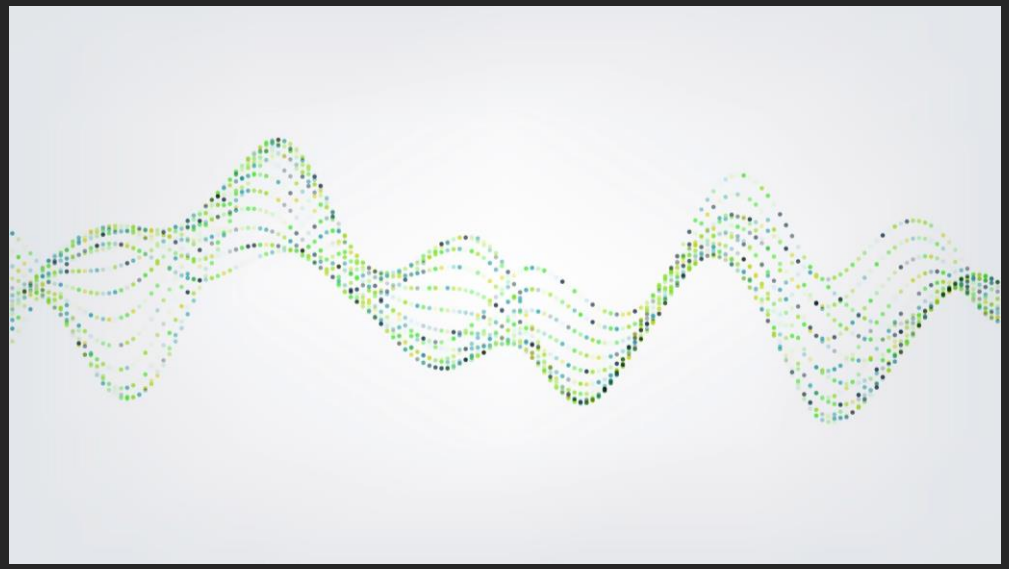
學校網管人員
資安教育訓練



推動中小學數位學習精進方案--113年嘉義縣中小學教師增能研習

研習內容綱要

- 關於資安這件事
- 資安管理
- 資安管理業務
- 專題分享：嘉義縣教育網路資安監控(SOC)服務
- 問題與討論

講到資安這件事.....

資安是什麼？如何管理？

病毒？

駭客？

防毒軟體？

防火牆？

木馬？

網攻？

限制上網？

入侵？

資安＝資通安全

- 資訊：資訊是具有價值的資產，可能是書寫或列印於紙上、儲存在電子儲存媒體上、以郵寄或電子儲存傳輸、顯示於影片上或在對話中說出，需要受到適當的保護。
- 資安：保障資訊資產免於「不可承受的風險」，包括
  - 機密性(Confidentiality)

    確保只有經授權的人 保只有經授權的人，方能存取資訊資產。
  - 完整性(Integrity)

    確保資訊資產的內容及處理方法都是正確而且完整的。
  - 可用性(Availability)

