出國報告（出國類別：其他）

參加 SEACEN 研訓中心第 17 屆
支付及清算系統高階課程出國報告

服務機關：中央銀行

姓名職稱：龔玲雅 副科長

派赴國家：印尼

出國期間：107.7.2-107.7.4

報告日期：107.9.28

摘要

科技支持各種支付創新，帶來前所未有的便利，卻也吸引金融犯罪者利用科技謀取不法利益。支付基礎設施與支付生態體系參加者面臨愈來愈多的網路威脅，網路攻擊事件可能導致一個或多個系統失序，嚴重者可能危及金融穩定。鑑此，國際清算銀行支付及基礎設施委員會發布網路安全相關指引，提供會員國規劃支付清算資訊安全作業參考。

金融基礎設施肩負重要金融業務支付與結、清算作業之順暢運作，應具備辨識網路相關風險之能力，並發展全面性的業務持續運作計畫。為確保支付清算網絡中各節點的資訊安全，金融基礎設施尚應制定參加者應符合之網路攻擊復原最低標準，並藉由落實定期模擬演練及實地測試，確保業務持續運作計畫之有效性。

本報告藉由近年若干國家大額支付系統及零售支付系統發生遭金融駭客攻擊事件，說明網路攻擊無所不在，未經防範之系統漏洞，或是組織內缺乏資安意識員工無意間洩漏內部網路帳號密碼資訊，均可能成為駭客入侵的跳板。此外，並分享馬來西亞重要金融基礎設施 PayNet 公司（該公司營運該國大額支付系統 RENTAS 及數個零售支付系統）有關業務持續運作之實作經驗，包括公司治理、風險管理架構及運作規劃暨跨部門作業安排等，提供本行營運及管理支付系統之參考，以強化大額支付系統及其參加機構之業務持續運作能力。

目錄

圖目錄

表目錄

壹、前言

本次奉派參加由東南亞國家中央銀行研訓中心（SEACEN Centre）於印尼峇里島舉辦之第 17 屆「支付及清算系統高階課程」，由該中心與 VISA 等機構資深講師，以及韓國、泰國、印尼及馬來西亞等國央行資深官員授課，共 13 國（或地區）總計 32 名學員參加，包括我國、香港、韓國、泰國、印尼、馬來西亞、越南、巴布亞新幾內亞、斯里蘭卡、寮國、柬埔寨、尼泊爾及不丹等國。

近年來快速進展的科技，支持各種支付創新，一方面為使用者帶來前所未有的便利，另一方面卻也吸引金融犯罪者利用科技謀取不法利益，使得金融機構與相關之金融市場基礎設施暴露在網路威脅之中，金融監管機關如不善加管理網路安全，則網路攻擊事件嚴重者可能危及金融穩定。

為使學員具備網路安全治理之專業知識與技能，本次課程內容包括：(1)支付創新對中央銀行監管職能與法規制定者帶來之挑戰、(2)提升系統安全與促進支付效率之策略與支付基礎設施及(3)因應網路攻擊之國際建議準則。

馬來西亞講師分享該國網路安全治理之實務作法，係以整體支付生態系統為考量，涵蓋資訊、人員與作業程序等 3 大要素，發展各利害關係者（包括中央銀行、金融機構監管者及金融機構等）之橫向溝通協調機制，建立事件發生中處理程序及事後復原安排，並透過明確規範及模擬演練測試，冀有效防範網路攻擊，由事件中迅速復原。

本報告內容主要分為 5 章，除本章前言外，第貳章介紹國際清算銀行發布網路安全風險相關指引；第參章為國際間近年駭客攻擊金融事件；第肆章分享馬來西亞 PayNet 網路安全治理作為；第伍章為結論與建議。

貳、國際清算銀行發布之網路風險管理相關建議報告

網路攻擊僅是金融市場基礎設施眾多作業風險之一，金融市場基礎設施並非單獨營運，尚包括生態系統各參加者。因此，為因應網路攻擊，除資訊軟硬體設施外，需預先制定一系列制度性安排，如公司治理、法規、作業程序、模擬與實地演練及資訊分享機制。

一、BIS 網路風險管理相關報告書簡介

國際清算銀行支付暨市場基礎設施委員會（Committee on Payments and Market Infrastructures, CPMI）為因應日漸增多之金融系統網路攻擊事件，發布相關建議準則，提供會員國於規劃其支付清算資訊安全作業之參考，並推動各國擬訂業務持續運作計畫（Business Continuity Management, BCM），包括：

(一) 金融市場基礎設施準則報告書（Principles for financial market infrastructures, PFMI）

PFMI 由 CPMI 與國際證券管理組織（IOSCO）於 2012 年發布，該報告書指出金融市場基礎設施（以下簡稱 FMI）面對的主要風險之一為作業風險，FMIs 應具備管理包括網路風險在內的治理機制與全面性風險管理架構。PFMI 準則與網路攻擊復原作業有關者，為準則 2 治理、準則 3 全面性風險管理、準則 8 清算最終性、準則 17 作業風險及準則 20 金融市場基礎設施之連結，要求 FMIs 應能在受到網路攻擊後 2 小時內，恢復主要系統運作。

(二) 金融市場基礎設施網路攻擊復原報告（Cyber resilience in financial market infrastructures）

國際清算銀行於 2014 年發布金融市場基礎設施網路攻擊復原報告，以 FMIs 能在嚴重網路攻擊事件中復原且完成當日最終清算為前提假設，提出遭受網路攻擊之作業復原架構。FMIs 可參考該架構自行發展整合性之復原策略[1]，抑或選擇採用其他專業機構設計架構，如美國國家標準技術協會（National Institute of Standards and Technology, NIST）發布之提升重要基礎設施網路安全架構[2]，以達成 PFMI 之 2 小時復原作業目標。

縱然各機構提出之網路安全架構各不相同，整合性之復原策略可歸納為 3 個共同要素，即網路攻擊型態、網路安全治理及防禦方法。考量金融基礎設施內部與外部系統具有相互連結之特性，網路安全不僅涉及單一機構之內部資訊安全，更擴及相互連結之外部機構資訊安全管理，然要達成全市場之網路安全復原作業，在實務上有其困難性。金融市場中的參與者與各個金融基礎設施之業務可能環環相扣，牽一髮而動全身，部分機構遭受網路攻擊事件，為復原受影響之作業，可能需要延長其他金融基礎設施營運時間，以完成當日最終清算。因此，報告指出，有效的復原策略尚應涵蓋跨機關之溝通協調，並事先商討為完成當日清算所需之作業時間上限，對於同時在多個司法管轄區營運之金融基礎設施更應審慎處理。

(三) 金融市場基礎設施之網路攻擊復原作業指引（Guidance on cyber resilience for financial market infrastructures）

[1] 參見吳桂華(2015)。

[2] 美國國家標準技術協會（NIST）提供美國政府機構、學術機構與產業界相關技術服務，包括為美國中央主管機關提供科技服務，以支援機關制定電腦及電信系統方面之政策，並發行一系列標準叢刊，以供電腦技術方面之參考利用。該協會於 2014 年 2 月發布提升重要基礎設施網路安全架構(Framework for Improving Critical Infrastructure Cybersecurity)，提供業界發展實務策略之參考。

本作業指引係由 CPMI 與 IOSCO 於 2016 年 6 月共同發布，目的是作為 PFMI 網路攻擊復原作業相關準則之補充資料，提供 FMIs 提升其網路攻擊復原作業能力（Cyber resilience）之相關指引。鑑於金融市場結、清算作業具有高度依存性，強調 FMI 應考量與業務流程相關之所有其他機構合作，共同強化網路攻擊復原能力，主管機關間亦應密切合作，有助於達到一致性監管。本作業指引建議 FMI 應以受網路攻擊 2 小時內復原關鍵作業為目標，提出強化網路攻擊復原能力的具體計畫。

網路威脅復原架構的設計，應遵循 5 項風險管理原則[3]，包括治理、辨識、保護、偵測及因應與復原作業等，復原作業並應納入有效性測試、覺察網路風險及持續學習精進網路安全知識與能力。相關復原架構之制訂與實施，需要由 FMI 董事會及高階管理階層參與及支持，組織方能提供包括資訊專業人員在內之足夠資源，管理網路風險。

二、業務持續運作計畫近期發展趨勢

近期由於國際間網路攻擊金融市場事件頻傳，且多由專業駭客集團使用類似手法，連續在不同地區發動攻擊，因此，倡議區域聯防已成為國際間防範網路攻擊之發展重點。國際清算銀行或 SEACEN 等國際組織推動籌組區域型金融資安情資分享及分析中心（F-ISAC），參加 F-ISAC 聯盟之國家，可共同運用資安情資聯防駭客攻擊事件。

