出國報告(出國類別：實習)

參加「網路保安基礎技術管理暨領導能力課程(Foundations of Aviation Cybersecurity Leadership and Technical)」出國報告

服務機關：交通部民用航空局
姓名職稱：鍾臻賢 科員
派赴國家：新加坡
出國期間：**111**年**10**月**2**日至**8**日
報告日期：**111**年**12**月**22**日

摘要

網路保安為近年新興議題，綜觀近年大型網路攻擊事件，具備即時與跨國性，影響範圍甚鉅，從國家、區域乃至國際社會層面，航空產業亦會成為攻擊者所選定之目標。國際民航組織於2018年在國際民航公約第17號附約中增訂航空網路保安規範，要求相關單位應依據風險評估，辨識關鍵信息、通信技術系統及數據資料所存在之威脅及漏洞，並發展及執行適當的保護措施，以防制非法干擾事件發生。本次藉由參加國際民航組織與安柏瑞德航空大學合作主辦之「網路保安基礎技術管理暨領導能力課程」，蒐集並了解有關國際網路保安相關資訊，期能對我國航空網路保安工作之推動有所助益。

目次

壹、目的

自發生911恐怖攻擊事件後，航空保安成為全世界關注的焦點，惟911事件發生迄今恐怖主義的威脅仍方興未艾，與航空器有關之非法干擾事件及恐怖攻擊案件仍時有所聞，更凸顯航空保安工作之重要性，因此各國無不將保安列為該國航空安全之首要目標。

近年來航空保安面臨越來越多的新興威脅，網路保安即是其中之一，綜觀近年大型網路攻擊事件，具備即時與跨國性，影響範圍甚鉅，從國家、區域乃至國際社會層面，航空產業亦會成為攻擊者所選定之目標。為此，國際民航組織於2018年在國際民航公約第17號附約中增訂航空網路保安規範，要求相關單位應依據風險評估，辨識關鍵信息、通信技術系統及數據資料所存在之威脅及漏洞，並發展及執行適當的保護措施，以防制非法干擾事件發生。

過去一段時間，航空保安與資訊安全分屬不同領域，由不同獨立單位負責維運，然隨著資訊及網路技術的發展，網路漸漸成為有心人士的得力工具之一，這使得航空保安與資訊安全之間的界線日益模糊，甚至已有所重疊。惟如何整合兩不同領域之人員與技術並非一蹴可幾，因此，本局期透過積極地參網路保安相關課程，蒐集並了解有關國際網路保安相關資訊，以對我國航空網路保安工作之推動有所助益。

貳、課程概要

(一) 課程名稱：網路保安基礎技術暨領導能力課程(Foundations of Aviation Cybersecurity Leadership and Technical Management)

(二) 課程日期：111年10月3日至111年10月7日

(三) 上課地點：新加坡民航空學院(Singapore Aviation Academy)

(四) 課程規劃：本課程共40小時，含3大部分(16單元)、7次測驗及2次分課堂分組專題報告。

◎Both tracks

- Introductions
- How technology underpins all aviation systems and how technology is connected
- Interdependencies between aviation safety and cybersecurity
- Why and how adversaries attack systems, using examples and working through attack phases
- Identifying and scoping cybersecurity critical systems within aviation
- Regulatory and legal considerations of aviation cybersecurity
- The importance and value of aviation cybersecurity culture

◎Leadership Track

- Cybersecurity governance and oversight
- Cybersecurity risk management and assessment
- Information sharing
- Staff awareness and training
- Organizational resilience and incident response

◎Technical Track

- Identity and access management
- Data Security
- System Security
- Resilient networks and systems

(五) 講師介紹：

本課程為期一週共40小時課程多由講師 Dr Krishna Sampigethaya(如右圖)負責教授與領導學員討論。Dr Krishna 目前是 Embry-Riddle Aeronautical University 網路情報與安全系(Department of Cyber Intelligence and Security)主任。Dr Krishna 曾任波音公司(Boeing Company)航空網路保安技術研究員及聯合技術公司(United Technologies Corporation)研究中心網路安全副主任，研究領域包含航空網路保安、交通網路保安、車聯網網路保安等。

(六) 參訓學員：本次參與課程，除我方人員外，尚有來自泰國曼谷航空、Smith detection 公司、新加坡 CAA 及美國運輸保安署(TSA)人員參與。

參、課程內容

本次課程內容及上課討論內容略述如下：

一、第一部分：**Both Track**

(一)網路保安簡介

1、物聯網(IoT)技術，是指使用多個互相連結的設備來收集、傳輸、儲存及處理資料，這些設備使用網路相互連結，使用各種方式收集數據，後將數據傳輸到資料庫，並用於操作，其應用範圍已涵蓋生活中的各方面，包含機場設施管理及飛航營運等。得益於 IoT 技術之發展，民航產業結合製造供應鏈、機場營運、地面系統、飛航服務、航空器維護等各方面，儼然已成為一個複雜而龐大的系統，各系統間相互依賴，極具複雜性，其所衍生的脆弱點易遭受網路攻擊。近年以航空產業或系統為目標的網路攻擊，包含：未經授權惡意入侵、竊取資訊、破壞系統等，案例數量迭有增加的趨勢。

2、在數據化的時代，數據資料經分析可以提高營運效能及效率，毫無疑問成為各機關、企業的重要資產。過去，人們習慣將重點放在數位資料的安全上，其措施包含建設防火牆及設置反惡意軟體程式等，這些作為專注於保護資訊系統或數位資料本身，即資訊安全(Information Safty)。然而，隨著物聯網的發展和各種連接設備的出現，關注點已經擴大到包括網路攻擊對連接設備造成的物理傷害，例如與製造、運輸系統、工業控制系統和能源網相關的設備。隨著網路安全威脅範圍的擴大，制定有效防禦措施的需求也隨之擴大。

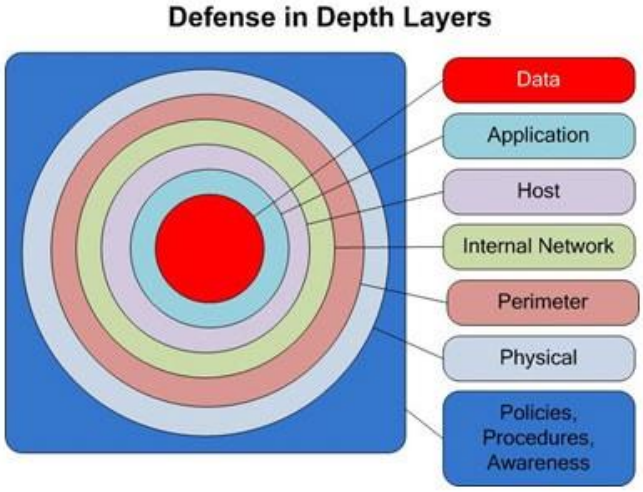
3、網路保安有三個核心元素，即所謂的 CIA 三元素，由機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)所組成。

