出國報告（出國類別：其他）

SEACEN
第16屆支付清算系統高階訓練課程報告

服務機關：中央銀行
姓名職稱：林智慧 辦事員
派赴國家：馬來西亞
出國期間：106年5月21日至26日
報告日期：106 年 8 月 7 日

摘　　要

東南亞中央銀行研究及訓練中心（SEACEN Centre）舉辦之第 16 屆「支付及清算系統高階訓練課程，主題為「技術創新與強化支付系統面對網路犯罪之復原能力(Technological innovations and Strengthening Resilience of Payment System to Cybercrimes)」，期間自 106 年 5 月 22 日起至 5 月 25 日。

課程內容重點包括：

1. 新創科技對支付清算系統的威脅、挑戰與機會。
2. 網路威脅的型態與風險管理措施。
3. 資安議題討論與實務經驗分享。
4. 支付清算系統發展趨勢與行動支付。

資訊及通訊技術快速發展雖然有助於增強支付清算系統運作機制及效能，但網路犯罪者亦可能藉這些新技術開發更先進的攻擊工具，使金融機構受到網路威脅的風險增加。面對網路威脅若未謹慎因應，不僅是單一金融機構可能造成損失，對於整體金融穩定亦可能產生嚴重影響。因此對於各項新科技發展與應用需持續關注並瞭解其運作方式及潛在風險；而對於網路威脅更需持續強化資訊安全管理措施，確保業務持續運作，維持金融穩定。

本報告將針對新創科技的應用及支付清算系統因應網路攻擊之防禦措施概略介紹，主要內容包括：一、新創科技於支付系統的應用，二、CPMI 資訊安全指引，三、資安威脅類型與因應措施，四、各國業務持續運作措施，五、結論與建議。

目　　次

壹、前言

一、目的

為瞭解國際間支付清算系統對於新創科技衝擊及其可能衍生之網路犯罪攻擊因應之道，奉派參加由東南亞中央銀行研究及訓練中心（SEACEN Centre）舉辦的第 16 屆「支付及清算系統高階訓練課程(Advanced Course on Payment and Settlement Systems)」。

二、過程

課程主題為「技術創新與強化支付系統面對網路犯罪之復原能力(Technological innovations and Strengthening Resilience of Payment System to Cybercrimes)」，期間自 106 年 5 月 22 日起至 106 年 5 月 25 日。講師來自國際清算銀行(BIS)所轄支付暨市場基礎設施委員會(CPMI)[1]、SEACEN研訓中心、SWIFT、馬來西亞、菲律賓、泰國、印尼等不同國際組織及國家，另邀請Ripple公司說明其利用新技術提供金融交易解決方案之作法。參加學員來自我國、馬來西亞、新加坡等共 14 個國家。

課程內容重點包括：

1. 新創科技對支付清算系統的威脅、挑戰與機會。

2. 網路威脅的型態與風險管理措施。
   (1) 網路攻擊手段及造成的後果。
   (2) 各種網路防護措施的效果及盲點。
   (3) 金融市場基礎設施資訊安全指引及制定目的。
   (4) 透過個案研究熟悉上述安全指引分析方法。

1. 「支付暨清算系統委員會」(Committee on Payment and Settlement Systems, CPSS)自 2014 年 9 月 1 日起更名為「支付暨市場基礎設施委員會」(Committee on Payments and Market Infrastructures, CPMI)。

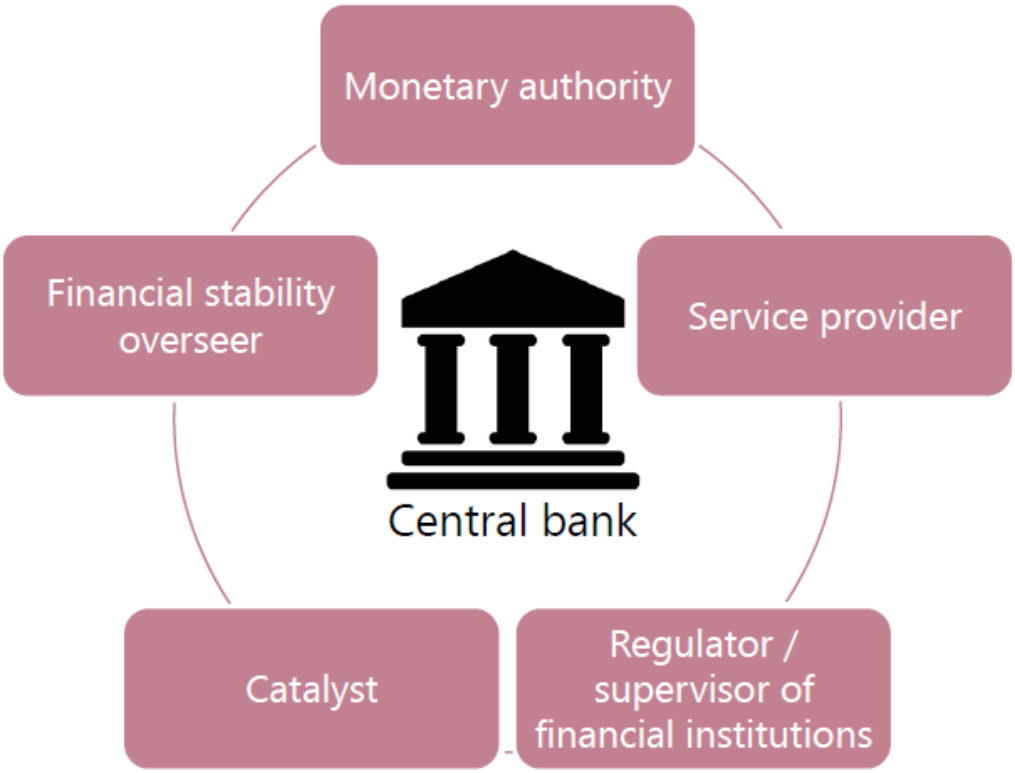
3. 資安議題討論與實務經驗分享。
   (1) 業務持續運作管理，包括備援中心建立、人力配置，及定期演練以驗證業務持續營運計畫有效性。
   (2) SWIFT 制定 Customer Security Programme，使用者端須採行雙因子認證機制。
   (3) 學員分享該國資安議題經驗。
4. 支付清算系統發展趨勢與行動支付。

貳、新創科技於支付系統之應用

資訊及通訊技術的進步，讓網路銀行、行動支付等各種金融服務及支付方式被廣泛應用。金融科技(Financial technology，FinTech)的興起更是由非金融機構創造出新的營運模式與產品提供金融服務，這樣的演變，已對現有的金融機構及監管單位產生影響。

支付系統的運作與金融體系穩定息息相關，維持金融穩定是中央銀行重要職責之一。中央銀行基於本身職掌及在金融市場扮演的各種角色(如圖 1)，對於維持支付系統的順利運作責無旁貸，同時對於各項新科技發展與應用亦須持續關注。

圖 1　中央銀行在金融市場所扮演的角色



資料來源：上課講義

由於使用者的需求加上資訊及通訊技術進步，支付系統發展重心已朝向提供快速及持續之快速支付服務(Fast payments，即時交易或接近即時交易並 7 天 24 小時運作[2])，與Fast payments系統相關之技術發展及相關議題皆引發注意，其中從比特幣(Bitcoin)衍生出來兩項重要議題：「分散式記帳技術(Distributed Ledger Technology，DLT)」及「數位貨幣(Digital Currencies)」更是目前金融科技的焦點。另由於行動支付(Mobile Payments)蓬勃發展，行動支付系統間互通性(Interoperability of Mobile Payments)亦是重要議題。

