出國報告（出國類別：其他）

強化支付清算系統之資訊安全

服務機關：中央銀行

姓名職稱：陳佑任 資訊處四等專員

派赴國家：馬來西亞

出國期間：105年7月16日至7月22日

報告日期：105 年 10 月 5 日

目　　次

壹、前言

一、目的

為增進東南亞國家央行區域合作、支付清算系統營運經驗分享及資訊安全管理實務交流，奉派參加由東南亞中央銀行研訓中心（SEACEN Centre）舉辦的第 15 屆「新興經濟體支付及清算系統高階訓練課程」。

二、過程

本次課程主題為 ”Strengthening Resilience of Payment System to Cybercrimes”，課程自 105 年 7 月 17 日起至 105 年 7 月 21 日，由 SEACEN Centre 邀請來自支付暨市場基礎設施委員會(Committee on Payments and Market Infrastructures, CPMI)、SWIFT、馬來西亞及菲律賓央行等資深人員擔任講師。參加學員來自我國、泰國、韓國及印尼等 16 個國家。

授課內容範圍廣泛，包括：(1) 支付系統技術演進帶來的資安問題。(2) 資訊安全與風險管理簡介。 (3) 支付系統的資安措施，包括資安治理、資安工具及事件因應等。(4) 支付系統資安框架的發展。(5) 各國央行資安實務交流。研習課程並安排以個案研討方式，藉由討論與分享的過程，幫助學員瞭解支付清算系統資安議題的各種面向。

三、報告摘要

由於資訊科技快速發展與支付系統對資訊科技的依賴加深，支付系統面臨各種由科技發展驅動的議題，如：非銀行支付業者提供金融

服務、各種金融服務與資訊服務彼此互聯等。在科技進展的同時，除與日俱增的網路犯罪外，也使資訊安全相關議題更趨複雜。

支付系統營運方或監管機關應持續改善資安管理措施，以確保作為金融市場基礎設施的支付清算系統在網路攻擊下有足夠韌性以保持金融體系的穩定。本文針對如何強化支付清算系統對網路攻擊之防禦能力作概略介紹，主要內容為：第貳章介紹支付系統相關的技術背景。第參章概述資訊安全原則。第肆章說明支付系統資安威脅與因應措施。第伍章介紹新近資安管理框架。第陸章為結論與建議。

貳、支付系統的技術背景

伴隨著資訊科技的演進，支付系統乃至金融服務與技術間的關係出現幾個趨勢：

- 支付系統對科技的依賴加深：如網路銀行、行動支付。
- 各種金融與資訊服務間的相依性提高：如財金通匯系統相依於本行同資系統，而商業銀行之存款系統亦相依於財金通匯系統。
- 科技與創新紛陳：如區塊鏈、大數據。
- 非銀行機構提供金融服務：如各種 Fintech 業者提供之支付服務。

社群媒體、行動裝置、雲端服務、區塊鏈與數位貨幣等技術的普及除帶來新的商機，也改變組織既有的資訊環境。例如以雲端服務降低成本的同時，仍須考量資料相關的法律遵循問題、使用社群媒體可能帶來的公關危機、行動裝置造成的資料外洩等。因此各種技術的出現，對支付系統的營運來說，既是機會亦是挑戰。

除上述科技趨勢持續影響金融機構的運作外，ISO20022 與即時零售支付系統是與支付系統特別相關之技術發展：

一、ISO20022

ISO20022 是金融機構間訊息交換的最新國際標準，目的在於推動金融產業內及與其他產業間的訊息標準整合，以提升各種自動化作業的互通性與效率。

ISO20022 的一大特色在於其並非僅是訊息格式的標準，更是提供一套訊息格式制定的方法論，亦即產業如何制定訊息格式標準的標準。ISO20022 將訊息分為描述商業行為、流程及概念的邏輯層，以及描述訊息格式的語法層。因此ISO20022除中立於特定訊息格式外，