(1)機密性(Confidentiality)：破解密碼為最常見針對機密性的攻擊，其攻擊目的旨在獲得信息的訪問權。

(2)完整性(Integrity)：對完整性的攻擊通常為竄改性質的攻擊，如勒索軟體、嵌入惡意程式之網站等。

(3)可用性(Availability)：對可用性的攻擊通常為破壞性質的攻擊，其旨在阻止系統正常運作，使得目標客戶無法使用該項系統。

4、確保網路安全是一種非對稱性的的挑戰，攻擊者只需識別多層系統中的一個漏洞即可發起攻擊；另一方面，防禦者卻必須完善在其組織結構內的系統和流程的每一層系統，以防止或減輕攻擊。因此，網路防禦者必須開發操作方法和技術來保護其係統的每一層，這種方法被稱為縱深防禦。



(二)航空與數位科技之連結與相互關係

1、隨著科技發展，航空電子設備廣泛用運於航空通信、導航、飛航管制、天

氣預報等領域，亦可顯示航空器系統的狀態。所謂航空電子系統包括：FMS（飛行管理系統）、ACAS（自動防撞系統）、ATTOL（自主滑行起降系統）、ADS-B（廣播式自動相關監視系統）、GBAS/SBAS（陸基增強系統/星基增強系統）、CPDLC（管制員機師資料鏈通訊）和 EFB（電子飛行包）系統等。

2、航空新興技術的另一個重點為飛航管理系統（ATM）的數位化。這涉及到更多系統的連接，包括語音通信、ADS-B 通信以及商用現成或商用現貨 (COTS) 硬體或軟體的使用。此外，人們也越來越依賴人工智能來分析和管理空中交通。這種不斷擴大的連接性和復雜性，以及潛在的軟體和硬體漏洞，使得新興的 ATM 系統更容易受到網路攻擊。ATM 的數位化也增加了這些系統的網路風險，因為它們的連接性和復雜性擴展到包括許多通信途徑：商業軟件產品和無線技術，這些因素結合後使得風險增加。

(三)飛航安全與網路保安之間的關係

多年來，由於對飛航安全及航空保安的重視，空中交通變得越來越安全可靠，在航空相關軟硬體系統的開發中，皆參照飛航安全及航空保安的關鍵指標設計。過去，一旦系統的設計和測試符合安全標準，製造者就會假設它們不會受到與系統相關的外部風險或危害的影響。這種概念的產生，係源於系統是封閉的並且與外部隔離。然而，隨著互聯網技術在所有行業中普及，航空業也積極研究如何利用這項技術來提高性能和效率。先進的航空電子設備、防撞和其他系統等新技術旨在使用互聯網作為通信媒介。儘管這些技術的導入在製造和營運上帶來益處，卻也衍生了新的網路安全風險。

(四)攻擊者的動機

1、追求認可及「口碑」：與其他專業人士一樣，網路犯罪分子可能尋求提高他們的認可度和「口碑」，以在同行和潛在雇主中獲較高的地位。他們需要發展自己的品牌和口碑，以吸引網路犯罪客戶。

2、經濟利益：網路犯罪有利可圖，本樣態也是最常見的網路攻擊動機。據研究，網路犯罪分子每年從網路犯罪中賺取超過 1.5 萬億美元。

3、社會/政治目的：以網路攻擊以實現社會和政治目標，如社會示威、駭客行動及網路戰等。專注於政治或社會目標的網路攻擊者經常攻擊和破壞其政敵的網站和網路。另一種常見的策略是洩露政治上或社會上對立者的個人資料。

4、復仇：內部人員竊取信息以出售給競爭對手或其他公司；或由一些內部人員攻擊他們過去所屬的組織，以報復被解僱或曾經受到的不公平對待。

攻擊者如何攻擊：

1、 偵查：網路攻擊的第一步是盡可能多地了解攻擊標的，包括確認該標的所使用的軟、硬體型號，以及它們是否已更新和修補漏洞。可能包括發送測試信息以確定是否可以突破防火牆或入侵檢測系統；人員是偵查的另一個重點，網路釣魚電子郵件等社會工程方法通常用於了解攻擊標的組織之安全策略。偵查並不侷限於攻擊標的組織，第三方和其他系統供應者通常可能遭到池魚之殃。

2、 武裝化：偵察完成後，攻擊者將製定攻擊計畫，這包括旨在利用已識別漏洞的攻擊類型。

3、 傳遞：一旦構建了網路攻擊武器，攻擊者必需確保交付攻擊的最佳路徑，包括發送網路釣魚電子郵件、誘導其從網站下載的惡意軟件、散布含有病毒的 USB 隨身碟、破壞防火牆或使用網站缺陷等方法。攻擊者只需要說服

或誘導一個人打開惡意電子郵件或點擊惡意連結即可入侵系統。

4、 發展：一旦網路攻擊武器被成功傳遞，必須確保能夠在不被檢測或緩解的情況下執行。用於逃避檢測的方法包括逃避監測軟體、修改日誌紀錄、偽裝成合法使用著或修改現有程序等。

5、 內部偵查：一旦進入系統，攻擊者就會繼續執行內部偵查，以識別將進一步攻擊的其他系統、進程和數據，並將權限提升到最高級別，以便隨意讀取或修改系統。

6、 指揮與控制：取得系統的控制權並執行惡意操作或讀取/修改系統的能力。

7、 維護：為確保能繼續對系統存取或修改，網路攻擊者必需盡可能使系統狀態正常，使攻擊行為不被管理者發現，以延長攻擊的效益與時間。

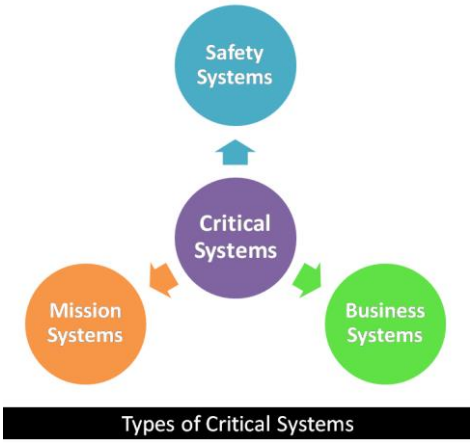
(五)識別關鍵系統

1、管理網路風險需要識別、評估和緩解這些風險，必需找出較關鍵之系統，並將其置於最高優先級別。在航空產業中，這些高度優先的系統被稱為關鍵系統(Critical Systems)，可分為三大類：

