長庚科技大學

112年資訊安全宣導教育訓練

（資訊安全暨智慧財產權）

漢昕科技
左寧生 Ningsheng Tzuo

諮詢 輔導 訓練 稽核 .永續營運

講師簡介— 左寧生 Ningsheng Tzuo

- **證照**
  - Information Security Management Systems (ISMS) Auditor / Lead Auditor (in Accordance with ISO 27001:2022)
  - 個人資料管理系統主導稽核員認證(BS 10012)
- **經歷**
  - 國防部通資次長室 資訊安全官
  - 教育部資訊及科技教育司 資訊安全專責人員
  - 漢昕科技股份有限公司 管理顧問處 顧問
- **輔導實績**
  - 衛福部疾病管制署\新竹縣政府\私立長庚科技大學\台灣自來水公司\新北市立圖書館\國家衛生研究院\新竹縣警察局

教育訓練的目的?

- 對資訊安全應有之認知
- 瞭解長庚科技大學資訊安全政策及相關規範，並落實遵行
- 瞭解資訊安全重要性與威脅，及其保護的措施與方法
- 瞭解智慧財產權保護規範

資訊安全概念 ***

- 有效的防止資訊遭到竊取、竄改、毀損、滅失或遺漏。簡言之，就是確保資訊的機密性、完整性、可用性，並遵循法規要求：
  - 機密性(Confidentiality)：保護資訊不被非法存取或揭露。
    - 如果資料遭非法存取或揭露，可能造成單位聲譽損失，個人可能被處份。
  - 完整性(Integrity)：確保資訊在任何階段都沒有不適當的修改或損毀。
    - 如果資料損毀或不正確會影響業務的分析或決策。

資訊安全概念

- 可用性（Availability）：經授權的使用者能適時的存取所需資訊。
  - 如果資訊無法順利取得，會影響業務正常執行，例如：公文系統故障會影響公文製作。
- 法規遵循:
  - 例如遵守個人資料保護法、採購法規等。如果未能遵守，可能會有法律責任或處分。