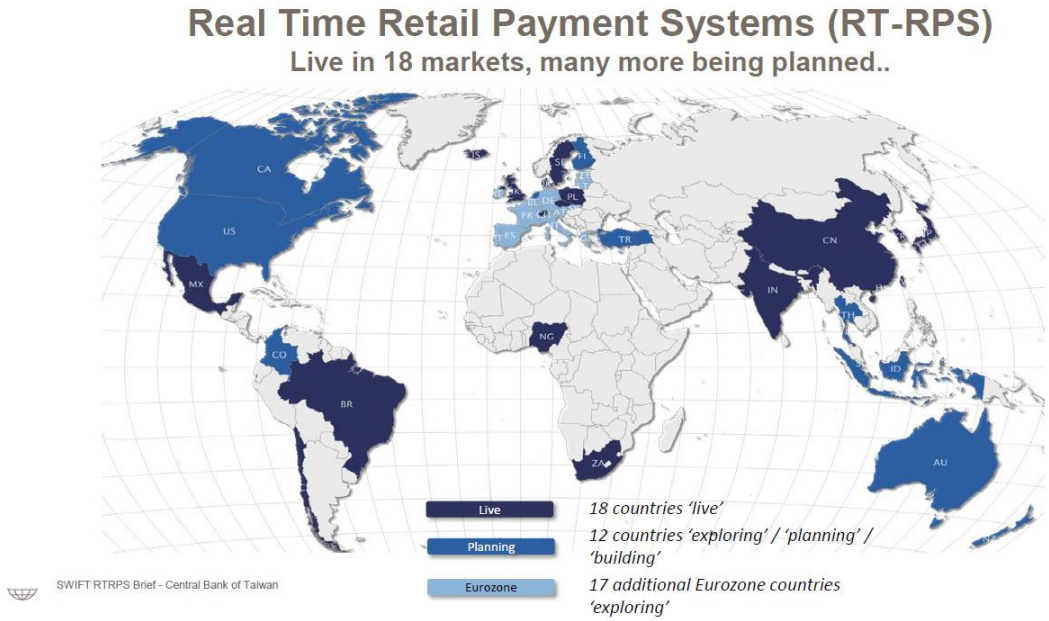
也有助於不同訊息格式間的互通。

對支付系統而言，ISO20022 提供了描述支付清算交易及與其他系統介接的共通語言，亦提供依自身需求發展訊息格式的框架，例如因反洗錢需求而於支付交易訊息加入額外的資訊。各國新發展之支付清算系統已逐步採用 ISO20022，值得持續關注此標準之發展。

二、即時零售支付系統

相較於大額支付系統，零售支付具有交易金額小、交易筆數多且不具急迫性等特性。但由於科技進展與使用者需求影響，且為進一步降低交易參與者的信用風險與流動性風險，即時或近乎即時支付的需求開始增加。

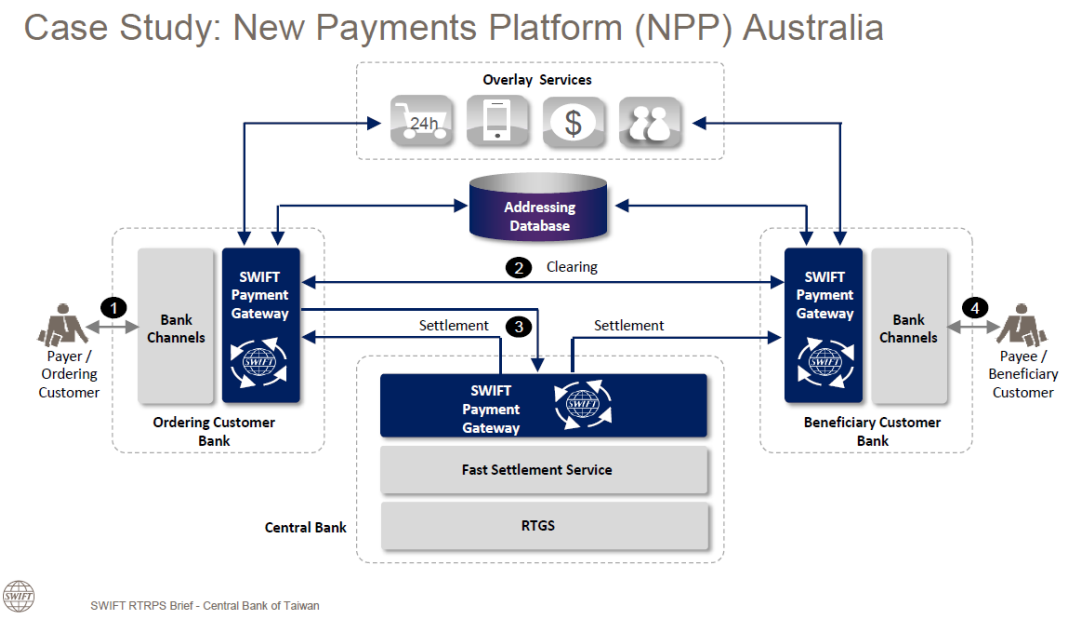
圖 1　零售支付系統發展現狀



資料來源：SWIFT

如圖 1 所示，已有許多國家已發展或是正在發展即時零售支付系統，例如澳洲的 New Payments Platform(NPP)，其系統架構可見圖 2。

圖 2　澳洲 NPP 系統架構



資料來源：SWIFT

由於零售支付系統的交易量極大，且有 24 小時全年無休（24/7）的結算需求，若零售支付系統走向即時或近乎即時結算，對其連結的大額支付系統可能帶來效能影響，或是需要調整大額支付系統的系統架構或是與其他系統的介接方式，因此本議題值得大額支付系統營運者持續關注。