(1)**安全關鍵系統(Safety Systems)**：若故障或失效可能導致人員傷亡或設施遭嚴重破壞之系統。

(2)**關鍵任務系統(Mission Systems)**：若故障或失效可能導致部分目標或任務無法正常活動或營運之系統。

(3)**業務關鍵型系統(Business Systems)**：若故障或失效可能導致龐



Types of Critical Systems

大的經濟損失或商譽損失之系統。

2、航空器系統攻擊樣態：

(1)導航和飛行儀器的攻擊方面：

- 遮蔽或影響衛星定位系統的精度
- 破壞航空器的向指示器
- 輸入錯誤飛行控制指令使航空器俯仰或偏航
- 影響航空器駕駛員對於航空器的操作

(2)空中交通管理方面：通過竊取的密碼和惡意軟件入侵 ATM 系統，並惡意讀取或修改系統資料。

3、航空站系統攻擊樣態：

(1)針對機場系統的勒索軟件和電腦病毒攻擊以擾亂航班運營

(2)攻擊航空站電子告示牌以擾亂運營

(3)對行李處理系統進行惡意攻擊

(4)創建偽造的網站以蒐集或傳播旅客資訊

(5)對地面系統進行攻擊，例如除冰系統和燃油泵

(6)操縱或刪除臉部辨識或特定旅客資料

(六)全球性組織及相關法規

1、組織：

(1)ICAO（國際民用航空組織）是聯合國的一個專門機構，負責制定標準和建議做法 (SARPs)，以支持國際民用航空在其不同領域的協調統一發展。關於網路安全，國際民航組織在國際民航公約第17號附約中發布了網路安全標準和建議措施，在 Doc 8973和 Doc 9985中發布了網路安

全指南、航空網路安全戰略和網路安全行動計畫。

(2)FAA（美國聯邦航空管理局）是美國政府負責監督航空的機構。在網路安全方面，FAA 發布了信息安全認證和認可 (C&A) 手冊。

(3)AIAA（美國航空航天學會）是世界上最大的航空技術組織，其成員來自85個國家。在網路安全方面，發布了《航空網路安全框架》。

(4)RTCA（航空無線電技術委員會）是一個私人的非營利性協會，成立於 1935 年。RTCA 發布了適航保安方法和注意事項、適航保安程序規範。

(5)EUROCAE（歐洲民用航空設備組織）是一個致力於航空標準化的非營利組織。

(6)AEEC（航空公司電子工程委員會）是 ARINC（航空無線電公司）的一個委員會，該委員會是一個私人組織，由航空公司、航空器及航空電子設備製造商的成員組成。該組織通過定義各種技術要求來促進飛機系統的標準化。AEEC 也將網路安全納入開發指南。

(7)NIST（美國國家標準與技術研究院）是美國商務部的一部分，負責發布所有技術領域的標準。在網路安全方面，NIST 建立了信息安全框架。

(8)SAE-Aerospace–Aircraft（汽車工程師協會–航空）是一個專業的工程組織，負責制定與航空航天相關的標準。

(七)網路保安文化的重要性

1、「人」是網路安全的中心。他們是第一道防線，但也是最脆弱的元素。全面的網路安全戰略在「人」的方面有兩個重點。其一是網路安全意識的培訓，讓員工了解網路風險以及如何在工作中確保網路安全。其二是建立一支網路安全專業人員團隊，以設計和實施網路安全計畫以保護組織或企業

免受網路攻擊，且具有相關知識和技能，若要成功預防或防禦網路攻擊，一支知識淵博且經驗豐富的網路團隊必不可少，該團隊應建立明確的職責，以便所有成員都知道他們在組織或企業中的作用。這些角色必須持續得到教育和培訓，才能使員工及時了解網路威脅及防禦知識。

2、強大的網路安全文化有一些關鍵特徵。

(1)這種文化應該建立一種信任的氛圍，使員工不會因為害怕受到指責或報復而害怕報告相關訊息。

(2)領導層應鼓勵和認真對待所有員工的問題和疑慮。

二、<u>第二部分：Leadership Track</u>

(一)網路安全領導方針

1、國際領導的作用：國際民航組織為國際民用航空部門提供網路安全領導。國際民航組織聚集了193個國家，其任務包括制定國際標準和建議措施(SARPs)、空中航行服務程序(PANS)以及向其成員國提供的指導材料，涵蓋所有國際民用航空領域，包括網路安全戰略和實踐。目標是支持所有民航領域的網路安全協調和跨領域方法。國際民航組織第 40屆大會通過了航空網路安全戰略以及 A40-10 號決議——解決民用航空網路安全問題。國際民航組織還通過了網路安全行動計畫（CyAP）以實施其航空網路安全戰略。該行動計畫為國際民航組織、各國和利益攸關方共同努力提供了基礎，並提出了一系列原則、措施和行動，以實現航空網路安全戰略的七大目標。

2、高層領導的作用：一旦各個國家根據國際規定確定其國內航空網路安全監管框架，組織就有責任建立網路安全計畫以實現這些目標。網路安全計畫

的製定會影響整個組織，並且必須由高層直接領導，如果沒有高層的支持，網路安全計畫將很難推行。高層領導在建立有效的網路安全計畫中的作用對其成功至關重要，其職責包括：

(1)確保建立目標和政策並與組織的戰略和運營目標以及法規或其他要求相符。

(2)提供計畫所需的必要人力、系統和財務資源。

(3)就該計畫的重要性進行直接的部門間溝通。

(4)指導和支持管理層和員工制訂和實施該計畫。

(5)確保計畫的政策、程序和目標得到實施和執行。

(6)對不足之處持續監督改進。

3、建立治理流程：要成功實施和執行安全策略，它們必須得到高階管理層自上而下的支持。在大多數情況下，高階管理層為組織定義和批准網路安全政策；中階管理人員將這些政策轉化為標準、程序和指南。組織內的員工則有責任遵守既定政策。在構建網路安全治理結構和戰略時，需要考慮以下事項：

(1)從整體角度檢查網路安全威脅對組織的影響，詢問有關數據、漏洞和風險的問題。

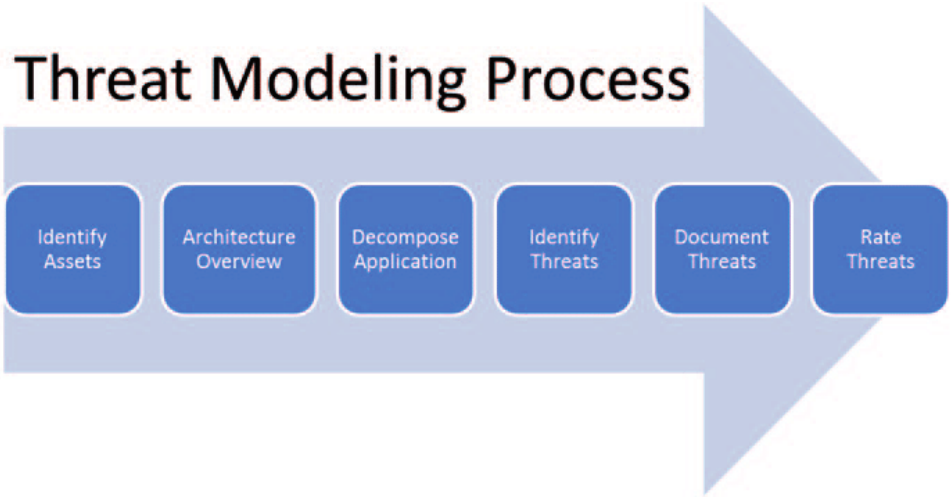
(2)人為因素仍然是最大的網路安全威脅。組織應自上而下強調安全意識培訓的必要性。