一、資訊安全事件分享

二、使用者面臨之威脅

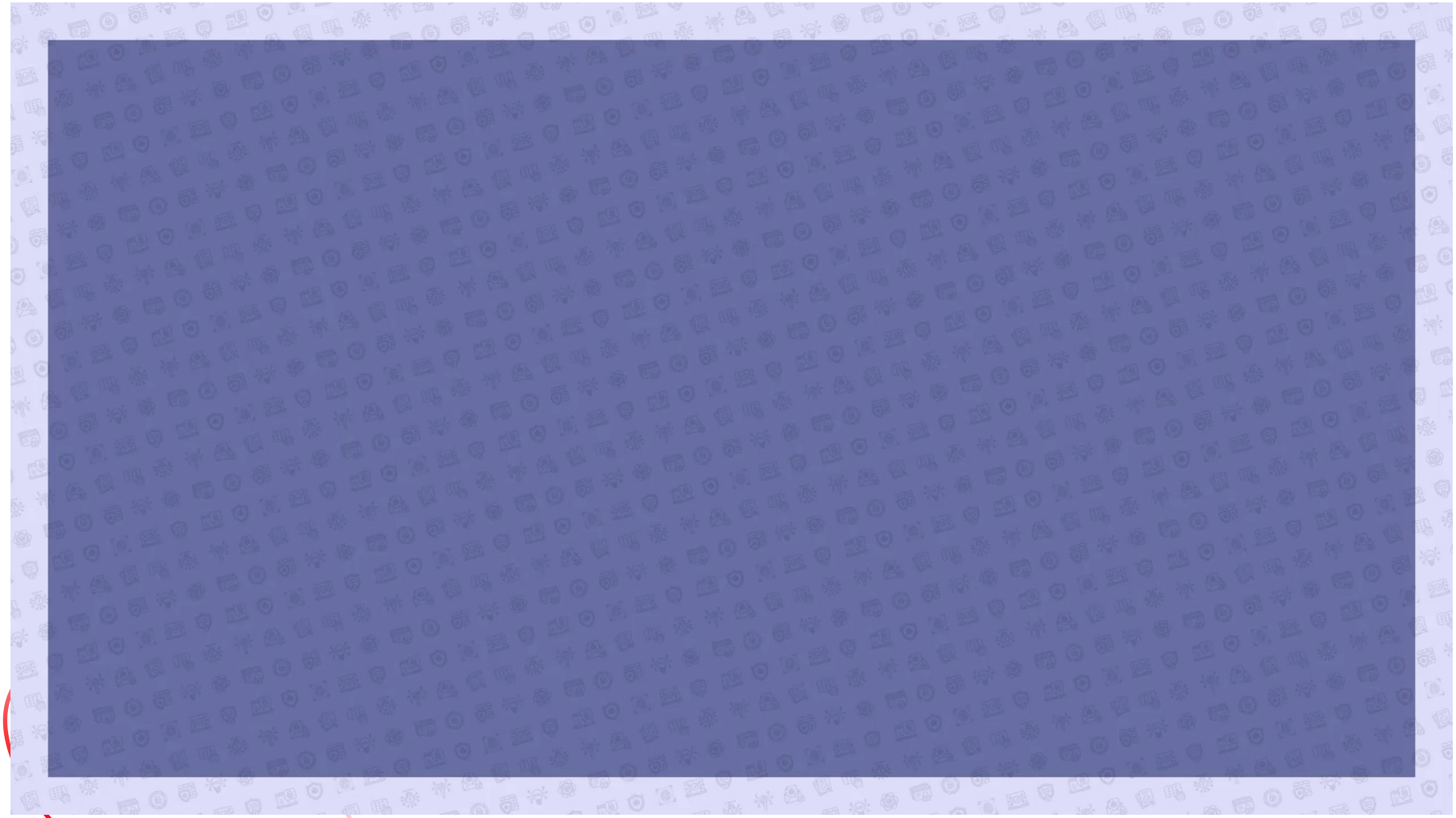
三、預防社交工程攻擊

四、個資管理與保護

五、長庚科技大學資安規範宣導

六、智慧財產權

真實的網路攻擊



台灣個資外洩嚴重,估1040萬手機號碼流出

一、資訊安全事件分享

二、使用者面臨之威脅

三、預防社交工程攻擊

四、個資管理與保護

五、長庚科技大學資安規範宣導

六、智慧財產權

使用者為什麼成為目標? ***

- 針對性竊取與蒐集檔案/文件
- 線上遊戲、網路購物及網路銀行等服務之有價財產
- 部落格或社群網站之帳號密碼
- 工作商業機密資料
- 跳板(殭屍電腦)
- 監控使用者行為
- 智慧型手機富含使用者個資(通訊錄、E-Mail等)

何謂惡意程式

- 指的是病毒、間諜軟體、蠕蟲等

- 惡意程式的設計目的 ***
  - 竊取使用者電腦的資料
  - 破壞獨立的電腦或已連接網路的個人電腦
  - 作為駭客跳板(肉雞)發動攻擊

電腦病毒

- 病毒是一段電腦程式碼，它會嘗試將自身附加到主機程式，在電腦之間傳佈，可能會損壞您的軟體、硬體和檔案。
- 病毒可能會佔據一些系統的記憶空間，並尋找機會自行繁殖複製， 您電腦效能將會變得比一般正常的電腦慢。
- 使用瀏覽器來瀏覽含病毒的網頁， 可以強迫您的Windows不斷的開啟新視窗，直到系統資源被吃光。

電腦病毒

【娜妲病毒(PE_Nimda.a)】

- 對全球數十萬的企業網路及個人電腦造成嚴重影響，災情已經逐漸擴大。
- 中毒的電腦會大量散播電子郵件並夾帶名為Readme.exe(讀我)的檔案，造成網路頻寬的壅塞明顯發現網路速度變慢。
- 會自動發病毒信以及尋找網路上的芳鄰及微軟IIS網頁伺服器進行感染。

電腦蠕蟲

- 蠕蟲是一種惡意程式碼，可以自行大量複製，它可以透過電子郵件附件、文字訊息、檔案共用程式、社交網站、網路共用、可移除磁片磁碟機和軟體弱點來散佈。
- 可能竊取敏感性資訊、變更安全性設定、傳送資訊給惡意駭客、防止使用者存取檔案等惡意活動。