由於金融基礎設施肩負重要金融業務支付與結、清算作業之順暢運作，應具備辨識網路相關風險之能力，並制定參加者應符合之網路攻擊復原最低標準，是以基礎設施本身之 BCM 強度應高於參加者，

[3] 參見劉素珠(2017)。

並定期辦理包括網路攻擊等情境之模擬測試。

(一) 重視支付清算網絡中各節點或利害關係人資訊安全維護

近期東南亞國家央行在大額支付系統業務持續運作計畫之實務發展，係考量網路攻擊可能來自支付網絡中多個攻擊點，包括FMI本身、FMI參加機構、委外作業合作機構等利害關係人，尤其近年SWIFT遭受攻擊並非該機構本身，而係由參加機構端受駭延伸之案例，使得支付網絡各端點資安強化議題躍上檯面，爰馬來西亞及泰國等東南亞國家央行，在本次課程中分享，網路安全必須涵蓋支付生態體系各利害關係人，並落實大額支付系統業務持續運作計畫之實地演練，方能檢視並優化相關作業程序。

(二) 落實業務持續運作計畫並定期實地演練

為能有效防範網路攻擊並由事件中迅速復原，馬來西亞央行分享其網路攻擊安全措施，涵蓋資訊、人員與作業程序等3大元素，並發展能確保整體支付生態系統之網路安全防護措施，為達到CPMI要求2小時復原時間目標(Recovery Time Objective, RTO)，除預先規劃攻擊事件中涉及之各利害關係者（包括中央銀行、金融機構監管者及金融機構等）之橫向溝通協調機制，事件發生中有序處理與事後復原安排亦相當重要，並明確規範大額支付系統及其參加機構每年度應實施業務持續運作計畫之演練測試，確保復原作業能力。

(三) 研議建置採不同設計與網路架構之備援中心以隔絕網路風險

為使BCM之備援系統能迅速接續重要支付清算業務運作，目前係採用自動即時備援機制（Automated Real-Time Backup

Systems)，將主中心系統程式及交易資料同步保存在同地與異地備援系統；然此種備援模式在系統遭受網路攻擊時，反將惡意程式與錯誤資料即時傳送到備援系統，導致主、備中心均無法運作。

因此，針對金融市場基礎設施網路攻擊復原報告中所提，採用不同於現行系統之技術（non-similar facility, NSF），預先複製重要金融基礎設施核心業務功能，俾重要系統遭遇網路攻擊而無法運作時，尚能透過 NSF 維持重要業務之運作。泰國學員在課程中分享，該國研擬建置採用不同架構暨防火牆設計之大額支付備援系統，惟初步評估將花費大量成本，並需長時間規劃重要清算業務之人工作業程序，值得我國繼續關注其後續發展。

參、國際間近年金融駭客攻擊事件

金融機構掌握大量客戶資產，並提供各種金融服務，易淪為國際駭客攻擊目標，謀取不法利益。國際間較常見的駭客攻擊金融機構事件，係鎖定各種與消費者日常生活切身相關的支付方式，如支付卡、遠端銀行服務[4]、支票及推式支付[5]等。

專業駭客不僅攻擊前述零售支付系統，近年屢見大額支付系統遭入侵。為清算銀行間交易，參加機構存放在清算帳戶之餘額通常維持極高水位，因此如成功被駭，單筆交易金額大，總損失金額通常遠大於零售支付系統遭駭損失；如 2016 年 2 月孟加拉央行在美國聯邦準備銀行帳戶資金被盜事件，約損失 8,100 萬美元，以及 2018 年 5 月

[4] 遠端銀行服務(remote banking)泛指透過網際網路取得的銀行服務，包括網路銀行(internet banking)、電話銀行(telephone banking)及行動銀行(mobile banking)。

[5] 推式支付(push payment)係指帳戶所有人透過支付服務提供者事先授權綁定帳戶付款，利用網路銀行、行動銀行或 Facebook、WeChat 及 LINE Pay 等第三方機構支付平台，自其帳戶將資金移轉至受款人帳戶，包括 C2C、C2B 及 B2C。相較於拉式支付(pull payment)則係由受款人發動支付請求。

墨西哥央行大額支付系統之參加銀行帳戶資金遭竊事件，約損失 3 億墨西哥披索（約 1,520 萬美元）。

一、大額支付系統遭駭風險

大額支付系統為中央銀行貨幣政策執行的重要基礎設施，且因其負責清算銀行間大額交易之特性，通常由中央銀行建置並營運，清算完成的交易即達到最終清算（final settlement）[6]效力，各國大額支付系統清算業務範圍因地制宜，部分國家系統僅接受銀行間清算交易，如本行同業資金調撥清算作業系統；部分國家則接受零售支付系統一定金額以上之客戶間交易，如日本 BOJNET（Bank of Japan Financial Network System）受理銀行跨行支付 Zengin 全銀系統 10 億日圓以上大額交易；亦有國家之大額支付系統同時處理銀行間大額清算交易與一般客戶間交易者，如墨西哥央行 SEPI （Interbank Electronic Payments System）。

(一) 2016 年 2 月間孟加拉央行遭駭事件

1、事件摘要[7]

(1) 2016 年 2 月 5 日（營業日），美國紐約聯邦準備銀行大額支付系統收到來自孟加拉央行 35 筆轉帳指示，總計轉出金額 9.51 億美元，其中 8.5 億美元被擋下，另外 1.01 億美元共 5 筆交易指令成功被執行。

---

[6] 依據 PFMI，最終清算為法律定義之時點，係指 FMI 或其參加者依據相關契約條款，進行資產或金融工具之不附條件且不可撤銷的移轉或解除債務。採即時總額清算機制之大額支付系統，於支付指令成功執行完成，該筆支付即具備清算最終性，有效降低清算風險，資金可立即使用，且不可撤銷。

[7] 參見 Devnath(2016)及 Larano(2016)。

(2) 1.01 億美元分別匯至 4 個外國銀行帳戶，其中 1 筆因拼錯受款人名稱，致交易被攔阻，最終總計 8,100 萬美元被駭客成功轉出。

2、入侵手法

(1) 潛伏並蒐集資訊

駭客利用惡意程式取得使用者存取系統之合法權限，潛伏一定期間蒐集所需資訊。

(2) 挑選例假日前夕發動攻擊

駭客透過 SWIFT 客戶端使用的 Alliance Access[8]軟體連結至 SWIFT 網路，並選擇在孟加拉連續假期前夕，發出 SWIFT 匯款電文指示，非法移轉帳戶資金。

(3) 銷毀電腦軌跡，拖延對帳

竄改查詢帳戶餘額之程式，並刪除偽冒轉出交易紀錄及對帳報表，使得相關稽查管控點失去功效，且適逢孟加拉連續假期，成功拖延偽冒交易被發現時點。

3、補救措施：SWIFT 承認本次事件並非單一事件，因此，除要求會員機構更新 Alliance Access 軟體版本外，並需配合執行 SWIFT 之客戶安全計畫（Customer Security Programme, CSP）[9]。

(二) 2018 年 5 月間墨西哥銀行遭駭事件

1、事件摘要

[8] Alliance Access 係 SWIFT 提供參加機構端用以與 SWIFT 連線之應用軟體。
[9] 參見 SWIFT Customer Security Programme, www.swift.com/csp.