一、Fast payments 漸成零售支付系統發展重心

支付系統根據所處理之交易性質與金額大小，區分為大額支付(large-value payments)系統與零售支付(retail payments)系統。大額支付系統主要處理銀行間往來。目前各國大額支付系統多採行 RTGS(Real Time Gross Settlement)，以即時總額清算方式逐筆處理交易。大額支付系統主要發展時期為 1980 年代至 1990 年代，因發展時間甚早，已相當廣泛及成熟。

相較於大額支付系統，零售支付系統主要處理交易金額小、筆數多且不具急迫性的個人或企業之消費支付[3]。近年來，由於使用者需求及資通訊技術進步，零售支付系統已有大幅度的改變，發展重心逐漸朝向提供Fast payments服務。

國際間Fast payments系統發展於本世紀逐漸興起(如表 1)，根據國際清算銀行(BIS)的定義，Fast payments系統需符合快速及持續服務的要求。至 2003 年我國已陸續完成ATM(1987)、FEDI(1997)及

2. Fast payment is defined as a payment in which the transmission of the payment message and the availability of "final" funds to the payee occur in real time or near-real time on as near to a 24-hour and seven-day (24/7) basis as possible. See CPMI, Fast payments – Enhancing the speed and availability of retail payments, 2016.
3. Payments which are not included in the definition of large-value payments. Retail payments are mainly consumer payments of relatively low value and urgency. See CPSS, A glossary of terms used in payments and settlement systems, 2003.

FXML(2003)[4]等系統，提供快速及持續服務；2015 年通過實施「電子支付機構管理條例」(即第三方支付專法)，促進第三方支付市場發展；另外，金融機構或非銀行支付業者經主管機關金管會核准後亦可辦理行動支付服務。

表 1　國際間 Fast (retail) payments 現況

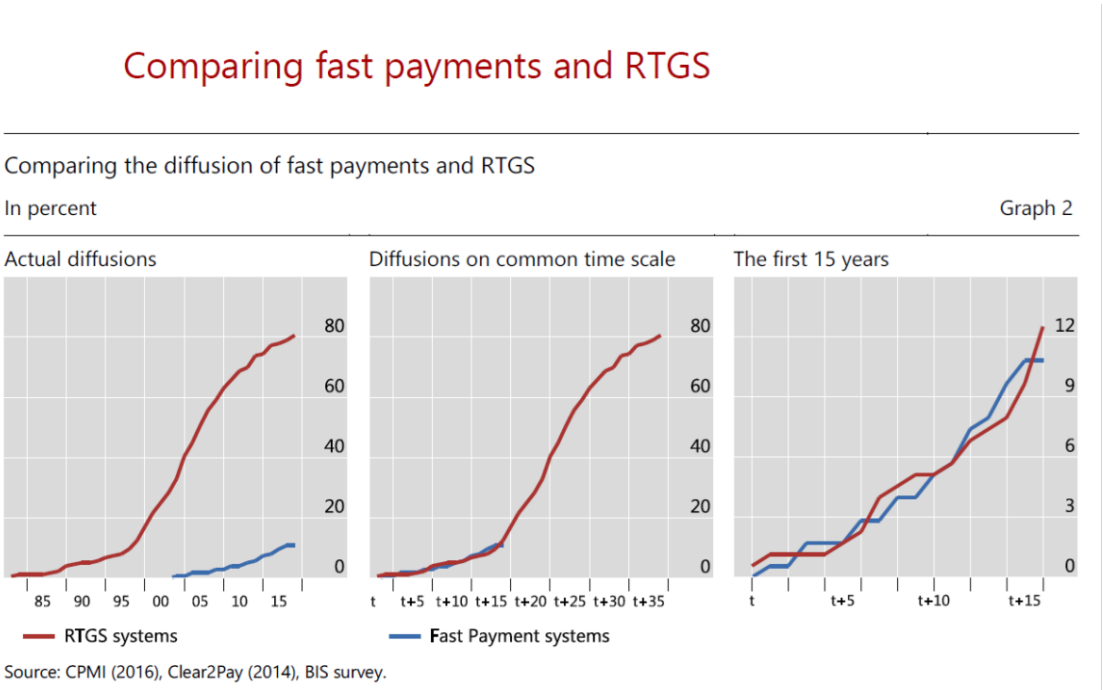
年	國家	系統名稱
2001	南韓	Electronic Banking System
2003	**中華民國**	**ATM, FEDI and FXML system**
	冰島	CBI Retail Netting System (JK)
2006	馬來西亞	Instant Transfer
	南非	Real-Time Clearing
2007	南韓	CD/ATM System
2008	智利	Transferencias en línea
	英國	Faster Payments Service
2010	中華人民共和國	Internet Banking Payment System
	印度	Immediate Payment Service
2011	哥斯大黎加	Transferencias de Fondos a Terceros del Sinpe
2012	厄瓜多	Pago Directo
	波蘭	Express ELIXIR
	瑞典	BiR/Swish
2013	土耳其	BKM Express
2014	丹麥	Nets Real-time 24x7
	義大利	Jiffy – Cash in a flash
	新加坡	Fast And Secure Transfer
2015	墨西哥	SPEI
	瑞士	Twint
2017P*	澳大利亞	New Payments Platform
2017/18P*	沙烏地阿拉伯	Future Ready ACH
2018P*	香港	To be determined
	日本	Zengin System
2019P*	匈牙利	Instant Payments
	荷蘭	Instant Payments

註：P*表示預計正式營運。
資料來源：BIS Quarterly Review, March 2017

4. 財金資訊股份有限公司公司紀事(https://www.fisc.com.tw/tc/profile/detail2.aspx)

本次課程講師針對大額支付系統與 Fast payments 系統發展過程的歷史資料進行比較，結果發現兩者初期發展趨勢相似度極高(如圖2)，並預期未來支付系統發展重心會轉為 Fast payments，進而如 RTGS 一樣蓬勃發展。

圖 2　Fast payments 與 RTGS 發展趨勢比較



資料來源：上課講義

二、分散式記帳技術

根據支付暨市場基礎設施委員會(Committee on Payments and Market Infrastructures，CPMI)的定義，分散式記帳技術(Distributed ledger technology，DLT)，係指讓網路(或協定)中的節點，對於已同步之帳本，能安全地處理及記錄狀態改變(或更新)，此類相關的程序和技術[5]。

5. DLT refers to the processes and related technologies that enable nodes in a network (or arrangement) to securely propose, validate and record state changes (or updates) to a synchronised ledger that is distributed across the network's nodes. See CPMI, DLT report. (http://www.bis.org/cpmi/publ/d157.pdf)

分散式記帳技術潛在優點包括：

1. 可進行點對點交易。

2. 可快速的處理過程，並確保紀錄不變性。

3. 可採用自動化程序減少人工介入。

4. 可降低處理成本。

5. 可強化復原能力，避免電腦單點失靈造成系統性風險。

6. 可透過網際網路提供跨境交易。

由於具有上述種種潛在優點，各方嘗試提出不同運作模式與應用，例如應用於簡化證券交易後交割制度(Post Trade Settlement)，應用於提供跨境支付(Cross-Border Payments)的快速支付服務(Fast payments)，或應用於支付系統。主要希望能提升交易效率，節省交易成本等。表 2 為目前 DLT 常見的運作模式與應用。