參、資訊安全概述與原則

資訊安全逐漸引起重視與日趨嚴重的網路犯罪有關，例如孟加拉央行遭盜轉、第一銀行 ATM 遭盜領及 SONY 影業資料遭駭等等案件都使受害機構遭受龐大損失，並引起社會廣泛關注。

根據國際電信聯盟(ITU-T)的定義，資訊安全範疇包括：工具、政策、安全概念、安全措施、指引、風險管理方法、行動、訓練、最佳實務、保證與科技的集合，可用來保護資通訊環境、組織及人員的資產[1]。可見資訊安全所涉及的面向與領域十分複雜，難以簡易的框架涵蓋，因此以下將從資安的原則及要素等角度介紹資訊安全。

一、資訊安全原則

資訊安全有三項重要的原則：

- **主動因應及持續改善**
- **資訊分享與跨部門合作**
- **領導階層的支持**

從單一組織角度觀之，這代表組織需主動因應風險，包含風險的識別、預防及風險事件的辨識、復原。組織需有資安資訊的蒐集分析能力，並具備跨部門的因應能力。而上述資安作為需在領導階層的支持下，持續透過反饋改善各流程與機制，才能使組織在變動的環境下達到安全(secure)與強健(resilient)的目標。

[1] Cybersecurity refers to the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

從金融主管機關的角度出發，代表監理政策框架及相關政策應導入資訊安全的思維、應鼓勵金融業資訊安全資訊的共享，並主動監控相關金融機構及市場的資安強健度，同時金融主管機關還需兼顧資安監理與創新發展間的平衡。

二、資訊安全要素

資訊安全亦可由組織運作的要素加以說明：

(一)人員

資訊安全與組織所有人員都密切相關，包含作業人員、技術人員、中高階管理階層以及組織領導階層。在風險管理、品質管理等領域中，尤其重視領導階層的角色(tone at the top)，認為經由領導階層的行動與策略，才能形塑組織的品質、資安等文化。而唯有建立資訊安全文化，組織才能有效達成資安的目標。

(二)政策

由於資訊領域的變化快速，資安問題的應對策略也需時時修正。因此組織的政策必須能夠支援各種資安措施的變革，包含：管理階層需能在認知的狀況下快速決策、具備敏捷的回饋機制、人員需有足夠與持續的教育訓練及組織需能快速有效地導入各種資安措施。

(三)技術與流程

資安一方面需要各種技術與工具的幫助，如叢集架構、防火牆等，以達到安全與強健的目標。另一方面組織的各種流程，如對外服務的作業流程、資訊科技的投資與採購流程及組織架構中資訊安全的權責劃分，都會影響資安措施的成效。

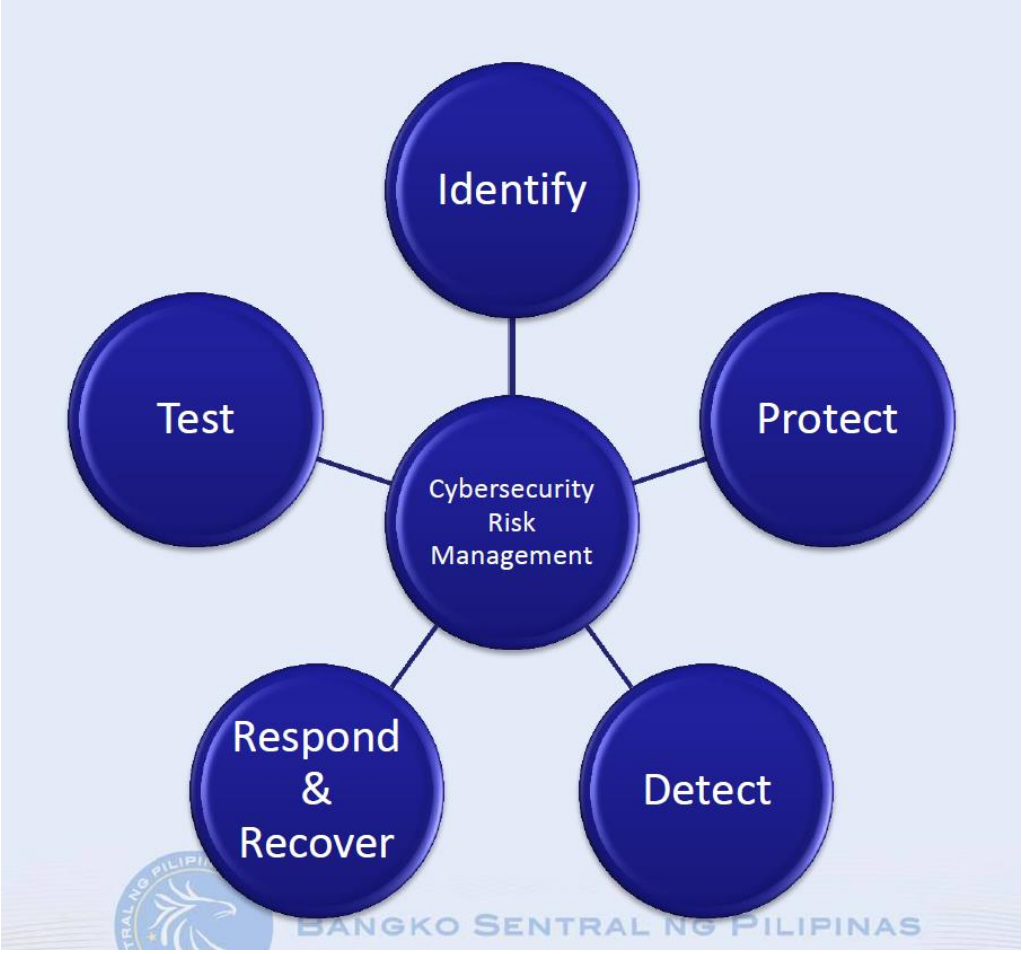
(四)資安治理(governance)

