Deloitte.
勤業眾信

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

開展新局：
2022 數位與金融脈動展望報告 - 資料共享、保險科技與金融資安

MAKING AN IMPACT THAT MATTERS since 1845

目錄

序文

近年金融科技發展快速，去年(2021)勤業眾信攜手國立政治大學金融科技研究中心發布《2021台灣金融科技趨勢展望》，分別從Digital Banking（數位銀行）、InsurTech（保險科技）、Asset Management（資產管理／投資管理）以及SupTech/RegTech（法遵科技）等領域研究，結合Deloitte Global的Future of Bank八大趨勢，綜觀國內外金融科技發展比較與台灣Fintech發展的挑戰，提出有關政府政策、監理方向和管理策略之建言。

在Deloitte Future of Bank八大趨勢中，台灣金融機構普遍以「提高數位化程度」、「降低數位網路風險與金融犯罪」、「強化數據整合與分析」及「有效採用數位與新興科技」等，作為主要發展的面向。在全球金融科技創新持續推進的同時，適逢COVID-19疫情的影響，加速了數位轉型，服務與工作型態也隨之改變，從線下轉入線上或遠端模式，而工作模式的變革同時使得駭客入侵的機會增加，進而讓資安成為須立即面對的重要議題之一。為與國際市場接軌，金管會在去年底發布「金融機構間資料共享指引」，主要內容為提升金融業客戶便利性，以促進新生態圈的建立; 純網路保險公司預計於今年 (2022)8月開始申請，並推廣電子保險存摺平臺，帶動台灣保險科技的創新和便利; 暨強化金融資安等措施。

今年勤業眾信與政大再次合作《2022數位與金融脈動展望報告 - 資料共享、保險科技與金融資安》，研究報告主要針對金管會金融科技發展路徑圖中之現行重點發展進行分析及建議，並供政府及業者參考，主題分別為: 金融資料共享、純網保與保險存摺平台、金融資安。

本研究報告透過回顧國內外金融科技之發展，彙整金融科技的框架與各國在法令、業務、技術等不同構面上的差異與進程，並審視台灣金融科技導入進程，結合訪談金融機構與第三方服務業者，了解台灣在金融科技上的準備進度及所遇到的困難與挑戰，提供金融產業策略規劃的建議，在政策層面上給予相關金融監理單位對於金融科技在監理與治理方面之管理策略與建議，期待與金融產業各界攜手挹注Fintech能量。

勤業眾信聯合會計師事務所
金融服務產業負責人
吳怡君會計師

國立政治大學
金融科技研究中心
王儷玲主任

國際金融科技之應用與發展

資料共享

1. 全球資料共享發展概況

開放銀行是近年全球在資料共享創新發展的重要推動力，希望透過應用程式介面(API)的串聯來開放資料，以創造更多金融創新的機會，同時期望實現資料賦權，讓消費者能夠享受到更好的體驗。The Financial Brand 的報導分析指出，API在資料交換上將會取代原有的螢幕截取 (screen scraping) 功能，因為螢幕截取方式不但不安全，也容易將個資外洩，而API可在資料交換時對資料使用進行一定的追蹤及控管，並建立資料交換平台，搭配身分識別後可用於有個資、隱私議題的資料。根據 Allied Market Research 在 2020 年發表的報告， 2018 年全球開放銀行市場規模為 72.95 億美元，預計到 2026 年可達到 431.52 億美元，2019 年到 2026 年的複合年增長率為 24.4%。[1]

目前全球開放銀行發展較成熟的國家包括歐盟、英國、澳洲、香港以及新加坡等，其中又以英國的發展最成熟，美國的發展最為快速，主要原因在於美國監管機構選擇採用不具約束力的準則來推動開放銀行，例如美國消費者金融保護局(Consumer Financial Protection Bureau, CFPB)於2017年頒布的《消費者保護原則：消費者授權的金融數據共享和匯總》，至於實際的運作方式則交由市場上的銀行以及合作的第三方服務業者(TSP)自行決定，這樣的運作方式讓美國能夠迅速推動開放銀行[2]。另外，在Allied Market Research研究中認為，2018年開放銀行的市場商機有超過三分之二來自美國，然而未來成長最快速的地區則是歐洲[3,4]。