墨西哥央行於 2018 年 5 月中發表聲明，5 月初該國銀行間電子支付系統（SPEI）遭受網路攻擊，共 5 家商業銀行受害，約損失 3 億墨西哥披索（約 1,520 萬美元）[10]。

2、入侵手法

(1) 墨西哥央行並未對外說明駭客入侵手法，以及是否追回損失金額，僅表示雖發生該起攻擊事件，該國支付系統仍正常營運，惟受到攻擊銀行之交易因增加檢核緣故，致交易程序會受到延遲。

(2) 據其他非官方消息來源，駭客應係利用金融機構委外開發 SPEI 系統應用軟體有安全漏洞，致駭客得以利用假帳戶，發出偽支付指令移轉資金。

3、補救措施

針對本次墨西哥央行遭到網路駭客攻擊事件，該行將成立網路安全管理委員會，該管理委員會將制訂銀行資訊安全指導原則，就資訊安全政策、指導準則與管理策略全方位加強墨西哥央行的內部資訊安全系統。

二、零售支付系統遭受詐騙風險

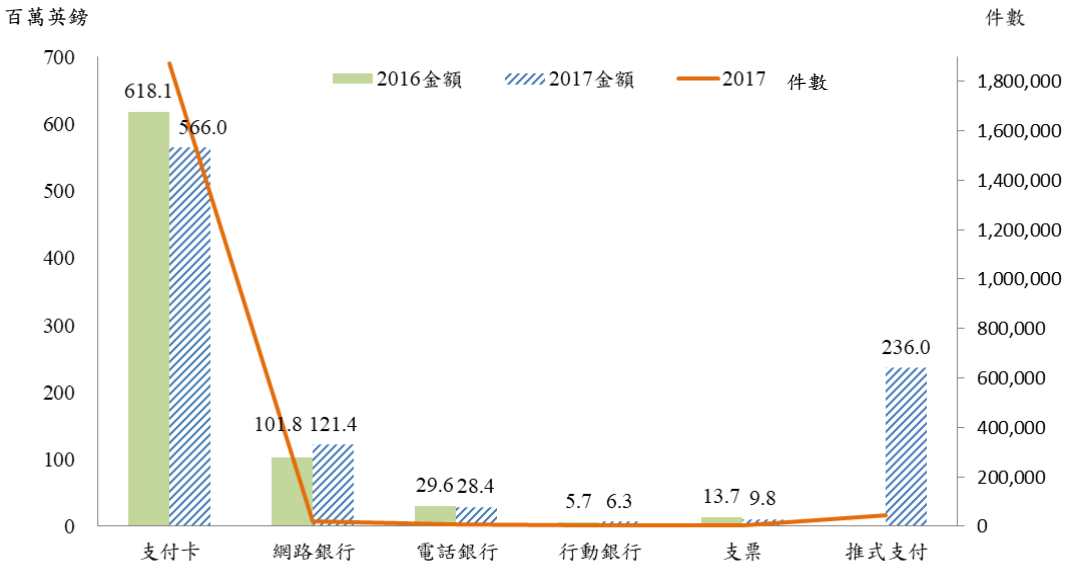
依據 UK Finance 發布 2017 年英國金融業遭詐騙統計報告[11]，金融詐騙交易分為未經授權詐騙交易（unauthorised fraudulent transaction）及經授權的推式支付（authorized push payment）2 種。經統計，英國 2017 年包括支付卡、遠端銀行服務及支票等未經授權交易之詐騙案

[10] 參見 King(2018)。

[11] UK Finance 前身為 Financial Fraud Action UK (FFA UK)，原係金融業為防制卡片詐騙所成立之機構，參見 UK Finance(2018)。

件，共 191 萬餘件，金額總計 731.8 百萬英鎊 ，較 2016 年減少 5%；成功阻止的詐騙交易則高達 1,458.6 百萬英鎊。然而首度公布經授權推式支付之詐騙案件，總計 4.3 萬餘件、236 百萬英鎊，僅追回 60.8 百萬英鎊。（圖 1）

圖 1 英國金融詐騙案件統計



資料來源： UK Finance(2018)

近年各國因應智慧行動裝置滲透率提升，且消費者對資金移轉到款速度及便利的使用者介面等要求日益提高，驅使各國大力發展快捷支付[12]。零售支付系統講求服務覆蓋率（coverage ratio），資金到款迅速及服務隨時可用是吸引消費者使用的主要因素，因此多為開放式系統（open systems）[13]，亦即使用者能透過多個中介機構取得金融服務；例如支付服務提供者（Payment Service Provider, PSP）與銀行，相較

[12] 依據 CPMI 快捷支付(instant payment)的定義，係指一筆支付由傳送支付訊息至資金最終可被受款人使用係即時或接近即時，並且消費者幾乎隨時(24/7)可以使用快捷支付。

[13] 採開放式系統(open systems)的快捷支付，通常涉及多個支付服務提供者，因此在支付訊息傳送的規則及程序，以及結、清算機制，均需要事先協定。

於封閉式系統（closed systems）[14]，僅對其客戶提供金融支付服務，通常僅涉及 1 家 PSP。非銀行的支付服務提供者加入快捷支付，一方面有助於市場競爭，但另一方面因該二種機構之公司治理及適用之監管法規不同，其風險自然不同於受到高度監理的金融機構，特別是作業委外（outsourcing）風險及金融詐騙（fraud）風險。

銀行為了降低特定業務風險，將部分作業委由專業之非銀行機構承做，然而，作業委外無法確保所有可能的偶發狀況，萬一造成重大事故，銀行信譽將受損害，因此對於委外作業必須事先規劃因應策略，以共同處理可能發生的事故。

金融詐騙則可能因機構安全管理不當，致消費者帳戶或支付交易等機敏資料外流，或是遭受網路攻擊，駭客取得機構內系統使用者帳號、密碼等資訊，致其客戶暴露於詐騙風險。此外，**非銀行機構加入支付服務供應鏈，又會增加支付過程之節點；因此，供應鏈中的各機構，甚至銷售商店，均應實施合宜的資訊安全維護措施，方能降低詐騙機率，確保消費者權益**。

快捷支付資金快速到款的特性，衍生詐騙交易資金被迅速提領之問題，通常藉由系統限制單筆交易資金移轉上限，或者系統自動於交易完成後，即時發送交易明細，通知轉出方及受款方，則有助於降低遭詐騙金額，並使消費者及早辨識遭受詐騙交易之風險。

三、運用金融科技防範詐騙

國際間支付發展趨勢，非銀行業者如科技公司加入金融支付產業，提供消費者便利的支付。為提升支付交易在跨系統間傳遞的效

[14] 一般而言，封閉式系統(closed systems)因僅服務其參加者，因此服務覆蓋率較開放式系統為低，例如銀行客戶在該銀行體系帳戶資金移轉之自行(on-us)交易；惟部分傳統銀行金融服務普及率較低國家如肯亞，由電信商營運 mPesa 雖屬封閉式系統，其金融支付服務之覆蓋率很高。

率，建立系統互通性愈形重要，爰需發展標準化之技術、資料格式及業務流程，以確保金融支付安全，例如應用多重驗證技術強化使用者登入管理，以及運用區塊鏈技術在銀行間清算交易，可追蹤交易狀態提升安全性。

(一) 雙因子驗證機制

近年 SWIFT 網絡發生多起被國際駭客藉道攻擊支付系統的案例，提醒支付系統營運者與監管者，在支付交易傳遞過程中，均可能成為駭客攻擊的進入點。

為加強防範外部滲透攻擊與內部資安威脅，會員機構安全控管計畫分為 3 個層面-「用戶層面之安全與防護」、「交易對手層面之預防與偵測」及「社群層面之資訊分享與準備」，共 27 項安全控管措施，其中 16 項為強制措施、11 項為建議性措施。

多數網路攻擊均利用機構內部資安弱點，盜取員工之系統帳號密碼以取得權限；因此，SWIFT 新措施採用雙因子認證（two-factor authentication，2FA），防止帳號權限被盜用，除傳統的使用者名稱與密碼之外，增加第 2 種確認使用者身分的機制，防止駭客冒用合法使用者權限進行業務活動。

目前常用於加強使用者身分驗證之因素，包括持有因子（possession factor）與固有因子（inherence factor）：

1、持有因子：係指使用者持有之憑證，例如發送至使用者手機之簡訊動態密碼、USB 金鑰驗證、存有使用者身分資訊的 Smartcard、公正第三方機構簽發之憑證等。

2、固有因子：係指運用使用者的生物特徵作身分識別，包括指紋、聲紋、虹膜、臉部特徵、簽名等。

(二) 機器學習

駭客攻擊金融支付系統之目的係為盜取資金，除了強化前端資訊安全防護之外，導入機器學習，以及早偵測後端業務活動之異常情況，亦有助於及時攔阻被駭資金。

1、偵測使用者存取支付系統之行為改變

例如針對登入系統地點改變、登入時間改變、以失效帳號嘗試登入系統等使用者紀錄，加以確認，可提升異常活動偵測機率，從而降低駭客冒用使用者系統權限之風險。

2、偵測系統異常交易

例如一段時間內支付交易頻繁轉至某特定地區或某特定受款人、非營業日支付交易筆數異常增加等。

(三) 區塊鏈技術

現行資金移轉方式，係建構在綿密金融支付網絡與集中式系統處理架構上，一般認為金融機構受到高度監管，交易受到極高安全等級保護。然而，資金移轉過程的作業複雜度及資金到款通常未與發動交易時點同步，當資金撥轉方提送一筆資金撥轉交易，資金收受方並未同時收到該筆資金，真正收到款項的時間，可能在數小時甚至數天之後。