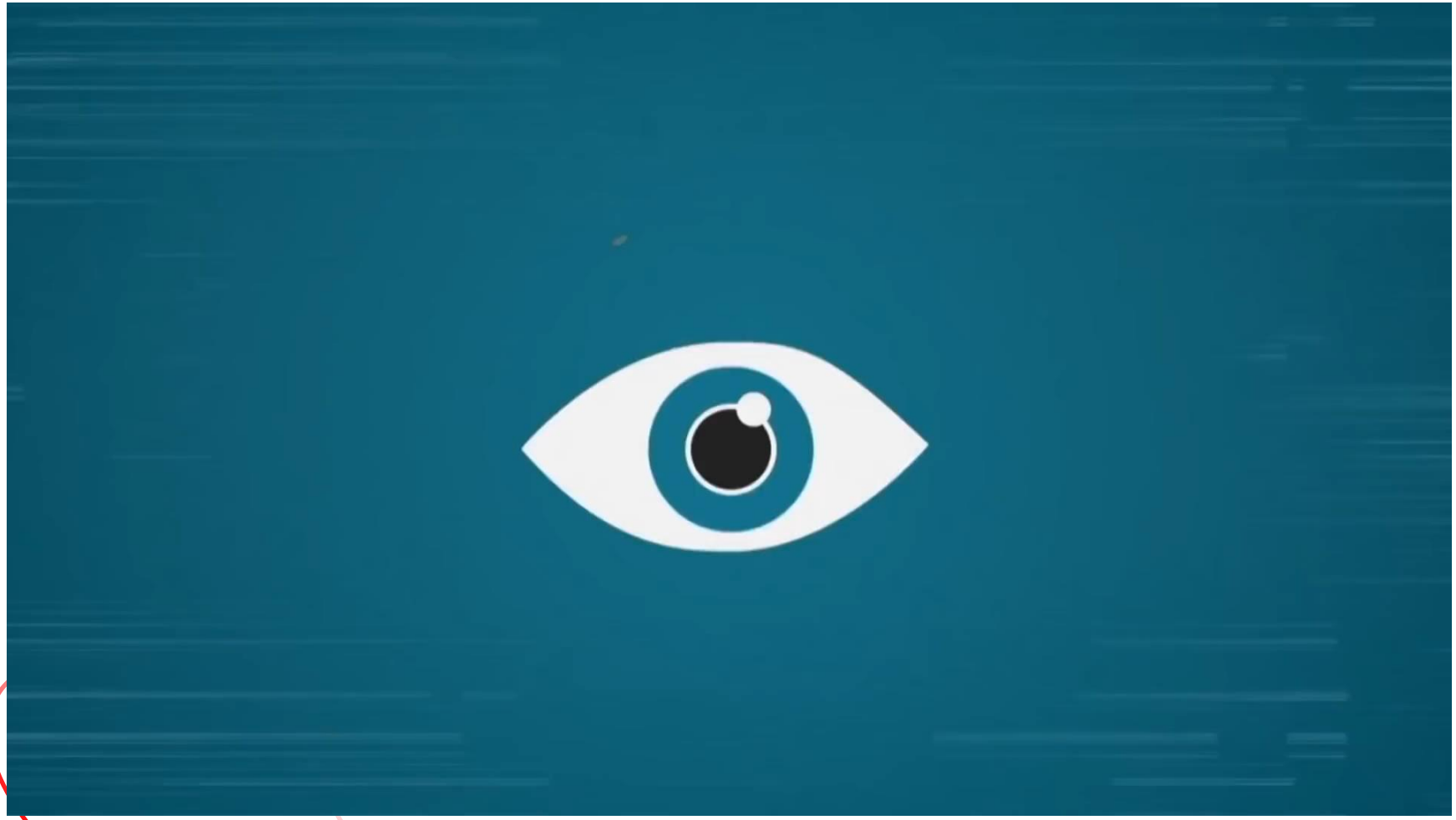
電腦蠕蟲

- 【蠕蟲程式Raspberry Robin】
- 主要針對使用西班牙語與葡萄牙語的組織而來，歐洲的金融和保險業者成為目標。
- 駭客使用包含惡意的Excel檔案，開啟後會濫用電腦上的程式庫，在受害電腦上運作。
- 駭客取得客戶資料，包含了客戶姓名、電話號碼、電子郵件信箱、住址、薪資、付款記錄等。

間諜軟體

- 透過造訪儲存空間與記憶體等系統資源來監控電腦或手機活動的惡意軟體，它會獲取訪問鍵盤、滑鼠和螢幕等系統資源，甚至可能會要求擁有相機和麥克風的權限，可以監看近乎所有在電腦或手機執行的操作，包含瀏覽網頁、線上交易、影片來源...等。

間諜軟體



勒索病毒

- 勒索軟體僅是單純地將受害者的電腦鎖起來，而另一種則系統性地加密受害者硬碟上的檔案。
- 勒索軟體通常透過木馬病毒的形式傳播，將自身為掩蓋為看似無害的檔案。
- 可能導致業務中斷，無法存取關鍵檔案。對企業而言意味著營業損失、作業延遲、無法出貨，甚至為了救回或重新製作被加密的檔案而損失大量生產力。


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
Chinese (traditional)
我的電腦出了什麼問題？
您的一些重要文件被我加密保存了。
照片、圖片、文檔、壓縮包、音頻、視頻文件、exe文件等，幾乎所有類型的文件都被加密了，因此不能正常打開。
這和一般文件損壞有本質上的區別。您大可在網上找找恢復文件的方法，我敢保證，沒有我們的解密服務，就算老天爺來了也不能恢復這些文檔。
有沒有恢復這些文檔的方法？
當然有可恢復的方法。只能通過我們的解密服務才能恢復。我以人格擔保，能夠提供安全有效的恢復服務。
但這是收費的，也不能無限期的推遲。
請點擊 <Decrypt> 按鈕，就可以免費恢復一些文檔。請您放心，我是絕不會騙你的。
但想要恢復全部文檔，需要付款點費用。
是否隨時都可以固定金額付款，就會恢復的嗎，當然不是，推遲付款時間越長對你不利。
最好3天之內付款費用，過了三天費用就會翻倍。
還有，一個禮拜之內未付款，將會永遠恢復不了。
對了，忘了告訴你，對半年以上沒錢付款的窮人，會有活動免費恢復，能否輪
Payment will be raised on
5/15/2017 23:41:55
Time Left
02:23:55:59
Your files will be lost on
5/19/2017 23:41:55
Time Left
06:23:55:59
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

十全果菜市場中勒索病毒 付1200美元贖金

惡意程式來源

1. 隨身碟
2. 電子郵件
3. 不良網站
4. 盜版程式
5. 被駭客入侵的網站
6. 系統萬年不更新
7. 免費、無加密的WiFi

傳播方式

- 通常電子郵件(E-mail)都會包含以下檔案類型來散播：
- *.EXE、*.COM：可執行檔
- *.ZIP、 *.RAR：壓縮檔
- *.PIF：Windows程式資訊檔
- *.SCR：螢幕保護程式檔
- *.DOC、 *.XLS、 *.PPS：Office檔
- *.VBA：Office巨集檔

水坑式攻擊

水坑式攻擊：
駭客攻擊特定群體(組織、企業、政府)會分爲三階段進行

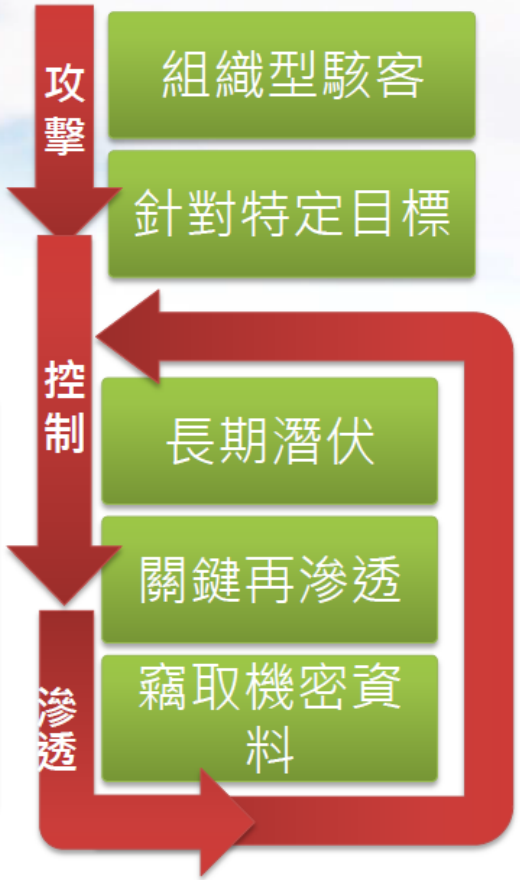
1.猜測目標群體經常瀏覽的網站
2.入侵網站並置入惡意程式
3.目標群體瀏覽網站後遭受感染

進階持續威脅
(Advanced Persistent Treat)