表 2　DLT 運作模式與應用

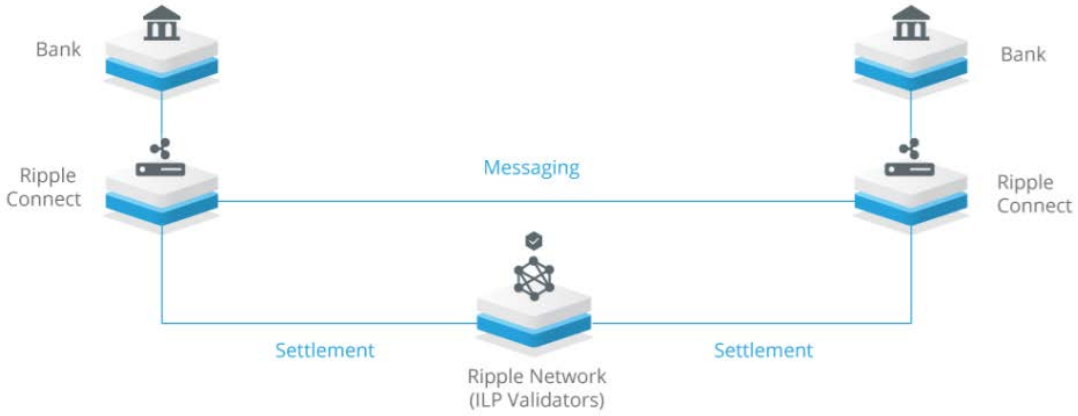
應用模式	**模式 1**	**模式 2**	**模式 3**
開放/封閉系統	開放系統	封閉系統	封閉系統
帳本數量	單一	單一	眾多
存取權限	非許可制	許可制	許可制
參與者	任何人	需核准	需核准
帳本紀錄維護方式	單一帳本，供所有人存取	單一帳本，所有參與者維護	參與者各自維護自身帳本
應用實例	比特幣	證券交易對帳	Ripple

資料來源：上課講義

來自 Ripple 的講師以汽車工業發展過程為例，闡述其對於 DLT 技術未來應用可能性的樂觀看法：汽車工業從福特 T 型車(Ford Model T)開始，經過不斷地改良演進，由非常陽春(以現代觀點而言)車款，發展到現今各式各樣專業化與功能化的車款，例如貨櫃車、休旅車、超級跑車等等。技術突破初期要將其套用至各種應用(one design for all use cases)當然不容易也不可行；但當技術成熟後，各式各樣產品與應用便會逐漸應運而生(designs specific to use cases)。

Ripple 的講師表示，該公司將「分散式記帳技術」應用於提供跨境支付(Cross-Border Payments)的 Fast Payments，並已在國外成功為商業銀行建立交易系統(如圖 3)。

圖 3　Ripple 運作示意圖



資料來源：https://ripple.com/technology/

不可諱言 DLT 雖具潛力，但有許多相關法規議題或風險問題待解決，普及化仍需要很長一段過程。

法規議題

1. DLT 相關系統或應用由誰負責管理維護，是否值得信賴。

2. 相關法規制度訂定與遵循，如何進行監管。

3. 現有商業環境是否可配合。

4. 隱私權議題考量。

風險考量

1. 資料隱私性：當帳務紀錄分散儲存在不同節點時，各交易者的交易隱私如何保護。

2. 網路資訊安全議題：可能面臨之網路風險類型及如何消弭、防止系統受到網路攻擊，資料遭洩漏、竄改或毀損。

3. 系統運作的復原力：如何避免單點失敗造成系統失靈，以及減少程式碼錯誤時產生的風險。

4. 對技術廠商管控與治理：金融機構是否具備足夠能力有效管理廠商。

三、數位貨幣

許多技術推崇者都相信在不久的未來現金(Cash)會消失不見，尤其比特幣的出現後，越來越多人相信數位貨幣將會取代實體貨幣，但實際情況比想像中更加複雜。

SEACEN 研訓中心的講師從經濟學者角度探討私人單位或中央銀行「數位貨幣」(Digital Currency，DC)的發行，對於金融監管、貨幣政策與經濟環境的影響。

貨幣具有交易媒介(medium of exchange)、記帳單位(unit of account)、價值儲存(store of value)等功能。現金本質上是難以追溯持有者身分、容易攜帶、可靠且被廣泛接受；而且當電力消失，或電子

系統的網路環境出狀況，現金仍然存在，不會無法使用。因此某些情況下現金還是最好的選擇，即使技術上有大幅進步，現金的部分特性仍是難以取代。

(一)電子化支付工具與數位貨幣不同

講師認為，雖然使用以現金為基礎之各項電子化支付工具(electronic means of payment)的民眾數量逐漸成長，而這樣的成長也確實推動許多中央銀行思考是否要發行「數位貨幣」(Digital Currency，DC)供民眾使用。但兩者趨勢是不可劃上等號，民眾減少使用現金支付並不代表其會增加使用數位貨幣。

將各種支付技術的發展和數位貨幣進行比較(如表 3)，可以看出電子化支付工具或支付技術創新與數位貨幣有其根本上的不同。部分支付技術創新其目的是讓付款過程更容易，藉以增加更廣泛的使用者(例如 Apple Pay)，但仍依靠一個值得信賴的中介(現有支付系統或法定貨幣)。數位貨幣則採用 DLT，屬於分散式結構，與現行採集中式架構的支付系統不同，並另發行新貨幣。

表 3　支付技術發展與數位貨幣比較

類別	說明	新支付系統	新貨幣
包裹支付[6]	提供包裹(wrapper)服務改善用戶介面和現有支付系統架構之介接。例如 Google 電子錢包，Apple Pay。	否	否
行動貨幣[7]	使用本國貨幣，並將其儲值在智慧卡或系統提供商帳戶以提供信用卡功能。如肯亞 M-PESA，透過行動電話提供金融服務，包括可付款給任何人。	是	否

6. Wrappers
7. Mobile Money

信用代幣[8]	藉由對新貨幣的信任作為儲存與交換媒介。例如私人企業公司利用現有的支付系統接受錢來換取替代單位並用於特定的平台或於特定地理位置使用。例如網路遊戲中的遊戲幣或遊樂場使用的代幣。或如英國布里斯托市本地所發行之布里斯托幣（Bristol Pound）。	否	是
數位貨幣[9]	新的分散式支付系統和新貨幣。例如比特幣	是	是

資料來源：上課講義、Bank of England Quarterly Bulletin 2014 Q3[10]

(二)由私部門發行需考量的議題與風險

數位貨幣依其發行機構可分為私部門發行(privately-issued digital currencies)與中央銀行發行(state- or central bank-issued digital currencies，CBDC)。需注意的是兩者可能共存，因此當多數民眾選擇使用私人發行的數位貨幣時，意味著私部門發行的數位貨幣可能取代流通的法定貨幣角色。換言之，即使是中央銀行發行的數位貨幣亦可能需與私部門發行的數位貨幣競爭。

開放私部門發行數位貨幣有以下主要議題需考量。

1. **貨幣供給量規則之制定及如何進行監管：**若突然大量發行，其幣值的穩定性將無法確保。
2. **使用者如何確保其債權：**雖然此類數位貨幣可作為支付工具並具備部分貨幣特徵，但本身無任何權力機構背書亦無內在值(zero intrinsic value)，唯有使用者相信其可藉以交換其他商品或服務或一定數量的主權貨幣

