新思維的金融資安技術

資策會 資安所⊙朱宇豐組長、顏思嘉副管理師

前言

近年來資訊技術突破性成長，對於電子商品的依賴性也越來越高，金融消費市場也導入電子化技術，Fintech議題開始在金融圈盛行。傳統的實體交易型態演變成線上處理，在這樣的情況下，金融業投入大量資源在技術研發，有限資源的分配下，資安的議題則容易被忽略。線上交易的過程不只涉及技術議題，另一層面更重要的是安全議題，以往金融產業、資訊產業、資安產業這三個產業被視為是獨立的，資訊技術在金融產業中是一種成本，而普世價值中資安也是資訊產業的成本，進而使得金融業導入資安的門檻提高。事實上資訊安全是廣義詞，但對於Fintech上最大風險點在於接觸網際網路的端口，其中交易過程的風險會直接傷害收益，嚴重的話還可能癱瘓整個金融系統。因此，在金融服務創新的同時亦有義務保障資安，才能維繫使用者與金融業者之間的信賴。

世界經濟論壇（World Economic Forum, WEF）在2015年6月的報告中指出，金融科技將帶來前所未有的破壞性創新，並重塑全球金融服務業的面貌。截至2019年，金融科技全球投資額已突破30兆新臺幣，顯示出金融業已逐漸拋開過去舊有思維與服務模式，轉而採用人工智慧、區塊鏈、雲端、大數據等先進技術解決問題。金融是高度監管的領域，過去金融業受限於點對點服務，各銀行及金融服務垂直受到嚴格的管控和法規遵循限制。綜觀全球，英國是最早發展金融科技的國家，率先鬆綁監管環境，並提出監理沙盒（Sandbox）的概念，讓創新者向市場推出新的金融服務和商業模式之前，在風險可控的場域中進行實驗。亞太地區則是金融科技發展最快速的地區，尤其東南亞地區的線上支付平台不斷推出，有望成為金融科技創新熱點。然而，會形成這樣快速發展的原因除了該地區傳統金融機構服務水平低下，僅有少量人口擁有銀行帳戶之外，不斷提高的網路滲透率亦是發展的一大關鍵。[1]

近年來，隨著全球掀起開放銀行（Open

1 Samuel Abraham and IF correspondent, "Southeast Asia becomes the fintech innovation hotspot," International Finance, July 10, 2019, https://www.internationalfinance.com/magazine/southeast-asia-becomes-the-fintech-innovation-hotspot/.

Banking）的熱潮下，銀行可在取得使用者授權後，將其資訊提供給第三方業者（TSP, Third Party Service Providers）使用。緊接著英國實行開放銀行政策，歐盟也在2018年推出第二版支付指令（The Second Payment Services Directive, PSD2），基於PSD1要求銀行建立數位及電子支付服務外，第二版的指令更擴大了適用範圍，要求銀行必須提供Open API給外部機構使用。如此一來，不僅讓銀行資料透明化，更提高用戶對自身財務的主控權。為實現開放銀行，銀行透過Open API（應用程式界面，Application Programming Interface）公開應用程序邏輯和機敏數據，例如個人識別資訊（Personally Identifiable Information, PII），這些資訊因而成為了駭客攻擊的目標，沒有安全的API，將無法達成快速的創新技術。[2]在法規層面，為了保護個人資料，歐盟於2018年提出一般資料保護規範（General Data Protection Regulation, GDPR），保護的範圍涵蓋了個人身分、生物特徵，以及定位資料等，顯示出金融機構對法遵科技（RegTech）的需求日益增長。因此，如何確保API在串連服務和傳輸數據的安全性，以保持其用戶的信任，成為了目前金融業首要解決的問題。

反觀臺灣的開放銀行政策採用不修法的香港模式，讓銀行與TSP業者共同推動，並以三階段循序漸進的方式，依序從商品資訊、客戶資訊到交易資訊，逐漸改變傳統銀行的營運模式。臺灣開放銀行的第一階段「公開資料查詢」於2019年9月底開始上線，第一階段以非交易金融資訊為主，不涉及消費者個人資料，TSP業者透過API介接到各家銀行的商品資訊，消費者可透過應用程式比較各銀行的相關產品服務。

