行政院所屬各機關因公出國人員出國報告書

（出國類別：其他）

參加「芝加哥聯邦準備銀行金融機構監理專業課程：Information Security Vulnerability Management」重點與心得報告

服務機關：金融監督管理委員會檢查局

姓名職稱：林綉蓮　稽核

派赴國家：美國

出國期間：106 年 10 月 21 日至 10 月 29 日

報告日期：107 年 1 月 16 日

摘要

芝加哥聯邦準備銀行(Federal Reserve Bank of Chicago)係美國聯邦準備銀行(Federal Reserve Bank, FED)12 個地區聯邦儲備銀行之一，設置 STREAM 技術實驗室，提供互動式、實作的教育訓練課程，協助金融監理人員瞭解現今資訊科技及新興科技帶來的資安風險與影響性，以及資安弱點管理措施的基礎概念。

芝加哥聯邦準備銀行於 2017 年 10 月 23 日至 27 日舉辦為期 5 天之「Information Security Vulnerability Management」研討會，指派美國聯邦準備銀行 8 位資深講師，與學員一起研討資訊安全弱點管理之基礎技術，藉此強化監理與檢查人員之資安風險辨識(Identify)、保護(Protect)、偵測(Detect)、應變(Respond)、與復原(Recover) 之能力，以及瞭解監理與檢查應關注重點。本次研討會共有美國、韓國、印度、奈及利亞、斯里蘭卡、墨西哥及我國等 7 個國家 26 位金融監理人員參加。

本次奉派出席本研討會，除期望藉由課程瞭解美國聯邦準備銀行對銀行業資訊安全之監理思維，並能加強與各國監理檢查人員互動交流相關議題及檢查經驗外，面對未來金融業數位金融之發展，將就本局在金融科技發展趨勢，面臨嚴峻資安風險挑戰下，如何逐步調整並強化檢查關注重點及監理措施提出具體建議。

目　次

壹、前言

「Information Security Vulnerability Management 研討會」係由芝加哥聯邦儲備銀行主辦之 5 天課程，參訓對象主要為美國監理人員，有 19 位是美國本土監理機關派來參訓人員，包括聯邦存款保險機構(FDIC)、美國通貨監理署(OCC)、FRB District(FRB St. Louis、Chicago 及 Dallas)及各州之監理機關等，另外 7 位參訓人員是來自全球其他國家監理機構，分別是我國、印度、南韓、奈及利亞、斯里蘭卡、墨西哥。上課主要議題為資訊安全風險評估、弱點評估與漏洞修補、弱點掃描及滲透測試、資料庫漏洞、資安事件回應與管理，以及檢查人員應關注之監理重點，並提供實驗室上機實作、個案分析及分組討論，各國金融監理人員藉此個案研討機會分享監理實務經驗。

本篇報告第一部分為「研討會目的」，說明主辦單位舉辦研討會之目的及本會派員出席擬達成之成效。第二部分為「研討會過程」，簡述授課講師、參加學員、授課內容與方式。第三部分為「研討主題」，彙整本次研討會主要講述與討論內容。第四部分為「心得與建議」，說明參加本次研討會之心得與建議。

貳、研討會目的

本次「Information Systems Vulnerability Management」研討會主要由美國芝加哥聯邦準備銀行之資深資訊安全講師授課，課程特色是以資訊安全漏洞管理(Information Systems Vulnerability Management)和安全資訊與事件管理(Security Information and Event Management)為主軸，包括網路和系統監控，風險評估和抵減，漏洞修補管理和資安事件回應，透過實作練習滲透測試、漏洞掃描和弱點管理工具，藉以強化銀行對資訊安全管理須進行準確的資產盤點和風險評估的必要性。

「Information Systems Vulnerability Management」課程是由 Federal Reserve System, STREAM Technology 實驗室舉辦，STREAM(Supervision Technology Risks Educate, Analyze and Manage)全名為科技風險監理實驗室，係美國聯邦準備銀行設立於芝加哥負責辦理金融監理檢查人員之資訊科技教育訓練，所有課程項目都是由 S.T.R.E.A.M./Technology 實驗室經驗豐富之專家，分享他們的監理經驗，透過全球重大的駭客攻擊事件案例，學員間互相分組合作、上機實作專業的漏洞掃描及滲透測試技術及個案研討，讓各國 IT（資訊科技）監理人員互相分享最佳監理實務做法。

本研討會學習目標在使監理與檢查人員能夠闡述與運用和漏洞管理計畫相關之關鍵要素，首先是銀行應該對所有系統進行盤點及準確的風險評估，涵蓋所有透過網路進行通訊的資產清單（伺服器和應用程式等）及每個系統（內部和外部）的潛在風險，並進行佈署管理，最後，金融機構必須能夠制定風險緩解策略進行審查，以確保新的應用程式或系統從整體的角度進行處理，並對所有系統控制有效的定期重新評估，研討會預期學員能夠完成下列目標，並能應用於未來工作範圍：

一、瞭解弱點管理及如何與銀行的整體資訊安全計畫和IT營運結合。

二、瞭解脆弱性管理計畫在保護資訊資產方面的作用。

三、瞭解漏洞修補管理、漏洞掃描和弱點評估以及測試工具的使用。

四、討論金融機構滲透測試程序的適當性。

五、討論金融機構資安事件回應程序的關鍵要素。

六、瞭解在監管背景下評估關鍵風險的控制和流程，及監管合規問題。

七、瞭解金融機構應對新興威脅所必須做的事情。

參、研討會過程

一、講師與出席人員

本次授課講師共 8 位，有 7 位係屬芝加哥聯邦準備銀行(Federal Reserve Bank of Chicago)監督與管理部門風險管理處(Department of Supervision and Regulation)監督和管理之技術專家，主要職務包括在 STREAM (Supervision Technology Risks Educate, Analyze and Manage)實驗室對聯邦準備體系、聯邦存款保險機構(FDIC)、美國通貨監理署(OCC)及州會員銀行等機構提供資訊科技例行教育訓練，並參與銀行資訊科技專案檢查，包括 Mr. David Balka、Mr. James Gilbert、Ms. Colin Gavin、Ms. Sandra Rolnicki、Mr. Roger O’ Farril、Mr. Nathan Viets 及 Mr. Ariel Briskman，另一位講師Mr. Frank Greenwell來自華盛頓D.C.聯邦儲備系統之資深資訊安全專家。

參與本次研討會之學員包括美國、印度、南韓、奈及利亞、斯里蘭卡、墨西哥及我國等 7 個國家 26 位金融監理機關人員。

二、課程進行流程

(一)10 月 23 日：各國參加研討會學員辦理報到，首先由主辦單位進行開訓致詞，並由各參訓學員自我介紹，隨即對學員進行資訊安全與風險控管線上測驗，並開始研討課程，當日主題包括：資訊安全之弱點管理、風險緩解及常見弱點與漏洞，瞭解為什麼脆弱性管理是金融機構應關注之議題，且無論其規模大小和複雜性，另討論漏洞監測和修補，漏洞評估在風險管理流程中的作用，評估脆弱性管理工具。

(二)10 月 24 日：講述主題包括修補程式管理相關定義，討論及時修補應用程式漏洞的重要性及評估修補程式管理部署工具，列舉不正確修補程式管理的風險，漏洞修補程序、檢查人員應關注之漏洞修補管理、弱點掃描、滲透測試，實機測試課程則為 Kali Linux 滲透測試，滲透測試不同的脆弱性評估和每個攻擊成功的標準。

(三)10 月 25 日：講述主題包括說明組態管理、變更管理和發佈管理之間的關係，導致安全性漏洞的不良作法、弱點掃描與滲透測試之差異、滲透測試個案研討分析、資料庫漏洞管理，並以個案研討方式介紹如何辨識漏洞風險，瞭解攻擊者利用一個資料庫漏洞所需的技術要素，檢視減輕攻擊的必要控制項，檢視銀行確保可快速復原的變更或回復計畫，實機測試課程則為資料庫漏洞攻擊。

(四)10 月 26 日：講述主題包括定義資安事件和事件回應目標，資安事件生命週期、資安事件回應規劃及資安事件回應團隊，前端的事件收集、中間的日誌管理和後端的事件關連分析及數位鑑識等，並由學員分組就個案之 IT 風險之監理檢查進行討論及分組簡報後，由講師以分組個案討論方式介紹如何辨識及分析資安事件，包括客戶通知之要求和其他監管原則。

(五)10 月 27 日：講述最後一項主題監理應關注事項，並由講師以分組研討方式介紹 Verizon 發布之 2016 年網路安全威脅報告(Verizon 2016 Data Breach Investigations Report)，並最後致閉幕詞及由 FED 頒發結業證書。

肆、研討主題

一、弱點管理(Vulnerability Management)

(一)弱點定義

弱點(Vulnerability)指電腦系統安全方面的缺陷，使得應用程式、系統、設備或其資料的保密性、完整性、可用性、存取控制和監測機制等面臨威脅，一些程式 bug、缺陷、程序或事件，都可被定義為弱點[1]，俗稱安全漏洞，部分資訊安全弱點是程式設計疏忽導致的，可稱為程式安全錯誤（Security bug），但有部分則是使用者操作與設定習慣不良所導致的，常見弱點有零時差漏洞（Zero-day exploit）、隱碼攻擊(SQL injection）、緩衝區溢位（buffer overflow）等。