8. Credits and Local Currencies
9. Digital Currencies
10. http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q301.pdf

(sovereign currency)，方能獲得價值。

3. **發行者為非銀行機構：**數位貨幣通常採用分散式記帳技術，其為數位貨幣架構中真正創新的元素。而積極開發和營運數位貨幣和分散式記帳技術的第三方機構，幾乎都是非銀行。

歐洲銀行管理局（European Banking Authority，EBA）亦在2014年對於私部門發行的數位貨幣提出各種潛在風險[11]。

1. **使用者的風險：**持有的數位貨幣大幅貶值或發行機構停止營運、遭受駭客攻擊或竊取、用戶遭受欺詐交易行為造成的損失等。

2. **非個人市場參與者的風險：**雙重支付(double-spending，或稱一幣多付）的問題、數位貨幣發行機構無法達成支付義務等。

3. **金融誠信(Financial Integrity)的風險：**成為洗錢工具或恐怖主義者融資管道等。

4. **法定貨幣支付系統和支付服務提供商的風險：**當數位貨幣的重要性越來越高時，若其無法及時完成交易，對於支付清算系統將會有嚴重影響。

5. **監管單位的風險：**對於法規的訂定、監管方式是否能有效落實，如何管理發行機構的數量等，均是監管單位需考量的議題。

11. EBA Opinion on 'virtual currencies' (2014) https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

(三)由央行發行需考量的議題

由中央銀行發行的數位貨幣雖可減少前述私部門發行的問題與風險，但仍有其他議題需考量。

1. **對於支付系統監管：**如同對於傳統支付系統，數位貨幣相關支付系統一樣，須進行監管。
2. **對於金融市場基礎設施影響：**分散式分類帳技術和去集中化的機制會改變金融市場基礎設施彙總和淨值的計算方式，例如擔保抵押品、股票、債券及其他資產的登記方式可能不同。將會對大額支付系統，證券集中保管機構，證券結算系統產生影響。
3. **對於金融中介機構影響：**央行發行的數位貨幣如果被廣泛使用，可能會挑戰現行金融體系銀行的中介作用。銀行是存款人與貸款人之間的金融中介機構，如果央行發行數位貨幣的使用者變得普遍，因持有者係直接面對央行，可能會對現有儲蓄或取得貸款的機制產生影響。

(四)其他潛在利益與議題

潛在利益

1. 降低交易成本。
2. 單位的高可分割性。
3. 縮短交易處理時間。
4. 收到付款的確定性。
5. 個人取得金融普惠(Financial Inclusion)的另一種方式。

潛在議題

1. 發行單位要如何確保帳戶或交易資料的安全，不被破壞、竊取或是受到駭客的攻擊。
2. 數位貨幣持有者交易隱私權的保障。
3. 外國人是否允許持有本國數位貨幣及其管理方式。
4. 電力與網路等基礎建設異常或失能時之應變機制。

四、行動支付間互通性

由於行動支付(Mobile Payments)的蓬勃發展，本次課程來自印度儲備銀行(Reserve Bank of India)及印尼銀行(Bank Indonesia)講師分享其國家推動行動支付系統間互通性(Interoperability[12] of Mobile Payments)之主要目的及措施。

(一)印度

主要目的

1. 為增強行動支付的網路效應(Network Effect)[13]。用戶數越多，每一位用戶能獲得越高的使用價值。
2. 支持將行動支付納入支付途徑。
3. 促進行動支付規模經濟。
4. 提高支付工具的實用性及強化用戶便利性。

12. a situation in which payment instruments belonging to a given scheme may be used in other countries and in systems installed by other schemes. See CPSS, A glossary of terms used in payments and settlement systems, 2003.
13. 又稱網路外部性（network externality），或需求方規模經濟（demand-side economies of scale），指在經濟學或商業中，消費者選用某項商品或服務，其所獲得的效用與「使用該商品或服務的其他用戶人數」具有相關性時，此商品或服務即被稱為具有網路外部性。例如電話或社群網路服務：用戶人數越多，每一位用戶獲得越高的使用價值。(節錄維基百科，網路外部性)

5. 讓資源有效分配，減少重複投資。

主要措施

1. Immediate Payment Service (IMPS)：建立一種快速支付系統，並提供網路銀行，行動銀行，各銀行之分行，ATM 等多管道服務。
2. *99# National Unified USSD[14] Platform (NUUP)：建立國家級的USSD平台，使用者透過手機輸入特定USSD指令即可取得金融服務。
3. Unified Payment Interface (UPI)：當交易雙方分屬不同行動支付服務提供者時，可透過此共通介面進行交易。
4. Bharat QR code：由印度國家支付公司(National Payments Corporation of India，NPCI)，萬事達卡(Mastercard)及 Visa 共同開發 APP，使用 QR code 系統來進行支付。

(二)印尼

主要目的係提供使用者在不同行動支付系統(mobile money schemes)之間或行動支付系統與銀行之間，能進行帳戶與帳戶間轉帳(account-to-account transfers)。

主要措施

1. 建立交易各階段互通性
   (1) 交易平台(Platforms)：銀行單位、非銀行單位、電信公司之間。

14. Unstructured Supplementary Service Data，非結構化補充資料服務技術；GSM 系統所使用的一種通訊協定，消費者透過手機輸入特定 USSD 指令之後，可以取得系統服務商提供的服務。

(2) 現金進出點(Point of cash out/in)：不同服務提供者在各服務使用點均可使用。(以我國為例，不同服務提供者如悠遊卡、一卡通，皆可在捷運、便利商店等不同服務使用點使用。)

(3) 終端使用者(End-users)：使用者可進行各類型的交易，諸如個人對個人(P2P)、個人對帳戶(P2A)、個人對企業(P2B)、帳戶對個人(A2P)。

2. 制定各類標準

(1) 技術標準：設備軟硬體、訊息格式(如 ISO 12812) 、身分驗證標準(PIN 驗證、雙因子驗證)。

(2) 企業運作標準：業務流程、契約規範、賠償措施。

(3) 支付清算運作模式建立。

(4) 消費者保護措施：客戶保護與爭議解決。

(5) 法規制定與監管措施。

參、CPMI 資訊安全指引

CPMI (Committee on Payments and Market Infrastructures)支付暨市場基礎設施委員會為國際清算銀行(BIS)轄下之委員會，其目的為制定支付、清算和相關協議(arrangements)的全球標準，促進安全和效率，以支持金融穩定和經濟發展。CPMI 會監督和分析這些協議的發展情況，包括內部和跨司法管轄區。它也是各國中央銀行合作相關監督，政策和業務事宜的論壇，並提供中央銀行服務。

一、Guidance on Cyber Resilience for FMIs

CPSS[15]於 2012 年發布「金融市場基礎設施準則(Principles for Financial Market Infrastructures，PFMIs)」及「金融市場基礎設施準則之揭露架構及評估方法」，該準則為對金融市場基礎設施的全面性評估，包括法規基礎、治理機制、全面性風險管理架構、信用風險、作業風險等原則，藉以發現可能存在的風險或管理缺失，以及可改善事項，確保金融市場穩定。

由於網路風險(Cyber risk)與傳統作業風險(Traditional operational risk)有許多方面不同(表 4)，有其特殊性，故 CPMI 針對網路風險於 2016 年 6 月發布「金融市場基礎設施資訊安全指引(Guidance on Cyber Resilience for FMIs)」。