Open API帶來的商業契機與資安挑戰

全球有17億成年人口沒有銀行帳戶，但其中有2/3的人擁有手機，開放銀行將增加銀行的收入來源，同時擴大金融機構的客戶範圍，讓使用者毋須舟車勞頓跑銀行，透過手機或是數位平台就可以進行金融服務，舉凡生活繳費、管理開支記帳、各銀行利率比較、開戶、信貸身分認證、微型保單等，創建與第三方業者收益共享的生態系統。Open API可以加速金融機構後端的連接和功能，增加服務商客戶的參與率。其中，Open API帶來的商機可歸納為以下幾項：[3]

1. 強化產品服務

透過開放API，銀行可以運用隨插即用（plug-and-play）的方式引入FinTech解決方案，進而輕鬆與市場上的API連接，擴展其服務範圍。透過開放銀行API經濟，銀行可以進一步增強和改變現有產品，從而增加對現有和潛在客戶的吸引力。

2. 改善整體客戶參與度

開放銀行API能夠滿足現有客戶及潛在客戶不斷變化的需求，除此之外，這些API還可以提高客戶的參與度，特別是在創新的

2. OWASP, “OWASP API Security Project,” https://owasp.org/www-project-api-security/.
3. MuleSoft, “How Financial Service Firms Can Benefit from Open Banking APIs,”

產品和設備進入市場的情況下，導致傳統銀行的競爭越來越激烈。這種競爭給傳統銀行帶來了挑戰，迫使他們不得不進行創新以保留原有客戶並吸引潛在客戶。

3. 增加數位收益

除了增強銀行提供的服務和客戶參與度之外，Open API還可以幫助銀行增加新的數位收益。例如歐洲國家PSD2監管標準將增加可用的API數量，鼓勵新創打入客戶與銀行間的關係並挑戰傳統的支付模式。

4. 銀行即服務—以Open API主導之開放銀行策略

開放銀行API是金融業寶貴的資產，API能夠增強其產品及服務。為了建立有效的開放銀行API策略，金融服務公司必須對它們的技術進行驗證，以確保這些API可以進行產品化和市場銷售。

金融業正在顛覆過去的傳統服務模式，意識到開放銀行的核心價值和API的基本作用，越來越多金融業者接受開放銀行計畫。整體來說，開放銀行在取得消費者同意後，透過應用程式介面（API）與其他銀行或是第三方服務供應商（TSP）合作，進而開發出更好的個人財務管理（Personal Financial Management, PFM）和新的金融服務與場景；在第三方業者方面，經過授權取得消費者資料後，更能提供個人化、多元化的金融服務；而開放銀行對於消費者來說，將更容易掌握自己的財務狀況，可以自行決定帳戶資料的分享對象，做出對自己最有利的選擇。API gateway讓業者有很大的空間創造新的解決方案，比傳統Web更具彈性，更多資源放置在用戶端。開放銀行的角色包含Bank（銀行業者）、TSP（第三方業者）、User（使用者），三方關係是透過驗證機制串連，使用者提供TSP業者資料和條件，而TSP業者則提供服務給使用者；TSP將透過各家銀行授權，整合使用者的帳戶資訊，最後再回傳給使用者。

過去，一個使用者會接觸多個銀行進行不同的服務，而現在TSP業者整合使用者在各家銀行的資訊，因此使用者只須要透過TSP平台即可進行一站式的操作服務。如下圖所示，一個使用者可以對多個TSP業者，同樣地，一個TSP業者也會和多間銀行有關係。（如圖1）