交易訊息由撥轉方至受款方的過程，係受限於金融體系支付系統之結、清算機制，以及中間代理銀行層層轉送之處理程序，資金

到款延宕情形尤以跨境交易最為明顯。冗長的作業處理時程，交易訊息因複雜作業流程致難以追蹤其狀態，導致資訊不夠透明，因而增加詐騙風險。（圖 2）

圖 2 Ripple 提供應用區塊鏈技術的跨境支付方案

(左圖)傳統單向跨境支付訊息

延後到款： 交易自發動到收款約需 2-4 個工作天

不確定性： 交易發動時不確知交易費用等成本

交易風險： 缺乏交易追蹤或可瞭解交易狀態的機制

(右圖) 應用區塊鏈技術
包含清算指令的雙向跨境支付訊息

快速到款： 4 秒內即可完成支付交易之清算

確定性： 交易發動時即確知交易費用及交易內容

透明性： 可追蹤整段支付流程

資料來源：SEACEN 課程講義

隨著分散式帳本（Distributed Ledger Technology, DLT）技術的興起，支付市場參加者倡議利用 DLT 之加密技術及點對點同步完成資金撥轉與交易訊息等優勢，提供新型態支付服務，例如 Ripple 提出運用 DLT 技術，改善傳統銀行間跨境清算作業流程，並增加交易的安全性，因支付訊息包含雙向的資金清算指示，並有利於追蹤支付流程及確知交易成本與詳細的付款訊息。

1、交易到款速度：相較於傳統支付系統跨境交易到款需耗時 2-4 天，如 Ripple 提供運用區塊鏈技術的支付方案，最快僅需 4 秒鐘便能完成跨境資金移轉。

2、訊息透明度：由於交易流程直接由資金轉出方的銀行發動，直接發送至資金收受方往來銀行，省去多個中間代理機構作業，交易狀態易於追蹤，可提升交易訊息透明度。

3、交易確定性：發動交易時，即可確定該筆交易成本與交易訊息包含的明細資訊；而傳統跨境支付交易，中間代理行尚另外收取費用，收款方需俟收到款項才能確知被收取的全部交易處理費。

四、 小結

零售支付系統攸關消費者使用體驗，是以重要服務因系統故障或受駭客攻擊致無法提供服務，將直接影響消費者對金融機構服務之選擇。依據英國金融市場行為監管局（Financial Conduct Authority）委託研究機構於 2017 年 7 月發布之消費者調查報告，技術服務的可靠性（technical service reliability）為消費者重視的銀行服務指標，其衡量標準包括重要服務出現問題之頻率、核心服務故障時間之長短、服務故障係因技術或作業問題所致，以及復原作業時間長短等。

此外，美國國土安全部 2018 年發布報告指出，將重要基礎設施如電廠等，視為網路攻擊目標之風險有升高跡象，攻擊重要金融基礎設施可對一國與民眾相關事項造成立即且重大的影響。重要金融基礎設施因與參加者、服務提供者及其他金融基礎設施相連結，負責重要金融交易之傳送處理與結清算作業，是以亦容易成為網路駭客攻擊目標。由於辨識網路攻擊之問題點較一般單純之系統或作業問題更為複雜，復以原規劃之作業復原管道亦可能受影響，無法發揮功效，因此，國際準則建議之 2 小時作業復原時間，實務上不容易達成。

網路攻擊無所不在，不論系統架構係屬開放式或封閉式，面對高超的國際專業駭客，均可能因未經防範之系統漏洞，或是組織內缺乏

資安意識員工於無意間洩漏內部網路帳號密碼資訊，而成為駭客入侵的跳板。因此，支付產業中的各個機構，應參考國際清算銀行發布之相關網路安全風險指引與建議，防範網路攻擊，減少支付系統遭駭損失。

肆、馬來西亞 PayNet 業務持續運作經驗分享

PayNet[15]公司負責營運馬來西亞大額支付系統（Real-Time Electronic Transfer of Funds And Securities System, RENTAS）及多個零售支付系統，本章先簡介馬來西亞支付系統營運與監管架構，接著說明該系統遭遇網路攻擊、重大天然災害及系統故障等重大事故時，相關公司治理、風險管理架構及業務持續運作管理之規劃與跨部門作業安排等。

一、馬來西亞支付系統營運與監管架構簡介

依據馬來西亞 2013 年施行的金融服務法（Financial Services Act, FSA），任何人欲提供支付系統或發行指定之支付工具，必須事先取得馬來西亞央行之核准；欲提供收單業務者，亦須向馬來西亞央行登記。馬來西亞央行身兼支付系統與支付工具之監管者，亦即，其職掌涵蓋總體審慎監理及個別銀行監管者，與我國支付系統由中央銀行監管、金融機構監理係金融監督管理委員會職掌之分治架構不同。

馬來西亞整體支付網絡，係以 PayNet 營運之該國大額支付系統 RENTAS，以及銀行間電子資金移轉（Interbank GIRO, IBG）、快捷支付 MEPS instant payment、全國繳費 JomPAY、金融卡消費支付

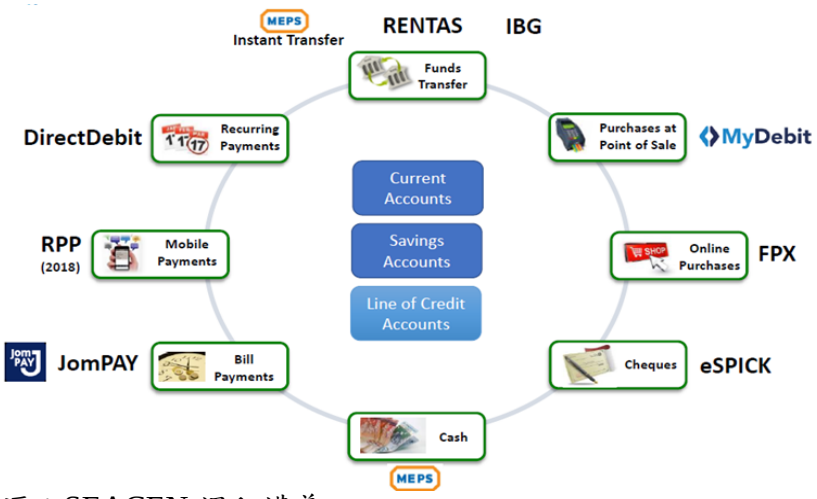
[15] PayNet(Payments Network Malaysia Sdn Bhd)前身為 MyClear(Malaysian Electronic Clearing Corporation Sdn Bhd)，原係馬來西亞央行百分之百持有的子公司，後於 2018 年 8 月 1 日與 11 家該國銀行持有之 MEPS(Malaysian Electronic Payment System Sdn Bhd)合併，合併後馬來西亞央行持有 PayNet 約 37%股權，為 PayNet 最大股東。

MyDebit、線上支付 FPX、代收系統（Direct Debit, DD）及票據結算（Sistem Penjelasan Imej Cek Kebangsaan, eSPICK）等零售支付系統所組成，PayNet 係該國具系統重要性金融基礎設施（圖 3）。

該國近年來積極推動提升支付系統功能，以增進支付效率與安全，2016 年 9 月 RENTAS 之跨境交易新增採用 SWIFT 網絡全球訊息標準[16]，提升支付與證券交易之可用性（accessibility），並擴增連結大額支付系統之通道。此外，在零售支付系統部分，為增加消費者快速、便利的支付體驗，預計於 2018 年建置完成的全時行動支付平台 DuitNow[17]，消費者得以手機號碼、身分證號碼或護照號碼，連結銀行帳戶或電子錢包帳戶進行轉帳及支付。

為引導消費者改變消費與付款習慣，由實體支付工具轉移至電子支付，該國調整交易手續費定價政策[18]，藉由提高支票等紙本支付工具交易費率，同時調降網路及線上平台交易費率，如自然人單筆交易 5,000 馬幣以內免收手續費、超過 5,000 馬幣僅收取 0.5 馬幣手續費。

圖 3　PayNet 營運的支付系統



資料來源：SEACEN 課程講義

[16] 國內銀行連結 RENTAS 之境內交易，仍採用該國原有之專屬交易訊息規格。

[17] DuitNow 正式商轉時程尚未公布，目前參加機構計 44 家，消費者及企業用戶將可透過網路銀行、行動銀行及銀行電子錢包行動 app 等通路，綁定其銀行帳戶或電子錢包帳戶，使用該項服務，單筆交易金額上限為 10 萬馬幣(自然人)及 1 億馬幣(企業戶)，參見 www.duitnow.my。