(3)建立強大的網路防禦戰略不是一次性的事情，必須確定關鍵指標，以觀察和衡量組織執行計畫之有效性。此外，隨著網路威脅和漏洞的不斷發展，亦須提高其網路防禦戰略的適應性。

(4)重要的是要在組織的各個層級之間建立開放的溝通渠道，以便可以公開

報告和討論漏洞、威脅、攻擊和潛在的補救措施。

(二)威脅模組及風險評估



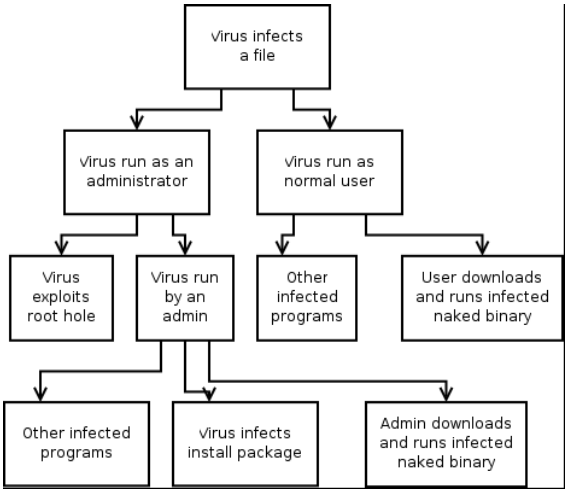
1、 管理航空產業系統中的網路安全威脅的重要第一步，是制訂一種方法來識別關鍵威脅的範圍。其中一種有效的方法是威脅建模，威脅建模是識別潛在安全威脅和漏洞及其風險和損害級別的過程。通過這個過程，組織或企業可以優先考慮預防和緩解網路威脅項目。

(1) 識別資產：識別所有需要保護的資產，此過程應識別數字資產，例如網路、數據庫、硬體、雲存儲庫、OT 設備、飛機系統、第三方連接和通信技術；另外，識別有風險的實物資產也很重要，例如製造設施、航空站、辦公設施、航空器、地面服務人員。

(2) 架構概述：識別資產所在的系統，並釐清各資產間可能存在的相互關係，這一步驟至關重要。例如：製造設施或航空站中支持物聯網技術的設備也可以為網路攻擊提供易受攻擊的破口，進而影響到其他系統。

(3) 分解應用程序：此步驟涉及深入研究每個數字和物理資產，以確定其在組織中的應用方式以及為網路安全漏洞途徑的所有相關流程。使用

流程圖有助於繪製各種資產及其操作相互關係，直觀的檢查潛在的漏洞及風險。「攻擊樹」為一種常見的，它詳細說明了潛在威脅如何通過系統傳播，如下圖所示。



(4) 識別威脅：紀錄前三個步驟中所發現的所有潛在網路安全威脅，為每個資產識別威脅。

Threat type	Examples
Physical damage	Fire
	Water
Natural events	Earth quake
	Flooding
Loss of essential services	Failure of air-conditioning
	Power outage
Disturbance due to radiation	Electromagnetic radiation
	Thermal radiation
Compromise of information	Eavesdropping
	Theft of documents
Technical failures	Equipment failure
	Saturation of the information system
Unauthorized actions	Unauthorized use of equipment
	Use of counterfeit software
Compromise of functions	Abuse of rights
	Forging of rights

(5) 建立威脅資料庫：紀錄每個潛在的網路安全威脅及其相關資產與漏洞間的關聯，並分析攻擊可能在組織內造成的潛在損害。

Threat Description	Attacker obtains authentication credentials by monitoring the network
Threat target	Web application user authentication process
Risk	High
Attack techniques	Use of network monitoring software
Countermeasures	Use SSL to provide encrypted channel

Threat Description	Injection of SQL commands
Threat target	Data access component
Risk	High
Attack techniques	Attacker appends SQL commands to user name, which is used to form a SQL query
Countermeasures	Use a regular expression to validate the user name, and use a stored procedure that uses parameters to access the database.

(6) 評估威脅：對威脅進行評級並確定優先級別及處理順序，以利將其資源集中在最可能和最具破壞性的威脅上。

Q: For each Threat Documented, Rate the Threat against the impact to the Organization.

Rating		High (3)	Medium (2)	Low (1)
D	Damage potential	The attacker can subvert the security system	Leaking sensitive information	Leaking trivial information
R	Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E	Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A	Affected users	All users, default configuration, key customers	Some users, non-default configuration	Very small percentage of users, obscure feature; affects anonymous users
D	Discoverability	The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it.	The bug is obscure, and it is unlikely that users will work out damage potential.

No	Threat	D	R	E	A	D	Total	Rating
1	Attacker obtains authentication credentials by monitoring the network.	3	3	2	2	2	12	High
2	SQL commands injected into application.	3	3	3		2	14	High

2、 風險評估

(1)定性風險評估：對每個風險進行主觀分析。在此分析中，評估每種風險的發生概率及其潛在影響。其中標示的低、中、高等級用於描述風險的潛在影響。定性風險評估的表示方式以發生概率和造成影響矩陣示之，如下圖所示。

RISK OUTCOME
Low
Moderate
Significant
High

Likelihood	Consequence				
	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5	10	15	20	25
Likely 4	4	8	12	16	20
Possible 3	3	6	9	12	15
Unlikely 2	2	4	6	8	10
Rare 1	1	2	3	4	5

概率或可能性(縱軸)：評估風險可能發生的可能性。例如，如果發生風險可能性為50%或更高，則視為高；介於10%至50%之

間，風險為中等；而在10%或以下者，風險為低。也可以使用其他術語，例如「幾乎確定」、「可能」和「不太可能」。

影響或後果(橫軸)：評估風險可能造成的損害程度。與概率/可能性類似，用於確定潛在影響，以「不顯著」、「輕微」、「中等」、「重大」和「災難性」等分類示之。

(2)定量風險評估：定量風險分析與定性方法的不同之處在於它是對風險概率和影響的數值分析。定量風險分析的目標是確定風險成本。包括一次事件將給組織或企業造成多少損失、事件在一年內發生的頻率以及潛在風險的年度總成本等。根據風險分析的結果，組織或企業將優先考慮如何應對風險。定量風險評估包括四個要素：