現今金融市場，金融交易從開始到最終清算，整個交易生命週期中各項事件和聯繫順序涉及多個實體(entity)，構成複雜的交易鏈(Transaction Chain)。由於金融市場基礎設施(FMI)、服務提供商和參與者之間多方交互影響，面對資安事件時，恢復時間成為重要關鍵。同時，在彼此相互依存下，FMI 不應該將其網路復原能力作為競爭工

15. 「支付暨清算系統委員會」(Committee on Payment and Settlement Systems, CPSS)自 2014 年 9 月 1 日起更名為「支付暨市場基礎設施委員會」(Committee on Payments and Market Infrastructures, CPMI)。

具，也無法藉以獨善其身。

表 4　傳統作業風險與網路風險比較		
風險類型	**傳統作業風險**	**網路風險**
風險特性	多以特殊情境為主進行評估，例如天然災害等	持續演進、變化
風險範圍	辨識複雜度較低	範圍廣泛 可能入侵點較多元
復原機制	營運持續計畫有效性高	復原過程較難明確及標準化
損失估計	潛在損失較能根據風險預測進行估計	網路攻擊造成的可能損失難以估計(資料洩漏、商譽損失)

資料來源：上課講義

(一)風險管理面向

CPMI 所制定之資安指引分為 3 個面向(Dimention)：範圍(Scope)、治理(Governance)、措施類別(Range of measures)，說明如下：

1. 範圍(Scope)
   (1) 機密性(Confidentiality)：避免資料遭竊取的風險。
   (2) 可用性(Availability)：資料保存及關鍵系統持續運作。
   (3) 完整性(Integrity)：避免資料遭竄改或毀損、確保關鍵系統運作可信度。
2. 治理(Governance)
   (1) 人員(People)：管理階層對於資安政策執行的支持、組織對於資安認知及內部文化的建立、對於內部員工提供完善的教育訓練、對於外部協力廠商進行規範並要

求其遵守資安規定及程序。

(2) 程序(Processes)：對外服務的作業流程及內部作業流程控管、權責劃分與規範。

(3) 技術(Technology)：資訊部門需對於資安相關科技有效的掌握，善用技術與工具協助，強化組織的資訊安全與復原能力。組織需提供充足的資源，進行必要的設備建置與設備更新、持續修補系統與平台的資安弱點。

(4) 溝通(Communication)：各部門或利害關係人之間資訊的分享，聯絡管道。

3. 措施類別(Range of measures)

(1) 預防(Prevention)：瞭解可能風險進行防範及保護措施。

(2) 檢測(Detection)：監測異常行為或事件進行即時管理。

(3) 回復(Recovery)：建立資料備份、備援系統等復原措施。

(二)資安指引框架

CPMI 針對資安議題所提出的「金融市場基礎設施資訊安全指引(Guidance on cyber resilience for financial market infrastructures)」，其框架要素(圖 4)由內而外分別為治理、辨識、預防、偵測、回復、測試、狀況認知、學習與進化。

其框架是個動態過程，包括風險辨識與管理、業務持續營運計畫制定、各種情境模擬、演練測試確認相關步驟及計畫有效性、對於各種可能資安狀況認知及技術資料收集、進行資訊分享與跨單位合作、人員教育訓練與作業方式改進等。隨著科技的發展與各種資訊系統及網路環境的改變，必須不斷主動發現潛在問

題加以因應，以達到持續改善的目標。

圖 4　Cyber Guidance components

資料來源：Guidance on Cyber Resilience for FMIs

二、清算最終性與業務持續運作

清算最終性(settlement finality)[16]係指款項或證券之移轉已不可撤銷且無附帶條件，致債務為確定性之消滅，亦即完成款項的收付及券項的交割。為達成清算最終性，CPMI針對金融市場基礎設施(FMIs)，面對資安事件時，復原時間以兩小時目標 (2-hour RTO)。而這是CPMI金融市場基礎設施準則(PFMIs)少數如此明確的要求。

(一)相關金融市場基礎設施準則

16. the discharge of an obligation by a transfer of funds and a transfer of securities that have become irrevocable and unconditional. See CPSS, A glossary of terms used in payments and settlement systems, 2003.

PFMI 原則 8：

FMI 至少應在交割日日終提供清楚、明確的最終清算，並應於必要時或最好能提供日間或即時之最終清算。

PFMI 原則 17：

FMI 應通過使用適當的系統、政策、程序和控制來確定內部和外部操作風險的合理來源，並減輕其影響。系統應設計為確保高度的安全性和運行可靠性，並應具有足夠的可擴展能力。業務持續運作管理主要目的應為及時恢復營運和履行 FMI 的義務，包括在發生大規模或重大破壞的情況下。

PFMI 原則 17，主要考量 6：

業務持續運作計畫應設計為確保關鍵資訊技術（IT）系統可以在破壞性事件後的**兩個小時內恢復運行**。此外，該計畫目的應該是使 FMI 即使在極端情況下能夠在破壞性事件發生日結束時，完成清算。

PFMI 原則 17，解釋說明 3.17.13：

業務持續運作計畫應該明確規定目標，並應包括政策和程序，允許在服務中斷之後迅速恢復和及時恢復關鍵業務，包括在發生大規模或重大干擾的情況下。

(二)2 小時目標復原時間

2-hour RTO 的主要原因是要達成事件發生日結束前清算最終性。講師提醒以下幾個重點需注意：

(1) 當檢測到服務中斷或異常時即應開始計時。成功的網路攻擊或攻擊嘗試，不一定會顯示出服務中斷的特徵。

(2) 須安全地進行回復關鍵作業，並確保決定回復時不會升高風險。

(3) 須能在中斷發生日結束前完整結算。

(4) 即使在極端但似乎合理的情況下，2h-RTO 也適用。

(5) 應擬訂計畫及進行測試，並考量不能實現 2h-RTO 的場景及因應之道。

一般常見的備援措施係建立主中心與備援中心，當主中心無法運作時，切換至備援中心繼續提供服務。然而複雜的網路攻擊可能會使這樣的備援機制失敗，使 2h-RTO 難以達成。原因在於主中心與備援中心多半會採相同軟硬體環境配置，而網路攻擊發生時主中心與備援中心均可能遭受相同的攻擊；若主中心遭到入侵成功，造成系統或資料完整性異常，此時備援中心亦可能因相同問題或漏洞遭受入侵而無法提供服務。因此須對於駭客入侵事件研擬各種情境之應變計畫、進行演練及修正既有備援程序。

肆、資訊安全防禦措施

資訊科技的普及，諸如智慧型手機、行動裝置、社群媒體、雲端服務等為人們帶來許多便利性。但從資訊安全的角度而言，卻也增加許多威脅與挑戰，而這些威脅與挑戰亦可能對支付系統的穩定造成嚴重影響，使其不斷面對外部的衝擊與內部的壓力。

外部衝擊：

1. 網路威脅倍增及防禦邊界不易建立：駭客攻擊的方式與管道越來越多元。
2. 網路犯罪的攻擊力增加：駭客攻擊手法更專業化及組織化，甚至有國家級的力量介入。

內部壓力：

1. 靈活性：面對資安事件時是否能及時因應。
2. 預算：防禦裝置的購置、舊設備或作業系統的更新是否有足夠的預算。
3. 技能：專業知識是否足夠，對於攻擊手法與防禦措施是否能迅速掌握。

一、攻擊類型及防禦措施

馬來西亞的講師對目前主要網路攻擊類型、攻擊方式、產生影響及後果，可採行的防禦措施及其限制與盲點進行說明。摘要整理如後。

(一)網路釣魚 (Phishing Attacks)