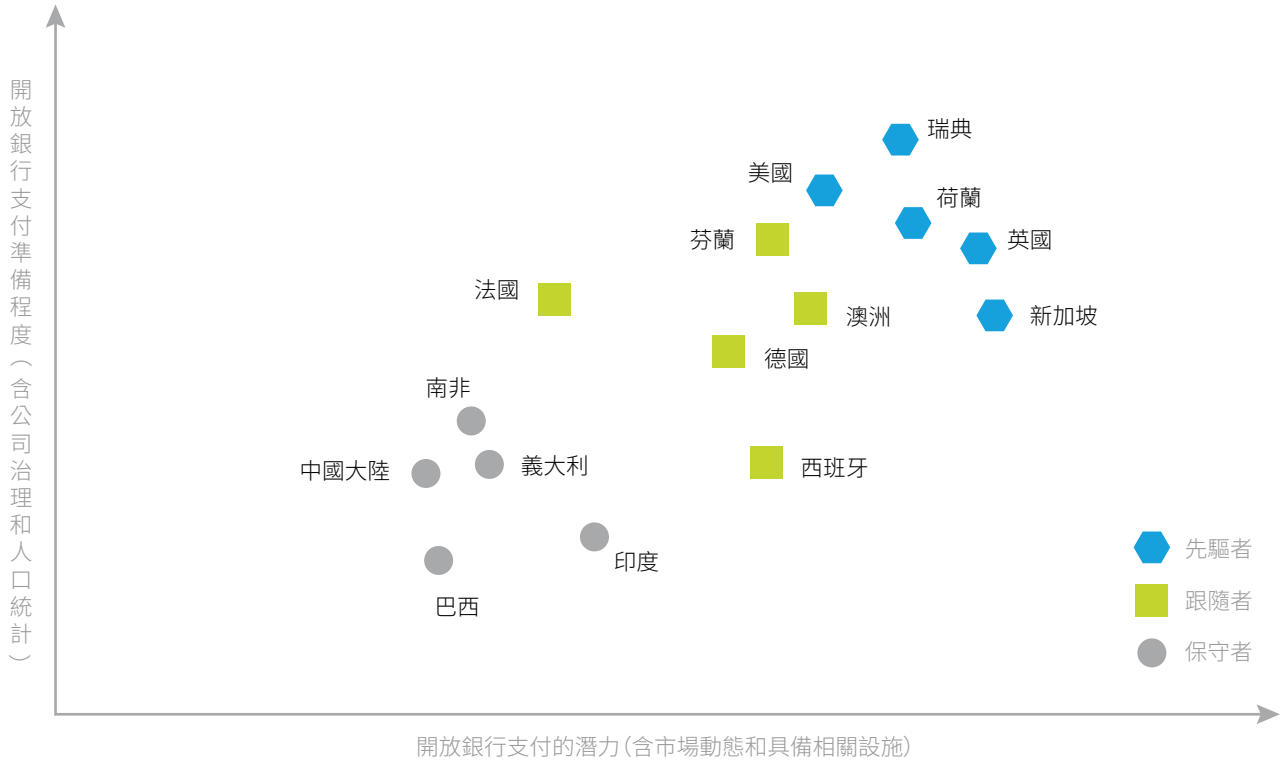
歐洲開放銀行的概念最早出現於歐盟在2015年10月通過的《支付服務指令修正案》([Revised] Payment Services Directive 2, PSD2)，PSD2的主要目的在於統合歐盟內部的電子支付市場，透過制定共同規範來讓歐盟內部各國間的支付規格化，提供歐盟範圍內的無縫支付服務。PSD2提出幾項變革，包括強化資安要求、落實消費者保護等等，而其中最重要的一項為：允許第三方支付服務提供者(Third Party Provider， TPP) 根據PSD對於「支付服務」定義，第七款「透過電信、數位或IT設備接收支付服務使用者的指示執行支付交易，而支付的進行也是透過電信或IT系統或網路營運人，而且只是擔任服務使用者與商品或服務提供人的中間媒介。」加入金融市場，同意TPP可以使用消費者的銀行帳戶資料，提供帳戶資訊服務，同時也可以進一步發動支付指令，在消費者同意之下直接對消費者銀行帳戶進行扣款支付。在這一條規範之下，銀行必須將資料開放給第三方使用，PSD2也因此成為開放銀行發展最早的一步，但是在歐盟的PSD2中並未使用開放銀行這個詞彙。

受到歐盟PSD2政策的影響，英國在2016年提出開放銀行的相關規劃，根據英國競爭暨市場管理局(Competition and Markets Authority, CMA)曾針對市場進行調查，發現英國的傳統大型銀行徹底壟斷市場，而且客戶黏著度極高，使得這些大銀行不必做出太多創新與競爭，即可維持現有的市占率，進而導致挑戰者銀行(challenger bank)無法打入市場，而開放銀行即是CMA所提出的解決方案之一。根據CMA 2016年公布的調查報告[5]中指出，英國四大銀行匯豐(HSBC)、巴克萊(Barclays)、駿懋(Lloyds)及蘇格蘭皇家(RBS)部份業務之市佔率高達8至9成，其中個人活存(77%)、企業活存(85%)及企業貸款(90%)；中小企業對往來銀行之轉換率偏低(約4%)。英國開放銀行的目的是期望透過大型銀行與歐盟PSD2中的TPP業者合作，加速英國銀行的創新能量，進而提昇英國銀行的競爭力。自從2017年英國宣布推行開放銀行計畫之後，截至2020年5月為止，累計共有175間TSP業者加入開放銀行體系，為市場注入強大的創新能量[6]。

除了上述的美國、歐盟以及英國之外，東亞地區的香港、新加坡也是開放銀行發展的領先族群，皆已建立起完整的開放銀行基礎架構。而台灣、印度、日本、紐西蘭、加拿大、澳洲以及南美洲、非洲等國的發展進程則相對較晚，大多處於研擬規範和建立配套的階段。

Capgemini & BNP Paribas《World Payment Report 2018》在2018年針對各國市場，依照競爭程度、監理環境、支付系統、銀行和第三方業者之間的資料共享程度等等，來判斷各國是否具備發展開放銀行的市場條件。如圖1所示，該報告將推行開放銀行的國家分為領先者、跟隨者以及保守者，領先者國家包括美國、新加坡，以及目前開放銀行發展最成熟的英國。[7]

圖 1 各國開放銀行發展評估[7]



全球的API經濟產業正以快速數位化的方式轉型，彰顯出數據日益增長的社會價值與經濟價值，以及數據共享的重要性與必要性，也就是所謂的資料共享。其中金融機構也持續透過串接不同系統的數據，以及強化跨產業的內外部合作，提供消費者更完善的金融服務。多數國家對於未來的發展都抱持樂觀態度，認為開放銀行可以加速金融創新並建立新形態的生態圈。根據經濟合作暨發展組織(OECD) [8] 的分析，資料的取得與共享約可產生相當於國內生產毛額(GDP)的1%至4%的社會與經濟效益，全球合計將會高達3.3兆美元。

世界各國政府藉由推動資料共享，期望在金融科技創新領域持續創造更大的經濟價值，其中，歐盟、新加坡皆已發展出較完整的資料共享框架，歐盟有針對個人資料保護的規範GDPR，新加坡則藉由建立資料共享框架以及發布共享手冊，建立資料共享的友善環境。除此之外，澳洲針對消費者資料保護(Customer Data Power, CDP)，分階段建置開放銀行的布局與API的開放、美國開放銀行的快速發展以及市場機制導向的模式，以上都是國際推展與實現資料共享的參考典範。