(二)弱點成因

1. 設計階段(Design Phase)：脆弱的演算法，或系統開發設計時未考慮到的問題，或是設計錯誤(Design error)，如設計時忽略的項目，未考慮到的安全問題等。
2. 實作階段(Implementation Phase)：因疏忽或是錯誤所造成的軟體問題，如輸入驗證的錯誤(Input validation error)，界限(範圍)檢查的錯誤(Boundary check error)，或是多個行程(Process)並行存取共用資源，系統若做好排程將可能造成資源內的資料不正確而造成的競爭情況(Race condition)。
3. 操作階段(Operation Phase)：使用者操作與設定習慣不良，因錯誤的設定與疏忽，或對於設定的知識不足，未正確設定檔案權限，導致攻擊者可以存取隱私資訊相關檔案。
4. 人為威脅(Human Nature)：人性上的弱點所導致，如脆弱的密碼(Weak Passwords)，不良的使用習慣(Unsafe habits)等。

[1] 維基百科， Vulnerability，俗稱安全漏洞（Security hole），指電腦系統安全方面的缺陷，使得系統或其應用資料的保密性、完整性、可用性、存取控制和監測機制等面臨威脅。

(三)弱點管理架構

1. 弱點管理重要元素

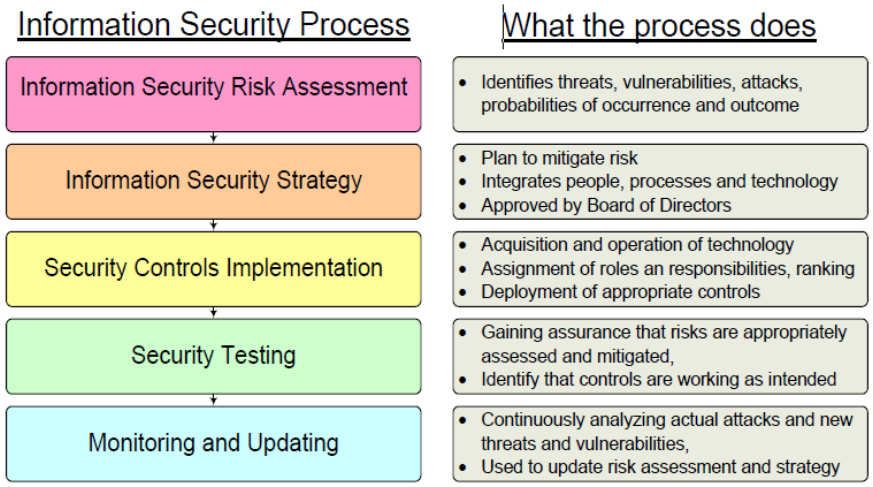
講師介紹弱點管理的重要元素，包括機構健全的資訊安全計畫，網路部署工程和資訊作業程序、資訊資產清查/盤點、風險評估、監控漏洞、漏洞修補管理、漏洞測試、安全情報、資安事件回應、數位證據、檢視相關的法規遵循等。

2. 資訊安全流程

金融機構軟、硬體及應用程式、自行開發或委外開發之軟體專案或系統，均可能因軟體開發設計、實作或操作上的錯誤或瑕疵導致潛藏資安弱點與面臨安全威脅，駭客所使用的手法及工具日新月異，攻擊的目標已從伺服器，轉向個人電腦，欲強化資訊安全，需透過健全的資訊安全流程，達到保護關鍵資訊系統之 C.I.A 三個目標，即隱密性(Confidentiality)、完整性(Integrity)、可用性(Availability)。

講師說明機構健全的資訊安全計畫應以資訊安全風險評估為基礎(如下圖)，先識別並評估內外部網路安全風險，再使用防禦性基礎設施並施行政策與程序，並應檢測網路安全事件，回應已辨識或檢測到的網路安全事件，最後從網路安全事件回復，並恢復正常運作與服務。

圖1：資訊安全流程及相應作法



資料來源：Federal Reserve System, STREAM

(四)關注弱點管理的重要性

1. 網路駭客風險

弱點和漏洞不斷的出現，駭客攻擊手法也不斷翻新，安全性漏洞是監理機關應關注的議題，現今機構面臨網路駭客風險包括：

(1)竊取資料(如敏感的客戶資料)

(2)欺詐交易 (如 ACH 電匯)

(3)分散式阻斷服務攻擊 (DDoS)

(4)系統當機

(5)網路釣魚

(6)惡意軟體滲透

(7)信譽損害

(8)操作風險

(9)財務損失

2. 駭客資源

每天都有新的軟體漏洞出現，如雨後春筍般出現的駭客網站，教人如何入侵網站、破解密碼，更有數不完的駭客工具，從事系統入侵的駭客包括新手、腳本小子(Script Kiddies)、程式設計師或高級知識攻擊者、有動機的專業人員、國家資助的間諜或恐怖分子，他們擁有的資源包括：

(1)駭客網站

(2)公共註冊服務

(3)商業可用和免費軟體工具

(4)安全資訊服務

(5)軟體服務供應商或開放程式碼

(6)在互聯網上銷售 Rootkits[2]

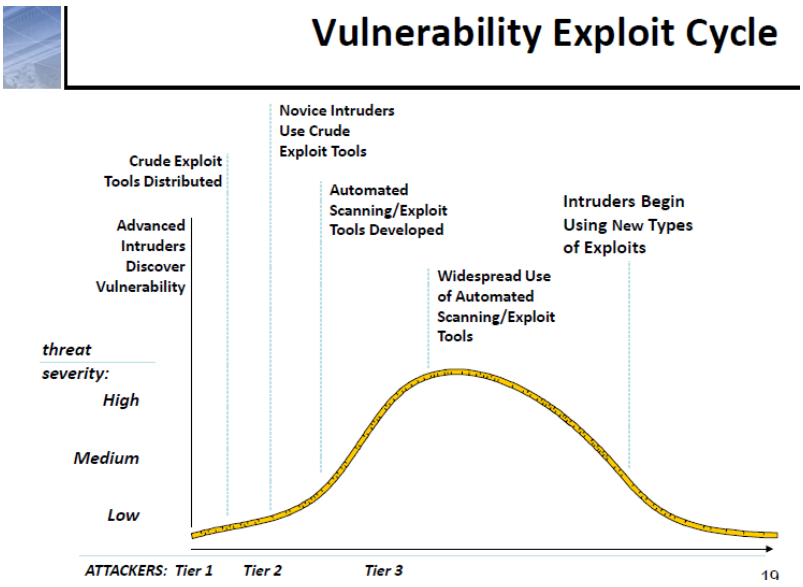
[2]維基百科，Rootkitst 一詞更多地是指被作為驅動程式，載入到作業系統內核中的惡意軟體。

Rootkit 是隱藏其他程式行程的軟體，可能是一個或一個以上的軟體組合，廣義而言，Rootkit 也可視為一項技術，值得一提的是 Rootkit 管理工具[3]，排除如今視為惡意軟體的觀點，其原本善意的用途在於便利管理者透過 Rootkit 指令集進行各種越權操作，這些指令皆是偽裝程式(masquerading program)，能不須授權直接以最高權限控制核心程序(Kernal-land)，甚至修改，類此 Rootkit 相關的管理工具，若不正視其存在，未來將會是資訊安全的風險。

3. 漏洞利用週期

弱點從被發現到採取補救措施的空窗期，可能造成有心人士利用系統弱點來撰寫攻擊程式碼(Exploit Code)進行入侵的行為，現代化工具和普遍的威脅軟體，使得網路攻擊者得以極快的速度運作，講師說明當駭客廣泛使用自動掃描/漏洞工具時，攻擊的威脅嚴重程度最高(如下圖)，現今的威脅攻擊(exploit)有很大部分是完全自動化的，它們使用廣泛掃描網際網路的工具，不斷偵測門戶大開的機構入口。

圖2：弱點利用週期



資料來源：Federal Reserve System, STREAM

[3]中央研究院資訊服務處 IT’ s 通訊，淺談安全軟體發展。

講師提醒一些常見的掃描工具可以幫助駭客進行掃描，甚至不需要具備太高深的電腦技術即可成功達到掃描被入侵目標主機的目的，像是免費軟體 Nmap，專用於網路探測掃描，它被設計來快速地掃描大型的網路，或是 Nessus 弱點掃描的工具軟體，專用於尋找各種軟硬體的設定漏洞和系統弱點，攻擊者可以利用此類工具軟體在目標電腦主機上尋找可供入侵的管道。

4. 制定最佳實務作法

(1)金融機構應強化網路安全計畫，包括作業系統、應用程式和資料庫安全管理，及強化週邊設備管理(包括防火牆、IDS、IPS 等)。

(2)金融機構應強化員工資安意識/社交工程風險。

(3)金融機構應強化監控漏洞(含軟體和硬體)。

(4)金融機構應強化程式修補管理機制。

(5)金融機構應進行漏洞測試（包含複測）。

(6)金融機構應建置資安事件回應計畫。

(7)金融機構應建立數位證據保全機制。

(8)金融機構應建立安全情報蒐集及分析機制。

(9)金融機構應導入安全軟體發展生命週期並確保遵循相關規範(Secure Software Development Life Cycle, SSDLC)。

學員提問系統開發人員過於強調功能面(求最短時間內完成產品)缺乏 Security design in & build in，軟體安全得到的關注不夠，講師補充說明越後期修補成本越高，機構應定期對系統開發部門教育常見的安全漏洞問題、安全的程式設計方法，以及如何測試與防範威脅的方法，經由教育訓練協助軟體開發者重視安全問題，從攻擊者的滲透行為中獲取適當的程式設計思路，並注意測試(Testing)階段驗證安全需求，提升軟體的安全性。