[18] 參見張逸綸(2018)。

二、PayNet 風險管理治理政策及架構

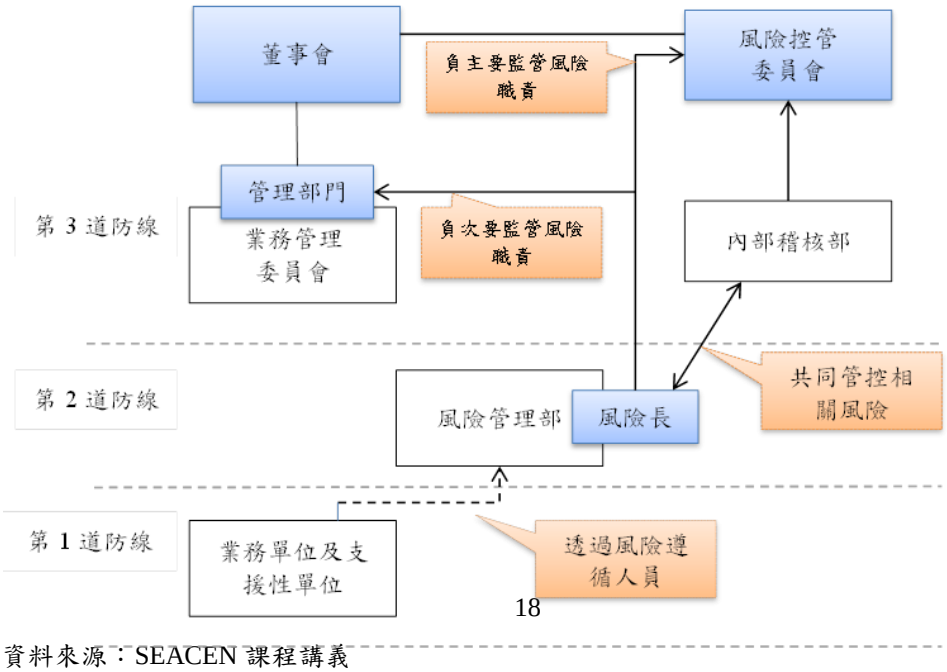
依據 PFMI 報告書建議，考量金融基礎設施具系統性重要地位，其作業流程涉及支付生態體系全體成員，無法單獨運作，面臨愈來愈多的網路攻擊威脅，金融基礎設施本身應具備健全的風險管理架構，包括治理、策略及程序。

(一) PayNet 風險管理治理政策

PayNet 風險管理架構涉及組織內各單位，包括董事會（Board）、風險控管委員會（Audit & Risk Committee, ARC）、內部稽核部（Internal Audit Department, IAD）、風險管理部（Risk Management Department, RMD）、業務單位（Business Units, BUs）及支援性單位（Support Units, SUs）。

為利風險管理及風險管理架構的執行，PayNet 制訂風險管理 3 道防線，明確定義各部門應負責之風險監管相關事宜，並使得董事會、風險控管委員會及業務管理委員會等高階管理階層，透過此機制傳遞 PayNet 風險政策至相關部門。（圖 4 及表 1）

圖 4　PayNet 風險管理架構



資料來源：SEACEN 課程講義

表 1 PayNet 風險管理架構各部門職掌與 3 道防線對照表

防線(LOD)	組織層級	主要職掌
第 1 道防線	業務單位 (BUs)/支援性單位(SUs)	• 透過自我評估進行主要風險辨識、業務衝擊分析及 BCM 程序 • 風險管控與監視 • 由風險遵循人員(Risk & Compliance Officer, RCO)/風險所有權者，向風險管理部彙報
第 2 道防線	風險管理部 (RMD)	• 領導協調組織內部風險管理架構之執行 • 協助業務單位進行風險管理與確保控制作業 • 設置風險長(Chief Risk Officer, CRO)，負責向業務管理委員會及風險控管委員會報告風險相關事宜，並與內部稽核部(IAD)共同合作管控相關風險
第 3 道防線	董事會 (Board)	• 風險所有權之最高層級 • 風險管理架構及整體風險管理之最高層級
	風險控管委員會(ARC)	• 負責執行風險管理架構、適時更新風險圖像、確保已實施合適的管控措施 • 制定風險管理部之職掌並督促作業
	內部稽核部 (IAD)	• 確保健全的風險控制自我評估作業 • 獨立檢視及評估風險，直接隸屬於風險控管委員會 • 協助風險控管委員會評估業務單位是否遵循核定的風險管理程序

資料來源：SEACEN 課程講義

(二) PayNet 風險管理架構

1、風險辨識

風險控管委員會係依據PayNet服務宗旨，在可接受的風險程度，制定風險胃納說明書（Risk Appetite Statement, RAS），透過有效的風險管理措施，將固有風險降低至可接受的程度。PayNet 主要涉及之

風險為作業風險、財務風險及系統性風險：

- 作業風險：PayNet 因內部不適當的作業程序、人員及系統，或外部事件，造成損失的風險。

  ✓ 內部作業風險：源自組織內部之人員作業疏失或員工管理不當、作業程序問題、系統等技術面因素、法規問題、設備問題及專案風險。

  ✓ 外部作業風險：源自組織外部之人員及作業程序問題，以及相關金融基礎設施無法運作、遭受外部攻擊，或者是業務相關第三方機構無法提供服務及管理面、法規面及設備面等問題。

- 財務風險：係指 PayNet 財務受到市場顯著變動影響，或受其參加機構、第三方服務提供者及其他相關機構問題影響，包括信用風險、流動性風險、擔保品風險、流動性風險、市場風險、或有負債風險、保險合約風險、模型風險等。

- 系統性風險：係指受到金融體系一部分或全部失序之影響，造成 PayNet 無法提供金融服務的風險，且對實體經濟造成嚴重負面影響。

  ✓ 國內系統性風險：與國內機構相關或國內市場相關的失序事件，其影響層面及於整體金融市場之風險。

  ✓ 國際系統性風險：與國外機構相關或國際市場相關之失序事件，其影響層面及於整體金融市場之風險。

2、風險監管與風險等級

PayNet 的風險管理架構，將風險區分為 4 種，亦即低、中、高

及極高，並將風險監管職責分為主要（primary）與次要（secondary）的監管職責；負主要監管職責者，對於風險負直接密切監控責任，並應監視風險減緩措施的執行；負次要監管職責者，僅需定期檢視並發現風險，幫助決策單位作出正確的風險減緩措施。組織內各單位對於不同風險等級，再依據原有風險（gross risk）及實施控制措施後剩餘風險（residual risk）承擔其應負之監管職責。（表 2）

表 2　PayNet 風險監管職責暨風險等級對照表

風險	監管職責	風險等級			
		極高	高	中	低
剩餘風險	監管作為應負責檢視/監視風險及採取行動者	董事會/ ARC	董事會/ ARC	董事會/ ARC	董事會/ ARC
		業務管理委員會	業務管理委員會	業務管理委員會	業務管理委員會
		內部稽核部	內部稽核部	內部稽核部	內部稽核部
		風險管理部	風險管理部	風險管理部	風險管理部
		業務單位	業務單位	業務單位	業務單位
原有風險	監管作為應負責定期檢視/監視風險者	董事會/ ARC	董事會/ ARC	董事會/ ARC	董事會/ ARC
		業務管理委員會	業務管理委員會	業務管理委員會	業務管理委員會
		內部稽核部	內部稽核部	內部稽核部	內部稽核部
		風險管理部	風險管理部	風險管理部	風險管理部
		業務單位	業務單位	業務單位	業務單位