2. API經濟的應用趨勢

在當今以網路串接世界的時代，應用程式介面(API)是實現資料共享的重要基礎技術[9]，允許多個不同系統之間互相交換資料[10]。根據IBM調查，市場中有將近70%的企業正在尋找外部的合作機會藉以增強實力，而API正是企業間完成數據系統串接重要的工具，也提升創新業務開展的能力，透過結合多元的功能來提供全新的客戶體驗，在金融科技時代下具有強大的商業策略價值。IBM也提出三種模型用來解釋目前市場中存在的API商業模式，分別是直接消費(Direct Consumption)、市場創造 (Market Making)以及生態系賦予(Ecosystem Enablement)，以下會利用上述三種模型分析企業是如何創造API的多元經濟價值[3]。

第一種直接消費模式: 是指企業將開發的API直接提供給其他業者進行串接，並收取使用費，因此其他業者無需投入大量研發費用與時間成本自行開發API，可以直接低成本的取得服務。以2020年3月推出的口罩地圖服務為例，此平台的創造工程師使用了Google地圖與地點搜尋的Place API服務，於上架的當天下午收到高達兩萬六千美金的使用費帳單，此即是Google透過提供API服務所創造出的經濟價值。根據IBM統計，由Twitter、Netflix和Google等提供公共API的公司，每天被觸及使用的次數可達到10-50億次，而Google每日藉由提供API服務約可賺取高達500萬至1億美元的收入。直接消費模型的優點包括使用者可以透過低成本獲取現成資料，大幅降低R&D費用以及時間成本。但相對來說，該模式的API使用者並不會主動推廣該項API的服務，也不易透過此模式來吸引或激勵其他業者加入使用。

第二種市場創造模型: 這種類型的企業匯集大量相關API且將其整合後，創造出全新的服務，藉以在原本的API上附加新的經濟價值，並收取佣金或服務費用，類似經紀人的角色。市場中最常見的案例包含類似booking.com的訂房網站，該類業者負責串接各大飯店的訂房資訊，提供消費者住宿比價、預約訂房等創新服務。另外，開放銀行目前於市場中最受矚目API應用之一的記帳軟體亦屬於此類模型，例如台灣的麻布記帳App提供消費者可以在單一平台上查看所有銀行帳戶存款金額、信用卡消費、持有股票行情等的整合性服務。

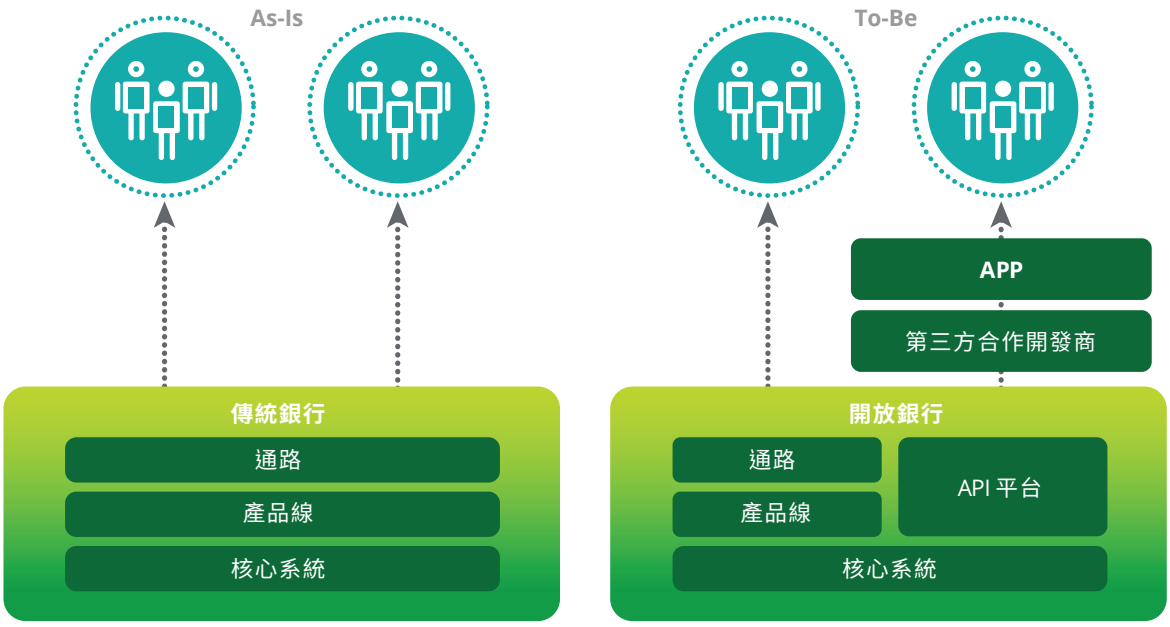
第三種生態系賦予模型: 概念上與第一種的直接消費模型雷同，兩者差別主要在於生態系賦予模型會在取得其他業者提供的API服務後，進行包裝與整合，建立創新服務後再進一步銷售該服務系統。印度的新創銀行RBL Bank即採此模式與其他業者合作，RBL Bank先將API提供給當地資產管理公司，而該資產管理公司應用RBL Bank的支付API以及帳戶API，建立屬於該企業的「錢包」，讓RBL Bank的客戶能夠簡化交易流程，使整個金流服務更加順暢，甚至能做到將共同基金及時贖回的功能。圖2彙整API商業模型之優缺點。

圖2：API商業模型優缺點

	直接消費模式	市場創造模型	生態系賦予模型
優勢	使用者可以透過低成本獲取現成資料，大幅降低R&D費用以及時間成本。	這種類型的企業匯集大量相關API且將其整合後，創造出全新的服務，藉以在原本的API上附加新的經濟價值，並收取佣金或服務費用，類似經紀人的角色。	生態系賦予模型會在取得其他業者提供的API服務後，進行包裝與整合，建立創新服務後再進一步銷售該服務系統。
挑戰	該模式的API使用者並不會主動推廣該項API的服務，也不易透過此模式來吸引或激勵其他業者加入使用。	• 高度依賴市場流量 • 因技術進入門檻低，因此容易出現競爭者	消費者體驗會因各API提供業者的系統更新而有所差異。

