精進及績效管理機制」
K6.業務持續運作演練	1.針對核心資通系統制定**業務持續運作計畫**，並定期辦理全部核心資通系統之**業務持續運作演練**。 2.將行政單位、系所網頁遭竄改納入業務持續運作演練情境。	可參考「資通安全維護計畫書」範本，「玖、資通安全防護及控制措施 五、業務持續運作演練」

參、撰寫建議-A2強化學校人員資通安全認知與訓練

次要項目	KPI (可依需求自行另訂量化指標)	備註
K1.配置資通安全專職人員	資通安全專職人員指**全職執行**資通安全業務者，並依其專業技能給予適當薪資。	可參考「資通安全維護計畫書」範本，「陸、專職(責)人力及經費配置」
K2.提升資通安全專職人員資安職能	1.資通安全**專職人員**各自持有**1張以上資通安全專業證照，及1張資通安全職能訓練證書**或通過教育體系資通安全專業課程評量。 2.資通安全**專責人員以外之資訊人員，每2年完成3小時以上資通安全專業課程教育訓練**。	可參考「資通安全維護計畫書」範本，「陸、專職(責)人力及經費配置」
K3.提升教職員資安意識	全校教職員**每年完成3小時**以上資通安全通識教育訓練。	可參考「資通安全維護計畫書」範本，「壹拾參、資通安全教育訓練」

參、撰寫建議-A3確保資通系統管理量能

次要項目	KPI (可依需求自行另訂量化指標)	備註
K1.資通系統集中化管理	資通系統資安管理作業，**原則集中至學校資訊(安)單位或其他具備資通安全專業能力之團隊統籌辦理**，並因應集中化管理需求增聘適當人力。	可參考「資通安全維護計畫書」範本，「玖、資通安全防護及控制措施 〇(新增)、確保資通系統管理量能」
K2.適度降低資通系統數量	**汰換、整併校內資通系統網站，以降低資通系統數量**。加強閒置網站（指使用率不高者）及因應臨時需求建置網站（如活動專用網站）之資安管理措施，依其專案需求下架或限制存取	可參考「資通安全維護計畫書」範本，「玖、資通安全防護及控制措施 〇(新增)、確保資通系統管理量能」

參、撰寫建議-A4落實管理危害國家資通安全產品

次要項目	KPI (可依需求自行另訂量化指標)	備註
K1.禁止公務使用大陸廠牌資通訊產品	依行政院政策要求，公務用之資通訊產品（含軟體、硬體及服務）**不得使用大陸廠牌**，已列管者儘速汰換。	可參考「資通安全維護計畫書」範本，「玖、資通安全防護及控制措施 ○(新增)、落實管理危害國家資通安全產品」加入資安具體策略及措施項目
K2.限制出租場域使用大陸廠牌資通訊產品	依行政院政策要求，針對學校出租場域，於學校**委外契約或場地租借使用規定，明訂不得使用危害國家資安之產品**（如大陸廠牌軟體、硬體及服務）。	可參考「資通安全維護計畫書」範本，「玖、資通安全防護及控制措施 ○(新增)、落實管理危害國家資通安全產品」加入資安具體策略及措施項目