Advanced Persistent Threat

APT「進階持續性滲透攻擊」一詞最早出現在美國政府官方解密的報告當中，意指某些國家 (尤其是中國) 所造成的網路安全威脅和能力。

1. 透過郵件、網頁等企業無法封閉之管道滲透。
2. 客製化惡意程式，藏在常用文件類型中(Office、PDF)，逃避防毒軟體偵測。
3. 結合社交工程，針對特定目標進行攻擊。



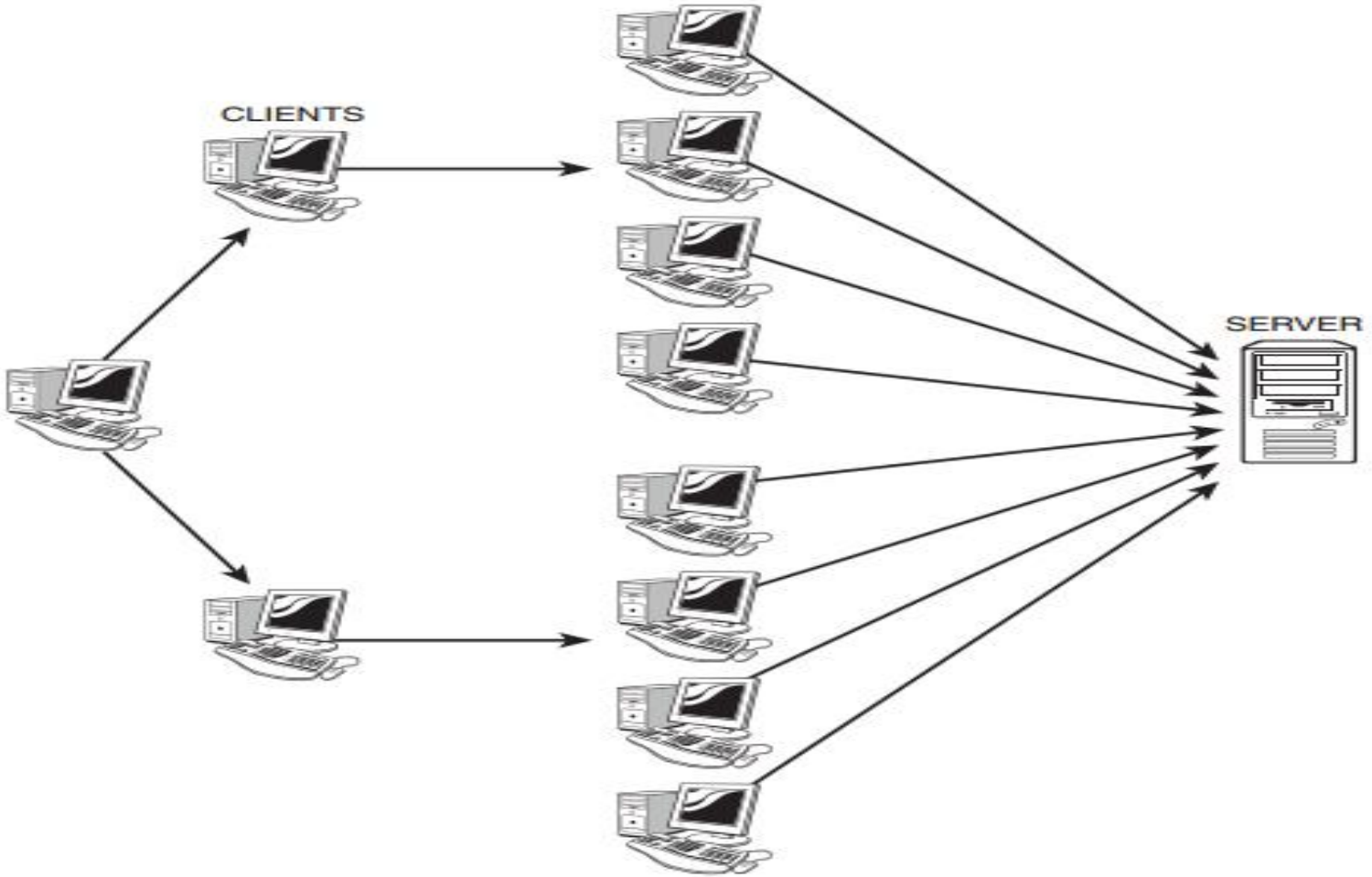
進階持續威脅


1 事前準備
2 初期入侵
4 情資探查
5 資料蒐集
1010100
1010101
WWW
IM
3 控制感染電腦
6 傳送機密資料回駭客電腦

DDOS攻擊

- 分斷式阻斷服務攻擊可分為二類：※※※
  - 頻寬耗盡型
    - 以消耗頻寬為目的，使正常使用者因頻寬耗盡而無法正常連線至系統。
  - 資源耗盡型
    - 以耗盡系統記憶體或處理器資源，阻擋目標系統處理合法資訊服務。
- 它們都是透過大量合法或偽造資訊服務請求，占用網路或系統資源，達到癱瘓網路或中斷資訊服務的目的。

DDOS攻擊



ChatGPT資安威脅

- 資安公司CyberArk Labs 針對 ChatGPT 所進行的一項研究，ChatGPT 可用於創建多種形態的惡意軟體，具有強大破壞能力，可以輕鬆規避資安防護。
- 經Check Point Research的團隊實際測試，發現透過ChatGPT以及基礎的指令系統，便可以生成以假亂真的釣魚郵件。
- 開放使用後，可能有不可預期的風險，尤其是員工誤將不該外流的資料放上ChatGPT，變成了訓練資料。

2022年資安風險

***


未來 1 年最可能發生的十大資安風險
勒索軟體最受關注，釣魚網站和 BEC 詐騙進入前五
勒索軟體資安事件 46.6%
駭客 40.6
社交工程手段 38
釣魚網站 36.5
商業郵件詐騙（BEC詐騙） 24.3
資安漏洞事件 24.3
網路犯罪者 22.4
以第三方為跳板的攻擊 16.1
資料外洩事件 15.4
行動應用的攻擊 12%
說明：百分比為自評該項未來1年極可能發生的企業比例
資料來源：2022 iThome CIO大調查，2022年8月