資安治理指的是使資安相關決策能達到企業目標的過程。在決策面，領導階層有賴資訊或資安部門主管持續提供有助決策的相關資訊與知識。在管理面，則需將資訊安全納入企業風險管理的一環。

肆、支付系統安全措施

資訊安全各種措施可由風險管理的角度切入，本章將說明辨識支付系統的資安威脅、各種預防及因應措施及支付系統有別其他資訊系統的特殊性(如圖 3)。

圖 3　資訊安全風險管理



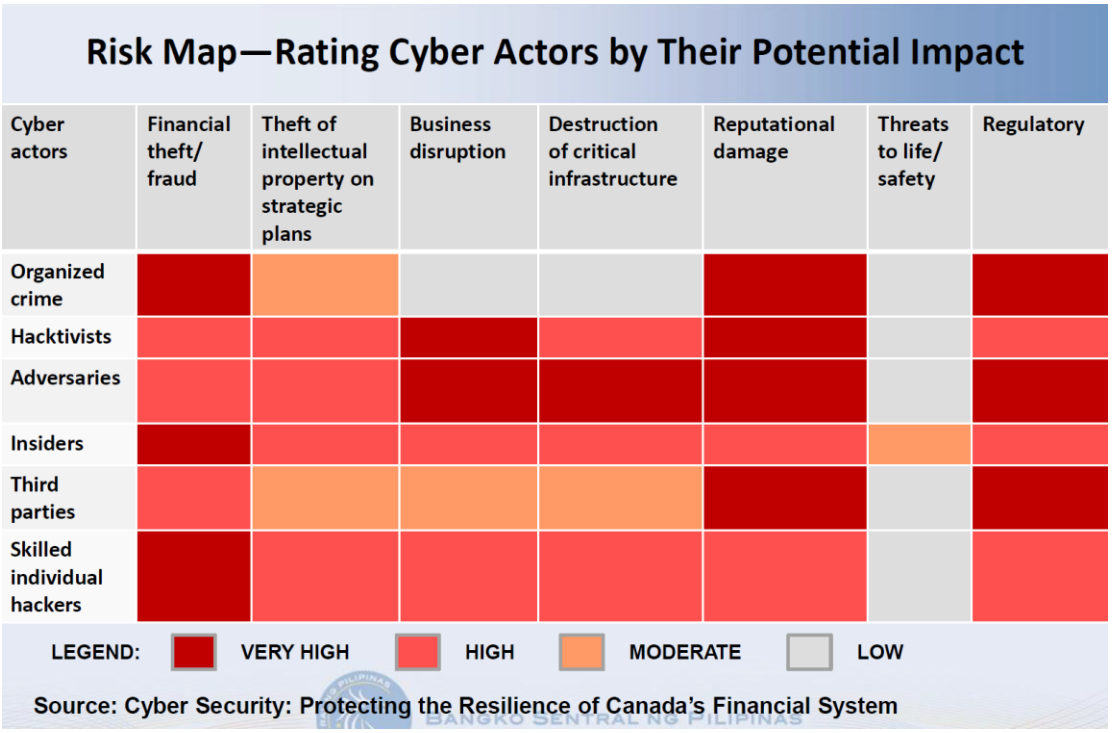
資料來源：上課講義

一、資訊安全風險

辨識風險是防禦的第一步，組織可以從網路犯罪的發動者、犯罪目標及組織的資安弱點三個構面來分析組織可能面臨的資安風險。