暴露因子(EF)是指已識別的威脅可能造成的損失百分比。

單一預期損失(SLE)是指資產價值乘以風險係數(EF)。

年化發生率 (ARO)是指威脅每年發生的估計頻率。例如，一年可能發生10次的威脅的 ARO 則為10。

化損失預期 (ALE)是指威脅的年化總成本，為單一損失預期(SLE)與年化發生率(ARO)的乘積。

(三)資訊分享

1、 航空業建立有效的網路安全戰略和實踐的能力有賴於航空產業系統中各成員之間的緊密合作。然而，只有當各方之間存在信任時，合作才能實現。建立對航空網路安全的信任取決於航空產業系統成員之間的透明度和資訊共享。資訊共享的主要目的是建立允許收集、存儲和發布網路安全資訊的程序，這種資訊共享使參與者能夠有效的對抗網路攻擊。

2、 為了創建資訊共享結構，必須克服在共享資訊和建立信任環境方面的猶豫，以及對共享資訊的格式及方式達成共識。共享資訊必須對其參與者有價值，並且應包括有關威脅和漏洞的安全警告、技術和系統的報告和研究，以及網路攻擊的預防和緩解策略。

(四)人員教育訓練

1、 實施網路安全意識和培訓計畫有幾個關鍵步驟：第一步是評估組織並確定網路安全目標，一旦確定了計畫目標，下一步便是編寫培訓材料，培訓材料應針對組織或企業面臨的網路安全漏洞和風險編撰。

2、 人員培訓不可能一步到位：它包括三個步驟，意識、培訓及教育。

(1)**意識**：在意識課程中，參與者為資訊的接受者，其範疇包括：密碼使用、病毒防護、公務用移動設備資訊安全及管理等等。

(2)**培訓**：在培訓課程中，參與者扮演更積極的角色，專注於建立知識和技能，而不僅僅只是接收資訊。其教授的知識和技能建立在意識課程的基礎之上。

(3)**教育**：是最後一個層次，其重點是將網路安全技能和能力整合到一個全面的知識體系中。

(五)恢復彈性與事件處理

網路恢復彈性被定義為組織或企業從網路攻擊中恢復的能力。恢復彈性的衡量標準是組織在預防網路攻擊、防禦網路攻擊、控制攻擊影響以及確保攻擊期間和之後的運營恢復方面的能力。建立恢復彈性有幾個目標：

1、**威脅防護**：持續監控系統漏洞並偵測威脅，採取相應的保護和防禦措施，例如：安裝防毒軟體、惡意程式偵測系統等。

2、**可恢復**性：終止系統受攻擊的狀態，並且建立從攻擊中重新恢復系統正常運作的能力。

3、**適應性**：讓組織不斷審視內部外部環境，以面對新型態的網路威脅之能力，包含對內及對外的訊息共享作為等。

4、**持久性**：維持修復漏洞後持續正常運作的能力。

三、第三部分：Technical Track

(一)身分辨識與驗證

身分驗證通常有三個類型：

1、你知道的東西(密碼)

2、你擁有的東西(證件、鑰匙)

3、你是什麼(指紋、臉部特徵)

(二)資料安全(加密)

加密過程係為確保僅授權用戶或使用者才能存取或修改系統資料。加密是一種雙向數學演算法，將原本任何人都可以理解的訊息，使用不同手段將之改變為密文消息。

1、 對稱密鑰加密：發送者和接收者擁有相同的密鑰，得以解讀密文。如果第三方獲得了密鑰，發送者和接收者之間的機密性就會受到損害。

2、 非對稱密鑰加密：也稱為公鑰加密；這項技術需要兩個密鑰（公鑰和私鑰），公鑰用於加密，私鑰則用於解密。使用公鑰把明文加密後所得的密文，只能用相對應的私鑰才能解密並得到原本的明文，最初用來加密的公鑰不能用作解密。由於加密和解密需要兩個不同的密鑰，故被稱為非對稱加密。

(三)系統安全

1、 程式碼是系統的構成基礎，程式碼編寫的基礎知識包含：

(1)清晰地設計和編撰程式碼

(2)避免使用重複的程式碼和數據

(3)限制權限

(4)建立信任邊界

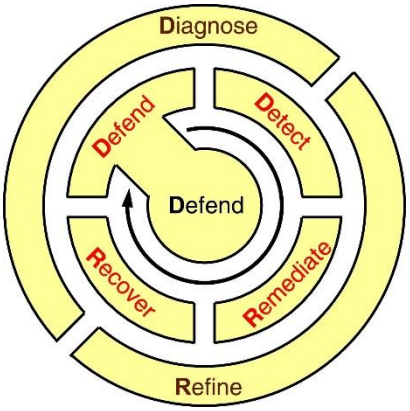
(5)妥善封裝

(6)建立文檔安全相關信息

(7)保護第三方程式碼

2、 僅擁有良好的程式碼是不夠的，另必須妥善的配置各項應用程序。成功管理的第一步是擁有合適的人員，該組織必須僱用經過培訓成為安全專家的人員。安全人員可以使用的一些工具包括數據封包嗅探器、端口掃描器等。數據封包嗅探器可以顯示 IP 數據封包的源頭和目標，接著可以使用自動化工具來查找是否有異常流量、異常端口等。

(四)系統恢復力



1、 儘管盡了最大努力保護網路和系統，但仍必須面對無時無刻遭受攻擊的潛在風險，故系統須具備受攻擊後的復原能力。然而，網路和系統非常複雜，各組件之間的通用性不高且多樣性繁雜，故設計恢復系統極具困難度。

2、 ResiliNets Resilience Control Loop，為一種網路縱深防禦的方式，亦可應用

於網路系統恢復的範疇。在內部循環中，包含了主動防禦作為，如使用防火牆防止攻擊者的網路滲透，其次為在發生網路滲透時進行檢測，隨後採取一切行動以補救或排除系統漏洞，最後，在威脅或滲透被排除後，將系統恢復到其原始正常運作的狀態。該圖的外部循環為一個回饋過程，用於辨識發生了什麼事件以及後續該如何修改完善流程，以提高系統恢復力。

3、 系統恢復力應具備兩種特性：

(1) 非單一連接性：網路或系統必須有足夠多的節點或連結，以防止其中一個組件故障或遭受攻擊時，不至於讓整個系統停止運作。

(2) 自主隔離性：當網路或系統被分區時，應確保個別區域有足夠的資源正常運行。

肆、心得與建議

一、航空保安的過去與發展

過去一個多世紀以來，航空器的發展帶動空運產業蓬勃發展，卻也衍生人為蓄意或疏忽所造成的地面設施與航空器破壞甚或因而導致人員傷亡的相關課題，這些課題隨著時空背景演進展現了諸多不同的樣貌。

1977年10月13日，漢莎航空181號班機由西班牙馬略卡島帕爾馬至德國法蘭克福途中，遭解放巴勒斯坦人民陣線4名成員劫持，並威脅西德及土耳其政府釋放若干人犯，隨後迫使駕駛將飛機開至索馬利亞摩加迪休，所幸整起劫機事件在五日後西德警方的成功攻堅後落幕。自此事件後，各國政府傾向不再與恐怖份子談判，並著手發展處理類似事件之專責組織。