    確保經授權的使用者在需要時能夠存取資訊資產。

校園資安

- 在有限的人力、經費成本負擔下，將可能造成學校資訊相關硬體、軟體、資料損失的風險降至可接受的程度，以保護師生避免遭受損害。

風險控制

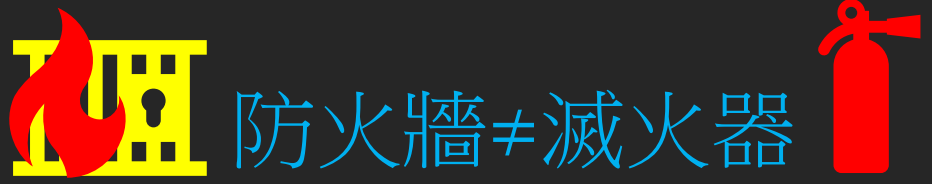
問題

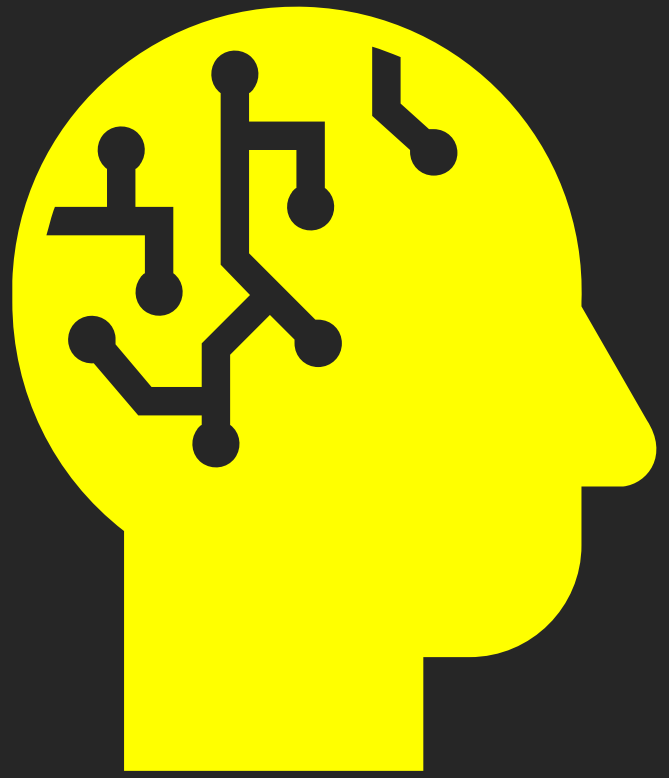
- 學校因為缺少經費購買功能完善的防火牆設備，以致於不斷發生資安事件。
- 學校因為推動數位學習，各種可上網的載具設備不斷增加且管理不易，以致於資安事件隨之大幅成長。
- 都會縣市學校及國立高中、大學因為人力及經費較為充裕，資安設備也較先進，因此資安防護比偏鄉縣市學校做得更好。

從實際的經驗中我們發現．．．

風險控制造成的風險

- 過度的防護措施以致使用不便—後門大開
- 複雜的資安設備但是無人監管—漏洞百出
- 嚴格的管理要求造成無法應變—業務停頓
- 繁雜的控管程序拖累工作進度—效率低落





當『加法』
無法解決問題

試試『減法』吧

我們的『減法』策略

- 集中管理
- 有效識別
- 開放原則
- 柔性防護
- 事件追蹤
- 動態清零

100%治療重於100%預防

資安管理

- 依據：資通安全管理法及其子法
- 主管機關：
  行政院（數位發展部／資通安全署）
- 適用範圍：
  公務機關(公立學校屬之)、特定非公務機關(如電信業者)

資安法規定要項

- 第7條：劃分資安責任等級（Ａ~E五級，由行政院核定）
- 第10條：訂定、修正及實施資通安全維護計畫（公立學校均需要）
- 第11條：設資安長並由副首長兼任（未設副校長者由教務／導主任兼任）
- 第12條：每年提報資通安全維護計畫實施情形
- 第13條：辦理資通安全維護計畫實施情形稽核
- 第14條：資通安全事件通報及應變處理

資通安全責任等級分級辦法

- 第 6 條
  - 各機關維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 C 級。
  - 前項所定自行或委外設置之資通系統，指具權限區分及管理功能之資通系統。
- 第 7 條
  - 各機關自行辦理資通業務，未維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 D 級。

*學校是否維運資通系統為劃分C、D等級分級之要件

資安責任等級『C』級之應辦事項

附表五　資通安全責任等級C級之公務機關應辦事項修正規定

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級；其後應每年至少檢視一次資通系統分級妥適性；並應於初次受核定或等級變更後之二年內，完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人；須以專職人員配置之。
	內部資通安全稽核		每二年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
技術面	資通安全弱點通報機制		一、初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。
	資通安全防護	防毒軟體 網路防火牆	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		具有郵件伺服器者，應備電子郵件過濾機制	
認知與訓練	資通安全教育訓練	資通安全專職人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照及職能訓練證書		初次受核定或等級變更後之一年內，至少一名資通安全專職人員，分別持有證照及證書各一張以上，並持續維持證照及證書之有效性。

資安責任等級『D』級之應辦事項

附表七　資通安全責任等級D級之各機關應辦事項修正規定

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
認知與訓練	資通安全教育訓練	一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。

*教育部自113年起將各校網管人員接受資安教育訓練情形納入一般性補助考核項目
*各校使用者應接受三小時以上資安通識教育訓練~~自行辦理

資通安全維護計畫

- ✓Plan：擬訂/修訂(#10)
- ✓Do：提報實施情形(#12)
- ?Check：接受上級(外部)稽核(#13-1)
- ?Act：提出缺失改善報告(#13-2)

＊請依縣府(綜合規劃處資訊管理科)函文規定辦理

資安通報與應變

- 教育機構資安通報平台：https://info.cert.tanet.edu.tw
- 分為：『告知通報』(聯絡人會收到告知簡訊&Email)及『自行通報』(自行發現)二類*(另有『資安預警』事件)*
- 每年執行『告知通報演練』
  - *第一、第二聯絡人負責接收告知簡訊*
  - *第五聯絡人負責至平台填寫通報單*

