**線上資安專題講座 心得 111522071 張凱東**

1.說明資通系統防護基準有哪些構面並說明其控制目標

存取控制:帳號管理、最小權限、遠端存取等

事件日誌與可歸責性:紀錄事件、日誌紀錄內容、日誌儲存容量、日誌處理失效之回應、時戳及校時、日誌資訊之保護

營運持續計畫:系統備份、系統備援

識別與鑑別:內部使用者之識別與鑑別、身分驗證管理、鑑別資訊回饋、加密模組鑑別、非內部使用者之識別與鑑別

系統與服務獲得: 系統發展生命週期需求階段、系統發展生命週期設計階段、系統發展生命週期開發階段、系統發展生命週期測試階段、系統發展生命週期部署與維運階段、系統發展生命週期委外階段、獲得程序、系統文件

系統與通訊保護: 傳輸之機密性與完整性、資料儲存之安全

系統與資訊完整性: 漏洞修復、資通系統監控、軟體及資訊完整性

2.電子病歷資訊系統有哪些機制並說明機制

一、標準作業機制：系統建置、維護及稽核之標準作業程序。

二、權限管控機制：電子病歷製作、存取、增刪、查閱、複製、傳輸及其他使用權限之管控。

三、緊急應變機制：系統故障之預防、通報、應變、復原及其他緊急應變措施。

四、系統安全機制：確保系統安全、時間正確、系統備援與資料備份及其他保護措施。

五、傳輸加密機制：網路傳輸電子病歷，使用國際標準組織通用之加密機制。

六、安全事故處理機制：因應系統遭侵入、資料洩漏、毀損或其他安全事故之預防、通報與應變、檢討及修正措施。

3.醫療儀器資通系統防護基準有哪些並說明其控制目標

一、 醫療/醫務專屬使用設備: 建議醫療/醫務使用之設備需與其他用途之設備區隔，並應定期盤點、造冊列管以維持最新狀態。

二、 電腦須安裝防毒軟體並隨時更新作業系統: 許多的惡意攻擊程式是透過作業系統的漏洞滲透執行。所以過舊的電腦及作業系統須儘速汰換，並應安裝合法的防毒軟體，或至少更新至Windows 10並開啟內建之Windows defender進行防護。

三、 強化內部基層及管理人員資安意識: 資安教育訓練、建議於電腦的明顯處提醒USB限用機制，也可以友善提醒資安宣導標語等

四、 加強委外廠商管理: 於委外廠商簽訂合約時，合約內容應新增/包含資安條款要求

五、 落實網路隔離: 獨立使用連結健保署VPN之電腦，應與任何連結形式之網際網路區隔

六、 強化IoT設備管理: 要求委外廠商將相關 IoT 設備(如：監視器、門禁、事務機、醫療設備…等)之韌體更新至最新版本。

七、 落實設備預設帳號密碼並使用較強的密碼規則

八、 設備報廢/再利用之管制: 設備及媒體報廢或改為其他用途時，應檢查其內容是否包含敏感資訊，確認其內容已被適當的處理後（格式化、刪除內容或實體銷毀），方可移交至相關人員作後續處理。

九、 進階資安防護建置建議: 為了強化醫院之資訊安全，可導入資安雲端訂閱型服務以介接健保署VPN 及民用網路並強化防護；對於經費預算及服務內容亦可保有較大的選擇彈性。

4.說明5G網路的資安威脅並說明對策

因為5G網路的快速傳輸能力使其易受到外部的攻擊，所以攻擊者可以利用這種情況，對網路進行破壞和攻擊。，包括資料安全漏洞、協定攻擊、偽裝攻擊、外在攻擊及資料泄漏等等，可以採取的對策包括：建立安全政策、加強網路監控、強化資料加密及建立資料備份等。

5.請從排名高至低列出110年網路攻防演練攻擊紀錄

1.遠端漏洞攻擊

2.網路掃瞄

3.木馬攻擊

4.DDOS攻擊

5.社工攻擊

6.釣魚攻擊

7.偽裝攻擊

8.範例攻擊

9.文件系統攻擊

10.資料庫攻擊

11.網路攻擊

12.模糊攻擊

心得:

於11/19禮拜六下午兩點舉辦了線上資安講座，講座主持人一樣是熟悉的許見章主任，當初在輔大讀學士時有聽聞這號人物，沒想到他投注這麼多心力在資訊安全領域，不由得讓我佩服。

今天這場講座也是請來了幾位資安領域的先進來分享對於資訊安全的看法以及如何落實，更進一步是推廣希望我們一起位資訊安全這個領域一起努力，講座中提到，現今網路資訊的安全是相當重要的，因為網路的普及，網路犯罪的發生也越來越多，如網路盜取個人隱私、金融詐欺等。因此，要確保網路資訊的安全，必須採取適當的安全措施，像是安裝防火牆、安全加密技術、安裝反惡意軟件等。除此之外，還要提醒大家要注意網路資訊的安全，務必不要在未經安全驗證的網站上輸入個人重要資料，不要輕信不明來歷的可疑電子郵件，以及不要暴露個人隱私等。

隨這網際網路的發展以及5G的降臨，我也認為資訊安全越來越重要，畢竟在這個社會，每個人最重要的資訊往往是由一連串數字所組成，而這串數字也往往可以代表你，如何保護自己的個資是我們這個世代需要學著去處裡的一項問題。