網際網路犯罪者冒充成某組織或企業，發送與使用者個人相關訊息進行欺騙。網路釣魚電子郵件通常冒充成一個已存在或合法的企業或組織騙取帳號密碼。釣魚郵件亦是惡意軟體攻擊的主

要途徑。惡意軟體通常透過惡意電子郵件附件或具有嵌入式惡意連結的電子郵件進行攻擊。

網路釣魚電子郵件有幾個常見特徵：

1. 出現並不想知道或並不想尋找的訊息內容。
2. 郵件內容要求提供個人資料或信用訊息，內容有時出現語法和拼寫錯誤。
3. 透過電子郵件將使用者引導到外部連結。

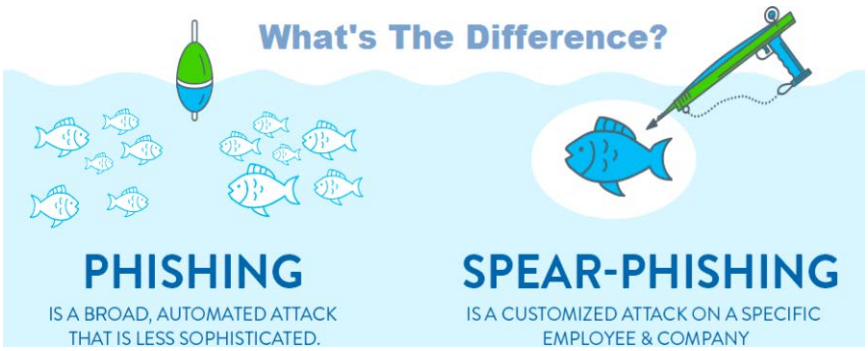
主要防禦措施：

1. 使用者資安認知訓練。
2. 刪除不必要的管理員權限。
3. 修補作業系統和應用軟體。
4. 個人電腦端點(End-points)防護措施。
5. 電子郵件過濾及安裝防護軟體。

(二)魚叉式網路釣魚攻擊 (Spear-phishing Attacks)

相較於前述網路釣魚攻擊方式，魚叉式網路釣魚攻擊更具針對性(圖 5)。此類攻擊會依據目標對象屬性進行調整策略，因此更難以預防，須隨時留意。攻擊過程需利用高度的駭客技能，並且通常難以偵測，是網路安全漏洞最常使用的切入點之一。

圖 5　網路釣魚 vs 魚叉式網路釣魚

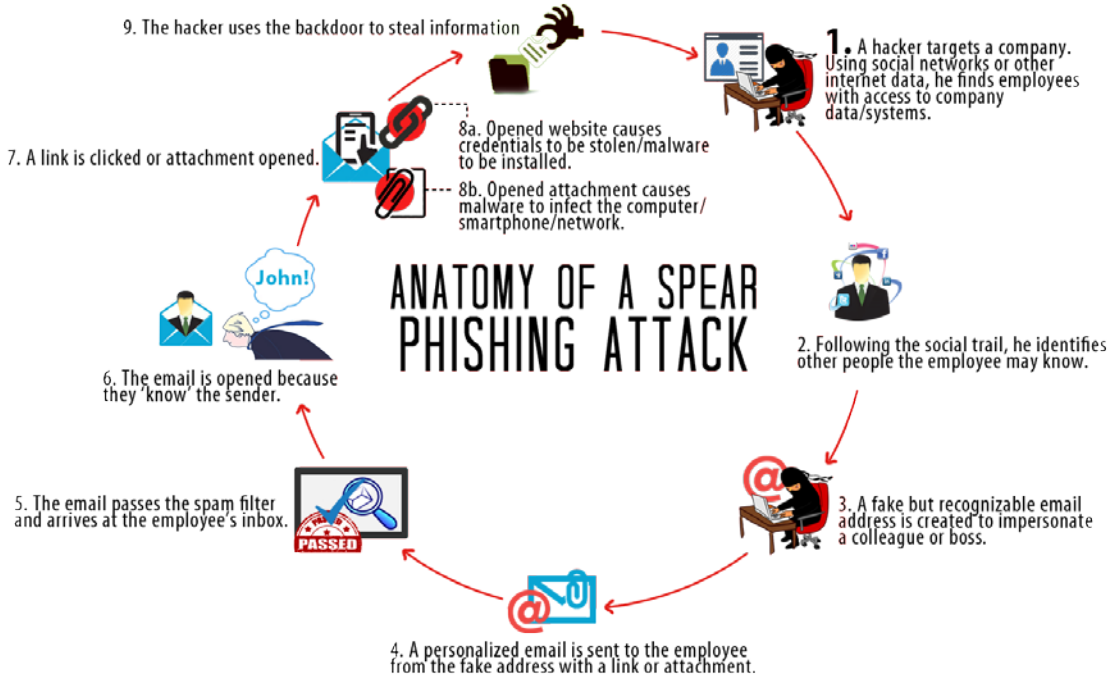


資料來源：上課講義、http://blog.nasafcu.com/wp-content/uploads/2016/11/phishing.png

有心人士會鎖定特定個人及其社群媒體帳號 (如 Facebook、Twitter 等)，偽裝成已知的或可信的寄件者，或是針對公司內的決策者，偽裝成為值得信賴的同事、朋友或合作廠商人員，精心製作出內容可性度極高的電子郵件，在電子郵件當中挾帶惡意附件檔案和連結，並且設法躲過郵件過濾系統的攔截進到目標使用者的電子信箱。

一旦目標使用者開啟檔案或連結，就會執行惡意程式或將使用者導向某個網站，以達成駭客目的。其結果可能造成機敏訊息外洩，或於使用者電腦植入木馬程式讓駭客建立祕密通訊網路，以進行下一階段攻擊。

圖 6　魚叉式網路釣魚攻擊過程示意圖



資料來源：上課講義、

http://www.astraid.com/wp-content/uploads/2014/10/infographic_hacker_update-gp-trans.png

由圖 6 可瞭解到這是一系列有計畫的攻擊過程。如此大費周章，其目的通常是為了取得高度機敏的資料或是龐大的利益。

而這類針對性且精心設計過的魚叉式釣魚郵件，使用者需要經過通盤教育訓練，才能有效地識別及避免觸發。使用者本身須維持警覺性及良好使用習慣，諸如公務上的電子信箱應避免使用於私人用途或任意流出，注意在社群媒體上個資的揭露情況等。

主要防禦措施與因應網路釣魚攻擊相同，惟對於使用者應提供全面性的資安認知訓練。

(三)網路探測 (Network-probes)

有心人士透過網路監控軟體，進行探測行為，例如 Port Scans 與 SYN Scans 等，再即時分析網路流量及其傳輸協定，試圖尋找網路系統中可能的入侵點，並利用系統中已知或可能的弱點嘗試進行存取電腦及其檔案。

當出現相關事件紀錄，資安人員應進行證據分析，並就後續如何因應作出決策，同時設置入侵檢測裝置並繼續監控活動。瞭解或聯繫此行為來源以確認其意圖，防止相關行為再次發生。

(四)暴力破解 (Brute-force Cracking)