根據資策會報告，全球主要開放銀行開放功能的API比重以帳戶資訊(32.9%)以及支付轉帳(28.7%)為最多和次多，接下來的依序是交易(18.2%)、借貸融資(7%)、分行資訊(7%)、投資(6.3%)、外匯交易(4.2%)以及保險(2.8%)[11]，同時，徵信服務也逐漸成為主要發展方向之一，而於證券、保險領域中的應用仍待有更多的發展

圖 3：銀行運作體系的轉變



資料來源: 資策會 開放銀行發展趨勢與展望

除了銀行營運模式的改變外，歐洲銀行業管理局(EBA)也提出金融市場最終會在開放銀行的發展下，形成類似零售業中的「平台」模式[12]，將所有服務、商品聚集至單一的匯集點，例如P2P借貸平台的出現、國際換匯(FXP2P)平台等等，讓交易的雙方能夠在特定平台上媒合，並獲取所需的金融服務。API的開放加速了相關服務的數據串接，平台藉由蒐集更多的消費者資訊，提供消費者更多客製化的服務，並採取一站式的服務模式，藉以創造更好的消費者體驗。圖3說明開放銀行對銀行運作體系的轉變。

3. 全球資料共享相關法規借鏡

英國

英國的開放銀行發展起源於2016年，在CMA提出的市場調查報告中可發現市場遭到大型銀行壟斷，且客戶轉換度極低，銀行不需要做太多創新和品質提升，就可以穩穩地維持市占率。由於市場上缺乏競爭意識，挑戰者銀行亦無法輕易進入金融業，因此CMA在2017年提出一份行政命令(Order)，要求英國市場上排名前九大銀行必須以安全且標準的形式將API開放給TSP串接，而其他銀行則不強制要求開放，這就是英國將開放銀行與金融業資料共享落地的開端。

在CMA於2017年頒布的行政命令當中規定了API開放的範圍以及內容，主要可以區分成兩大類：唯讀資料(Read)以及可讀寫資料(Read/Write)。其中唯讀資料包括銀行的總行地點及營業時間、分行的地點及營業時間、ATM的地點、個人及企業活存帳戶、利息、中小企業借貸條款及條件[13]。而可讀寫資料則規範了交易面以及支付面的API類別，包括國內外交易發起、國內外交易同意、個人借貸等等各種相關應用[14]。除了唯讀資料以及可讀寫資料，英國從2019年底便積極討論是否要開放數位身分的API，來解決開放銀行中身分認證的問題。

在資料共享範疇下，英國資安規範依據：GDPR、PSD2 RTS、其他OBIE制定之標準所組成。主要有規範下列幾項：

1. SCA (Strong Customers Authentication)： SCA是PSD2中對消費者授權的嚴格規範，PSD2和RTS將SCA定義為「對於使用者的知識(knowledge，只有使用者知道)、所有物(possession，只有使用者擁有)、固有屬性(inherence，使用者的屬性)，若要使用以上三種資料就必須要獲得授權，且三種資料授權相互獨立而不得混用，以保護資料授權的安全性」[15]。

2. FAPI (Financial Grade API) Profile： FAPI是一種REST API，負責提供代表高風險的JSON data。這類型的API會在OAuth 2.0 的架構下受到保護，並遵從[RFC 6749]、[RFC 6750]、[RFC 7636]以及其他相關規定[16]。

REST，中文為含狀態傳輸，全名為Representational State Transfer，是一種軟體架構設計風格。資源由URI指定，對資源的操作包括取得、創建、修改和刪除資源，這些操作正好對應HTTP協議提供之GET、POST、PUT和DELETE方法。

JSON，全名為JavaScript Object Notation，為網際網路應用的一種常見的輕量級資料交換格式。

OAuth，中文為開放授權，OAuth 2.0標準係指一個開放標準，允許消費者授權讓第三方服務提供者存取該消費者在授權機構上所儲存的受保護資料(又稱為保護資源)。

3. CIBA Profile： CIBA全名為Client Initiated Backchannel Authentication，由OpenID組織提出的TSP端驗證機制，其用途改善消費者體驗，讓消費者行使同意權後，可由銀行與第三方認證業者直接確認後續授權的流程[16]。

除了資安規範外，英國也提出了conformance certification的「一致性系統驗證」的機制。而在系統驗證中，分了四大類：

- 個資檔資訊一致性：Security Profile Conformance
- 功能一致性：Functional Conformance
- TSP端動態註冊一致性：Dynamic Client Registration Conformance
- 消費者體驗規範一致性：Customer Experience Guidelines Conformance

在Security Profile Conformance，ASPSP必須驗證其API系統必須符合FAPI與CIBA規範；而在Functional Conformance中，各個參與者則必須驗證其API系統符合OBIE的Read和Read/Write的API規格。但目前Conformance Certification是非強制性，而是採取自測或由認證單位進行後呈FCA發佈。

歐盟

歐盟認為支付服務應該滿足歐盟經濟區(EEA)內一致性、清楚的付款資訊、多元支付、消費者保護等項目。所以歐盟一直致力於建立一個單一支付區，使消費者和企業都能在支付區內安全的進行跨境支付，費用也應與境內支付相同。為了推行無縫支付環境，2013年歐盟提出支付服務指令修正案(PSD2)，主要目的在於整合歐盟內

部的電子支付市場，並為其提供統一的法律基礎和規則，讓歐盟內部的跨國支付就像在國內支付一樣快速、有效且安全。PSD2提到，根據客戶的要求，銀行和其他帳戶支付服務提供商必須開放API給註冊後且取得消費者授權的TSP，讓TSP能夠拿到消費者帳戶的讀寫權限[17]。此即PSD2為促進支付服務的良性競爭所採取之開放銀行政策，成為歐盟各國推動開放銀行的基礎。