網路犯罪發動者可分為組織犯罪、個別駭客、內部員工、協力廠商等類型，圖 4 說明不同類型的犯罪者在不同類型的犯罪將給組織帶來不同的風險。

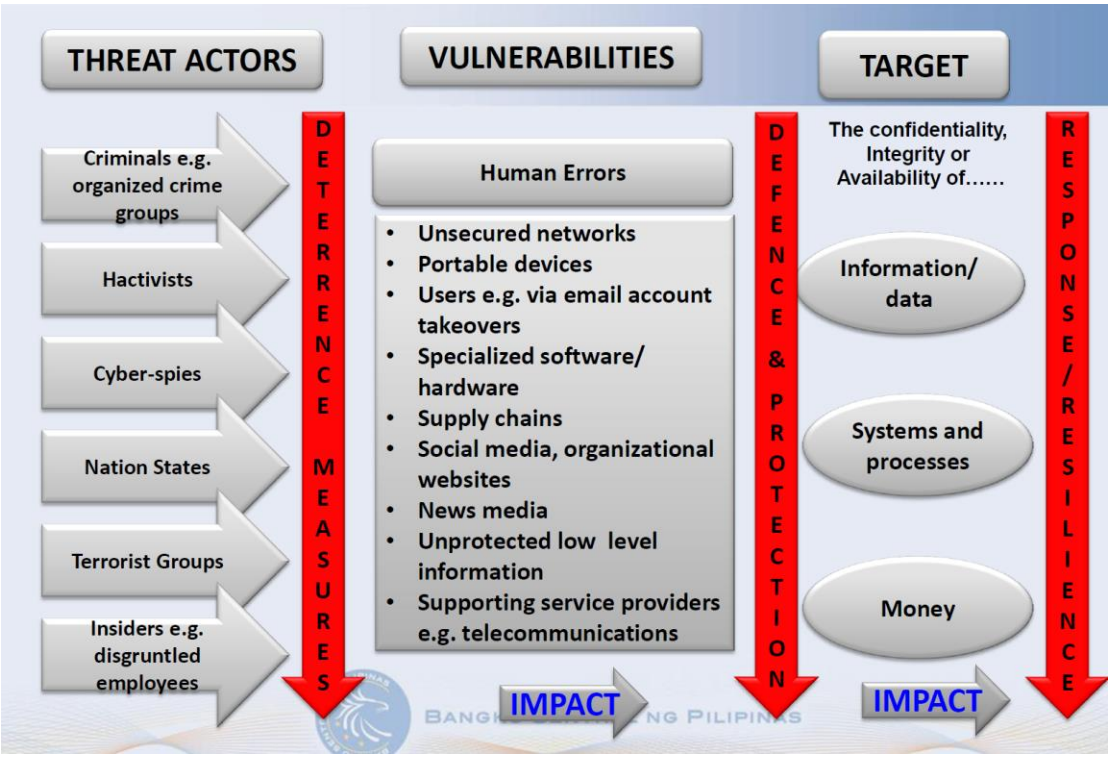
圖 4　網路犯罪者類型風險矩陣



資料來源：上課講義

網路犯罪的目標可分為金錢、資料及關鍵系統運作。另一方面，組織可由上章所述的人員、科技、流程等資安要素來分析組織可能的資安弱點，如未受完善訓練的操作人員、資源不足的資訊部門、未持續修補弱點的系統與平台、協力廠商規範不足等等。