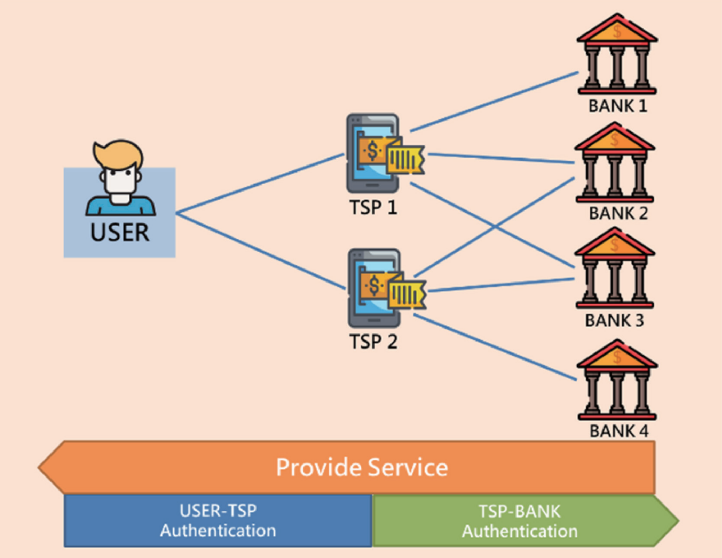

圖 1、開放銀行三方情境架構
資料來源：筆者自行整理

然而，透過應用程式介面（API）整合用戶端多個帳戶資訊，同時公開個人可識別資訊（Personally Identifiable Information, PII），在這樣的情況下容易將帳戶資訊暴露在高風險的環境下，形成資安漏洞。API安全性對企業來說至關重要，因為這些接口通常會暴露敏感數據，使得組織內部基礎架構被濫用。隨著個資保護意識抬頭，建構符合GDPR及安全API的成本亦不斷增加，開發人員在進行產品開發時也須將安全性考量到產品的生命週期。其中，常見的API漏洞的攻擊手法包含：[4]

1. 中間人攻擊（Man-in-the-Middle）

中間人攻擊是一種網路攻擊模式，其中駭客將自己插入兩方之間的對話中冒充了雙方，並取得了雙方試圖相互發送的訊息。若要減少這種攻擊，建議透過SSL / TLS升級到更安全的HTTPS協議，如此一來可以在服務和客戶端建立加密的安全連接，進而防止所有訊息被盜用，不過此種方法也只能針對部分，如下圖模式，中間人也是可以發憑證的，所以竊取傳輸中加密資料，不過此種方法會多一個發憑證過程，容易感受到傳輸效率下降。目前此種技術已經很成熟，突破傳輸效率也是有可能做得到，建議讀者在外盡量少用來路不明的網路。（如圖2）