歐盟所開放之資料類型，可分為帳戶資訊服務(Account Information Service, AIS)、支付發起服務(Payment Initiation Service, PIS)以及卡片支付服務(Card Based Payment Service, CBPS) [18]。其中AIS是開放銀行中最基礎的，使TSP能夠取得消費者的帳戶資訊，並且讓TSP透過詳細的金融資訊幫助消費者提供分析與建議；PIS則是讓TSP能夠代替消費者發起支付指令，簡化支付流程也提高應用性和方便性[19]；最後的CBPS也是一種支付服務，只是變成卡片形式，表示TSP能夠在取得授權後，代替消費者以卡片形式進行付款。

歐盟的資安標準最主要規範在PSD2的RTS中，但是歐盟的資安標準並未規範像英國開放銀行規範技術層面。RTS主要是以有關客戶認證和安全通信的資訊標準，這項標準將於2019年9月14日生效。該標準規定銀行和TSP應如何在提供消費者API時符合相關客戶認證與安全通信標準。RTS對於客戶認證的要求為SCA (Strong Customer Authentication)，是指客戶必須提供二項以上的認證機制。而在安全通信標準上則必須採用歐盟核可QWCA (Qualified Web Certification Authority)發行之憑證，再由銀行與TSP以TLS等級以上的通信傳輸進行資料交換。

澳洲

澳洲早在2014年便開始提倡資料分享的好處，並於2017年發布《Review into Open Banking in Australia》，開始推動消費者資料權(Consumer Data Right, CDR)，宣布消費者在交易和商品等數據可以交由第三方使用，實施順位以銀行最優先，接下來是能源、電信產業以及其他行業[20]。2018年澳洲修正《競爭與消費者法》，正式啟動開放銀行的建置計畫，並強制要求國內市佔共95%前四大銀行 必須加入開放銀行體系[21]。

> 澳洲四大銀為國民銀行、聯邦銀行、澳新銀行、西太平洋銀行。

澳洲在2018年5月25日宣布將API開放進程分成三個階段，目前四大主要銀行的完成進度包括第一階段商品相關的資料(2019年7月)、第二階段商品相關的資料(2020年2月)，以及第三階段商品相關的資料(2020年7月) [22]。至於全部資料的完成時間預計要到2021年7月才能夠開放完畢。澳洲的資訊安全規範是在消費者資料標準(Consumer Data Standard, CDS)規範，而 CDS是CDR的一部分，主要規定API、資料與安全的相關規定[23]。澳洲的資安標準是採歐盟與英國的標準整合而成。

新加坡

2016年新加坡金融管理局MAS和銀行公會發布《Finance-as-a-Service：API Playbook》(以下簡稱Playbook)，作為新加坡開放銀行的指導手冊。Playbook提出開放API的建議標準，並未強制要求業者遵循，由銀行自行決定開放哪些API，也可以自行決定合作夥伴。為了推動開放銀行，新加坡金融管理局轄下新成立了金融科技與創新部，負責開放API的相關業務。新加坡政府並未透過法令強制推動，而是發布Playbook來引導業者使用API技術及對應資安規範，此做法和香港類似。另外MAS與東盟銀行組織(ASEAN Bankers Association，ABA)、國際金融公司(International Finance Corporation，IFC)共同成立的東盟金融創新網路(ASEAN Financial Innovation Network，AFIN)也推出API Exchange (APIX)，作為一全球的開放架構API交換平台與市集[24]。

根據MAS官網2019年11月的資料，新加坡的API開放可分為交易、帳戶服務、銷售、產品、其他以及監管等六大種類。新加坡市場應用上最廣泛的API種類還是以交易和服務兩項為主[25]。依據新加坡Playbook[26] 規範，新加坡也是採用TLS與OAuth為主要API導入時的技術標準，主要也是依循英國Open Banking的技術規範。另外，新加坡於2018年推動「資料共享安排」機制（Data Sharing Arrangements, 下稱DSAs）與「可信任資料共享框架」（Trusted Data Sharing Framework），建構資料共享環境，帶動國內組織資料經濟發展與競爭力。而「可信任資料共享框架」的優勢在於：

1. 提升客戶體驗，創造新收入

機構間的數據交換可以提升對客戶需求的了解，並能夠提供客戶更相關的解決方案、體驗與優惠。如銀行選擇與電信公司(同時是數據提供者與數據使用者)進行雙

向的數據共享合作，目的為改善客戶體驗，並促進雙方的業務成果；雙方交換的數據可以用來深化對客戶的了解，並為客戶群體更符合需求的方案與服務；合作夥伴關係使雙方都能夠更好的預測並回應客戶不斷改變的消費動機與偏好，提供超越單一機構或產業的價值。

2. 提高供應鏈效率進而降低成本

供應鏈服務提供商藉由提供當前庫存的實時數據，使企業客戶能更容易掌握庫存狀況，優化貨物的周轉時間，並運用相關數據最佳化貨物的配送路線。如：一家本地中小企業推出了提供管理實時訂單與庫存的整合性平台，他不僅能夠幫助降低倉庫中滯銷或即期商品等不必要的庫存量，提高了貨物周轉率，也透過最小化數據輸入、電子郵件和電話往來，提高精準度與生產力，同時運用客戶的實時數據最佳化配送路線，使客戶受益。

3. 提供產業整體市場效率的綜合資訊

藉由彙整並提供產業中的資訊，提高市場整體效率。如：新加坡的CBS (Credit Bureau Singapore)是新加坡銀行協會(ABS)和Infocredit Holding Pte Ltd 的合資企業，《銀行法》允許CBS成員（主要是銀行）互相揭露和獲取信用相關信息，並交由CBS彙整，提供給信貸服務提供者（如：銀行），協助其更有效預測客戶還款的可能性，並提高對風險的評估能力。

美國

美國一直都是自由競爭市場的代表，在這樣的市場環境下，各家業者的競爭意識較為強烈，總是不斷推陳出新來吸引消費者並搶占市場。這樣的市場也讓美國對於開放銀行的推行方式不同於英國、歐盟，美國採用市場自由發展的方式來推動，而未強制要求銀行業者開放API，政府僅作為提供建議的角色，頒布指導原則做為業者的參考。例如2017年美國的金融保護局(United States Consumer Financial Protection Bureau, CFPB)曾針對網路爬蟲的做法頒布「消費者授權的資料存取權」九項指導原則。由此可見美國政府肯認可金融消費者確實擁有將資料授權予第三方業者使用之權利，雖然當時規定的是網路爬蟲方式而非開放API，但核心概念皆以消費者的資料可攜權為出發，實現消費者賦權[27]。