請唯一支持

依縣網中心
通知處理

資安事件實務處理

- 技術面：配合縣網中心處理
  - 威脅緩解
  - 來源追蹤(事不過三原則)
  - 問題排除
  - 檢視改善
- 行政面：依相關法規

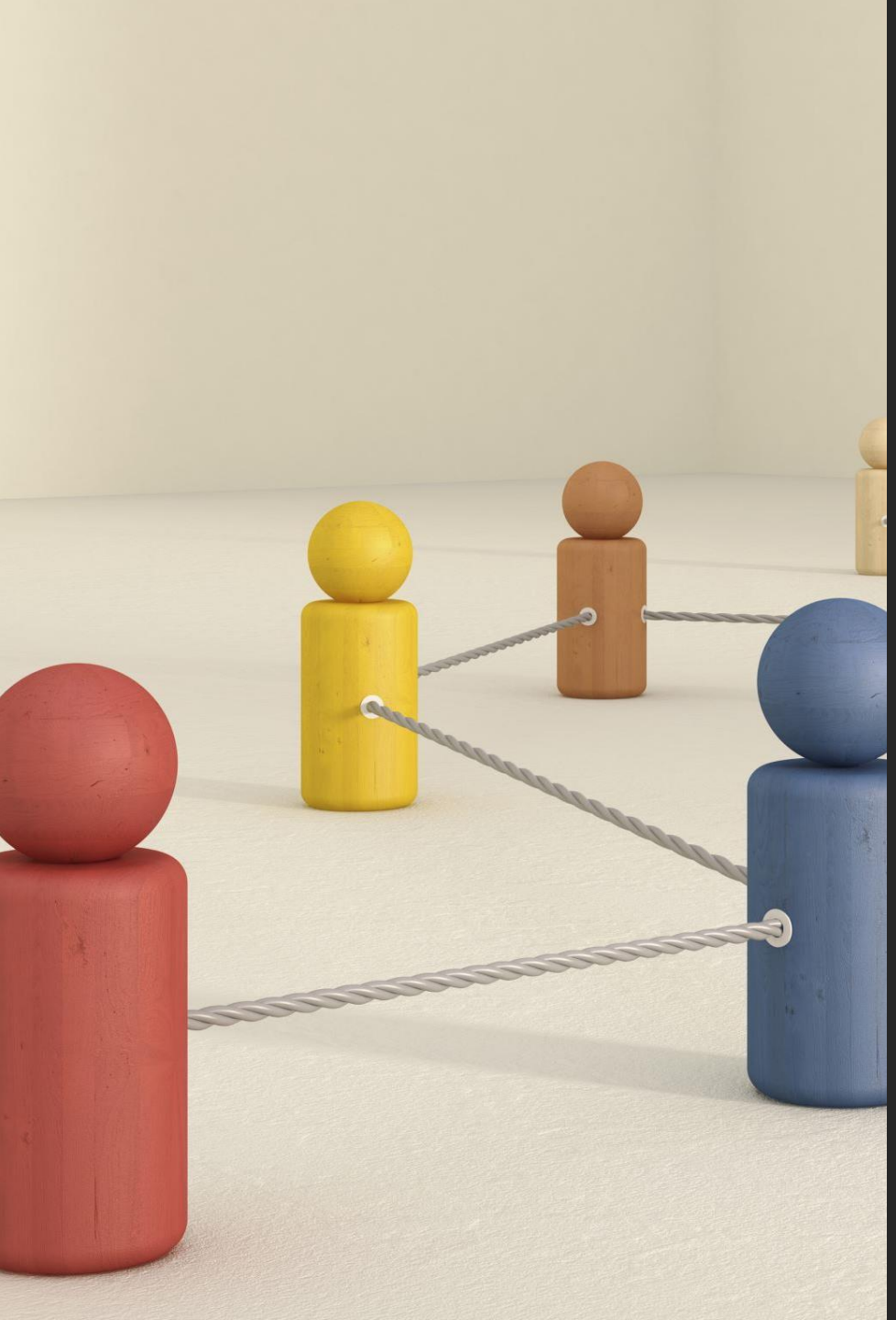
  行政通報

  校安通報

  刑／民訴案件處理

  檢／調查案件回應

  ……



其他

沒有絕對的安全，只有尚可接受的風險