透過應用軟體不斷地嘗試錯誤(trial and error)進行密碼猜測或進行資料解密。常見的暴力破解係利用密碼字典不斷進行猜測，直到得到正確的密碼。

而一般人為了方便記憶，容易會在不同系統使用相同一組帳號密碼，因此某一系統之帳號密碼一旦被猜測成功，可能也意味著其他系統帳號密碼亦將形同虛設。

主要防禦措施：

1. 增加使用者密碼的長度與複雜度，提高破解難度。
2. 在系統中限制密碼錯誤的次數。
3. 當同一來源的密碼輸入錯誤超過一定次數，立即示警以通知系統管理員。
4. 系統設置「驗證碼」功能(Completely Automated Public Turing test to tell Computers and Humans Apart，CAPTCHA)，避免有心人士利用程式進行破解。
5. 使用者對於不同系統應使用不同帳號密碼。

(五)偷渡式下載 (Drive-by Download)

在使用者不知情的狀況下，自動下載程式到個人電腦的攻擊方式。一般又稱為網頁掛馬、隱藏式下載或強迫下載。其手段係利用使用者電腦系統、應用程式和瀏覽器的漏洞，植入惡意程式例如木馬程式或勒索軟體。即使只是瀏覽網站(如同開車路過)，但網頁上如被植入惡意廣告(Malvertising)，也可能在不知不覺中被迫下載惡意程式，因此亦被稱為路過式下載。

主要防禦措施：

1. 作業系統、應用程式和瀏覽器及外掛程式等軟體或應保持最新。
2. 安裝防病毒軟體及網頁過濾軟體並保持更新。
3. 刪除不必要的管理員權限，在 PDF 檔中禁用 JavaScript 等安全設定。
4. 刪除不必要的管理員權限。

(六)勒索軟體(Ransomware)

是一種惡意軟體，將受害者電腦硬碟上的檔案進行系統性加

密，並要求受害者須繳納贖金（比特幣），方能對檔案解密取回資料。因駭客可透過此方式取的經濟利益，故勒索軟體越來越廣泛。甚至出現「勒索軟體即服務（Ransomware as a service）」，使得有更多的網路犯罪分子可取得自己的勒索軟體。

主要防禦措施：

1. 全面性的使用者資安認知訓練
2. 刪除不必要的管理員權限。
3. 個人電腦端點(End-points)防護措施。
4. 電子郵件過濾及安裝防護軟體。
5. 作業系統、應用程式和瀏覽器及外掛程式等軟體或應保持最新。
6. 定期進行資料備份,安全的資料備份是最佳防禦方式。

(七)分散式阻斷服務攻擊 (Distributed Denial of Services, DDoS)

「阻斷服務」係指駭客使攻擊目標的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常用戶無法存取。「分散式阻斷服務」則是駭客使用網路上兩個或以上的電腦向目標發動「阻斷服務」式攻擊。攻擊方式可分成頻寬消耗型以及資源消耗型。兩種形式都是透過大量合法或偽造的請求，占用大量網路及設備資源，藉以癱瘓網路與系統。

值得留意的是,DDoS攻擊往往會透過許多殭屍電腦[17]組成的殭屍網路(Botnet)發動。而隨著物聯網(IOT)裝置的普及，這類設備逐漸成為駭客攻擊及利用的對象。面對這樣的發展，相關單位及資安人員宜密切關注加以因應。

17. 受害電腦被植入可遠端操控該電腦的惡意程式，像殭屍(傀儡)一般任人擺佈執行各種惡意行為。(什麼是「Botnet 傀儡殭屍網路」？https://blog.trendmicro.com.tw/?p=106)

主要防禦措施：

1. 設定路由器、防火牆規則，針對特定 IP 與通訊埠加以阻絕，但無法抵抗複雜的攻擊方式。
2. 安裝入侵檢測系統。
3. 安裝 DDoS 緩解設備。

(八)進階持續性攻擊(Advanced Persistent Threat Attack, APT)

讓未經授權的人員可以持續存取網路並長時間不被檢測到。攻擊的策略是保持對網路的隱密及持續存取，讓駭客藉以持續收集系統資訊或機敏資料，而非關閉網路服務。由於 APT 攻擊相當複雜，需要多種技術加以因應。

主要防禦措施：

1. 需要具體的安全設定，全天候的監控和事件通報。
2. 關鍵系統應進行網路隔離，建置入侵檢測系統和應用軟體白名單功能。
3. 系統弱點掃描及修補管理。

二、支付系統資安措施

(一)實體防護

實體防護包含獨立區域、門禁管制、監視器等設施，以降低機房遭實體侵入的可能性。

(二)資訊系統縱深防禦

採取多層次防禦措施(如防火牆、入侵防護系統等)，以降低網路攻擊成功的可能性。支付系統與網際網路應進行有效隔離。

(三)備援機制

應建立備援中心，以確保主中心無法運作時，可切換至備援

中心繼續運作；並應定期進行演練，確保可用性。

(四)管理措施

1. 支付系統參加單位應經支付系統營運主管單位許可。

2. 協力廠商須符合資安規範。

3. 對人工作業程序應有適當內控。

4. 使用者電腦端點資安防護機制落實。

(五)資安事件回應

1. 資安事件原因辨識。

2. 相關數位資料證據收集及協助調查。

伍、各國業務持續運作措施及經驗

本次課程菲律賓中央銀行(Bangko Sentral ng Pilipinas，BSP)及馬來西亞中央銀行(Bank Negara Malaysia，BNM)講師分享其國家對於業務持續運作所採行措施及經驗。

一、菲律賓中央銀行(BSP)

(一)對 BSP 內部運作

1. 設立業務持續運作辦公室(Business Continuity Office，BCO)，作為 BSP 業務持續運作管理之技術顧問。

   (1) 確保適當的因應單位立即採取行動，並在需要時順利實施現有計畫和程序。

   (2) 提出適用於 BSP 各部門、區域辦事處和分支機構的業務持續運作管理政策、程序、指導方針和標準。

   (3) 透過 BCO 要求所有 BSP 部門、辦公室、區域辦事處和分支機構訂定其業務持續運作計畫。包含明確的目標、政策和程序、明確的系統恢復時間和恢復點。在大規模或重大服務中斷的情況下，能快速及時恢復關鍵業務。

2. 建立備援中心，並具有足夠的資源，能力和功能適當的人員配置，使其能夠於主中心受災害影響時立即接管運作。

3. 要求所有與業務持續運作計畫相關單位進行定期檢查及測試，以確保所有軟硬體，線路與通信設備有效地運作。

4. 要求所有參加單位、關鍵服務提供商和相關的 FMI 參與定期測試。

5. 對員工教育訓練，確認能執行業務持續運作計畫。

(二)對外部金融機構的監督

1. 執行各種通告(Circular)之 BSP 政策和指令。例如通告 808 (BSP Circular 808)，即被稱為所有銀行和其他 BSP 所監管機構的資訊技術風險管理指南，用以確保系統可用性，可靠性和可恢復性。

2. 對銀行和金融機構、支付系統提供商和運營商以及其他 FMI 進行定期監督，確保遵守現有 BSP 關於業務持續運作管理和技術風險管理的政策。

(三)溝通和危機管理策略

1. BSP 部門、辦公室和區域辦事處和分支機構的業務持續運作管理和業務持續運作計畫包括溝通計畫(Communication Plan)，內容為內部和外部溝通的強制性指示、建議、流程或指導原則。

2. **中斷期間的外部溝通是關鍵的業務流程。**BSP 業務持續運作管理團隊（BCMT），經由「危機長（Chief Crisis Officer，CCO）」決定，當發生機構或業務單位特定中斷事件的情況下，所需傳達給新聞界和 BSP 人員的訊息。