目前有多個組織同時進行制定API的標準以及範圍，例如部分銀行、金融科技業者自行組成的金融數據交換組織(Financial Data Exchange, FDX)，在2020年3月發布了FDX API的第四版更新，目的是加強串接的相互性並支援更廣泛的使用範圍[28]。另外，NACHA和Accenture合作成立的標準化API行業組織(API Standardization Industry Group, ASIG) 也試圖使美國金融服務業能有標準化的API使用[29]，開放的種類包括帳戶確認(Account Validation)、媒體交換自動轉帳支付服務(ACH Payment Initiation)、銀行連絡資訊(Bank Contact Information)、即時付款帳戶確認(Real-Time Billing Account Validation)、交易狀態(Transaction Status) APIs。依據NACHA和FDX分別發布的API標準，美國對於API的資安規範建議大有不同，且不具法令強制性，主要是以加入組織必須遵守的技術標準為主。彙整如下：

- NACHA建議的內容：比較像是研究報告，沒有真正提出建議的標準，目前內容僅提到架構採用RESTful APIs，而資料交換格式為以ISO 20022為標準的JSON格式。
- FDX僅針對API進行相關規範，並未建議資訊安全規範

保險存摺對保險市場的發展影響

「保險存摺」另一名稱為「保單存摺」，二者並無不同，雖市場上已習慣稱保單存摺，本報告均以保險存摺稱之。

1. 保險存摺衍生的新商機

從銷售端的角度而言，當業務員進行陌生招攬時，往往都需要先請客戶告知既有的保單狀況，以便幫客戶健檢保單，藉以瞭解對方的風險缺口，才可以規劃出更精準的風險規避建議。然而，客戶大多不會耗費心力蒐集保單並提供予業務端，導致業務員難以蒐集到保戶的投保狀況。未來若保單全面電子化，且若保險存摺服務推動順利，以上問題自然也能夠迎刃而解，對銷售也會有很大的幫助與改變。

保險存摺的出現讓保戶更完整了解擁有保單全貌，若需要保價金等詳細資料，保戶可以自行上各家保險公司查詢；對於保險經紀人、保險代理人來說，他們可以省下整理客戶保單的繁瑣，直接研究保險存摺上的商品即可提供相對應的服務。因此，對於業務單位而言，保險存摺的出現對於在開發客戶上無疑是個福音。保險經紀人對商品有更廣泛的了解，他們得以從客戶的需求出發，協助保戶找尋最合適的保單。

2. 擴大資訊價值開創保單數位健檢服務

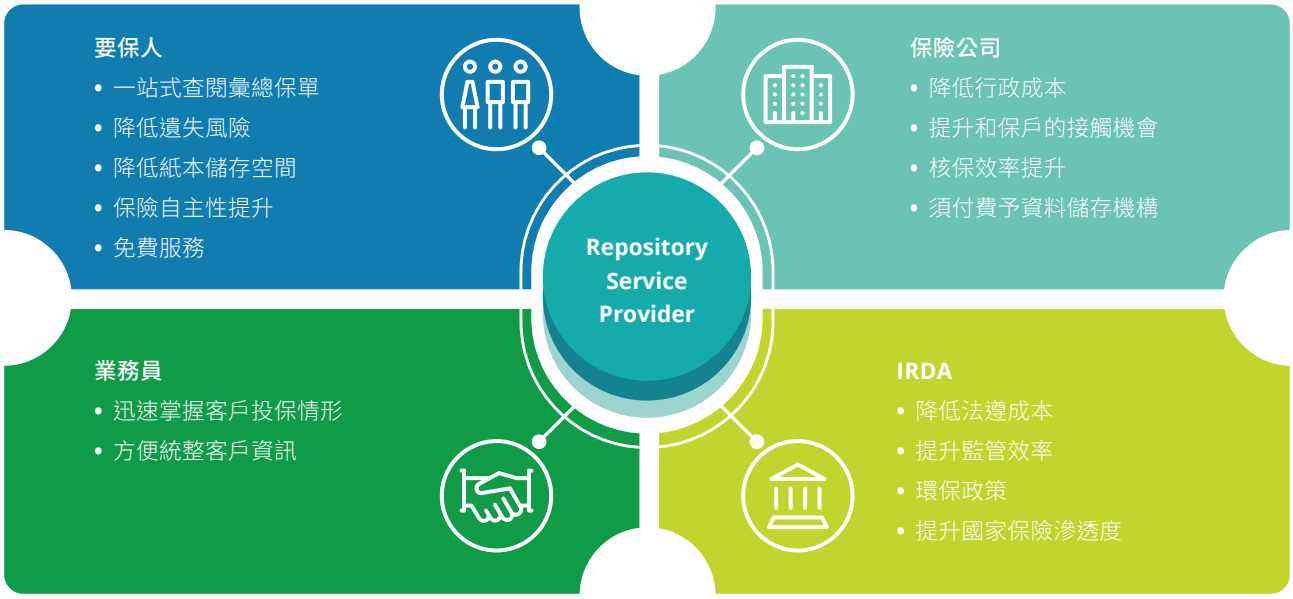
對於僅以單一公司商品進行招攬的傳統保險公司業務員來說，在保險存摺推動後，民眾可以更方便地取得各家保險公司的保單資訊，而他們所需要面對的保單健檢問題可能變得更多元。若保險公司能夠建立更全面的保單健檢機制，抑或是由業務員向第三方保單健檢服務軟體商購買保險健檢服務，都能協助傳統業務員進行保單健檢諮詢服務的更多解決方案。