二、風險緩解(Risk Mitigation)

(一)風險範圍

1. 現今有 25 種不同類型的金融犯罪由美國特勤局[4]調查，主要有身分盜竊、銀行詐騙、信用卡詐騙、洗錢、退稅欺詐、郵件詐騙等威脅。
2. 其他犯罪活動，包含騷擾、網路霸凌、威脅、攻擊性的材料、勒索、網路恐怖主義、網路間諜(IP，情報、工業、APT 攻擊)、護照欺詐、駭客行為等。

講師主要說明威脅情資，建議金融機構可從社群媒體的談論主題、媒體報導、部落客文章及 CERT 的公開資訊等廣泛蒐集公開情資，並針對所使用的特定軟體去偵測相關弱點，再透過 CVE 漏洞編號加以關聯整合，瞭解機構所使用軟體的相關漏洞是否已遭攻擊的參考。

(二)弱點管理程序

1. 資產識別：金融機構應建立需要保護的資訊資產清單，包括資訊資產、軟硬體資產、設備資產及人力資產等。
2. 威脅評估：金融機構應能辨識和描述威脅，威脅是指特定類型攻擊的來源和手段，包括：
   (1)金融機構應完整考慮各種威脅，包括非人為的、犯罪的、恐怖主義及意外事故等範圍。
   (2)金融機構須進行威脅評估，以確定確保機構系統能抵禦特定威脅或威脅類別的最佳作法。
3. 脆弱性評估：金融機構應評估其關鍵資產對特定威脅的脆弱性，脆弱性評估在風險管理過程中的作用為找出最具風險的系統與資訊，並排列其優先順序。
4. 風險評估：金融機構應分析風險，包括對機構特定資產產生威脅的

[4] 維基百科，美國特勤局（United States Secret Service，USSS）是美國聯邦政府的執法機構。

可能性及其影響程度等。

5. 風險緩解：金融機構應根據組織政策，確定並優先考慮減少風險的措施。

講師說明資訊系統可能因意外或故意觸發資訊系統安全漏洞弱點(Vulnerability)所產生的威脅(Threat)，以及對組織產生的衝擊影響(Impact)程度評估風險，評估資訊風險可就弱點、威脅及衝擊三者計算其風險值，並以威脅程度進行風險評估，從威脅發生的可能、能力、意圖三個層面(如下圖)，評估弱點潛在的風險高低和衝擊度。

圖3：風險評估表

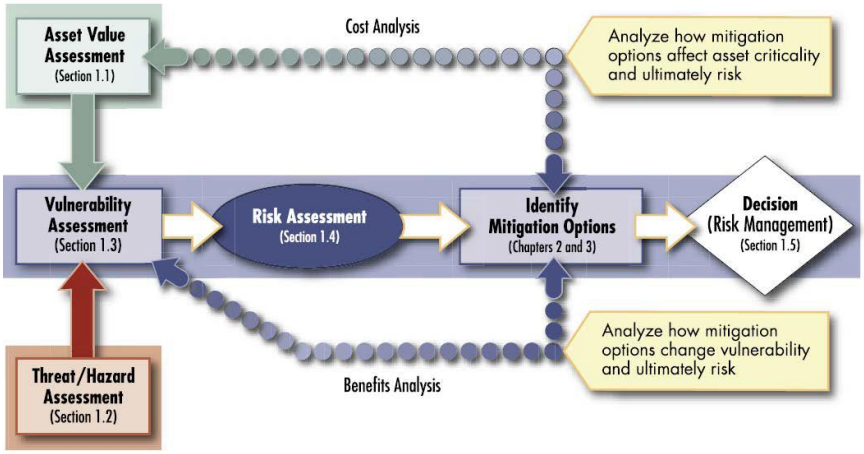
	Threat			Opportunity/ Vulnerability	Impact
	Credibility	Capability	Intent		
High (2)	Information from highly reliable source or has been independently confirmed	Actors possess Expert level knowledge and extensive resources indicative of organized efforts	Targeted confidentiality, integrity, or availability (CIA) attack of dataset or individuals. Disruption of critical Organization mission or function.	Systems vulnerable to known vectors or methodology and/or available to known Actors.	Significant impact to Organization Programs, Project, Operations, People, Data, Systems, or Cost.
Moderate (1)	Information from normally reliable source but unconfirmed	Actors possess Moderate to high levels of sophistication with moderate resources	Non-targeted Attacks of Organization's systems affecting confidentiality, integrity, or availability (CIA) of data. E.g. web defacement, botnets, etc.	Systems potentially vulnerable to known vectors or methodology and/or potentially available to known Actors.	Moderate impact to Organization's Programs, Project, Operations, People, Data, Systems, or Cost.
Low (0)	Information from unreliable source or source without established history (or Unknown)	Actors possess Low level of sophistication with little resources required. (or Unknown)	"Drive by" or opportunistic attacks (or Unknown)	Systems not likely vulnerable to known vectors or methodology and/or not likely available to known Actors (or Unknown)	Low impact to Organization's Programs, Project, Operations, People, Data, Systems, or Cost. (or Unknown)

資料來源：Federal Reserve System, STREAM

講師引用美國聯邦緊急事務管理署 The Federal Emergency Management Agency（FEMA[5]）制定的風險評估指引(Assessment Process Model）說明風險評估與風險緩解的關聯性(如下圖)。

[5]維基百科，美國聯邦緊急事務管理署 The Federal Emergency Management Agency (FEMA)，是美國聯邦政府行政部門防災減災機構。

圖4：FEMA 風險評估流程模型



資料來源：Federal Reserve System, STREAM

(三)建置管理機制

1. 惡意軟體檢測

主要檢測項目包括病毒、蠕蟲、間諜軟件、Rootkit 的工具、殭屍網路(Botnet[6])、DDoS 攻擊、鍵盤記錄器(又稱鍵盤側錄)等，以確保電腦免受盛行的惡意程式碼威脅，講師提醒學員應特別注意危害級別高的殭屍網路(Botnet)。

2. 弱點修補和監控

(1)金融機構須制定有效的漏洞修補管理程序，並落實弱點修補作業。

(2)金融機構應設置自動更新修補程序，原則包括：

①須能確保即時獲取最新的弱點資訊。

②應儘量縮短發佈修正檔至機構各單位所有電腦設備應用修正檔的期間。

(3)金融機構應設置持續警示監控機制，包括：

①建置入侵偵測系統（Intrusion-detection system，IDS），監控網路傳輸或系統，並檢視有無可疑或違反組織政策的活動，並應即

[6]維基百科，是指駭客利用自己編寫的分散式阻斷服務攻擊程式將數萬個淪陷的機器，即駭客常說的傀儡機，組織成一個個命令與控制節點，用來傳送偽造包或者是垃圾封包，使預定攻擊目標癱瘓並「阻斷服務」。

時發出警報或採取主動防禦措施。

②建置入侵防禦系統（Intrusion Prevention System，IPS），監控網路或網路裝置的網路資料傳輸行為，以即時中斷、調整或隔離不正常或是具有傷害性的網路資料傳輸行為。

③建置安全性資訊和事件管理系統(Security Information and Event Management，SIEM)，即時掌握所有系統、網路、資料庫與應用程式的所有活動，獲取所需的可行情報，檢視並排定優先順序和調查威脅，並能做出適當回應。

(4)安全情報蒐集，包括：

①應建立蒐集與漏洞相關聯資訊的方法，以及系統安全控制的措施。

②快速檢視、有效正確的確認網路上的弱點。

③評估對機構的潛在影響程度。

④應透過抵減風險和修補程式管理過程，排定優先順序和補救級別，並建立定期弱點掃描機制，找出是否存在未更新修正檔、安全性組態設定不當或其它潛在弱點。

⑤瞭解目前的漏洞對脆弱性評估的有效性和解釋至關重要。

(四)安全情報資源運用

講師透過實機操作，指導學員利用下列開放資源，瞭解現今主要公開的漏洞來源：

1. Security Focus(http://securityfocus.com/bid)：

(1)美國私人資訊安全公司，現今由賽門鐵克所擁有。

(2)進行維護 Bugtraq 漏洞報告列表，可供公開搜尋，是一個大型的安全和漏洞訊息庫(包括漏洞)。

2. NIST[7] Vulnerability Database(NVD)，NIST 的國家漏洞資料庫

[7]維基百科，美國國家標準技術研究所（National Institute of Standards and Technology，NIST），是一家測量標準實驗室，屬於美國商務部的非監管機構。

(http://nvd.nist.gov/)，優點包括：

(1)向 NIST 和其他實體報告的漏洞目錄。

(2)使用常見漏洞和披露（CVE）索引進行組織分類。

(3)可供搜尋的，且按嚴重程度評分。

3. Computer Emergency Response Team (CERT[8])CERT 的漏洞通報資訊 (http://www.cert.org/)：

(1)隸屬於美國匹茲堡卡內基梅隆大學行業事件報告小組。

(2)屬於明確的可供搜尋的漏洞和事件資料庫。

美國聯邦政府於 1988 年資助成立第一個電腦緊急應變團隊 CERT® Coordination Center(CERT/CC)，並由卡耐基大學負責營運，目的在於針對資安事件協助緊急應變、協助其他組織建立電腦緊急應變團隊及擔任協調中心進行資訊分享，其他國家亦陸續效法成立電腦緊急應變團隊。