2001年9月11日，美國本土發生了一連串自殺式恐怖攻擊，19名蓋達組織恐怖分子分別劫持4架民航客機，並使用其攻擊紐約世貿中心、五角大廈等設施。此事件對當時政經情勢影響甚鉅，對後續各國航空保安作為亦影響深遠，如加強駕駛艙門防護及加強行李檢查等措施。

二、網路保安之我見

確保航空保安為一種非對稱性的挑戰，防禦者必須在各方面做到面面俱到，始能將風險降到最低，即便如此，仍然無法完全杜絕攻擊事件發生。隨著進入到數位時代，透過網路遠端操作及不易追蹤的特性，使得攻擊者不需再冒著自身生命危險，親赴航空站或航空器進行破壞，事後逃避追捕的機率亦大大提升。因此，確保航空保安面臨新的形態與挑戰，新的名詞─「航空網路保安」油然而生。

物聯網(IoT)是指連接各種裝置的集體網路和幫助裝置與雲端和裝置之間互相通訊的技術，得益於電子運算設備及通訊技術的發展與普及，現今有數十億個裝置與網路互相連結，

時至今日，物聯網與我們的日常生活息息相關。簡而言之，物聯網技術將「物」與「網路」整合在一起，得益於該項技術，企業或組織可以在營運上時間高度的自動化，並提升時間與資源的使用效率；另可透過分析龐大的資料庫，做出適當的決策。然而，其相互連通及依賴資料庫的特性，也衍生各項安全風險：以航空站內的助航設施為例，位於跑道地帶上的助航設施，平時受界圍妥善的保護，即可達到杜絕非法干擾事件的效果。然隨著各項技術的發展，助航設施與其他系統深度聯結整合，使航空站營運更具效益，卻也增加了受攻擊的風險與，使得原本有效的保安措施(界圍防護)不再有效，需要額外與其他有關部門合作建立新的保安措施，始能降低受攻擊的風險。

1990年上映的《終極警探2》(Die Hard 2)即演繹出類似情節：一群匪徒入侵並破壞航空站航管、助航及通信系統，並使用臨時架設的航管系統錯誤的引導航機，導致其墜毀於跑道上，雖然劇情中迭有不合理之處，但該片完整詮釋「資安事件亦可能擴大為非法干擾事件甚或造成人員傷亡」及「透過發現並入侵其中一個系統漏洞即可危害整個系統」等概念。

「奇異點」(Singularity)在數學上被定義為「無法定義的點」，在物理學中則為「連續的曲線中一個斷掉的點」，有人也將之解釋為「完全被顛覆」之義。航空保安史上亦曾出現數個「奇異點」，如前文所述的「911事件」，在事件發生之前，人們往往無法理解該事件的脈絡與內涵，少數先知先覺者反而容易被貼上「異端」或「騙子」的標籤，在雲淡風輕、歌舞昇平的時代，上位者往往也不願意得罪廣大群眾而貿然做出變革。故人們往往在重大事件發生之後，才集體意識到其重要性，拋下固有的本位主義，共同解決眼前的問題。

隨著網際網路及通訊技術的發展，是否將演繹出下一個航空保安的「奇異點」呢?透過觀察近年趨勢，不可排除其可能性，但也沒有人說得準。所幸我們已從過去的經驗中學習良多，面對未知的挑戰，平時做好各式風險評估自是不可缺少，據評估結果制訂事件應變計畫以充分緩解甚至防禦各種事件亦有其必要性。

三、網路保安的窒礙與挑戰

有別於過去僅是借鑒或運用不同領域的技術或作法以減少或杜絕非法干擾事件，「網路保安」更像是門「航空保安」與「資訊安全」深度結合的學問。然而現階段世界各國多數航空保安從業人員並不具備資訊專長及知識。「我在機場工作了20年，從來不知道機場內有這樣的東西，更不知道它如何運作。」在課堂中完成「助航設施網路保安應變計畫」隨堂分組報告後，一位 TSA 資深檢查員這樣感嘆道。航空保安已是一門獨立、專業且龐大的學問，要「斜槓」至另一門晦澀的學問(資安)，顯然多有窒礙之處。