一、資訊安全事件分享

二、使用者面臨之威脅

三、預防社交工程攻擊

四、個資管理與保護

五、長庚科技大學資安規範宣導

六、智慧財產權

社交工程的定義

- 社交工程是一種利用人性的弱點及無知，透過欺騙、威脅，取得被害人的信任，讓被害人作出對自己有利的舉動。
- 常見的手法有透過電話、手機簡訊、即時通訊等管道，設計詐騙劇本，讓被害人主動的告知個人機密資訊或交付財物。

社交工程方式

- 早期社交工程是藉由電話或假扮身份問些看似無關緊要的問題等各種方法來獲取所需資訊。
- 透過電子郵件進行攻擊之常見手法
  - 假冒寄件者
  - 使用與業務相關或令人感興趣的郵件內容
  - 含有惡意程式的附件或連結
  - 利用應用程式之弱點(包括零時差攻擊)

誘人話題

- 常用手法
  - 通知民眾中獎、退稅等詐騙方式
  - 美女錯傳簡訊
  - 威脅恐嚇
- 人性
  - 貪心：撿便宜的個性
  - 好奇：探索八卦訊息的個性
  - 不在意：沒那麼倒楣吧的想法
  - 警覺力：無所謂後果的嚴重性
  - 恐懼：寧可信其有不可信其無

簡訊釣魚(1/2)


手機詐騙流程圖
1 ▶用戶收到釣魚SMS簡訊
2 ▶用戶誤觸網址，下載病毒進駐手機
3 ▶詐騙集團透過病毒，利用該用戶的電話號碼網購消費
4 ▶電信商不知情，回傳消費認證簡訊
5 ▶病毒攔截認證簡訊，幫用戶確認交易，完成詐騙
6 ▶病毒再偷取用戶通訊錄，發送釣魚SMS簡訊給其他朋友
資料提供：立委蔡其昌辦公室 整理：記者吳柏軒

簡訊釣魚(2/2)


0987571669
土耳其強震，部分地區斷水無暖氣。台灣中心緊急救援災民，面臨資金缺乏危機！立刻支援>> http://bit.ly/3I1WeSU

遭受社交工程攻擊之後果 ***

- 電腦被植入惡意程式後門程式
- 行為舉動遭到監視
- 個人資訊與機密檔案被竊取
- 如同監聽般的鍵盤側錄
- 使用者電腦遭感染成為殭屍電腦
  - 當成網路攻擊行動的跳板
  - 被操控並且發動惡意攻擊

對於社交工程應有的警覺性 ***

- 為何我會收到這封郵件或簡訊
  - 應確認寄件來源及寄件者
- 我是否應該收到這封郵件或簡訊
  - 應確認郵件主旨及郵件內容
- 我是否應該開啟這封郵件或簡訊
  - 是否與業務工作相關
  - 不開啟(點選)連結是否有影響
  - 審慎查證(寄件者或資訊中心)

防範之道-停

- 使用電子郵件軟體前，先確認以下設定
  - 安裝防毒軟體，確實更新病毒碼
  - 取消郵件預覽功能
  - 關閉自動下載圖片及其他功能
  - 以純文字模式開啟郵件
  - 設定過濾垃圾郵件機制

防範之道-看

- 收到郵件後務必留意
  - 查看郵件來源是否正常(寄件者、寄件來源帳號)
  - 審慎注意郵件中網址的正確性，避免直接點選
  - 標題或內容是否與本身業務相關
  - 無關公務之郵件應與相關承辦人電話確認，如確認非承辦人寄送時應避免開啟與點閱

防範之道-聽

- 若懷疑郵件來源務必進行確認
  - 透過電話向對方確認信件真偽
  - 檢視郵件內容之<FROM>資訊

一、資訊安全事件分享

二、使用者面臨之威脅

三、預防社交工程攻擊

四、個資管理與保護

五、長庚科技大學資安規範宣導

六、智慧財產權

何謂個人資料（個資法第二條第一款）？

自然人的
- 姓名
- 出生年月日
- 身分證號碼
- 護照號碼
- 特徵
- 指紋
- 婚姻
- 家庭
- 教育
- 職業
- 病歷
- 聯絡方式
- 財務情況
- 社會活動

一般資料

特種資料
- 醫療
- 基因
- 性生活
- 健康檢查
- 犯罪前科
- 病歷

其他資料
- 得以直接或間接方式識別該個人之資料

Q1. 學校活動（含社團）是否可透過信件寄發給所有學生？誰可以寄發或使用？

Yes!

學校或社團辦活動可以透過信件寄發通知給學生，因為此舉符合學校教育及成立社團之特定目的。

Who?

學校辦活動之單位、以及社團都可以寄發及使用學生的個人資料。

NG!

若學校活動是廠商的行銷活動，則有爭議空間；學校不可把學生資料給合辦活動的廠商來使用。

More

學校須評估學校使用學生個人資料之用途與目的，確認是否符合學校之「教育興學」目的。

Q2. 教授要求助理、行政人員或電算中心提供學生資料，在何種情況下可以提供？

Yes & No

老師因為教學所需（如與學生聯繫課業有關事項、了解學生家庭背景與能力等），可能會需要學生的個人資料。

學校負責保管資料的人員須判斷老師索取學生資料之目的，是否逾越教學必要範圍，以判斷是否提供。

More

建立個人資料調閱的申請與審核機制。

Q3.學生畢業後是否仍可寄發活動通知?或應該在學生畢業前先取得其同意授權？歷屆畢業生個人資料應如何管理才符合個資法?

Yes!