■ 主要（primary）監管職責：對於風險負直接密切監控責任，並應監視風險減緩措施的執行

□ 次要（secondary）監管職責：僅需定期檢視並發現風險，幫助決策單位作出正確的風險減緩措施

資料來源：SEACEN 課程講義

3、風險管控措施

負責管控風險之單位，根據風險等級及其被賦予之權責，並考量解決方案暨時程，以及投入的財務資源等 2 種因素，實施風險減緩措施（圖 5）。

圖 5　解決方案及財務資源等級

資料來源：SEACEN 課程講義

有關風險管理工具的選擇，包括：

(1) 風險管控自我評估（risk control self-assessment, RCSA）

係辨識、評估及監控 PayNet 面臨風險之主要工具，每年檢視 1 次，並將歷年已辨識的風險、影響程度評估及所實施的相關控制措施，建立 excel 資料庫留存。

(2) 關鍵風險指標（key risk indicators, KRI）

由業務單位風險遵循人員每月報告是否發生風險事件，以及風險事件可能發生的機率及其影響。

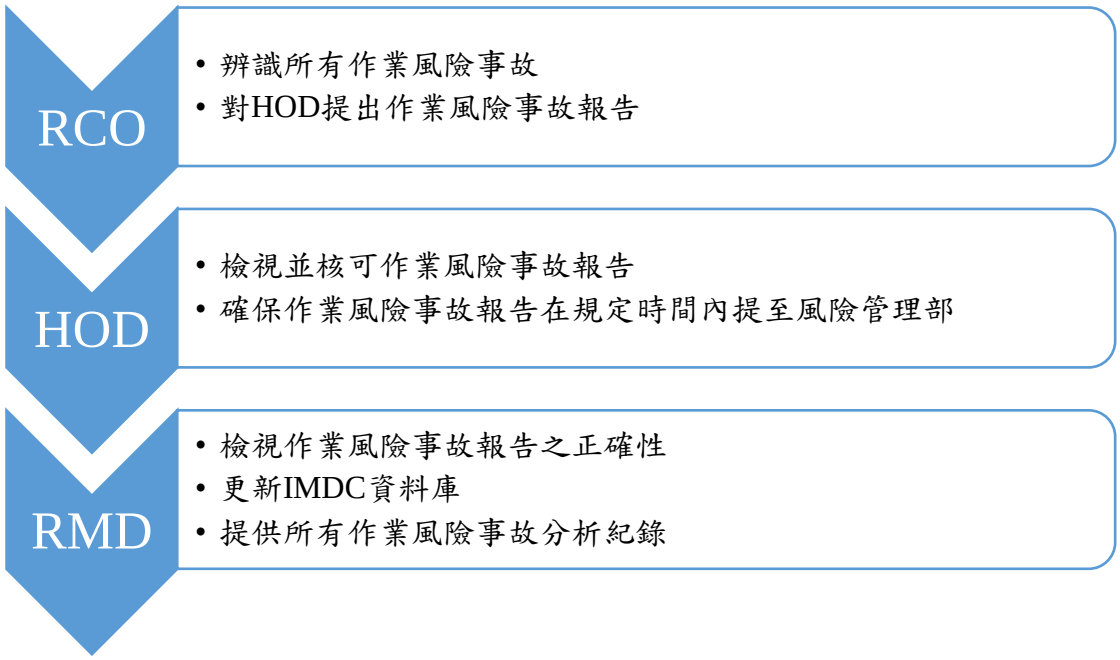
(3) 關鍵控制指標（key control indicators, KCI）

就特定風險事件之降低發生機率、事件偵測或減緩事件影響等，提供評估實施控制措施之有效性。

(4) 事件管理與資料蒐集（incident management and data collection, IMDC）

建立資料庫，記錄所有曾經發生之事故及事故分析，作為評估目前內部控制作業無效或不適宜之指標。涉及風險遵循人員（RCO）、RCO 隸屬部門主管（Division Heads of the respective RCOs, HOD）及風險管理部。（圖 6）

圖 6　事故管理與資料蒐集(IMDC)流程



資料來源：SEACEN 課程講義

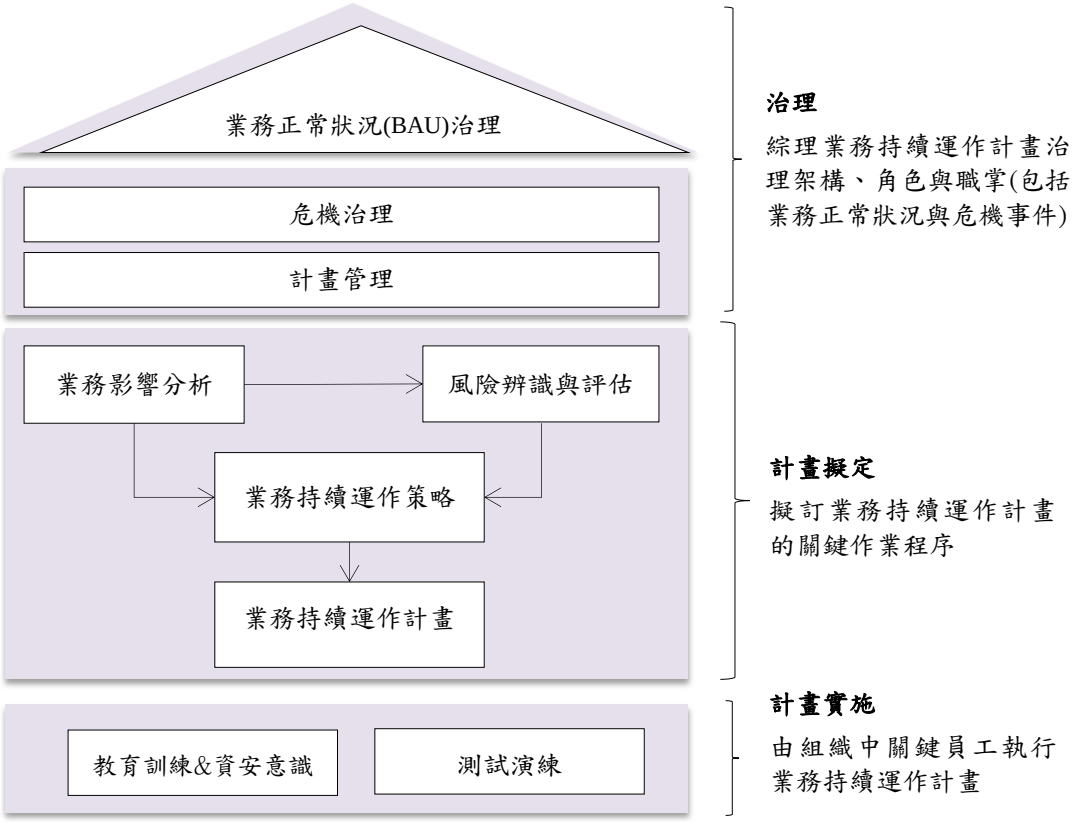
三、PayNet 業務持續運作計畫

為確保業務持續運作計畫之有效性，由 PayNet 高階管理單位負責綜理一般業務（business-as-usual, BAU）之運作。另設置危機管理小組（crisis management team, CMT），當發生危機事件，能在有限的時間內進行評估、決策並迅速反應。（圖 7）

馬來西亞央行亦設置危機管理小組（BNM CMT），當危機事件對 PayNet、馬來西亞央行及金融機構造成重大影響，並啟動 BCM，該事件之復原作業才會由馬來西亞央行危機管理小組接掌，處理與新

聞媒體聯繫、發布新聞稿等事宜。

圖 7　PayNet 之業務持續運作計畫治理架構與政策



資料來源：SEACEN 課程講義

(一) 失序事件 5 等級

為管理危機事件之風險，風險管理架構依影響程度區分為 5 個失序等級（Level of Disruption, LoD），作為馬來西亞央行及 PayNet 決策者處理失序事件之判斷依據（表 3）。並以馬來西亞大額支付系統 RENTAS 為例，模擬發生不同程度失序事件之情境。（表 4）

表 3 失序事件等級

失序事件等級 LoD	受影響機構	危機事件時負責提出下個階段採取措施(包括媒體溝通及發布新聞稿)
1	僅 PayNet	PayNet 危機處理小組
2	馬來西亞央行、PayNet	馬來西亞央行危機處理小組
3、4	馬來西亞央行、PayNet 及金融機構	馬來西亞央行危機處理小組
5	全國性	國家安全會(National Security Council, NSC)

資料來源：SEACEN 課程講義

表 4 馬來西亞大額支付系統失序事件模擬情境

失序事件等級	馬來西亞大額支付系統失序事件模擬情境
1	PayNet 因辦公室問題、網路問題及(或)內部系統故障，例如發生火災、暴動或實施管制(受隔離地區)， PayNet 對外通訊網路無法使用；或一段時間停電；或是與馬來西亞央行資料中心間連線斷斷續續，造成 PayNet 無法連線至 RENTAS
2	位於主中心的 RENTAS 系統故障無法使用，必須以備援中心接替運作
3	主中心及備援中心所有的通訊網路無法使用
4、5	發生全國性的暴動並實施戒嚴管制

資料來源：SEACEN 課程講義

1、業務持續運作暨災害復原測試計畫

PayNet 作為馬來西亞重要金融基礎設施，為確保在發生重大失序事件時，能快速回應並使關鍵服務繼續運作，對於所營運具系統重要性之大額及零售支付系統，依據該國業務持續運作計畫，

訂定年度演練之模擬情境、時程與辦理次數(表 5),且遵循 PFMI 報告書建議，金融基礎設施本身應具備健全的 BCM 架構，且其標準應高於參加機構。

表 5　PayNet 營運支付系統年度實地模擬演練辦理次數

支付系統	每年實地模擬演練 辦理次數	辦理日期
RENTAS	12	7 個工作日前 通知參加機構
eSPICK	12	
Inter Bank Giro	4	
MyDebit	2	
FPX	2	
Direct Debit	2	
JomPAY	2	