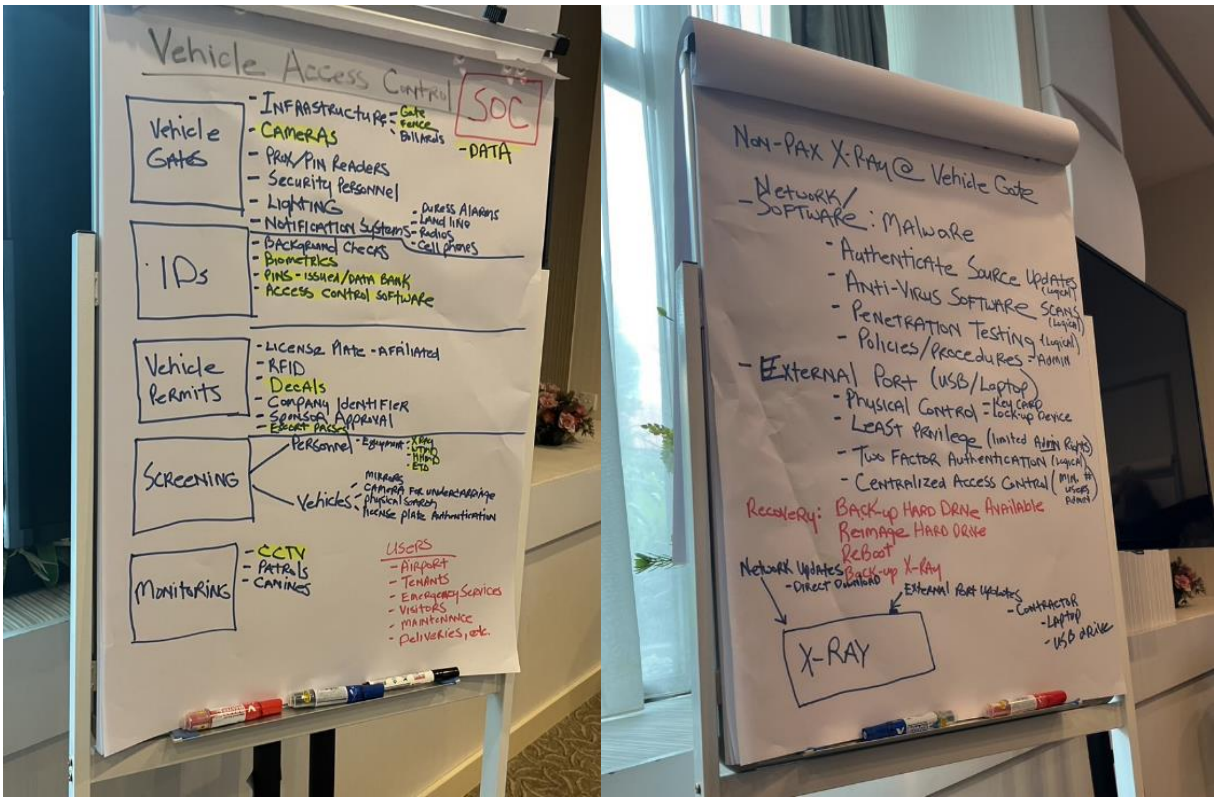
四、解決方案與建議事項

對於上述的難題，課堂中已給予相應的建議，無論在組織的營運或建立文化方面，建立一支專業人員團隊是極為重要的事情，該團隊成員必須對航空保安及資訊安全上有充分的了解與認知，以利機關或組織進行各類業務評估及對其他員工進行訓練或宣導等；此外，為了打破部門本位主義的藩籬，有關網路保安之相關計畫應獲得高層(機關)自上而下的支持，由高層(機關)定義和批准政策，再由中階人員將政策轉化為標準或程序，最後則是所有員工或所屬成員遵守該既定政策及作法。

網路保安所涉層面極廣，其運作內容橫跨多項領域，日前我國為因應5G 和物聯網時代的來臨，著手設立橫跨資訊、資安、電信、網路及傳播五大領域的數位發展主管機關—數位發展部，足見我國對資訊、網路及資安等領域的重視，期能獲得專業上層單位的政策指導與行政資源分配；另本次課程中除與各國航空保安專業人士進行交流外，於課間亦建立良好友誼，可作為後續資訊交流之重要管道，對往後本局獲得國際相關資訊及規範時有所助益，故建議我國持續派員參與相關國際課程，俾與期他國際專業人員保持聯繫，以利國內相關政策修訂與業務之推行。

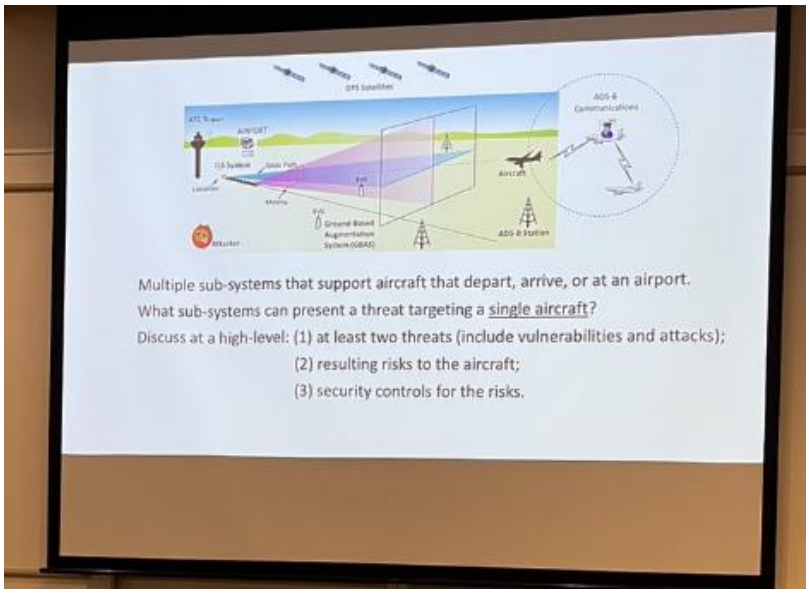
伍、附錄

附錄1、課間小組討論內容

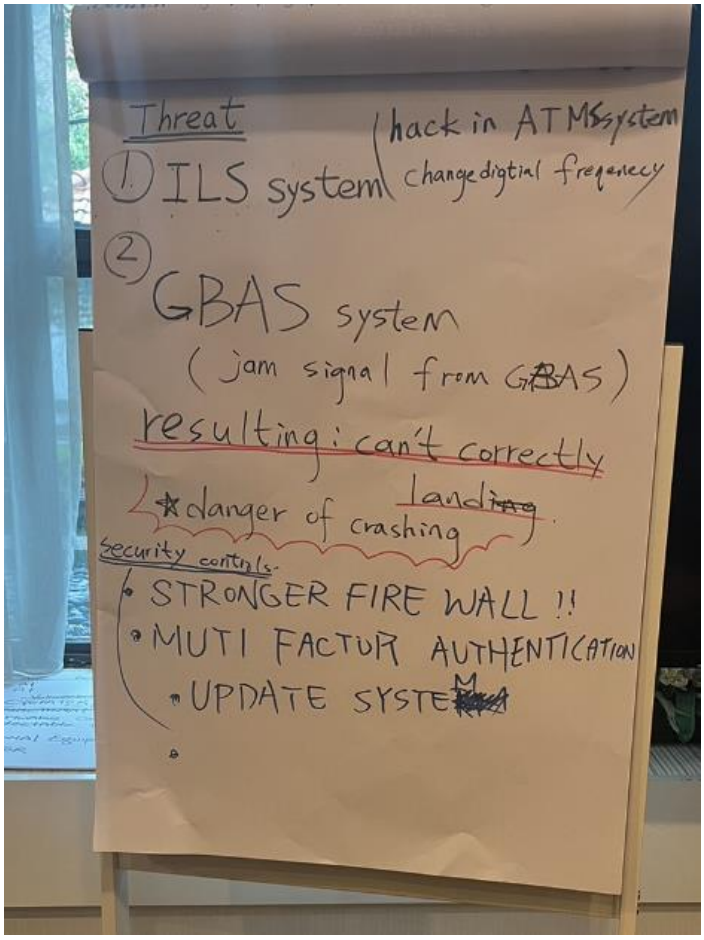


討論題目：試擇定一航空站內設施(或資產)，並分析其主系統及子系統間的相對關係，以及識別該設施面臨的潛在威脅及風險。

討論內容：本組原選定車輛識別系統(Vehicle Access Control System)作為分析標的，惟後來發現該標的太過龐大不利分析，故改分析其子系統-車輛 X 光設施(non-passenger X-Ray)，風險、威脅及攻擊緩解措施分析如上。



討論題目：試分析助航設施遭到攻擊時，對航機的影響與緩解措施。



討論內容：本組假定 ILS 系統及 GBAS 系統遭到攻擊時，航空器即無法對準跑道中心線(甚或是被誘導偏離跑道中心線)，故最嚴重之結果為衝出跑道或墜毀，緩解或預防措施包含：建立更強大的防火牆、對操作權限做多階段認證及確保設施或天線周邊人員淨空等。

附錄2、Final Tabletop Exercise 題目及小組討論內容

Airport Cybersecurity TTX – Part 1

*[CISA Tabletop Exercise Package]

(Day 0)

- The FBI issues a FLASH alert about a phishing campaign targeting airports.
- The phishing campaign consists of emails containing a malware infected PDF file.
- The alert details the contents of the file and email along with analytics on malware.
- The report cites a recent string of ransomware infections called "MyTopGuns".