學校使用校友個人資料還須符合「教育行政」之特定目的，若超過特定目的則不能使用，可能需要在畢業前取得學生授權。

More

一般人並不會反對辦校友活動會超過特定目的，但學校應參照上級主管機關相關規範，確保學校能繼續使用校友資料。

此外，學校應建立控管機制避免校友資料外洩。

Q4. 老師擔心學生最近可能因閱讀某些讀物而造成行為偏差，所以向圖書館調閱學生的借書紀錄，請問圖書館是否可以提供？

Yes!

借書紀錄含學生姓名、社會活動或其他得以識別學生之資料，此屬於個人資料之範疇。

No !

圖書館保存借書紀錄之目的為「學生資料管理」，並不具評估學生行為偏差與否之目的。

老師向圖書館調閱學生借書紀錄，固然可認為是學校內部「教育或訓練行政」目的，但仍應於該目的之必要範圍內為之，並應尊重當事人權益。

如有證據可合理懷疑某學生偏差行為與閱讀有相當關聯，老師為進一步確認而向圖書館調閱學生借書紀錄，或可被認為符合「教育或訓練行政」目的之必要範圍。若老師在無任何證據情況下，全面調取學生借書紀錄，恐被認為逾越「教育或訓練行政」目的之必要範圍，因而違反個資法的規定。

社交網站上的個人資料

公寓大廈要求填「訪客資料」恐違個資法

一、資訊安全事件分享

二、使用者面臨之威脅

三、預防社交工程攻擊

四、個資管理與保護

五、長庚科技大學資安規範宣導

六、智慧財產權

資訊安全政策

- 健全資安管理制度，提昇資訊服務效率。

資訊安全目標

- 落實資安政策、推動和督導本校執行資訊安全預防、危機通報、緊急應變處理等工作。
- 建立資訊安全機制、強化資訊安全防護，提昇資訊安全之水準。

資訊資產管理

- 資訊資產類別：
  - 硬體類資訊資產：電腦設備、通訊設備、可移除式媒體及其他設備等。
  - 軟體類資訊資產：應用軟體、系統軟體、開發工具及公用程式等。
  - 資料類資訊資產：資料庫與資料檔案、契約與協議、系統文件、操作手冊、訓練教材、研究報告、永續運作計畫、災難復原計畫、稽核紀錄及已歸檔資訊等。
  - 服務類資訊資產：計算與通信服務、一般公用設施，例如：電源、空調、網路及照明設備等。
  - 人員類資訊資產：資格、技能及經驗等。

實體及環境安全管理(1/2)

- 設備應安置在適當地點並予以保護，以防止遺失、損害、竊盜或未經授權存取設備之機會。
- 應妥善維護資訊設備，以確保設備之完整性及可用性。
- 依據維護廠商建議之維修服務期限及說明進行設備維護。
- 設備置放在外部之場所時，應遵守資訊安全管理授權規定，維持與內部設備一樣之安全水準。
- 內部之攜帶型設備在外部場所使用，應提供適當之存取保護措施，例如設定通行密碼或將檔案加密。
- 支援資訊作業之相關設施如影印機、傳真機等，應安置在適當之地點，以降低未經授權人員進入管制區之風險，減少機密性資訊遭破解或洩漏的機會。

實體及環境安全管理(2/2)

- 辦公桌面應實施淨空政策，以減少文件及儲存媒體等，遺失或遭未經授權的人員存取。
- 個人電腦及電腦終端機不再使用時，應登出、或以鎖定螢幕或以其他控制措施保護。
- 設備置放在外部之場所時，應遵守資訊安全管理授權規定，維持與內部設備一樣之安全水準。
- 設備需送修時，應採取適當之控制措施。（例如：將內部機密性之資料清除）

網路使用者安全管理(1/2)

- 被授權之網路使用者，只能在授權範圍內存取網路資源。
- 網路使用者應遵守網路安全規定，並確實瞭解其應負之責任；如有違反網路安全事件，應依資訊安全規定，限制或撤銷其網路資源存取權限，並依相關法規處理。
- 網路使用者不得將個人帳號與通行密碼交付他人使用。
- 禁止網路使用者以任何儀器設備或軟體工具竊聽網路上之通訊。
- 網路使用者不得將色情檔案建置在網路，亦不得在網路上散播色情文字、圖片、影像、聲音等不法或不當之資訊。

網路使用者安全管理(2/2)

- 禁止網路使用者發送電子郵件騷擾他人，導致其他使用者之不安與不便。
- 網路使用者不得以任何手段蓄意干擾或妨害網路系統之正常運作。
- 各網路使用者應配合網路管理人員，確保其所使用之系統有安裝修補程式及啟動自動更新病毒碼功能。

存取控制管理

- 資訊資產之存取應與本身業務相關之範圍為主，任何人不得未經授權存取業務範圍外之資訊資產。
- 非因業務需求不得將系統存取帳號提供給外部人員，若因業務需要開放帳號，應考量業務需求及資訊資產之機密性，授與適當之存取權限及有效日期。
- 負責保護通行密碼，維持通行密碼的機密性。
- 避免將通行密碼記錄在書面上，或張貼在個人電腦或終端機螢幕或其他容易洩漏秘密之場所。
- 原則上本校不提供遠端連線服務，若開放維護廠商連線作業，應建立遠端使用者身分鑑別機制，降低未經授權存取系統的風險。