圖 5 網路犯罪風險評估與因應



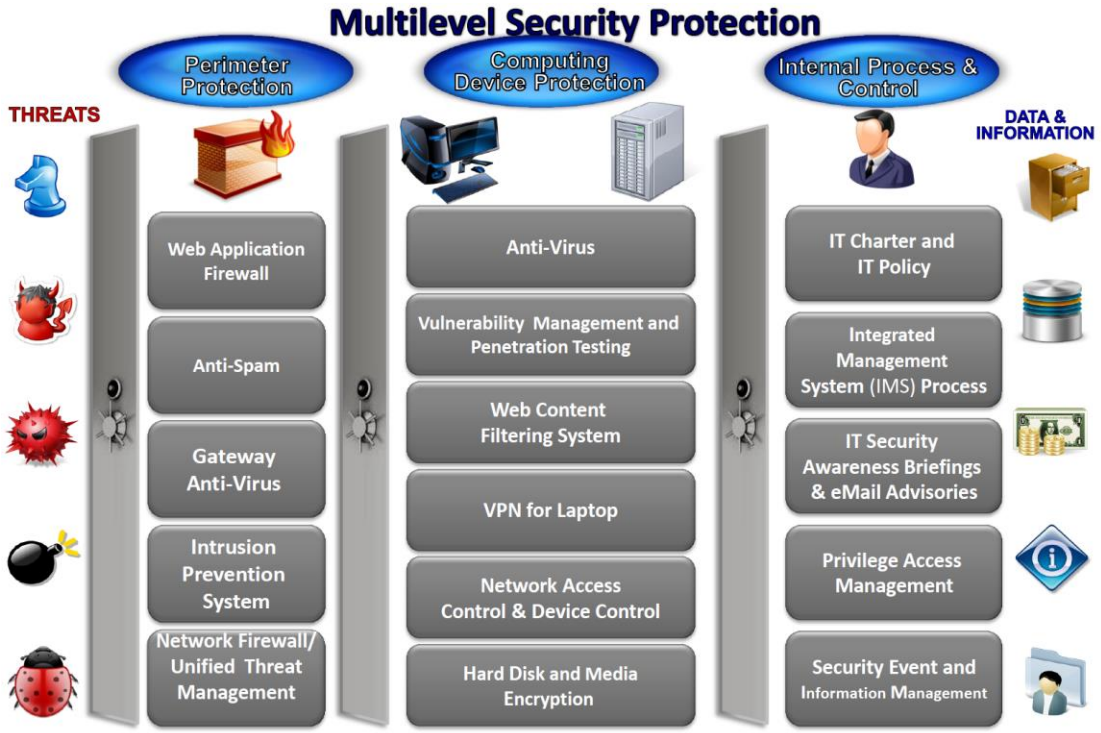
資料來源：上課講義

分別分析犯罪者類型、組織資安弱點及犯罪目標後，組織可根據威脅的可能性、犯罪動機、對金融市場衝擊、各種資安措施等因素評估犯罪者類型、資安弱點、金錢資料損失各面向在資安犯罪中對組織帶來的衝擊，再據以建立事前、事中、事後的防範、保護及復原措施。

二、資訊安全措施

資訊安全措施包含實體防護及資訊防護措施，且兩者皆著重所謂縱深防禦，亦即採取多層次防禦措施以降低網路攻擊成功的可能性，如實體防護包含圍牆、警衛、監視器、各處所門禁等設施以降低機房遭實體侵入的可能性。資訊防護措施則涉及更多技術與工具，如圖 6 所示。

圖 6　各種資訊安全防護措施



資料來源：上課講義

由於資安技術眾多，以下僅擇要進一步說明。

(一)多因子驗證(Multi-Factor Authentication)

多因子驗證指利用兩種以上使用者所知(what they know，如密碼)、所有(what they have，如憑證)、所為(what they are，如生物特徵)的因素來進行身分驗證與授權，以降低冒用風險的機制。

部分支付系統使用兩層密碼方式驗證，因僅涉及所知因子，並不能稱為多因子驗證。菲律賓央行自行管理、製發憑證卡片以用於 RTGS 系統的身分驗證，該作法可供其他支付系統營運方借鏡。

(二)安全資訊與事件管理(Security Information and Event Management, SIEM)

SIEM 工具可彙整組織資訊環境中各種設備與應用系統的資訊與事件，並提供資安相關的監控與預警功能。根據已經導入SIEM的香港金融管理局所分享的經驗，此類產品除需編列一定預算，整合各應用系統亦是牽連甚廣的大型工程，非一朝一夕可完成。

導入 SIEM 方案，可先行規劃以 SOA (Service-Oriented Architecture)為基礎的應用系統間資訊交換機制，除可簡化各應用系統傳送資訊至 SIEM 的成本，以強化資安預警外，亦可通過相同機制傳送系統偵錯訊息予維護人員、傳送系統運作訊息予網管人員等，以提升日常營運之效率及降低符合資安規範的成本。

(三)駭客入侵事件應變機制

根據課程講師的建議，若系統已遭到入侵，應考慮採取下列步驟：

(1) 組成應變小組。小組負責人應有一定決策能力；小組成員應包含業務、資訊、公關人員；組織應發展標準應變程序。
(2) 辨識原因並控制。如將中毒電腦離線；應注意保存鑑識所需相關證據。
(3) 評估嚴重性與影響範圍。
(4) 主動通知受影響的個人與機構。並請受影響方採取因應措施，如更改密碼。