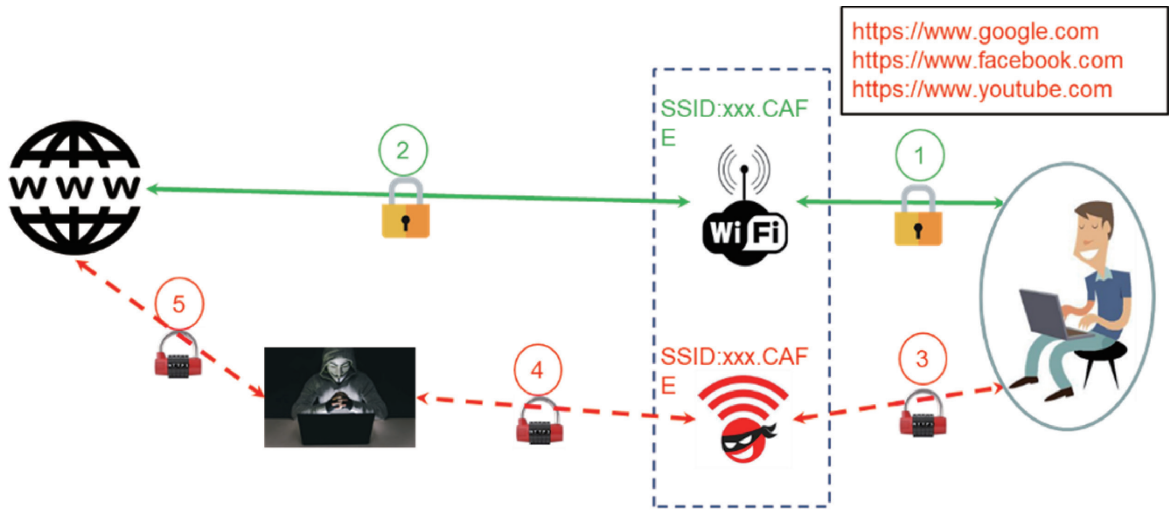

圖 2、中間人攻擊　資料來源：筆者自行整理

2. CSRF攻擊（CSRF Attack）

在跨網站的請求偽造攻擊中，駭客可在用戶不知情的情況下，透過身分驗證的Web應用程序中採取諸如匯款或更改電子郵件地址之類的操作。用戶可透過token來防止CSRF攻擊，這些token作為隱藏字段嵌入HTML中，並隨每個請求發送回伺服器，讓伺服器可以驗證該請求是否來自經過身分驗證的來源。（如圖3）

4 Jason Skowronski, “Common API Vulnerabilities and How to Secure Them,” solarwinds papertrail, Jan 7, 2019, https://blog.papertrailapp.com/common-api-vulnerabilities-and-how-to-secure-them/.

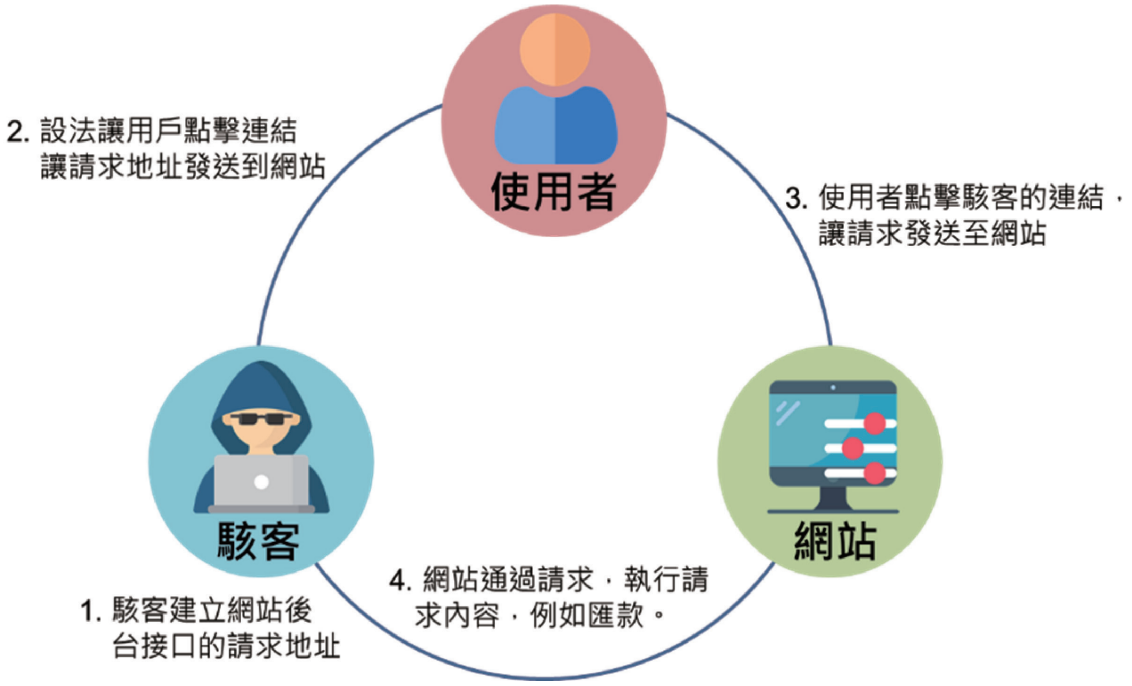

圖 3、CSRF 攻擊　資料來源：筆者自行整理

3. XSS攻擊（XSS Attack）

跨網站腳本攻擊（Cross site scripting attacks）的原理是將惡意腳本注入易受攻擊的應用程序，使用戶洩露其對話cookie。透過適當轉譯數據以消除惡意腳本並驗證用戶的數據中是否存在有害內容，即可以防止此類攻擊。