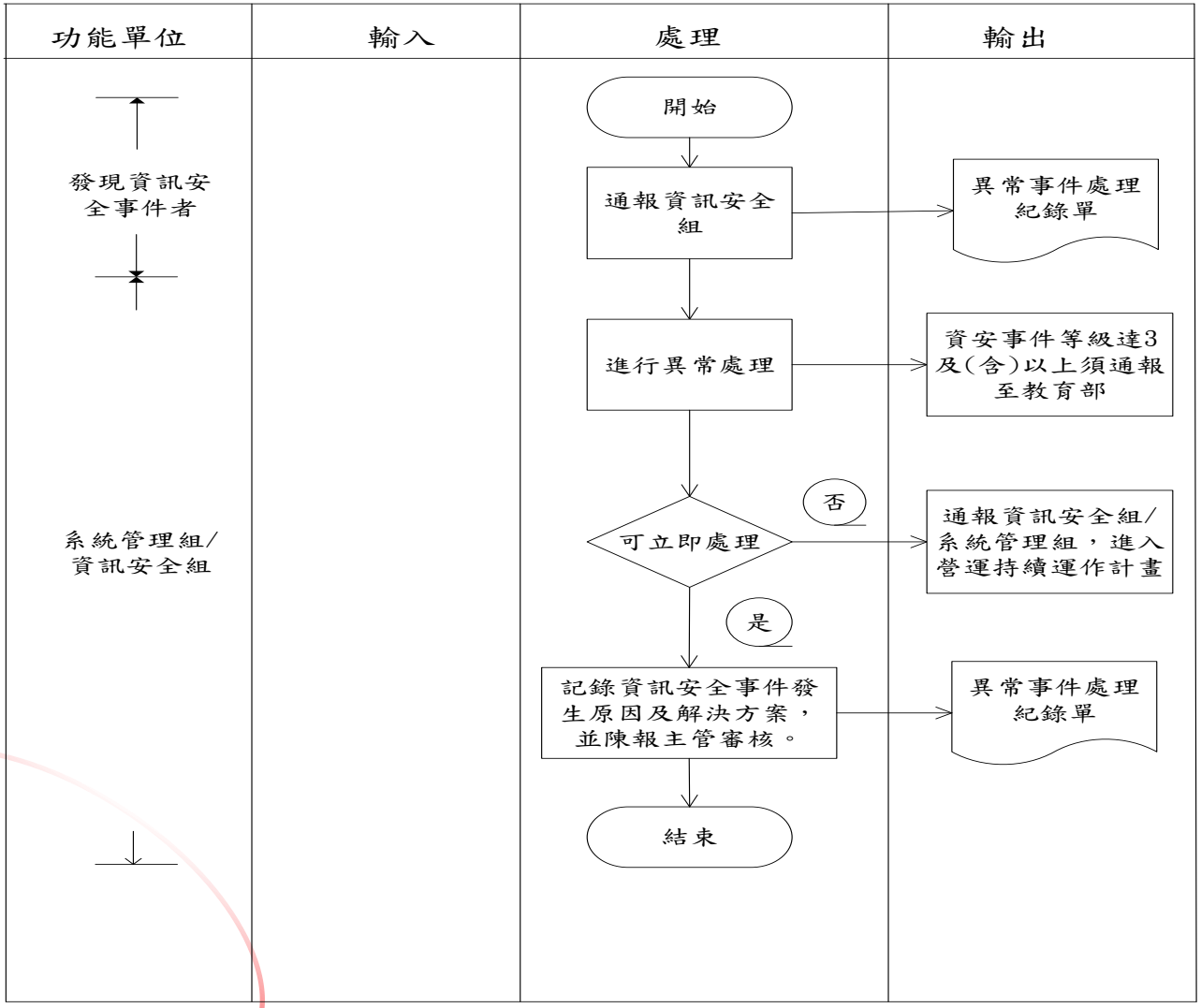
重要資料要備份 ***

- 備份的重要性
  - 預防重要資料或設備損壞遺失
  - 確保可用性
  - 防範勒索病毒
- 可藉由以下方式達到備份目的
  - 不同的儲存媒體
  - 各式各樣的工具軟體
  - *Windows*本身所提供的程式
  - 網路存放及備份

勒索軟體如何預防 ***

- 定期備份重要的檔案。
- 定期更新修補漏洞。
- 不開放共享資料夾寫入權限。
- 不共用帳號。
- 使用安全評價較高的瀏覽器。

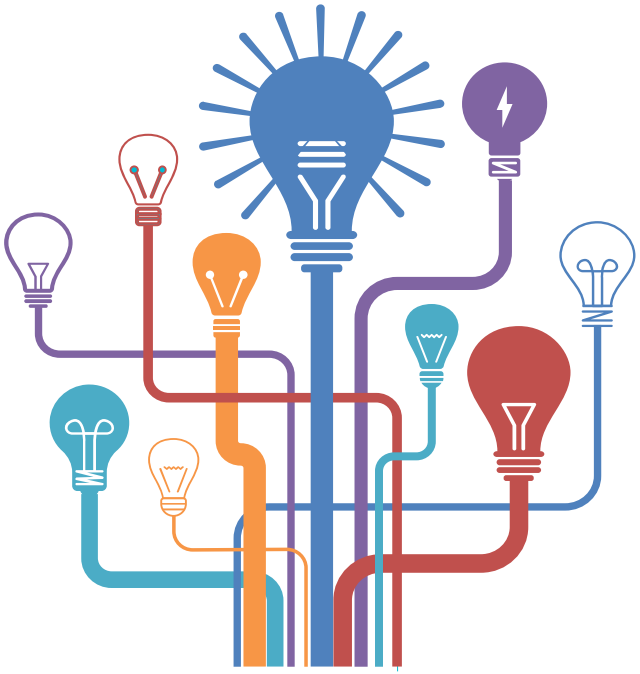
本校通報流程


功能單位
輸入
處理
輸出
發現資訊安全事件者
系統管理組/資訊安全組
開始
通報資訊安全組
異常事件處理紀錄單
進行異常處理
資安事件等級達3及(含)以上須通報至教育部
可立即處理
否
通報資訊安全組/系統管理組，進入營運持續運作計畫
是
記錄資訊安全事件發生原因及解決方案，並陳報主管審核。
異常事件處理紀錄單
結束