3. 國外保險存摺案例

除了台灣順應保險科技的潮流開辦相關建設之外，國際上也有發展保險存摺的類似經驗。印度於2013年在主管機關的推動下，由政府委外制度的保險存摺平台。印度民眾保險意識興起較晚，因保險滲透率直至今日只有4.2%相較國際甚低。不僅如此，由於印度民眾教育水平差異較大，為提升購買保單的透明度、便利性以及降低保險公司與監管單位的法遵成本，印度政府在十年前即開始策畫類似保險存摺的集保機制。印度所開發的保險存摺服務，擔任起民眾與各保險公司聯絡的窗口，當保戶成功開設保險存摺後，他們便可逕行透過其查詢保單相關資訊，甚至進行特定保全服務[30]。

參與保險存摺的民眾除了享受保單查詢及更改服務外，存摺更建立了授權代表(Authorised Representative)的服務，「授權代表」由要保人指定，當要保人發生事故時，授權代表有權查閱要保人生前的投保情況。換句話說，授權代表的機制不僅讓家屬得以準確且迅速地向保險公司申請理賠，更同時顧及了要保人生前對保單財產的隱私疑慮。

圖4 印度保單及保險利害關係人圖



然而根據印度The Economic Times調查指出[31]，因為過去投保習慣使然、對數位服務不熟悉，以及對於該措施的不信任，即使保單存證制度推行已久，仍有高達80%的民眾偏好取得紙本保單，因而選擇不申請保單存證服務。

1. 類似保險存摺的新創服務

台灣-保險小存摺

保險小存摺是一款台灣CWMoney公司開發保單儲存APP服務，其主要服務特色有三，其一，拍照存取保單資訊，對於用戶來說，使用拍照讀取資訊省下自行輸入的繁瑣。其二，完整的視覺呈現；對要保人而言，當遇到保單數量過多的狀況下，用戶若能有清楚的視覺化以及以被保險人為類別歸類的功能，則能自主了解投保情形。其三，內建了保費繳交提醒及理財試算的服務，即使現階段部分資訊仍無法直接串接保險公司，但透過以上服務已能向用戶傳達相當清晰的投保輪廓。在台灣開放銀行政策啟動後，透過開放銀行第一階段，CWMoney以第三方服務公司(Third-Party Service Provider)與銀行合作串接開放API，提供記帳專業且完善的功能基礎上，打造記帳整合金融服務的新體驗，提供了更加個人化、多元的金融服務，可以更精準的在理財面提供用戶真正需要的資訊，未來將開放的個人帳戶資訊、支付開放，也將讓用戶掌握自己的財務資料應用權利。

香港-PortfoPlus

於香港成立發跡的PortfoPlus，發現到保戶難以自行理解保單條款及孤兒保單相當普遍的痛點，以及多數業務員認為要管理眾多客戶並非易事，因此開發了民眾使用版本以及顧問版本，兩者分別針對投保民眾及保險經紀人或代理人，前者免費後者須付月費。以一般民眾方案而言，民眾登記成為用戶之後，便可以輸入個人資料及其所擁有的保單資訊。不同於傳統的保單存放服務，除了提供民眾儲存、缺口分析及視覺化外，更有獨創的家庭共享保單資訊的功能，以備緊急狀況發生及時尋求協助。另一方面，顧問方案提供給希望管理客戶保單狀況的業務族群使用，一般用戶的保險顧問若同樣是PortfoPlus的會員，則PortfoPlus會將兩者的帳號串聯起來，讓業務端得以了解客戶的投保狀況。此外，PortfoPlus更協助業務端進行客戶的保單健檢服務，挖掘更多潛在業績。

新加坡-PolicyPal

PolicyPal是一間提供一般用戶保單整合的軟體公司，透過PolicyPal的服務，讓消費者可以從APP掌握其投保情形。除此之外，PolicyPal與市場上契約管理服務的不同之處有以下兩點，其一，其提供不同於自行輸入保單細項的儲存方式，使用者可以選擇使用APP所設置的相機上傳保單至管理服務當中。比起使用相機拍照上傳，此方式更加便捷，也減少了人為輸入錯誤而取得錯誤資訊

的風險。其二，PolicyPal也深知要保人的保險規劃很可能隨著年齡、人生規劃而有所改變，因此也提供了線上問卷以識別用戶的人生階段，以提供資訊讓用戶可自主了解潛在保險缺口。PolicyPal的保險營運角色以台灣的監管角度而言，可以稱其為所謂的「保險經紀人」，意即當用戶透過其服務了解保險缺口後，即能透過PolicyPal平台選購保險商品，其獲利來源便是用戶透過PolicyPal購買保險商品而取得的佣金。

小結

在保險存摺上路後，台灣消費者對於保險商品的購買習性若可以變得更加自主，相信網路通路的銷售商業模式在台灣也會有一塊獨特的市場。舉例而言，2014年印度推行保險存摺，在廣大的紅海市場當中，即有著B2C網路投保的成功案例。例如印度公司Policy Bazaar是知名的保單比較平台，目前已成為全世界規模最大的網路保險經紀人平台，探究其背後成功的因素，大致可以分為以下幾個因素，首先，該平台介面設計美觀、使用者體驗直覺且提供消費者背景知識輔以決策，不僅能夠透過網路足跡進一步分析客戶的需求，還以流暢的介面引導消費者直接線上投保，甚至提供各保險產品的價格與關鍵效益的比較分析。其次，保險經紀人的特色在於銷售許多不同公司得產品供與客戶比較選擇，隨著平台規模越大，所能銷售的商品就更多元，也因此可以吸引更多使用者加入。

台灣CWMoney也是一個例子，在開放銀行政策下，CWMoney扮演第三方服務公司角色，提供保險管家APP與銀行合作，讓用戶可以在APP中輕鬆試算保險產品價格、還能透過保險小存摺APP繳交保費，並推薦適合繳保費的信用卡等資訊。藉由開放API共享金融數據，提供更多元的普惠及便民服務，同時為金融產業注入新的活力。