資料來源：SEACEN 課程講義

2、訂定 MTD 及 RTO 復原時間標準

系統無法運作最大容忍時間(MTD):係指自發生危機事件開始，至系統與資料完全恢復正常並可正常執行業務為止,包括危機處理小組決策時間、復原目標時間、人員調度及資料比對等作業時間等。

復原目標時間（RTO)：指自危機處理小組宣布危機事件開始，至資訊系統及應用服務恢復可支援正常業務運作為止。

PayNet 營運大額及零售支付系統之 MTD 與 RTO 設定原則，係依業務對金融市場影響之重要性,大額支付系統業務最大可容忍 2 小時中斷，其資訊系統及應用服務復原作業必須在 1 小時內完成，零售支付系統 MTD 與 RTO 目前分別為 6 小時及 4 小時，至 2020 年目標將達到 4 小時及 2 小時。(表 6)

表 6　PayNet 營運支付系統之 MTD 與 RTO

PayNet 營運支付系統		用途	資金可用時點	MTD (小時)	RTO (小時)
大額支付系統					
1	RENTAS	銀行間大額資金撥轉與金融市場交易結清算	即時	2	1
2	eSPICK	支票處理系統	-	2	1
零售支付系統					
3	IBG	銀行間電子資金移轉系統 提供銀行客戶自帳戶撥轉資金，約 42 家銀行加入	即時	4	2
4	DD	適用定期性授權扣帳之代收系統 交易手續費:最低 0.5 馬幣/筆	當日	4	2
5	FPX* (24*7 營運)	電子商務及線上購物消費支付(B2C、B2B) 提供銀行客戶以銀行存款帳戶進行支付，該國銀行幾乎全數加入 交易限額:個人 3 萬馬幣/筆；公司 1 百萬馬幣/筆 手續費:最低 0.5 馬幣/筆	即時	6	4
6	JomPAY*	全國繳費系統 提供消費者透過行動銀行、網路銀行及 ATMs，以銀行帳戶及信用卡支付逾 2,500 種帳單，共 42 家銀行加入	即時	6	4
7	MyDebit*	消費者使用晶片金融卡在商家銷售點進行支付	T+1 日	6	4

* FPX、JomPAY 及 MyDebit 等 3 個系統之 MTD 與 RTO，預定於 2019 年 1 月及 2020 年 1 月分別達到 5 及 3 小時、4 及 2 小時。

資料來源：SEACEN 課程講義

(二) 參加機構業務持續運作管理

PayNet 考量其作為金融基礎設施之系統性重要地位，相關支付作業流程涉及支付生態體系全體成員，若參加機構未具備業務持續運作之作業復原能力，許多與金融市場密切相關的重要支付系統亦無法單獨運作，爰於 2016 年制定「參加機構使用 PayNet 服務之業務持續運作標準」[19] ，規範參加機構應就其所參加之系統服務，遵循相關標準。

1、適用範圍：大額支付系統 RENTAS 與 eSPICK，以及零售支付統如 IBG、JomPAY、FPX、Direct Debit 及 MyDebit 之參加機構，並包括作業委外辦理之受委託機構，如技術服務提供者等。

2、實施日期：2017 年 1 月 1 日。

3、業務持續運作計畫（BCP），應包括：

(1) 至少每年進行風險評估（Risk Assessment，RA）暨業務影響分析（Business Impact Analysis，BIA）乙次，找出可能嚴重影響大額支付系統與零售支付系統運作的威脅，並分析災害期間因無法使用系統，對於業務造成之財務與非財務影響

(2) 採取其他有效的風險管控措施，以降低大額支付系統與零售支付系統無法運作造成之可能影響。

(3) 制訂經高階管理階層核准之作業復原策略，並定期檢視，內容應包括復原時間、備援及復原中心、業務運作模式(人工作業、

[19] PayNet 前身 MyClear 於 2016 年 12 月 22 日發布「The guidelines on business continuity management for participants of MyClear's services」，作為 PayNet 營運之大額支付系統與零售支付系統作業程序文件之一，所有參加機構均需遵循本項準則所訂定 BCM 標準，並自 2017 年 1 月 1 日生效。

部分人工作業或系統自動處理)、復原作業關鍵人員、辦公場所、資料、設施及技術支援。

(4) 訂定災害復原計畫（DRP）標準，每年定期執行計畫內容、定期測試與維護，並向 PayNet 報送執行結果報告。

(5) 遵循 PayNet 訂定之系統無法運作最大容忍時間（MTD）及復原目標時間（RTO）。（同表 6）

(6) 與重要服務提供者、供應商及相關交易對手以合約約定為符合 MTD 及 RTO 之復原作業與可容忍服務中斷之服務水準。

4、業務持續運作計畫及災害復原測試

PayNet 要求其參加機構應提送業務持續運作計畫及災害復原測試結果報告，並統一各機構模擬個案之時程，測試個案如不需危機處理小組決策者訂為 30 分鐘；如涉及危機處理小組決策之測試個案則依個案安排時程。

為方便參加機構進行模擬測試演練，PayNet 會將年度 BCP/DRP 實地演練日期時程表，於 7 個工作天前通知相關參加機構。參加機構應於年度 1 月 31 日以前向 PayNet 提出其 BCP/DRP，並在預定執行演練的 3 個工作天以前，將機構名稱、指定辦理系統、聯絡電話、電子郵件及聯繫窗口等資訊通知 PayNet，完成演練作業 7 個工作天內將演練報告寄送 PayNet。

(1) 大額支付系統參加機構每年度應辦理 6 次業務持續運作或災害復原計畫（BCP/DRP）模擬演練，包括 RENTAS 銀行端閘道/SWIFT 應用軟體、eSPICK 客戶端閘道。在復原目標時間內，

必須從災害復原中心執行系統運作，若是未達到相關演練標準，需重新安排再次測試。（表 7）

表 7 大額支付系統參加機構年度應辦理之模擬演練

模擬情境		參加機構業務地點	參加機構資料中心地點*	PayNet 資料中心地點*	年度演練執行頻率及時間
1.	測試參加機構 DR 功能及連結至 PayNet 正式主機情形	主/備中心	DR	Production	至少 1 次 1-2 個工作天
2.	全市場測試 PayNet 與其參加機構的 DR 設施，且業務單位在備援中心作業	備援中心	DR	DR	2 次 1-2 個工作天
3.	測試發生傳染病時之作業準備能力，需要較長時間	分散至主、備中心	Production /DR	Production /DR	1 次 至少連續 3 個工作天
4.	測試因火災、天災等事故致業務無法運作一段時間或是基礎設施故障	備援中心	DR	Production /DR	1 次 至少連續 5 個工作天
5.	由參加機構決定/有時由 PayNet 指定	由參加機構決定 (若演練係由 PayNet 指定則依其決定)	由參加機構決定(若演練係由 PayNet 指定則依其決定)	Production /DR	1 次

* DR 係指災害復原中心；Production 係指正式作業中心。

資料來源：SEACEN 課程講義及 PayNet(2016)

(2) 零售支付系統參加機構每年度應辦理 2 次業務持續運作或災害復原計畫（BCP/DRP）模擬演練，包括 IBG 使用端、MyDebit 主機及收單主機、FPX 閘道、Direct Debit 使用端、JomPAY 閘道。在復原目標時間內，必須從災害復原中心執行系統運作，若是未達到相關演練標準，需重新安排再次測試。（表 8）

表 8 零售支付系統參加機構年度應辦理之模擬演練

模擬情境		參加機構業務地點	參加機構資料中心地點*	PayNet 資料中心地點*	年度演練執行頻率及時間
1.	測試參加機構 DR 功能及連結至 PayNet 正式主機情形	主/備中心	DR	Production	1 次 至少 1 個工作天
2.	全市場測試 PayNet 與其參加機構的 DR 設施，且業務單位從備援中心作業	備援中心	DR	DR	2 次 1-2 個工作天
3.	測試發生傳染病時之作業準備能力	分散至主、備中心	Production /DR	Production /DR	1 次 至少連續 3 個工作天
4.	測試因火災、天災等事故致業務較長時間無法運作或是基礎設施故障	備援中心	DR	Production /DR	1 次 至少連續 5 個工作天
5.	由參加機構決定/有時由 PayNet 指定	由參加機構決定 (若演練係由 PayNet 指定則依其決定)	由參加機構決定(若演練係由 PayNet 指定則依其決定)	Production /DR	1 次

*DR 係指災害復原中心；Production 係指正式作業中心。

資料來源：SEACEN 課程講義及 PayNet(2016)