4. SQL注入式攻擊（SQL Injection）

當用戶輸入最終將在數據庫上執行的SQL語句而不是輸入有效數據時，就會發生SQL注入。防禦這類攻擊的最佳方法是透過開發框架（Framework）、SQL準備的語句，或者使用ORM工具（如Hibernate）提供的命名參數。

5. 阻斷式服務攻擊（Distributed Denial of Services, DDoS）

阻斷式服務攻擊是一種惡意透過大量互聯網流量淹沒目標或其周圍基礎架構，從而破壞目標伺服器、服務或網路的正常流量。DDoS攻擊使用多個受損的電腦系統作為攻擊流量的來源，被利用的機器包括電腦和其他網路資源。此攻擊最困難的部分是難以區分攻擊和正常流量，尤其是當流量來自看起來像一般用戶的使用。

OWASP（The Open Web Application Security Project，開放網路應用程式安全專案）是網路安全權威性的非營利基金會，致力於提高軟體安全性，定期提供Web應用安全領域相關的文章、分析報告、工具和技術

新知等資訊。其中，跟金融科技發展最有關聯性的即是API安全風險的議題，為解決Open API風險問題，根據OWASP 2019所提出之前10大API安全風險，說明資安風險的管控機制，其說明如下：

- API1: 無效的對象層級授權（Broken Object Level Authorization）
  (1) 實施用戶規範與等級制度之授權機制
  (2) 利用授權機制檢查登錄用戶是否存在每項功能的授權記錄中且有權進行操作
- API2: 無效認證與授權（Broken Authentication）
  (1) 採用多元之身分驗證機制，多重把關用戶登入的安全性
  (2) 實施帳戶鎖定、驗證碼機制、弱密碼檢查，避免駭客輕易取得帳戶資訊
- API3: 大量資訊外洩（Excessive data exposure）
  (1) 檢查API反饋之資訊為合法數據
  (2) 規定帳戶數量限額
- API4: 缺乏資源與速率限制不足（Lack of Resources & Rate Limiting）
  (1) 限制用戶在一定時間內調用API頻率
  (2) 利用提供限制編號和重置限制的時間來通知用戶超出時間限制
- API5: 無效功能權限控管（Broken function level authorization）
  (1) 進入每一個功能介面時都須進行身分識別，而非採用預設值登入，確保進入另一個介面時是該用戶登入
  (2) 檢查API端點是否存在功能級別授權漏洞
- API6: 批量分配不當（Mass Assignment）
  (1)避免將用戶資訊自動綁定到系統內
  (2)建立假帳號黑名單
- API7: 不安全的組態設定（Security Misconfiguration）
  (1) 定期審查用戶資料真實性和更新API配置，審查內容應包括：業務流程文件、API組件和雲端服務
- API8: 注入攻擊（Injection）
  (1) 定期驗證、過濾和清理所有用戶端提供的數據
  (2) 使用參數化接口的安全API
  (3) 限制反饋記錄的數量，以防止在注入時洩漏大量資訊
- API9: 版本控管不當（Improper Assets Management）
  (1) 記錄API服務，確認其數據流合法性及敏感性
  (2) 使用API防火牆，確保軟硬體間之安全性
- API10: 記錄與監控不足（Insufficient Logging & Monitoring）
  (1) 記錄所有失敗的身分驗證、拒絕進入和輸入驗證錯誤
  (2) 利用監視系統以連續監視網絡和API之運作
  (3) 利用安全性資訊與事件管理（Security Information Event Management, SIEM）解決方案來管理API

為確保安全的API，應保障以下功能：[5]