遠距工作注意事項

1.最低授權管理

2.連線安全管理

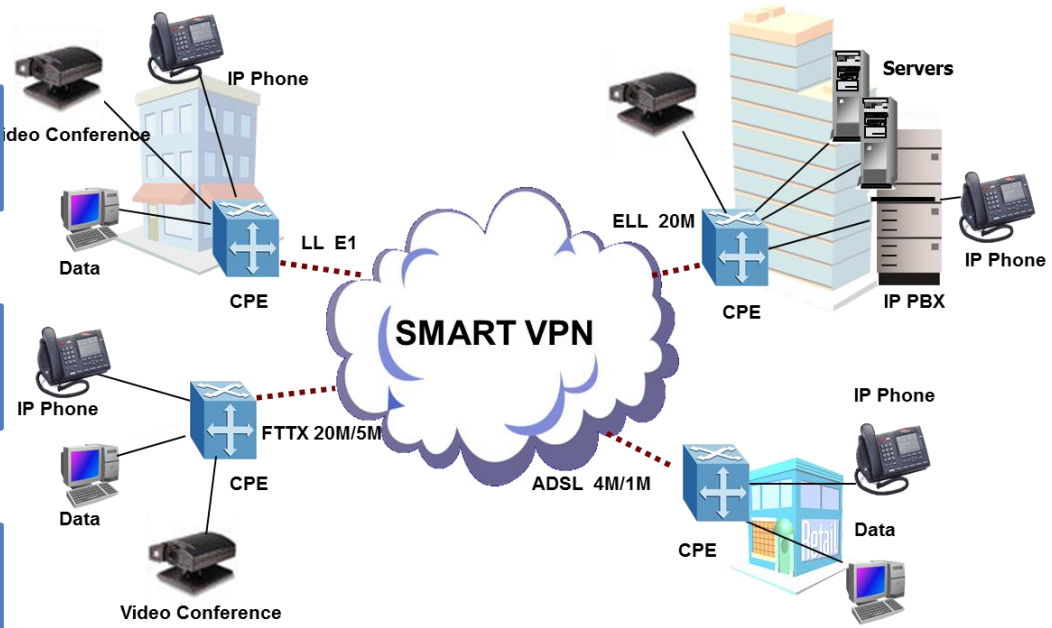


3.遠距視訊會議

4.自有（BYOD）設備管理

連線安全管理

- VPN
- HTTPS
- 檔案加密



一、資訊安全事件分享

二、使用者面臨之威脅

三、預防社交工程攻擊

四、個資管理與保護

五、長庚科技大學資安規範宣導

六、智慧財產權

著作權案例一

- 怡君就讀於某大學一年級，由於非常喜愛聽流行歌曲，上週末她花了新台幣三百五十元購買了一片的音樂光碟。
- 她將該音樂光碟中的所有歌曲，在另外的一片光碟上重新複製一份，以便加以保存，供自己往後使用家用音響，在家中欣賞該音樂光碟中的歌曲，並轉檔成為MP3的檔案格式，然後儲存在該MP3數位隨身聽中。--這項屬合理使用情形，不構成著作權侵害。
- 她得知其同班同學李健、蔣慧珠、張如欣也想要買這片音樂光碟，基於「好東西要和好朋友分享」的心情，於是就很熱心地使用自己個人電腦中的的燒錄機，將該音樂光碟重製了三份，分送給三人，每人一份。--這項「重製」三份的行為，並不符合重製行為的「合理使用」，因此侵害唱片公司的重製權。

著作權案例二

- 金志美目前就讀科技大學四年級，她平常很喜歡看網路上流傳的文章或照片，也常常利用電子郵件，將她覺得有趣的或重要的文章或照片，轉寄給親朋好友，或將上述文章或照片，轉貼在BBS站上，以便與更多的人分享。
- 金志美將語文著作，轉貼在BBS站上供網友欣賞，因為未獲得著作財產權人的授與公開傳輸權或同意，她從事上述行為，便是不法的公開傳輸行為。

著作權案例三

- 王天才今天終於完成了他的碩士論文初稿，想到這些日子以來的夙夜匪懈，一切的辛苦，終於有了初步的成果。
- 但是，在興奮的同時，他的內心，也有許多的疑惑與不安，因為他在撰寫這篇碩士論文時，參考了蔡得容教授發表在期刊上或是網路上最新的學術論文。
- 蔡得容教授發表在期刊上或是網路上的學術論文，是著作權法所保護的標的。
- 依學界通說認為，引用他人著作時，自己所創作之質量應大於引用他人著作的質量，亦即須以自己創作為主，他人著作為輔，如果沒有自己的創作，就不能主張是「引用」行為。簡單來說，引用是一種「部分重製」的行為，並且必須有自己的創作為要件。

結語

- 資安威脅持續存在，且不斷變化，防護觀念與措施要不斷更新。
- 「人」是資訊安全防範重要關鍵。
- 使用者的資安認知教育為防範的基礎。
- 時時刻刻保有警覺心。

資安防護矩陣

	Identify 識別	Protect 保護	Detect 偵測	Respond 應變	Recover 復原
Devices 裝備	盤點硬體設備與裝置	安裝電腦防毒軟體	裝置的異常現象	設備適當隔離	啟動備援主機設備
Applications 應用程式	盤點軟體(含版本與修補)	使用應用程式防火牆	軟體異常現像	進行軟體修補	啟用備援容器
Networks 網路	盤點網段及網路架構	使用網路防火牆	網路傳輸異常現像	網段隔離	啟動異地備援機制
Data 資料	盤點資料	防範資料外洩	資料異常現象	資料封存	啟動還原備份資料
Users 使用者	盤點帳號與權限	特權帳號管理	帳號與權限發生異常	帳號凍結	重新還原帳號與權限

Thank You

感謝聆聽 敬請指教

左寧生 Ningsheng Tzuo

ningsheng@bccs.com.tw