(五)漏洞管理

1. 挑選適合的掃描工具軟體，業界提供免費軟體與商用軟體供機構選擇使用，其中，免費軟體雖得免費使用，但受維護成本的限制，更新頻率較商用軟體低，相對影響工具的效能與準確度，常見掃描工具包括：

(1)Nmap，是一款免費的開源實用程式，用於網路探測或安全審核，快速掃描大型網路和單一主機，可運用在多數類型的電腦上，且可以支援大多數作業系統。

(2)Nessus，是一款免費的開源弱點掃描工具，支援各種平台，如 Linux、Solaris 等，主要用於系統服務的弱點評估，採外掛方式可不斷擴充功能，目前已超過 1,000 個以上的弱點偵查能力。

(3)SuperScan，是一款免費的工具，功能強大，卓越的掃描速度，支

[8]美國電腦危機處理中心 (US-CERT)，2003 年美國國土安全部成立 US-CERT，建立國家體系之預警系統，以強化國家資安事件緊急應變與協調能力，是專門處理計算機網路安全問題的組織。

持無限的 IP 範圍。

(4)SAINT，提供企業為主的漏洞掃描，是基於伺服器的解決方案，可在 Unix 平台上運行，並提供全自動滲透測試軟體。

(5)Metasploit，是一組開源漏洞檢查及管理工具，可利用模組化方式不斷擴充功能，Metasploit 的模組主要分成弱點利用(Exploit)、載荷(Payload)及輔助模組(Auxiliary)。

(6)Backtrack (Kali Linux)，是一款資訊安全掃描工具，提供大量和全面的安全相關工具，常見的包括 Metasploit 及 Nmap，BackTrack，也是駭客的常用工具，涵蓋一系列駭客工具及附加軟體和腳本。

2. 漏洞發現、分析、管理

(1)使用弱點掃描工具，偵測並掃描位於主機上的各個端口或節點的弱點資訊後，與自身的資料庫進行比對，並將分析出的相關弱點或漏洞資訊產生報告，供系統管理者快速瞭解並進行設備管理的修正決策。

(2)掃描發現弱點後，利用風險指數評估，其一為 CVSS 的指數，另一種則是綜合主機重要程度、漏洞的嚴重程度與造成危害的程度，進行較精確的風險評估指數，並提供漏洞修補的建議，當今業界公認規模較大的弱點資料庫，包括 BID、CERT、CVE、IAVM、MS、MSKB、OVAL 等。

(3)在評估風險的嚴重性後，根據相關的分析結果安排漏洞修補的優先順序，在惡意攻擊者出現前先進行防範。

三、漏洞修補管理(Patch management)

(一)通用漏洞披露 (CVE，Common Vulnerabilities and Exposures)[9]

1. 通用漏洞披露（CVE, Common Vulnerabilities and Exposures）又稱常見弱點與漏洞，是由美國非營利組織 MITRE 所屬的 National Cybersecurity FFRDC 營運維護的一組已知資訊安全漏洞字典資料庫，收集各種資安弱點及漏洞並給予編號以便於公眾查閱。
2. 藉由 CVE ID 及 bugtraq ID 可以快速索引到該弱點的相關資訊。
3. CVE 是一個目錄(Directory)包含許多弱點或安全漏洞的標準名稱，其設計目的是為了讓不同的系統或機構對相同的弱點或漏洞有共同遵循的名稱。
4. 弱點被放進 CVE 目錄正式定名前，會先成為候選弱點，經過社群接受後才成為 CVE。

(二)漏洞 CVE 編號

1. 每一個通用漏洞披露都賦予一個專屬的編號，格式如：CVE-YYYY-NNNN。
2. CVE 為固定的前綴字，YYYY 為西元紀年，NNNN 為流水編號（該年度被發現的序號），例如於 2014 年發現的心臟出血漏洞編號為 CVE-2014-0160。

(三)CVE 弱點資料庫

1. CVE 列出了弱點及其他資訊安全暴露的標準化名稱，其目標是將所有已知弱點和安全風險的名稱標準化，包括訂定一個唯一的名稱，提供一個標準化的描述，每一個通用漏洞披露都賦予一個專屬的編號、統一名稱，使評估報告更容易被理解與解讀。
2. CVE 是一本詞典，其目的是有利於在各個弱點資料庫和安全工具

[9]維基百科，通用漏洞披露（CVE, Common Vulnerabilities and Exposures）又稱常見弱點與漏洞，是一個與資訊安全有關的資料庫，收集各種資安弱點及漏洞並給予編號以便於公眾查閱。

之間發佈資料，CVE 使得在其他資料庫中搜尋資訊變得簡便，因此，不應該單獨將其視為弱點資料庫。

3. CVE 由一個稱為 CVE 編輯委員會的全社群共同合作維護，該編輯委員會包括來自許多安全性相關組織的代表，例如安全工具廠商、學術機構和政府，以及其他著名的安全性專家，目前由 MITRE 公司負責維護 CVE 並協調編輯委員會的討論。

(四)CVSS 通用漏洞評分系統

1. SCAP 安全內容自動化協定

維基百科，安全內容自動化協定（Security Content Automation Protocol，SCAP[10]）是用於自動化漏洞管理、評估和條件符合檢測的一套標準，美國國家漏洞資料庫（NVD）是美國政府為安全內容自動化協定制定的知識庫，SCAP 是一系列用於評估軟體缺陷和安全相關問題的開放標準，用於系統測試來發現漏洞，並根據漏洞可能造成的影響提供評分標準，SCAP 協定組成包括：

(1)通用漏洞披露 (CVE)

(2)通用配置評估 (CCE) (prior web-site at MITRE)

(3)通用平台評估 (CPE)

(4)通用漏洞評分系統 (CVSS)

(5)Extensible Configuration Checklist Description Format (XCCDF)

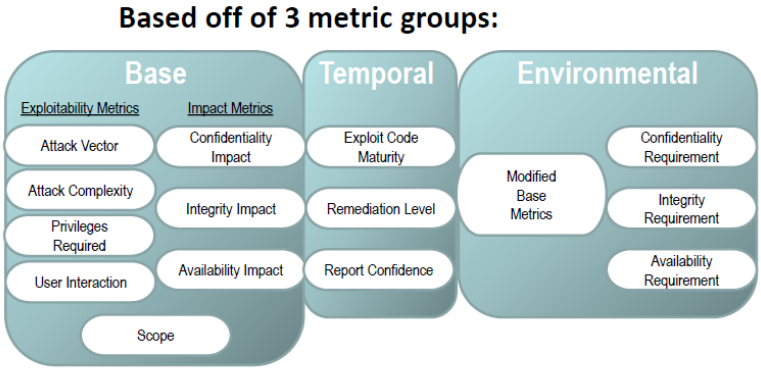
(6)開放漏洞評估語言 (OVAL)

2. CVSS 通用漏洞評分系統

講師介紹漏洞評分系統(Common Vulnerability Scoring System，CVSS)，是一個評估資訊系統安全防護漏洞嚴重程度的業界開放標準，CVSS 由三個度量組成，包括「基礎-Base」,「時間-Temporal」和「環境-Environmental」，每一組又由一些度量指標組成(如下圖)。

[10]維基百科，安全內容自動化協定(Security Content Automation Protocol，SCAP）

圖 5：通用漏洞評分系統



https://www.first.org/cvss/specification-document
https://www.first.org/cvss/calculator/3.0

資料來源：Federal Reserve System, STREAM

基礎度量組由可利用指標和影響指標兩組指標組成，反應了一個漏洞的固有特徵，即它不隨著時間和用戶環境的變化而變化；可利用指標反應漏洞可以被利用的簡單程度和技術手段，也就是代表漏洞易受利用的特徵；影響指標則反應成功利用該漏洞可以導致的直接結果，以及受該影響產生的後續結果；時間度量組反應一個可能隨時間而變化的漏洞特徵；環境度量組代表一個與某特定用戶環境相關且獨特的漏洞特徵。

3. CVSS 的優點，包括：

(1)一套資安漏洞評分標準

(2)屬開放式框架

(3)風險導向

4. 通用漏洞評分系統的使用者，包括：

(1)漏洞公告提供程序

(2)軟體應用程序供應商

(3)組織用戶

(4)漏洞掃描和管理人員

(5)安全管理人員

(6)研究人員

(五) 漏洞修補管理(Patch management)的重要性

1. 我們面臨的問題

(1)講師說明 2015 年 APWG 網路釣魚活動趨勢報告[11]，全世界約 35%的個人電腦感染了惡意軟體，APWG 成員實驗室(Panda Labs)獲取了 8400 萬新的惡意軟體樣本，漏洞發佈和漏洞利用之間的差距是縮小了，但是惡意軟體傳播速度變快，攻擊技術的複雜性也穩步提高。

(2)依據 2016 年第四季網路釣魚活動趨勢報告中，Panda Labs 技術總監兼趨勢報告分析師 Luis Corrons 認為，世界上最高受感染的國家是中國（47.09%），其次是土耳其（42.88%）和台灣（38.98%）(如下圖)，此一問題值得我國關切。

圖 6：惡意軟體感染國家-2016 年第四季

Ranking	Country	Infection Rate
1	China	47.09%
2	Turkey	42.88%
3	Taiwan	38.98%
4	Guatemala	38.56%
5	Ecuador	36.54%
6	Russia	36.02%
7	Peru	35.75%
8	Mexico	35.13%
9	Venezuela	34.77%
10	Brazil	33.13%