(5) 採取預防措施。如聘請外部顧問、加強教育訓練、加強委外廠商規範、加強內部流程與政策等，以避免問題再度發生。

除上述流程外，入侵事件應變亦有其特殊性。例如若主中心遭到入侵，則使用相同軟硬體環境配置的備援中心亦將有相同漏洞。因此需針對駭客入侵事件研擬相關應變程序。

三、支付系統資訊安全

如第貳章所述，支付系統對資訊科技的依賴與各系統間的相依性逐漸加深，使得網路犯罪可能從各種管道影響支付系統的運作。支付系統為金融市場運作的骨幹，支付系統的資訊安全亦為金融穩定的一環。

課程中講師建議支付系統應採取下列措施：

- 支付系統參加方應經支付系統營運方許可
- 參加方應管理系統使用者，並經正式程序提交營運方
- 營運方應有密碼處理程序，建議採用多因子驗證
- 應使用獨立專用之工作站電腦，並採取門禁措施
- 對人工發送交易指令應有適當內控
- 營運方應要求參加方及協力廠商符合資安規範

伍、新近資安管理框架簡介

除資安產業外，金融業及政府機關皆逐步發展與支付清算系統資訊安全相關的管理框架，例如美國國家標準技術研究所(National Institute of Standards and Technology, NIST)發展的 Framework for Improving Critical Infrastructure Cybersecurity、美國聯邦金融機構檢查委員會(Federal Financial Institutions Examination Council, FFIEC)發展的 Cybersecurity Assessment Tool，或是國際結算銀行 BIS 所轄 CPMI(Committee on Payments and Market Infrastructures)委員會所發展的 Guidance on Cyber Resilience for FMIs(Financial Market Infrastructures)。

這些框架一方面反映金融業及政府對於資訊安全逐漸重視，另一方面也考驗各組織資安管理能力，是否能持續蒐集、分析產業動態，以及是否根據最新標準改善既有資安措施。

一、Guidance on Cyber Resilience for FMIs (From CPMI)

CPMI 在 2012 年已推出金融市場基礎設施準則之揭露架構及評估方法(Principles for Financial Market Infrastructures：Disclosure framework and Assessment methodology, PFMIs)，該準則為對金融市場基礎設施的全面性評估，而在其中的治理、風險管理、清算最終性、營運風險及基礎設施之連結等原則亦涵蓋資安相關議題。

CPMI 並考量資安具有持續變化、複雜、復原方式不如其他營運風險明確、損害無上限等等特性後，認為資安議題有其特殊性，爰發展金融市場基礎設施資訊安全指引(Guidance on Cyber Resilience for FMIs)作為 PFMIs 在資安議題上的補充文件。

圖 8 指引框架

資料來源：Guidance on Cyber Resilience for FMIs

圖 8 為該指引之框架。圖中內圈的治理、辨識、預防、偵測與回復即前章已提及的風險管理步驟，而外圈的測試、學習等要素其精神為透過測試現有系統的表現、資訊分享、教育訓練等機制，以達到持續改善的目標。

此次課程中該指引較受參加學員關注的是 PFMI 中的兩小時目標復原時間(2-hour RTO)。由於網路攻擊的態樣複雜，如主中心與備援中心亦可能遭受相同的攻擊，因此兩小時目標復原時間咸認是困難的挑戰。為達到此目標，建議可研擬各種情境之應變計畫、持續修正既有備援程序並檢討異質備援系統可行性。

二、Cybersecurity Assessment Tool (From FFIEC)

FFIES 發展的資安評量工具(Cybersecurity Assessment Tool)主要提供一套系統化的方式來評估一組織的資安水準,其步驟包含組織原生風險值評估、組織資安成熟度評估、建立組織風險矩陣,最後根據風險採取相關因應措施。

該工具將組織的特性分為五類:科技與網路、服務提供管道、產品與服務、組織特性及外部威脅。並在各子類下以量化方式評核風險等級。如在科技與網路項下,組織根據聯網裝置的數量不同,有不同的風險等級(例如小於 250 個裝置最低,大於 50000 個裝置最高),綜合所有項目後,可得到組織的原生風險值。

該工具亦將組織的資安措施分為五類:風險管理、資訊分享與協作、資安控制措施、外部關係管理、資安事件因應。並在各子類下提供明確標準以評估成熟度,如資訊分享的最高成熟度須建立資安情報的即時分享機制。

圖 9 風險評估矩陣

Maturity Level	Inherent Risk Profile			
	VH	H	M	L
4	MR	LR	LR	LR
3	MR	MR	LR	LR
2	HR	MR	LR	LR
1	HR	HR	MR	LR