1. 最新版本的通信安全性（HTTPS / TLS 1.2）（Most current version of communication security(HTTPS/TLS 1.2)）：透過加密協議傳輸資料。
2. 反向代理URL（Reverse proxy URL）：反向代理URL可以提供負載平衡和故障轉移，創建對銀行API的單點路徑，並大大降低了潛在的駭客使用DDoS攻擊等風險。反向代理還提供了附加等級的抽象和控制，以確保客戶端和服務商之間網路流量的順暢流動。
3. 客戶認證（Client certificate）：客戶認證使駭客無法在沒有客戶同意的情況下提交API請求。這需要透過建立標準，使所有請求都必須與客戶端認證一起發送。
4. 先進的認證模型（如OAuth 2.0）：使用開放授權OAuth 2.0等高級身分驗證模型。API使用「基本身分驗證」，要求用戶為每個請求提供ID及密碼，但在用戶ID及密碼未加密或散列的情況下，用戶資料容易被盜，則會帶來風險。但是，透過在專用線路上傳輸可以減少這類風險。開放授權OAuth 2.0則提供了更好的解決方案，因為包含了過期令牌的路徑。
5. 認證模型（Authentication/role model）：認證模型可以限制應用程序API的路徑，進而降低了駭客進入的風險。
6. 限制的客戶數量（Access to a limited set of customers/accounts）：在特殊情況下限制對特定帳戶的路徑可以減少安全漏洞，特別是當客戶端在使用第三方應用程序時。
7. 超越HTTPS / TLS提供的加密（Encryption above and beyond what is provided by HTTPS/TLS）：除了HTTPS / TLS所提供的加密之外，也應該合併其它的安全性考量，使客戶端和服務商在加密算法相互達成共識。
8. 日誌（LOG）的安全概念（Secure concepts regarding logging）：REST API在統一資源標識符（URI）中包括客戶編號、帳號和其他機敏數據。大多數銀行在調用API之前都會記錄URI。此外，合作夥伴應在收到請求時記錄URI，限制對日誌的路徑和對URI中的敏感數據進行加密將有助於降低風險。

大多數銀行負擔不起建立自己的API的能力，或是沒有足夠資源來支援自己的API。因此，許多銀行會尋求API技術合作夥伴來提供API解決方案。在這樣的情況下，銀行的API及敏感數據將會被公開，並期望API合作夥伴能夠減少欺詐等攻擊風險。API合作夥伴應提供完善的API解決方案，使銀行將風險降到最低，並透過持續的監控來避免新的風險。[6]（如圖4）

5 Scott Biesterveld & Senthil Senthil, “Ensuring Security With Open APIs”, white paper, FiS, 2018, p.1-7.
6 Scott Biesterveld & Senthil Senthil, “Ensuring Security With Open APIs”, white paper, FiS, 2018, p.1-7.