Ranking	Country	Infection ratio
36	United Kingdom	24.54%
37	Germany	23.66%
38	Belgium	23.32%
39	Switcherland	22.69%
40	Netherlands	22.43%
41	Japan	21.79%
42	Denmark	21.54%
43	Finland	20.78%
44	Norway	20.51%
45	Sweden	20.03%

資料來源：APWG, 2016

2. 漏洞修補管理的重要性

(1)講師說明 2016 年 Flexera Vulnerability Review[12]報告指出，75%的網路攻擊者使用公開的商業軟體漏洞，而透過經常修補是可以防止的，84%的漏洞披露後，在最受歡迎的 50 個程式中，披露當天有一個修復，違規使用特定漏洞的數量在披露後 2 個月左右達峰值，補丁管理不斷排在首位最重要的準則和行業標準安全配置，包括美國國家標準和技術研究院（NIST）和 SANS 20 關鍵安全

[11] APWG，美國反網路釣魚工作組織（Anti-Phishing Working Group，簡稱 APWG），每季提出網路釣魚活動趨勢報告。

[12] 講師簡報引用資料來源：Flexera Vulnerability Review, 2016 年

控制。

(2)資料外洩的經驗教訓

①依據 Verizon(DBIR)[13]「數據失竊調查報告 2016」指出，89%的攻擊與詐財或間諜活動相關，雖然一些網路漏洞修補程式已存在多月或甚至多年，大部分網路攻擊的入侵點，都是從未修補過的資安漏洞。事實上，85%成功的網路攻擊，都是利用報告中提及的常見十大漏洞，儘管攻擊的複雜性越來越高，大多數是可以輕鬆地預防，很多機構仍嚴重缺乏基本的防禦措施。

②講師特別說明，在 Verizon 數據失竊調查報告中，不足 1%的資料竊取行為使用了在 VERIS 難度量表上被評為「高」的手法，事實上，我們看到的手法中有 78%是屬於「低」或「非常低」的類別。

3. 無效修補程序的風險

(1)金融機構因伺服器或最終用戶停機而導致的收入損失。

(2)金融機構失去客戶滿意度，信任度和忠誠度。

(3)金融機構資料丟失或被盜取。

(4)金融機構聲譽受損。

(5)金融機構之法規遵循失敗（如 HIPAA[14]，美國健康保險隱私及責任法案（Health Insurance Portability and Accountability Act）。

(6)金融機構可能面臨法律責任。

(六)檢查應關注事項

1. 金融機構程式修補過程，包括驗證修補程式：

(1)機構已安裝的電腦、應用程式和修補程式的清單。

(2)機構確認辨識相關的修補程式。

[13] 維基百科，威訊通訊（Verizon Communications），是美國一家主要電信公司，全球領先的寬帶和電信服務提供商，自 2008 年開始每年發布 DBIR 資料失竊調查報告。

[14] 維基百科，美國政府 1996 年頒布 HIPAA，詳細規定醫療機構處理病人訊息規範。

(3)機構透過掃描以確定修補程式的狀態。

2. 檢查重點項目

(1)檢視金融機構修補程式管理的策略和過程。

(2)檢視金融機構變更控制的策略和過程。

(3)檢視金融機構制定的系統部署標準文件。

(4)檢視金融機構的系統清單，包括主機名稱、主機 IP 位址、主機角色/應用程式的特性、主機作業系統名稱和版本，主要應用程式名稱、伺服器版本以及網域等資訊。

(5)檢視金融機構詳細的網狀圖，按名稱和/或 IP 位址描述各個伺服器。

(6)檢視金融機構目前使用的任何自動修補程式管理系統的名稱和版本。

(7)檢視金融機構針對目標系統的當前修補程式級別的詳細報告。

3. 檢查的程序

(1)確認檢查範圍(Scope)

①特定元素的特定修補程式級別，包括 DMZ、作業系統、工作站、伺服器等。

②驗證資訊，包括場內、場外的驗證。

(2)修補程式評估(Patch Evaluation)

①金融機構相關人員是否收到安全修補程式的通知？

②金融機構是否有足夠熟練的人員執行修補程式管理？

③金融機構如何確定補丁的相關性、真實性和緊迫性？

④金融機構測試補丁如何確保它們是安全的？

⑤金融機構是否有標準操作流程並落實到位，或者日常操作基本上不明確和不精確？

(3)組態設定管理(Configuration Management)

①金融機構如何確保只有經批准的標準配置才能佈署到正式環境？

②金融機構是否有組態設定管理的作業程序？

③金融機構是否具有識別組件之間關係的基礎架構邏輯圖？

④金融機構如何維護最新的組態設定資訊？

⑤金融機構是否定期調整組態設定數據與實際環境之間的差異？

(4)變更管理(Change Management)

①金融機構如何審查和授權緊急變更？

②金融機構如何根據優先級，類別，緊迫性和影響對變更進行分類？

③金融機構之變更管理和過版管理是否存在作業程序？

(5)過版管理(Release Management)

①金融機構如何佈署到正式環境中？

②金融機構過版如何測試？

③金融機構是否具有用於發佈部署的標準流程和工具？

④金融機構是否更新配置數據以反應新版本？

四、弱點掃描與滲透測試

弱點掃描及滲透測試的主題，講師授課主要透過實機操作，指導學員使用滲透測試工具Kali Linux，模擬駭客攻擊手法，及個案研討、分組討論等方式，內容涵蓋基礎IT技術、網路安全及相關法規遵循概念，以促進學員對安全漏洞，包括弱點名稱、類型、弱點描述、修補方案等資訊評估和控制之瞭解。

(一)弱點掃描(Vulnerability scans)

隨著網路技術的蓬勃發展，網路上的惡意活動愈來愈頻繁，企業更

加重視在網路世界的安全防護，因此，資訊安全防護，除了大家所熟悉的防火牆、防毒軟體及入侵偵測防禦系統等，弱點掃描技術也是資安的重要技術之一。

講師介紹弱點掃描的概念及目的與其他類型的安全測試之差異，弱點掃描在銀行安全策略與實踐中的作用，並實際透過在實驗室環境中使用通用軟體工具執行弱點掃描來瞭解弱點掃描的過程，再以通過案例分析方式，讓學員瞭解弱點掃描的重要性。

1. 弱點掃描執行者，包括：

(1)四大會計師事務所。

(2)網路安全專家，如 Digital Defense、Riptech 等資訊安全廠商。

(3)託管安全監視/服務公司，如 Security Focus、ISS、Tru Secure 等網路安全公司。

(4)老虎隊(Tiger teams[15])，資訊安全單位。

(5)IT 單位人員，通常作為軟體發展生命週期(Software Development Life Cycle, SDLC)測試方案的一部分。

2. 弱點掃描執行廠商之條件

(1)道德和正直：資安專家須具備高度企業倫理與道德，確保不會將測試資訊以任何方式傳遞給第三方。

(2)較強的溝通能力：能將技術問題傳達給管理高層，並使機構積極參與技術討論。

(3)知識和經驗：適合規模和複雜性的專業技能，尋找強大的研發團隊、檢查引用、應用經驗。

(4)知識移轉：應該能夠協助機構員工加快速度進行掃描結果的後續建議修補事項。

[15]Tiger team（老虎隊）是指一個臨時的任務編組，任務完成後成員各自歸隊，組建的團隊成員通常來自各個部門的精英或佼佼者，以及針對需要解決問題的專家。

講師說明弱點掃描是使用自動化工具對系統進行檢測，目標是系統錯誤，找出所有已知的風險，這種測試比較依賴程式本身的品質，不同廠牌、不同種類的規則，都會有不同的結果，又因為是程式自動化掃描，可以一次做大規模數量的掃描，但也因為程式自動化，恐有誤報的問題，同時可能也無法提供修補建議，若要做完整的資安檢測，建議還是聘請專業資安公司進行滲透測試，因為滲透測試所針對的目標是受測系統與所有大環境的運作，像是程式中的邏輯問題、系統運作流程瑕疵、社交工程漏洞等，都包含在滲透測試範疇內。

臺灣學員向講師提問有關機構向供應商採購的套裝軟體或應用系統，多有未取得原始程式碼的問題，此時機構會要求供應商於交貨時提交弱點掃描報告，而這弱點評估或弱點掃描應由誰來執行，講師表示，基於軟體開發設計上的錯誤或瑕疵易致潛藏資安弱點的考量，建議由獨立的第三方機構執行較佳，同時第三方檢測專家也可提供修復協助或諮詢，目的均在於設法避免程式碼中的資安問題。

(二)滲透測試(Penetration Testing)

依據美國國家標準技術研究院(National Institute of Standards and Technology，NIST)所提出的文件「Guideline on Network Security Testing」，滲透測試的定義為：「滲透測試是測試者藉由對 Web 應用程式設計以及執行的瞭解，試圖繞過系統的安全防護以發動攻擊的一種安全測試，目的是借由常用的工具及技術取得系統權限」，此種檢測方法為黑箱測試(Black-Box Testing)的一種。