5、參加機構未遵循業務持續運作計畫標準之罰則

PayNet 可對其參加機構未確切遵循本項業務持續運作計畫標準，處以最高 5,000 馬幣或最高 10,000 馬幣罰鍰（表 9），演練結果未達本項規範訂定之最低標準者，參加機構需再次辦理測試演練，直至符合相關標準。

表 9 參加機構未遵循 PayNet 業務持續運作計畫標準之罰鍰

罰鍰標準	未遵循事項內容	罰鍰 /每一未遵循事項
「參加機構使用 PayNet 服務之業務持續運作標準」明訂事項(10.3)	參加機構執行年度業務持續運作計畫及災害復原計畫測試，未依本項規範要求，以備援中心及(或)災害復原中心成功執行相關演練測試事項，包括辦理次數、演練作業時間及執行情境等。	最高 10,000 馬幣
其他未於規範中明訂者	未在本項規範明訂之業務持續運作應遵循一般事項。	最高 5,000 馬幣

資料來源：PayNet(2016)

四、小結

網路威脅暨事故僅是金融基礎設施面臨眾多可能造成業務失序的原因之一，馬來西亞 PayNet 之業務持續運作計畫，係涵蓋網路攻擊、天然災害及資訊系統問題等事故原因，進行風險辨識與評估、制訂風險管理組織架構暨各部門職掌、配置適切風險管理資源、執行日常風險事件監控、緊急應變措施、災害復原作業。

為使相關人員在啟動業務持續運作計畫時能熟稔各項作業程序，俾在一定時間內掌控事故影響，定期執行業務持續運作計畫測試演練，並分別以正式環境及災害復原中心作業，檢討改進演練結果不足之處，是業務持續運作計畫在危機時能否發揮功效之關鍵。

伍、心得與建議

一、心得

(一) 國際駭客網路攻擊層面已由零售支付系統擴及至大額支付系統

國際駭客攻擊金融機構謀取不法利益，不再只是鎖定各種與消費者日常生活切身相關的零售支付，為盜取更龐大金額，目標轉向

清算銀行間交易之大額支付系統。大額支付系統參加機構之清算帳戶通常維持極高餘額，近年發生數起資金被盜事件，如孟加拉央行在美國聯邦準備銀行帳戶損失事件，以及墨西哥央行支付系統之參加銀行帳戶金額遭盜轉事件等，單次損失金額通常遠大於零售支付系統總遭駭損失，且因該等系統係由中央銀行營運，造成中央銀行之信譽受損，因此，大額支付系統資訊安全防護之重要性不言而喻。

(二) 馬來西亞支付體系已訂定全面性的風險治理架構，並落實業務持續運作計畫演練

PayNet 負責營運馬來西亞大額支付系統及數個具系統重要性零售支付系統，馬來西亞央行對 PayNet 具有實質控制權，PayNet 遵循 PFMI 國際準則風險治理規範，董事會為最高治理單位，並設置風險控管與業務管理委員會綜理風險控管事務，明訂風險管理 3 道防線暨各單位風險控管職掌，據以執行日常風險辨識、風險分級及管控措施等職責。PayNet 與馬來西亞央行均設置危機管理小組，負責業務持續運作事宜。為確保重大失序事件關鍵服務能快速恢復運作，PayNet 規劃重要支付系統年度演練計畫，並設定不同模擬情境、時程與辦理次數，期能使相關人員熟悉作業流程，於實際發生事故時，業務能持續運作發揮功效。

(三) PayNet 明訂參加機構應達到重要支付系統之業務持續運作標準

PayNet 考量其營運馬來西亞多個具系統重要性支付系統，且支付作業流程涉及支付生態體系全體成員，無法單獨運作，爰參加機構亦應具備重大失序事件之業務復原能力，PayNet 於 2016 年制定「參加機構使用 PayNet 服務之業務持續運作標準」，明確規

定參加機構就所參加系統服務，其業務持續運作計畫應達到的標準，並實施嚴謹的業務持續運作計畫及災害復原測試，包括大額支付系統參加機構每年度應辦理 6 次模擬演練，零售支付系統參加機構每年度應辦理 2 次模擬演練，並訂定未遵循 PayNet 業務持續運作計畫標準，最高可處以 5,000 馬幣或 10,000 馬幣罰鍰。

二、建議

(一) 本行宜建立大額支付系統風險事故資料庫，強化支付系統管理

參考馬來西亞 PayNet 風險管理措施，對於曾發生之作業風險事件，均由風險遵循人員簽報事故檢討報告，經主管核准後提送風險管理部門，檢視作業風險事故報告正確性，將事件予以建檔管理。本行於大額支付系統風險管理，亦逐次檢討並簽報事故檢討報告，建議可參考該國將歷次作業風險事故建檔管理之作法，以提供本行相關業務及資訊人員參考，強化管理支付系統相關作業。

(二) 為提升大額支付系統業務持續運作能力，本行宜加強規劃失序事件模擬情境並演練相關作業流程

目前本行大額支付系統年度實地演練，係著重於發生重大失序事件，以備援中心接續業務運作之可用性，建議參考馬來西亞大額支付系統 RENTAS 業務持續運作年度演練作業規劃，就已定義的失序事件等級，評估受影響機構範圍，再據以發展各等級模擬情境，完成問題辨識、危機管理小組決策、媒體聯繫、相關系統復原、人員調度、資料比對及恢復業務正常運作之全段作業，並涵蓋參加大額支付系統之金融機構。由於模擬演練作業涉及許多系統層面作業安排，且需業務單位協助規劃，爰本行資訊部門與

業務部門可共同規劃業務持續運作相關細部作業，強化大額支付系統業務持續運作能力。

(三) 本行宜制訂業務持續運作計畫最低標準，強化大額支付系統參加機構災害復原作業能力

業務持續運作計畫之有效性，係取決於演練作業是否落實，並為確保支付清算網絡中各節點資訊安全維護，應涵蓋整段支付清算作業之參加機構。建議參考馬來西亞央行大額支付系統業務持續運作計畫之相關規劃，大額支付系統每年度辦理不同情境之業務演練測試，並為強化支付系統使用端的參加機構業務持續運作能力，制訂參加機構應達成業務持續運作計畫之最低標準，包括風險辨識與評估、風險控管措施、作業復原安排、MTD 及 RTO 時間，以及模擬暨實地演練次數，相關演練結果應向本行彙報，以提升大額支付系統各參加機構之業務持續運作能力，確保重要金融支付基礎設施正常運作。

參考文獻

中文部分

1. 本次訓練課程講義(2018)。
2. 吳桂華(2015),「支付系統受到網路攻擊之復原方案暨金融市場基礎設施準則(PFMI)評估」，中央銀行出國報告，7 月。
3. 陳美惠(2018),「淺談 SWIFT 客戶安全強化措施」,財金資訊季刊，第 91 期，1 月。
4. 張逸綸(2018),「參加 SEACEN 支付及清算系統基礎訓練課程」，中央銀行出國報告，6 月。
5. 劉素珠(2017),「參加國際貨幣研究機構舉辦之中央銀行支付會議」出國報告，9 月。

英文部分

1. BIS (2012), “Principles for financial market infrastructures,” CPMI Report, No. 101, April.
2. BIS (2014), “Non-banks in retail payments,” CPMI Report, No. 118, September.
3. BIS (2014), “Cyber resilience in financial market infrastructures,” CPMI Report, No. 122, November.
4. BIS (2016), “Guidance on cyber resilience for financial market infrastructures,” CPMI Report, No. 146, June.
5. BIS (2016), “A glossary of terms used in payments and settlement systems,” October.
6. BIS (2016), “Fast payments - Enhancing the speed and availability of retail payments,” CPMI Report, No. 154, November.
7. BIS (2017), “Quarterly Review,” March.

8. Devnath, Arun(2016), “New York Fed had ‘major lapse’ in theft, Bangladesh Says , ” Bloomberg, March 22.
9. Financial Conduct Authority (2017), “Retail banking market investigation: Understanding customer views on current account service indicators,” Revealing Reality Research Report, July.
10. King, Rachail(2018), “Bank of Mexico admits $15.2 million went missing in cyber heist,” Central Banking, May 18.
11. Larano, Cris(2016), “Criminal complaints filed againt two in Bangladesh central bank heist,” Wall Street Joural, March 22.
12. PayNet (2016), “Guildlines on business continuity management for participants of MyClear’s services, ” Risk Management Department, MyClear, December.
13. UK Finance (2018), “2017 annual fraud update :Payment cards, remote banking , cheque and authorized push payment scams,” March.