(Day 2)

- An anonymous entity Aviator posts a vague social media message directed at a Tier-1 *Terminus* Airport that reads: "All things connect at airports. I control your things!"

(Day 3)

- Some Terminus employees turn in USB drives to front offices (found in parking lot).
- One of the employees plugs the found USB drive into his airline computer. He finds no user information but a bunch of random files. He unplugs and hands it to security.
- Some Terminus employees receive an email with a Cargo Booking Form PDF attached. Some report the email as suspicious, but several click/open the PDF file.
- Terminus employees receive an email with link to a memo "Terminus Family Day." Some report the email as suspicious; others click and see a memo about the event.

(Day 6)

- Network users at Terminus begin reporting computer issues (e.g., slow performance).
- Some users notice they now have access rights to folders not previously available.
- Users are reporting missing information in the system and access issues.
- Aircraft begin experiencing problems at the airport, to include shutdown of navigational systems and malfunction of operational technologies/systems.

Airport Cybersecurity TTX – Part 2

*[CISA Tabletop Exercise Package]

(Day 7)

- "Aviator" posts another social media message: "Greed and corporate corruption will end you. There will be a day when you pay, could be getting all dark soon!"

(Day 10)

- Network systems and workstations that operate some Terminus functions (such as baggage handling) experience delays and in some cases are inaccessible.

(Day 13)

- An employee from Terminus is having difficulty logging into his workstation.
- After rebooting, the employee sees a screen showing the "MyTopGuns" ransomware.
- The screen says all files are encrypted and will be destroyed unless payment is made.
- The malware has spread across the airport network (to several stakeholders).
- There are multiple reports of ransomware disrupting Terminus's critical systems.

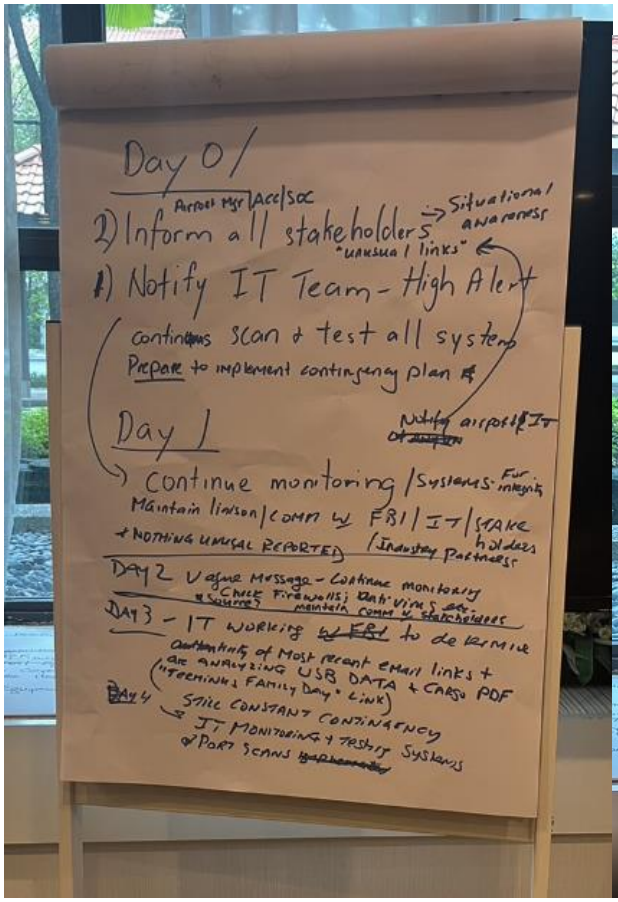
(Day 15)

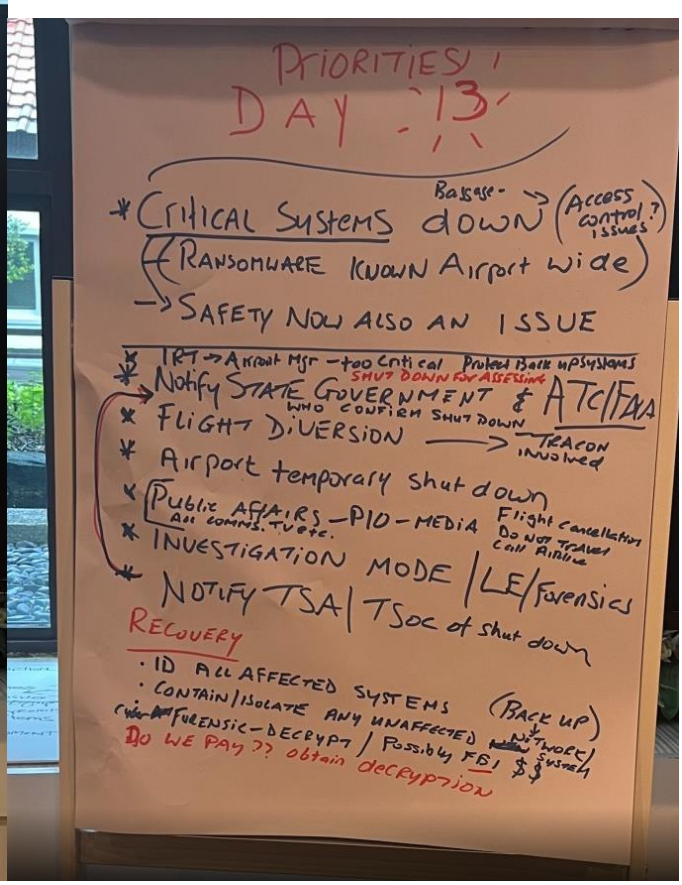
- Terminus airside and landside operations slow down
- The ransomware seems to spread to aircraft systems connecting to airport network.
- Aircrew members report having difficulty accessing airport systems from aircraft.

(Day 15)

- Media affiliates are contacting Terminus and affiliates for comments on the attacks.
- Calls come in from partners asking about the state of Terminus and risk to business.

討論題目：假定各組為航空站管理者，試討論面臨網路攻擊各階段的應處作為。





討論結果：本組成員除本人外均為美國運輸保安署資深檢查員，故相關應處作為，如通報聯邦政府、州政府或其他鄰近機場(轉降)等，多承襲美國運輸保安署規定推演

附錄3、結訓證書

EMBRY-RIDDLE
Aeronautical University

TRAINAIR
PLUS

This certificate is presented to

Chen-Hsien Chung

In recognition of successful completion and certification

Given this 7 October 2022

Foundations of Aviation Cybersecurity

Leadership & Technical Management Tracks

Singapore

Matthew N Flaherty
Vice-Chancellor & Head of Asia
Embry-Riddle Aeronautical University

Diego Martinez
Chief
Global Aviation Training