1. 滲透測試的重要性

(1)找出各種潛在的漏洞，驗證機構的資料與設備是否可被竊取或破壞。

(2)測試組織安全配置文件之外的安全政策略和程序，包括機構抵抗非技術攻擊，如垃圾搜尋 dumpster-diving[16]、社交工程之檢測和回應能力。

(3)評估機構的資訊系統與硬體的整體架構，確認其安全性是否有待加強，提供問題領域的詳細快照(snapshot[17])。

(4)得到管理階層的關注。

2.滲透測試的局限性

(1)未考慮系統配置問題的影響，採取阻力最小的路徑，然而實際環境可能存在更多的路徑。

(2)隨著資訊系統的變化，可能產生新弱點，滲透測試的價值有限。

(3)滲透測試在有限的時間內完成，然而攻擊者總是有更多的時間。

(4)測試有效性仰賴測試人員本身的資安素養、專業知識以及經驗。

(5)測試須花較長時間與較多資源，有可能對正常運作造成影響。

3.滲透測試基本攻擊流程

(1)偵查：可以同時使用網路探測、弱點掃描、社交工程等手法。

(2)網路與主機掃描：利用漏洞以取得使用的作業系統、網路應用程式版本及是否存在已知的弱點等資訊。

(3)弱點利用提升權限：取得對主機的管理存取權限。

(4)維持存取：重複這個過程，直到實現滲透測試的目標，通常是對關鍵系統的完全遠程管理控制。

(5)清除入侵軌跡：確保未來的安全和可用性、刪除後門(backdoors)、刪除嗅探器(sniffers)，講師特別說明，一些機構傾向於滲透測試供應商進行清除和回復，其他人則更願意根據供應商提供的攻擊訊息自行處理，任何一種方式都有風險。

[16]維基百科，垃圾搜尋 Dumpster Diving 蒐集被監視者所傾倒的垃圾，從垃圾中去尋找關鍵資訊的蛛絲馬跡。

[17] 維基百科，在電腦系統中，快照（snapshot）是整個系統在某個時間點上的狀態，它儲存了系統映象（System image），讓電腦系統在出現問題時，可以快速恢復到未出問題前的狀況。

4. 滲透測試報告:滲透測試專家於測試結束後,較能提供完整的報告。包括目標的說明、測試的流程、 漏洞的描述、漏洞利用的方式及修補的建議等。透過完整的報告輔以資安顧問的輔導，針對這些漏洞進行修補。

講師特別提醒在修補完畢之後,必須再針對有漏洞的頁面進行複測，檢視修補的方式是否完整，駭客是否還可以透過此漏洞進行攻擊，經過複測無問題，則滲透測試才告完成。

講師介紹免費的滲透測試工具 Kali Linux，指導學員透過實際應用,於虛擬伺服器(VM)實機安裝 Kali Linux 滲透測試工具，建立滲透測試環境，然後執行偵查、掃描、破解密碼等步驟，讓學員模擬駭客攻擊的手法，瞭解滲透測試之目的以及流程，並掌握其所需之相關技巧。

(三) 弱點掃描與滲透測試之差異比較

1. 目標不同

(7)弱點掃描的目標：針對已知的弱點，檢查系統的弱點狀況。

(8)滲透測試的目標：針對已知和未知的弱點，藉由擬真之網路滲透技巧及入侵技術，進行特定系統的攻擊以及入侵，藉此發現系統潛在安全漏洞。

2. 範圍不同

(1)弱點掃描的範圍：網路裝置、作業系統、資料庫、應用程式等。

(2)滲透測試的範圍：網路系統。

3. 執行方式不同

(1)弱點掃描的作法：可以使用自動化的掃描工具，不需要專家，只要一般資訊人員即可執行。

(2)滲透測試的作法：由具備極高技術水準的資安顧問以人工方式模擬駭客的思維,針對系統做攻擊測試,以便發現現有的安全漏洞，

需要高度專業人員。

4. 使用工具不同

(1)弱點掃描：針對系統弱點掃描使用之工具有 Nessus、Openvas、Nexpose，Web 弱點掃描使用之工具有 ZAP(OWASP Zed Attack Proxy)、Acunetix、WebInspect、W3af 等評估工具。

(2)滲透測試：依照滲透測試檢測項目使用不同工具，使用之工具須經過實際測試並確認其用途，有 Kali Linux、Metasploit、PowerSploit、Acunetix WVS、NetSparker、Nessus Professional、Burp Suite Professional、Wireshark 、Nmap 等。

學員向講師提問有關測試工具的使用時，講師提醒上課所討論的產品或供應商僅供說明之用，不應被視為聯邦儲備系統對這些產品的認可。

(四)檢查關注重點

1. 金融機構怎麼能從一個不好的測試中得到一個好的測試結果？

2. 測試範圍與項目是否適當？

3. 測試方式是否有效？

4. 測試人員的資格？

5. 測試執行機構的獨立性？

6. 金融機構管理階層是否及時處理測試發現問題？

7. 是否需要重新測試？

五、資料庫漏洞(Database Vulnerabilities)

(一)網路攻擊致資料外洩

講師說明近年私隱外洩、資安漏洞等問題頻繁出現，根據Verizon 2016 DBIR的「數據失竊調查報告」指出，網絡犯罪的速度，因企業或用戶使用過於簡單甚至預設的密碼，以及未有及時為資安漏洞安裝修補程式，導致93%的個案中，攻擊者平均僅需225秒或更短時間把系統

攻陷；而在28% 的個案中，相關資料在幾分鐘內便被偷取，從調查報告亦顯示，僅25%的企業能在少於一天的時間內發現系統遭入侵或資料外洩，大部分企業可能要數週甚至數月後才發覺事件。

臺灣學員與講師討論有關臺灣金融機構面臨使用物聯網(Internet of Things, IoT)設備之安全性問題時，講師特別提醒學員，雖然Verizon 2016年與2015年的DBIR報告相較，行動裝置及物聯網裝置被駭客攻擊入侵的情況還不算太嚴重，但報告中指出，針對行動裝置和物聯網攻擊的概念並非虛構，這些設備的大規模資料外洩將來也有很大發生機會，各機構對智慧手機和物聯網設備應持續保持警惕，並加強對裝置之保護。

(二)資料庫安全威脅

講師介紹IMHO組織發布的2016年調查分析十大資料庫安全威脅(如下圖)，講師提醒在應對資料庫威脅和風險時，應該有針對性地從多方面入手，包括金融機構管理人員的資安意識、內部控制度、技術層面，以及遵循基本的威脅防範準則等。

圖7：2016年十大資料庫安全威脅

資料來源：Federal Reserve System, STREAM

1. 過多和未使用的特權帳號(Excessive and Unused Privileges)：

預設的資料庫特權授權過度是危險的，主要有員工被賦予超出工作所需的過多權限，及合法權限被濫用或惡意使用等兩大主要問題，當使

用者被授予超出其所被定義的工作職掌時，此資料庫帳號權限便存在被用來執行未經授權的不當資料操作或破壞資料庫的風險，且過多的群組和角色特權，易致權責不分。

2. 資料庫輸入注入(Database Input Injection)：

包括SQL injections、Buffer overflows、NoSQL injections、Weaponized Malware 等，SQL注入不僅是最常見的資料庫漏洞，也是OWASP組織應用安全威脅列表上的頭號威脅。

3. 惡意軟體攻擊(Malware)：

包括Phishing、Hopscotch、Botnets等惡意程式碼，為近年最熱門的入侵方式。

4. 失效的資料庫配置管理(Exploitation of Misconfigured Databases)：

包括佈署問題、未即時修補資料庫漏洞、欠妥適的建構管理、欠缺安全測試等。

5. 拒絕服務攻擊(Denial of Service Attacks)：

此類攻擊是針對提供特定服務之主機，執行大量且合法的操作請求，意圖占用大量網路頻寬及系統資源，以期造成資料庫主機資源耗盡及服務中斷之狀況。

6. 敏感資料未加密(Lack of Data Encryption)：

存檔資料加密，並嚴密監視存檔資料存取和使用情況，可以大幅減少內部人的威脅，建立資料外洩防護(DLP)，防止授權之使用者將資料庫中未加密的敏感資料，直接或轉存為其他檔案格式，透過網路外流至用戶端或其他儲存設備。

7. 稽核軌跡不全(Weak Audit Trail)：

留存稽核軌跡的重點在於能夠在資料存取流程中，正確且有效地記錄進行資料操作的使用者、資料庫物件、資料存取動作及執行時間等完整詳細的資料庫活動稽核紀錄，大多數本機稽核日誌記錄機制對資料

庫伺服器平台是唯一的、理想情況下，稽核權力和責任應與資料庫管理員和資料庫伺服器平台分開，以確保強有力的權責分離政策，講師並提醒學員應注意合規議題，包括GLBA、Sarbanes-Oxley（SOX）、HIPAA等符合標準的規則要求。

8. 儲存媒體外洩(Storage Media Exposure)：

備份資料遭竊或資料庫備份未加密，大部分機構對於資料庫備份儲存媒體常是疏於加密保護的，當有心人取得資料庫備份檔，是有可能將資料庫還原到異機，以取得原資料庫中所存放之機敏資料。

9. 多個資料庫管理不一致(Inconsistent Management of Multiple Databases)：

管理者需要建立一個管理數個資料庫的一致性標準，內容須涵蓋資料庫管理員、系統管理員及資料庫開發人員，且必須意識到跨平台的威脅和漏洞。

10. 資安專業知識和教育不足(Limited Security Expertise and Education)：

人為因素占資料外洩的30%，許多企業在資料安全防護的策略規劃與處理能力上，並未隨著其業績獲利與營運資料的成長而提升，加上對內部員工亦疏於加強資安知識宣導與專業培訓，均為資料安全之潛在威脅。