資料來源：上課講義

建立原生風險值與成熟度後，即可建立如圖 9 的風險評估矩陣。組織可依自身需求決定原生風險值與成熟度的等級數，以及矩陣中的結果風險值。圖 9 是菲律賓央行使用的矩陣，原生風險值與成熟度各有 4 級，並有高中低風險的三種結果，並分別對應密切監控、定期查核、低度監理的三種監理作為。

該工具提供一套系統性的方法，除可供機構自評，亦可作為監理機關的資安監理工具，用以瞭解其監理的金融機構的組織特性、資安措施及資安風險，並據以調整監理方式，值得參考。

陸、結論與建議

一、結論

(一) 資訊安全並非僅為技術議題

由於資訊科技的特殊性，使資安事件具有技術變化快速、手段複雜廣泛、沒有明確的復原方式等特性，且資安事件可能造成的財產與名譽損失亦沒有上限。

另一方面，資訊安全涉及事前對人員的教育訓練、對金融機構的監管，以及事件發生時的公關處理、證據保全等，比起颱風、地震等傳統的營運風險，資訊安全涉及的層面更為複雜。

因此確保組織的資訊安全並非僅是單純的技術議題，而需高階管理階層重視資安的價值，並投入足夠的資源，才能培養出組織的資安文化並具有足夠的能力，以因應日新月異的攻擊。

(二) 資安訊息分享是資訊安全的基石

隨著資訊科技的快速變化，網路攻擊、資安規範與措施也不斷變化，今天的資安規範很可能明天就已過時。對組織來說，重要的並非一套完整的作業程序，而是不斷因應環境持續改善的應變能力。

因此如何強化組織的資安訊息蒐集、分享、利用能力，並據以改善既有的防範措施，是最基礎的資訊安全能力。

二、建議

(一) 加強資訊單位與業務單位間資訊分享

資訊系統的發展與安全需由資訊單位與業務單位通力合作。若資

訊單位瞭解業務單位的政策目標與長期規劃，可更有效率地發展符合需求的資訊系統；若業務單位對資訊技術發展及資安議題有基本認知，在政策制訂面可更周延，在系統營運面可更安全。因此各種教育訓練建議擴大不同背景人員的參與，以加強合作並發揮綜效。

(二) 建立資安資訊收集機制

為持續提升資安能力，建議建立機制，定期收集來自政府、資安業、金融業或新聞媒體等來源的資安資訊，並加以分析、彙總後，分享給相關單位作為改善業務的參考。

此外金管會於金融科技發展策略白皮書中提出建立金融資安資訊分享與分析中心(F-ISAC)的構想，說明資訊分享對資安的重要性亦成為金融產業的共識。

(三) 持續改善各種資安措施

綜合參訓各國央行分享經驗，下列資安措施可供支付系統營運方參考：

(1) 研究導入多因子驗證(Multi-Factor Authentication)

對於主要使用密碼或雙層密碼方式驗證使用者身分的支付系統，建議可研究多因子驗證導入可行性，如使用憑證、Token或生物辨識等技術確認使用者身分，以加強應用系統安全性。

(2) 強化安全資訊與事件管理(Security Information and Event Management, SIEM)

由於SIEM導入期程較長，應於採購軟硬體與增修應用系統時，

一併規劃與 SIEM 之整合，以降低導入成本。

(3) 強化資安事件應變機制

傳統資安措施偏重事前防範措施，而較缺少以被成功入侵為前提的應變措施。建議備援措施可考量資安事件發生後的復原程序，如備援中心被入侵的可能性及證據保全的程序。

(四) 加強對支付系統參加方的資安監管

孟加拉央行因資安問題而遭盜轉帳後，提供連線服務的 SWIFT 亦難免於各種質疑。因此國內各結算機構可考量強化對連線機構的資安監管，例如要求連線機構提供資安風險評鑑與其因應之控制措施、適時接受實地查核或是建立結算機構間的資安監理合作模式。

參考資料

1. SEACEN（2016），「第15屆新興經濟體支付及清算系統高階訓練課程」上課講義。
2. SWIFT(2016)，「第15屆新興經濟體支付及清算系統高階訓練課程」上課提供資料。
3. 中央銀行資訊處(2016)，「金融網路安全」。
4. 王怡涵(2016)，「零售支付系統的近期發展與監管議題」，中央銀行出國報告。
5. CPMI (2016), “Guidance on Cyber Resilience for Financial Market Infrastructures”.
6. CPMI (2014), “Cyber Resilience in Financial Market Infrastructures”
7. CPMI (2012), “Principles for Financial Market Infrastructures”.
8. FFIEC(2015), “Cybersecurity Assessment Tool”.
9. NIST(2015), “Framework for Improving Critical Infrastructure Cybersecurity”.
10. The SWIFT Standards Team (2010)，“ISO 20022 for Dummies ”.