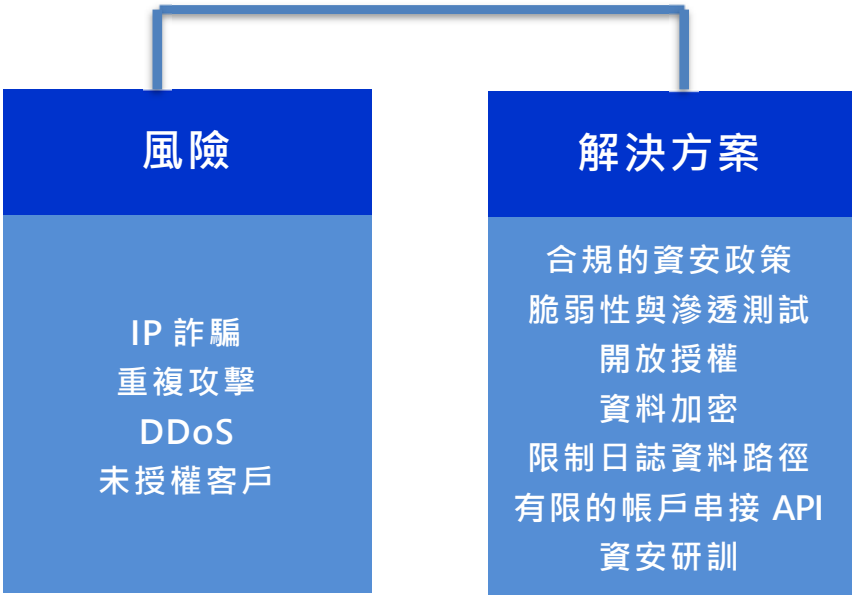

圖 4、Open API 風險與解決方案　　資料來源：筆者自行整理

金融科技多面向資安風險評估

金融業面臨新型態的資安威脅，數據洩漏的事件即是金融科技上資安議題，並且對於銀行、信貸、第三方支付商等都有被影響到；帳號的安全機制極為重要，近年來發生的有2005年的Card Systems Solutions有4000萬個信用卡帳戶被盜，2009年的CheckFree Corp有500萬人受影響，2010年的Educational Credit Management Corp.有330萬人受影響，2014年的 Heartland Payment Systems有1.3億人受影響，2017年的Equifax有1.43億帳戶受影響，2019年的Earl Enterprises有200萬張信用卡外洩。

依據金融科技特性，偏重於網路傳輸，針對Open API當基礎，導入五大金融科技資安風險評估，來源部分篩選信任IP、對於系統做健診、傳輸之資料加以保護、人因風險在內部網路上較不被防火牆發現、金融資訊容易在暗網中被洩露；透過蒐集暗網情資方式監控，五大風險評估機制如下：（如圖5）

1. 暗網情資（Dark Web Deep Intelligence）：

暗網中常出現可交易的資料，其中金融資訊的信用卡號、金融卡號、交易帳號密碼等…，都是機敏可交易之資訊，並且暗網中也會有可攻擊之手法。透過暗網蒐集資料技術，主動式蒐集與關聯相關資料，再以被動式比對偵測技術來偵測機敏資料。

2. 人因風險（Human Risk Evaluation）：

企業資安議題除了外部入侵風險外，企業內部發生的資安議題往往會被忽略，一般公司都裝防毒軟體，對於外部透過防火牆機制來限制、更進階一點會用入侵偵測系統，但這些防護端都在使用者或者企業外部，對於企業內部傳輸不被防火牆控制，使用者端

圖 5、金融科技風險評估技術　資料來源：筆者自行整理

防毒軟體也不一定會限制異常連線行為，此時對於內部有風險行為的存取不被控制，所以人因風險對於企業內部橫向感染問題，藉由內部行為基準作為異常偵測。

3. IP信評（IP Reputation Tracing）

網路資訊傳輸中IP的信用極為重要，對於提供外部網路服務之主機，來源IP過濾可以增加安全，並且可以節省運算成本，對於企業IP可以監控外部給的信用評價，所以建置評估系統和自動化更新機制。

4. Web診測（Web Security Assessment）

金融科技必定會提供網路服務，提供服務之端口就容易成為安全漏洞，透過網路掃描技術，持續監控網路服務營運。

5. 機敏資料保護（Sensitive data protection）

傳輸資料過程，被監聽和資料竊取問題容易發生，並且在金融科技中傳輸資料都該被高度監控，許多資料也是機敏資料，例如交易資訊，所以此資料需要經過加密傳輸，另一方面對於資料共享部分，至少也需要經過去識別化技術，才可更有保障。

結語

儘管新的商業模式和以客戶為中心的解決方案將創造機會，開放銀行及Open API為第三方業者帶來一線生機，但金融科技的快速發展趨勢中，資安能量未能充分結合運用，造成交易安全、個資外洩等問題……，日益推陳出新的金融科技服務也會使金融文盲的情形更加惡化，故提升金融資安的新思維勢在必行，才能在產業演變的腳步下保證自身的權益。

除此之外，金融業者應善用金融科技資安風險評估技術作為Open API的資安基礎，方能建立安全防護網，確保銀行業者、TSP業者，及使用者於三方關係中取得平衡，並具備正確的資安意識。