3. 透過已核准的頻道/媒體/工具/技術所發布的公告，應與現有的溝通計畫保持一致，尤其是對公眾。

二、馬來西亞中央銀行(BNM)

(一)設定期望目標

該國的RTGS系統RENTAS(Real-time Electronic Transfer of Funds and Securities System)的運作是委外給MyClear[18]。

1. BNM 設定監管期望、與 MyClear 之間服務水準協議(Service Level Agreement，SLA）。

   (1) 建立適當控制措施，確保可靠、效率及運作平穩，RENTAS 的系統正常運行時間不得低於 99.9%。

   (2) 實施全面有效的業務持續運作計畫，確保事故發生時及時恢復。

   (3) 提交報告和統計數據。

2. BNM 訂定業務持續運作管理指引。概述並執行對金融機構的最低 BCM 要求，確保其在發生嚴重干擾時，於特定時間內關鍵業務功能和基本業務可恢復運作。

3. MyClear 訂定其參與者之業務持續運作管理指引。

   (1) 要求第三方服務提供商參與。

   (2) 確保最大可容忍停機時間(MTD)為 2 小時，恢復時間目標(RTO)為 1 小時。

   (3) 進行業務持續運作計畫和災難復原計畫演練。

(二)有效監督是確保有效 BCP 的關鍵

BNM 對於受監督的對象進行下列檢查措施：

1. 檢視業務持續運作管理要求的規則和操作程序。

2. 檢視年度業務持續運作計畫，例如演練情境，測試次數等。

3. 檢視和評估實際運行和測試結果。

18. Malaysian Electronic Clearing Corporation Sdn Bhd (MyClear)。

4. 瞭解涉及 RENTAS BCP 的事件。

5. 評估參與者遵守運營商發布的規則和指引之情況。

6. 現場檢查項目應包含 BCP 手冊與 SOP 文件。

(三)業務持續運作管理之挑戰與改進方式

BNM 講師亦整理出目前在業務持續運作管理所面對的挑戰及可能改進方式，供學員參考。

1. PFMI 對於 2-hour RTO 要求，特別在網路攻擊的情況下。
   (1) 確定問題來源並確保恢復準確資料的過程可能會消耗時間。
   (2) 設計有效的恢復解決方案。採用於備份解決方案的不同技術、每小時資料備份（使用不同媒體）。

2. 如何在最壞的情況(主中心與備援皆停止運作)實現交易。
   (1) 考慮設立第 3 中心。
   (2) 採人工作業等。

3. 確保高強度的準備，例如「突發性」的業務持續運作測試。
   (1) 注意理想的成果與實際高操作風險的落差。
   (2) 模擬實際情景。

4. 確保有效的溝通和升級流程，以利及時啟用 BCP。
   (1) 延遲啟用 BCP，以改正問題。
   (2) 指定啟用 BCP 的時間，例如系統故障後 45 分鐘內。

5. 當多個參與者採用同一廠商提供災難恢復服務時，有風險集中的情況。
   (1) 定期審查並通知參與者可能的風險。

陸、結論與建議

一、結論

(一)資訊安全是必要投資

資訊科技及各類金融服務與應用不斷地創新發展，網路銀行或行動支付提供人們更多的便利性，但駭客攻擊管道與方式也因此變得更多元且複雜。資訊安全議題已成為風險管理的重要課題，需要投入更多資源(例如資安設備建置、軟硬體升級或更新)及人力配置加以因應，並應將其視為必要的投資。

(二)強化使用者認知與資訊分享

各國講師與學員們在分享資安議題的處理經驗時，均不約而同地談到「使用者對於資訊安全議題認知」以及「資安事件資訊分享」的重要性。課程中亦不斷強調，資訊安全不再只是單純 ICT 的問題(資訊與通信科技，Information and Communication Technology，ICT)，面對資訊安全，每個人都有責任而非僅限於資訊單位，使用者本身應加強資安意識，而各單位間甚至跨國間都應相互合作與分享訊息。

(三)瞭解新創技術有助風險管理

隨著資訊科技的進步，以及使用者對於交易的即時性需求增加，未來必然不斷地會有新的金融服務與應用。必須把瞭解新創技術如何應用在支付清算系統及其影響，納為風險管理的一環，越早瞭解越有助於風險評估與掌控。

二、建議

(一) 導入安全軟體發展生命週期

傳統資訊系統發展流程多為功能開發導向，以最短時間完成系統開發及上線為目標，較少從安全性的角度進行考量。然而不安全的程式碼，往往是網路安全漏洞的來源，被駭客或有心人士用以竊取資料或癱瘓系統運作。這類資安問題卻不易透過防火牆或入侵偵測等外部安全機制解決。

因此資訊系統開發階段即應考量資安風險管理，降低後續系統維護成本，及遭受攻擊的營運損失。導入安全軟體發展生命週期(Secure Software Development Life Cycle)，對於專案的需求、設計、開發、測試、佈署維運各階段進行資訊安全確認。

對於系統開發專案中各成員，包括程式開發人員、系統規劃人員進行相關資安教育訓練；對於委外廠商訂定相關規範等。

(二) 設置專職資訊安全人員與團隊

網路威脅已變得專業分工化及組織化，其中許多專業知識與技能，一般資訊人員並不一定具備。因此面對資安攻擊方式不斷進化，須有專職資訊安全人員與團隊對於資安應對策略進行調整與執行。

1. 負責資安訊息及技術蒐集與研究。
2. 制定資安政策，進行情境模擬，執行解決方案。
3. 協調跨部門間的合作。
4. 資安事件應變機制建立與強化，資安事件發生時進行訊息通報、決策、迅速回應，以及證據收集保全、損害控制與資料防護。
5. 對內部員工進行資安教育訓練。
6. 與外部單位資安訊息分享之溝通管道。

(三) 培育各單位資安種子人員

培育各單位資安種子人員，強化內部各單位間資訊安全訊息分享。透過資訊單位及業務單位種子人員相互配合，有效落實資安政策。資訊安全須由資訊單位與業務單位相互配合，資訊單位熟悉業務單位的業務運作與政策，方能開發符合需求且安全的資訊系統；而業務單位對資訊技術及資安風險有所瞭解，對於制定業務運作流程與政策考量能更全面及安全，亦有助對支付系統參加單位的資安監管。

參考資料

1. SEACEN(2017)，「第16屆支付及清算系統高階訓練課程」上課講義。
2. 陳佑任(2016)，「強化支付清算系統之資訊安全」，中央銀行出國報告。
3. 吳桂華(2016)，「區塊鏈技術應用於發行數位貨幣之近況」，中央銀行出國報告。
4. 王怡涵(2015)，「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. 陳啟超(2015)，「參加SEACEN舉辦之第2屆支付及清算系統監管訓練課程出國報告」，中央銀行出國報告。
6. 行政院資通安全辦公室(2014)，「安全軟體設計參考指引 (V1.0)」。
7. BIS(2017), “Quarterly Review, March 2017”.
8. CPMI(2017), “Distributed ledger technology in payment, clearing and settlement”.
9. CPMI(2016), “Fast payments – Enhancing the speed and availability of retail payments”.
10. CPMI(2016), “Guidance on Cyber Resilience for Financial Market Infrastructures”.
11. CPSS(2012), “Principles for Financial Market Infrastructures”.
12. EBA(2014), “EBA Opinion on ‘virtual currencies’”.
13. Bank of England(2014), “Quarterly Bulletin 2014 Q3”.
14. CPSS(2003), “A glossary of terms used in payments and settlement systems”.