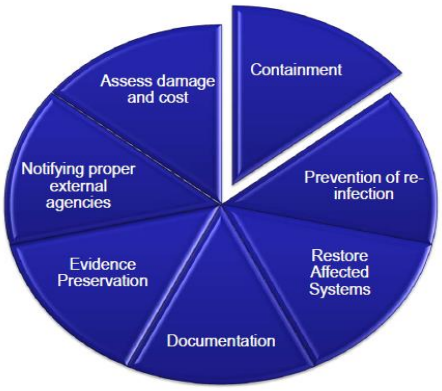
六、資安事件回應(Incident Response, IR)

(一)資安事件定義

1. 資安事件指中斷正常操作程式和沉澱某種程度的危機情況，包括：系統入侵、拒絕服務攻擊、內部盜竊資料，以及任何未經授權或非法的網路活動，需要資訊安全人員、系統管理員或資訊犯罪調查人員作出回應的。

2. 資安事件回應，指事件被識別和解決的過程，講師以下圖所示，說明事件回應的生命週期：

圖8：(一)資安事件回應的生命週期



資料來源：Federal Reserve System, STREAM

(二)電腦犯罪與數位鑑識

1. 電腦犯罪是涉及電腦的任何犯罪活動或問題，數位鑑識是資訊安全領域的一個新興學科，專注於在發生資訊安全事件後發現證據。

2. 電腦犯罪分子總是留下痕跡，所以這只是「找到這些軌跡的問題」，從電腦系統或存儲媒體中恢復證據有三階段，獲得、分析和報告。

3. 鑑識的結果可用於法律訴訟。

4. 網路調查員(Cyber Investigators)

(1)打擊電腦犯罪的關鍵武器。

(2)在調查中蒐集、檢查和呈現數位證據。

(3)鑑識，處理和檢查沒有污染的數位證據。

(4)事件回應程序的關鍵組成部分。

(5)金融機構是否具有執行數位鑑識的技術專業知識？如果不是，是否其他具體因應的做法？

(6)所有銀行都應該訂定明確政策。

5. 事件清理

(1)確定要清理的系統

(2)實施清理程序，一些銀行傾向於透過受託執行滲透測試之廠商進行清理和恢復，其他人則更願意自己處理由資安監控廠商(SOC)

提供的攻擊資訊，但是，講師提醒兩者皆存在風險。

(3)確保未來的安全和可用性，包括刪除後門及刪除嗅探器

(三)最佳實務做法

1.事先準備是成功的關鍵

(1)金融機構是否建立快速回應安全漏洞的計畫？

(2)金融機構蒐集初始訊息的效率如何？

(3)金融機構能夠多快地做出相關調查、隔離和阻擋、回復和客戶通知的決定？

(4)金融機構工作人員是否瞭解事件狀況並能作出決策？

(5)金融機構的準備工作對鑑識資料的分析尤為重要。

(6)金融機構是否能避免延誤？

(7)金融機構是否能驗證初始訊息以支持相關決策，包括：

①檢視哪些情境或狀況更有可能發生？

②瞭解在資安事件各個階段可不可能有明確的結論。

③完整考慮所有的觀點，如業務面、法律面、消費者等

(8)金融機構是否根據發生的新訊息評估風險影響程度，包括：

①如果可能發生的事件出現，那麼可能的情況為組織帶來風險範圍？

②會不會因機構目前的作業狀況而暴露更大的風險。

③未來的風險。

2.該機構是否準確地記錄一切決策資訊。

講師說明應迅速採取行動，儘量減少當前威脅的影響，同時儘量減少對營運資源的影響，且要盡可能迅速地減少根本原因的漏洞和暴露的影響，並提醒學員注意：

(1)數位鑑識非常複雜，數位證據規則是無情的，如果沒有做好充分的準備和測試，建議依靠外部的專業知識，使用可靠的工具，遵

循既定的、一致的、嚴謹的程序來蒐集證據。

(2)如果起訴不是目標，得使用較不嚴謹的工具快速蒐集證據，在工作站上託管金鑰記錄器，即時進行檔案分析。

(3)從各種來源蒐集資訊，證實多個來源的調查結果。

3.該機構是否留存詳實的文檔紀錄，是必要關鍵。

(四) 檢查應關注事項

1.對客戶通知－必要項目

包括通知決定的風險評估、通知紀錄、客戶信函清單、通知媒體(電話，電子郵件等)、計畫與分析確定受影響的客戶等文件。

2.其他必要檢查項目，包括：

(1)資安事件回應小組的組成，含高階管理階層參與情形。

(2)資安事件回應小組會議紀要/ IRT 會議紀錄。

(3)資安事件回應程序。

(4)資安事件通知清單和其他早期證據等軌跡紀錄的留存。

(5)資安事件回應的員工意識。

(6)資安事件回應小組在調查、隔離和控制階段(Containment Phases)的風險評估。

(7)網路調查員(Cyber Investigators)的技術能力文件，尤其是數位鑑識人員。

(8)資安事件事後的鑑識程序和其他調查程序。

(9)資安事件監管環(Chain of custody)的程序和分析資料等其他文件。

(10)資安事件根因分析。

(11)資安事件受影響基礎設施的技術檔案。

(12)資安事件工作人員回應能力的教育訓練。

(13)資安事件與管理階層回饋，包含任何可能提高風險的非法操作

或安全事件分析報告、事件調查後的風險處理計畫、管理階層針對各安全事件的回應。

七、監理關注事項

(一)與資訊安全和漏洞管理的各種要素有關的監理議題

1.監理應關注事項

(1)如何確保管理階層妥善保護金融機構資產，包括客戶資訊？

(2)金融機構的資訊資產的脆弱性？

(3)金融機構的資訊安全建構塊(Information Security Building Blocks)，至少包括：

①全機構的資訊安全政策。

②強化資安意識(包括管理，資產清查，監控)。

③強化資訊作業環境實體安全與環境控制(包括作業系統、Apps、資料庫、防火牆等)

④落實執行漏洞監控管理。

⑤落實執行補丁管理。

⑥弱點掃描及滲透測試計畫(涵蓋重新測試)。

⑦明確的資安事件回應計畫。

⑧完整的政策、標準及程序。

⑨落實員工培訓計畫。

⑩客戶意識倡議。

2.對弱點管理應關注事項

(1)金融機構負責單位的角色與責任。

(2)金融機構監視漏洞警報的運作情形。

(3)金融機構自動更新機制的有效性（標準操作程序）。

(4)金融機構對緊急、即時、高風險的漏洞之處理原則。

3.對修補管理應關注事項

(1)金融機構全面的資產清查/盤點。

(2)金融機構的風險評估、修補程式申請與批准、修補程式測試作業、安裝和記錄軟體修改的作業流程等。

(3)金融機構是否更換管理階層。

(4)金融機構的日常修補作業和緊急修補程序。

(5)金融機構程式漏洞修補的測試流程。

(6)金融機構的備份和復原程序。

4.對資安事故回應應關注事項

包括金融機構事前準備、發現攻擊活動、事中阻擋、根除攻擊、數位鑑識與資料分析、事後追蹤等程序。

5.金融機構人員角色和責任

包括高階管理人員、資訊安全人員、資訊技術人員、稽核人員、風險管理人員、委外廠商、終端用戶。

6.一個金融機構倘發生漏洞管理的問題，將會影響商業運作、公司聲譽、財務績效及該機構的安全與營運。

(二)檢查作業程序

1.檢查人員對金融機構之漏洞管理(Vulnerability Management)檢查應關注重點，包括：

(1)金融機構漏洞管理政策、程序與責任分工。

(2)金融機構資產清查/盤點結果。

(3)金融機構事件監控和鑑定風險辦理情形。

(4)金融機構風險緩解措施。

(5)金融機構滲透測試結果。

(6)金融機構資安事件回應機制。

(7)金融機構對資安相關法規之遵循情形。

2.場外監控(off-site surveillance)主要工作步驟，包括：

(1)獲取金融機構所有進行的弱點掃描及滲透測試報告的副本。

(2)獲取金融機構所有訂單信函或與外部廠商進行弱點掃描及滲透測試或類似測試的合約副本。

(3)審查金融機構管理階層對網路服務風險評估的文件。

(4)獲取金融機構網路拓撲圖的副本。

3. 實地檢查(on-site examination)主要重點，包括：

(1)金融機構弱點掃描及滲透測試等活動是否納入機構內部稽核查核計畫的一部分？

(2)金融機構弱點掃描及滲透測試等活動是否定期進行？間隔週期是多久？計畫的重點是否包括評估新的和最近修改的系統的安全性，而非僅評估現有系統的安全性？

(3)金融機構內部稽核在審核滲透測試的頻率和範圍方面是否發揮功能？

4. 金融機構的風險分析(Risk Analysis)，至少包括：

金融機構管理階層是否對其系統的潛在威脅進行風險分析？分析範圍是否包括以下所有類型的系統？

(1)防火牆

(2)DMZ 伺服器（包含電子郵件伺服器）

(3)網路銀行伺服器

(4)內部應用服務器

(5)網路設備（包含路由器，交換機，閘道設備等）

(6)網路連線到商業夥伴的設備

(7)與外部連接的撥號調製解調器(dial-up modems)

金融機構的風險分析應包括下列事項：

(1)金融機構網路架構的描述和拓撲圖。

(2)評估構成網路的每一個系統的硬體、操作系統、應用程式和資料

的重要性。

(3)審查有關資料安全維護和系統配置的現行政策和程序。

(4)討論每個系統的潛在風險(含內部和外部)。

(5)確定稽核要求事項。

(6)討論在營運系統上執行測試程序時減輕風險的方法。

5.金融機構的盡職調查(Due Diligence)

(1)金融機構的管理階層是否評估過測試人員/組織的獨立性？

(2)金融機構的管理階層是否評估了執行商定程序的個人的資格？

(3)金融機構的審查是否包括測試人員的經驗，參考資料或專業認證？

(4)金融機構對進行測試的個人是否進行了充分的背景調查？

(5)金融機構的合約或聘用函是否納入下列事項：

①測試的範圍

②在測試過程中收集的資料的機密性。

③測試結束後，工作底稿/機密資料的所有權或處置權。

④測試活動產生的責任。

⑤管理人員監控測試活動的能力。

⑥忠誠的依合約執行測試。

6.金融機構的滲透測試範圍

(1)金融機構滲透測試的範圍是否納入風險分析階段中定義的各項稽核要求？

(2)金融機構滲透測試的目標是否已明確定義？

(3)金融機構是否具體描述要使用的測試方法、工具和測試程序？

(4)金融機構管理階層對滲透測試活動的參與和監督職責。

7.網際網路服務提供者(ISP，Internet Service Providers)的注意事項

(1)完整獲取自上次檢查以來進行的各項漏洞評估與滲透測試分析

報告的副本。

(2)審查管理階層對網路服務風險評估的任何文件。

(3)審查聯邦金融機構檢查委員會(FFIEC, Federal Financial Institution Examination Council)頒發適用的測試服務供應商的查核報告。

8.滲透測試報告，至少包括：

(1)報告是否詳細說明了測試的範圍和目標？

(2)報告是否詳細列出了測試依賴的重要假設？

(3)報告是否說明測試的既定目標是否得到滿足？

(4)報告是否提供了所查明風險的結果和排名/評估？

(5)報告是否提供矯正措施的建議？

(6)報告是否討論了委外廠商管理階層接受糾正措施的結果和承諾？

(7)報告是否包含足夠的訊息供金融機構管理層評估測試人員或測試委外廠商的資格？

9.法規遵循(Regulatory Guidance)

美國FRB, FDIC, OCC, OTS陸續就資訊安全訂有約144項法規指引，包括FIL-66-2005, FIL-132-2004, FIL-103-2004, FIL-62-2004間諜程式、帳戶駭客、網路釣魚、電腦病毒等偵測防護指引等，聯邦金融機構檢查委員會(FFIEC, Federal Financial Institution Examination Council)負責陸續就上開資安規範訂定一整套相關查核程序(Information System Examination Handbook)，並於2015年6月發布網路安全評量工具(Cybersecurity Assessment Tool)，用以評估金融機構之網路安全潛在風險。

伍、心得與建議

一、金融科技蓬勃發展，資訊安全之弱點管理日趨重要

根據行政院國家資通安全會報報導，美國、歐 盟及德國等多個執法機構於 106 年 12 月 4 日宣布擊潰 Gamarue 殭屍網路，Gamarue 先利用隨身碟、社交媒體、垃圾郵件或木馬下載器等各種方式感染裝置，再於裝置上植入各種其他的惡意程式，從勒索軟體、間諜軟體、金融木馬、殭屍病毒到後門程式等逾 80 個惡意程式家族；另外，俄羅斯資安業者 Group-IB 於 106 年 12 月 11 日發布訊息，一俄國駭客組織一年來入侵銀行轉帳網路，至少 18 家美國、俄羅斯銀行遭自 ATM 盜領現金近 1,000 萬美元，Group-IB 研究人員指出，該組織發動攻擊的全是很容易公開取得的工具，目前得知該集團使用 Metasploit 等滲透內部網路，並運用 SSL 加密保護 C&C 伺服器及潛伏的 Meterpreter 之間的指令，來植入 ScanPOS 等惡意程式，凸顯攻擊者如何利用裝置與網路之間的資安漏洞與弱點，造成最大的打擊與影響。

國際金融環境變遷，伴隨著金融科技蓬勃發展，重大資安事件也頻頻爆發，如何控管資安風險是此次研討會各國監理機關人員所關注焦點，美國芝加哥聯邦準備銀行 STREAM 科技風險監理實驗室，提供內容豐富、創新的學習環境，結合專業講座，弱點掃描個案分析，滲透測試實機測試(Lab)，和美國資安組織年度威脅調查報告之分組研討等，協助學員更瞭解現今銀行業資安風險，及駭客的攻擊手法，奉派參加此次研討會獲益良多，期許能將所學運用於未來工作，並持續精進。

二、效法美國鼓勵並培育金融檢查人員之科技應用

因應數位發展趨勢，及新興科技發展帶來的網路風險及作業風險，金管會針對數位金融業務潛在之風險與相應之控管措施，藉由不定期會

議集思廣益，精進金融檢查人員之查核技巧，同時培育金融檢查人員之資訊素養。金融機構積極透過網路及新興科技，如雲端服務、大數據、物聯網(IoT)及區塊鏈等技術，提供整合創新服務是未來趨勢，金融科技發展下之資安風險是監理的最大挑戰。

美國聯邦準備體系 FED、聯邦存款保險機構(FDIC)、美國通貨監理署(OCC) 等監理機關，設有專職研究最新科技及金融業採用之資訊技術及軟體工具，分析其潛在風險，作為查核參考及培訓電腦稽核人員之使用。我國檢查作業方式雖與美國不同，惟可參酌美國培訓電腦稽核人員之作法，透過類似數位金融查核工作小組之單位，進行檢查作業之科技應用研究，鼓勵多方嘗試自動化工具或軟體之使用，再對相關檢查人員辦理完整之教育訓練，以因應快速變化之金融科技發展趨勢。

三、參考各國網路安全法規，適時調整監理與檢查重點

各國監理機關強化對資安與隱私保護之要求，陸續發佈網路安全實務準則或網路安全規範，值得我國密切關注，如美國國家標準技術研究所（National Institute of Standard and Technology, NIST）於 106 年 12 月 5 日發佈網路安全框架 1.1 版本(NIST Cybersecurity Framework)作為組織建置安全性環境之標準，框架核心包括辨識(Identify)、保護(Protect)、偵測(Detect)、應變(Respond)、與復原(Recover)等五項功能組成網路安全管理的生命週期，建議組織應透過由上而下且持續回饋的資安治理架構，以降低資安風險，該框架為一套適用於美國政府機構以及各關鍵資訊基礎設施運營商的最佳實踐指導方案，另香港金融管理局（Hong Kong Monetary Authority，HKMA）亦已於 105 年推出網路防衛計畫（Cybersecurity Fortification Initiative，CFI），網路防衛計畫核心三大支柱包含網路防衛評估框架（Cyber Resilience Assessment Framework，C-RAF）、專業培訓計畫（Professional Development Programme，PDP）及網路風險

資訊共享平台（Cyber Intelligence Sharing Platform，CISP），HKMA 期望透過實施網路防衛計畫全面提昇香港金融體系之整體網路安全防護水準。

我國本國銀行海外分行系統多委託臺灣母行進行系統維運，金融機構總行與海外分支機構均應熟稔並遵循當地法律規定及資安規範之適用範圍，並自我評估法規遵循情形，金管會檢查局已參考國外相關規範，訂定本國銀行檢查手冊資訊作業專篇，每季並就重大資安議題及新增修法令等進行檢視。因應各國陸續發佈網路安全法規，建議金管會持續透過各國監理機關網站、金融監理合作等管道，蒐集各國家之資訊安全相關法令規範，並得取法美國、香港、新加坡及日本等國家監理機構發佈之網路安全管理框架相關參考指引或文件，檢視我國對本國銀行檢查重點之調整方向，同時引領業者強化其海外分支機構之資安法令遵循。

四、因應資安事件管理仿效國際監理趨勢，強化金融機構數位鑑識調查機制

近年國內金融業陸續發生多起重大資安事件，顯示國內金融資訊安全環境及主管機關之監理已面臨巨大挑戰，從 ATM 盜領及 SWIFT 遭駭等資安事件發生之後，風險的觀念應該要調整為資安風險其實就是整體營運的風險，事後資安應變程序與鑑識技術方面，由於可能會面臨司法訴訟，因此金融業者的數位鑑識能力、數位證據留存技術都必須要做到可以確保相關證據的能力，金管會檢查局近二年亦已將金融業者是否建立數位證據保全標準作業程序納入查核重點之一。

參酌美國 FED、香港及新加坡等金融監理機關，針對資安事件之管理與回應，除了須完善事前準備工作之外，同時強調事後調查能力，因此，要求金融機構建立數位鑑識調查機制，值得我國效法，建議將金融機構建立資安應變與數位鑑識工作小組、強化資安事件與鑑識分

析工具，及數位證據留存與數位鑑識能力教育訓練等，納入對本國銀行之資安查核重點，以完整涵蓋金融機構緊急應變重要作業流程，此外，本國銀行海外分行系統委託臺灣母行維運時，包括美國、香港及新加坡等當地監理機關，對數位鑑識調查機制等有新增相關規定時，總行法令遵循單位是否及時配合因應，應於辦理檢查時併同瞭解。