純網路保險

1. 純網路保險公司特性

過去傳統保險業在產品研發、通路銷售、核保、理賠及服務等價值鏈的應用上，大都以線下方式進行為主，例如透過業務員銷售保險與人工核保及理賠等。而純網路保險(或稱數位保險公司Digital insurer) 則是利用網路或移動通訊等技術，透過數位通路(如自營網路平台、第三方網路平台或應用程式等)從商品報價、消費者購買保險、受理理賠等，進行部分甚至全部線上完成流程，並大部分以數位化方式進行營運。純網路保險高度利用數位工具技術與網路媒介強化客戶互動、數據可用性和業務流程，改變保險公司與客戶互動的方式[32]，盡可能透過社交媒體、聊天機器人和機器人顧問等新興通路銷售保險，並大量採用於自動化、標準化作業流程提高經營效率。

純網路保險與傳統保險商品主要差異，包括產品類型較多元、購買門檻較低、且無須透過業務員、代理人購買，價格可能更低，但純網路保險因需透過網路通路銷售，故網路通路及系統建置費用、以及促銷獲客的行銷成本也相對較高。

2. 國際純網保發展與案例

美國

1. 監理機構與規範

美國的保險監理主導權為各州監理機關所掌握，而各州之監理官共同組成國家保險監理官協會（National Association of Insurance Commissioners，NAIC）以統合各州監理官共同達成監理目的，包含建立法規指引和最佳實務標準，進行同儕評審，並協調其監理法規與措施。在監理上美國為州立法，對純網路保險公司並無特別規範或禁止事項，純網路保險之監理法規適用一般保險公司之監理法規。

2. 案例公司

Lemonade

2015年創立的Lemonade Insurance Company為美國紐約州核可之產物保險公司，Lemonade特色之一是將收取的保費中25%用於成本管理及本身獲利，剩下的75%在扣除保戶的理賠金額、稅金及保險費用後，所剩金額最高的40%可依保戶自由選擇的公益團體做捐贈就是所謂的回饋機制（Giveback）。Lemonade在保險科技的應用上分別透過AI機器人（Chatbot）Jim與Maya處理保戶的投保及理賠程序。透過AI最快兩分鐘就可以完成投保，而理賠申請視複雜程度由人工團隊及AI機器人一同處理，目前約有三分之一的理賠透過AI機器人即刻做出判斷。主要提供住宅保險，包含租客及自有宅保險，近期更推出寵物險與定期壽險的服務。Lemonade已 在2020年7月上市，成為保險科技獨角獸。

Oscar Health

Oscar Health於2012年創立，是位於美國紐約的網路健康險公司， Oscar Health分別針對個人、家庭、團體、企業及Medicare Advantage提供保險服務。主打流暢的線上體驗，透過簡單的介面設計，保戶可以輕鬆透過電腦或智慧型手機上的應用程式完成投保或申請理賠。保戶可以通過視頻聊天或電話，獲得基礎醫療保健的諮詢；保戶也可以借助Oscar的搜尋工具找到附近合作的醫生、醫院或藥房等進行免費諮詢。Oscar鼓勵客戶參與健康管理，並提供免費穿戴裝置，保戶每天步行達標可以獲得Amazon的商品卡。Oscar Health目前在美國9個州營運，2021年會員數約為529,000人，銷售險種主力為健康險。針對個人/家庭、團體、企業及Medicare Advantage提供不同方案。

中國大陸

1. 監理機關與規範

網路保險在中國稱為互聯網保險，中國的銀行保險監督管理委員會(簡稱銀保監會)主要統一監理銀行及保險業，維護其合法、穩健運作，並防止金融市場的風險，保護消費者合法權益。中國於2021年2月起實行「互聯網保險業務監管辦法」，純網路保險公司必須依此辦法運營，此辦法對互聯網保險的經營模式、風險控制、消費者保護等進行全面的監管。

2. 案例公司

眾安在線

眾安保險2013年由中國平安、騰訊、阿里巴巴創立，是中國第一家完全具備端到端保險的網路保險公司。目前用戶約4.6億人。2016年「眾安科技」為眾安成立的全資子公司，致力於研究和開發尖端技術。2017年9月眾安科技在香港上市，成為第一家在香港上市的金融科技公司籌集了1.5億美元。眾安保險目前是中國最大的互聯網保險公司，健康險、責任險、車險、意外險、旅平險都有銷售，更有銷售極具特色的創新保險商品，透過異業合作推出各種零碎化的保險商品，例如與輪胎業者合作的「輪胎意外保」、與3C品牌合作「步步保」、與電商業者合作「退貨運費險」。眾安的業務模式圍繞其對數據和分析的利用，以確保準確的產品定價和風險控制。

香港

1. 監理機構

香港保險業監理機關為保險監管局(Insurance Authority)，主要任務包含發放牌照、制定監管政策及促進全港保險業的發展及競爭力等等。純網路保險公司在香港仍被認為新保險領域，因此設立方式和一般保險公司不同， 2017年9月推出試驗計劃 - 快速通道（Fast Track）進行保險業務申請。除了設立規範不同外，其餘原則皆遵照保險業條例規定。而保監局也會針對條例規範中不適用於網路銷售的例外情況更改措施、豁免或增加一定的條件或限制。

2. 案例公司

保泰人壽（Bowtie）

2017年創立，2018年獲得壽險虛擬保險公司牌照，為香港第一家獲得牌照的純網路保險公司。線上投保的主力商品為人壽保險、意外保險、健康保險，其商品特色主打簡單、保障為主。由於保費中未含儲蓄性質，低保費可獲得高保障。不僅如此，其保險費採月繳制、且具有可隨時解約之特性，使客戶能隨時檢視自己的保障範圍並隨時調整，善用科技輔助，降低成本並回饋給保戶。此外保泰人壽也簡化了網路投保流程，告知事項採用選擇題方式，即時保費報價，並提供未來五年保費參考，五分鐘內可完成投保。保泰人壽線上平台可進行保單管理（查看持有保單、終止保單等）、更改信用卡資料、申請理賠等服務。

OneDegree

2016年8月創立，初期為科技公司，於2019年完成A輪融資，2020年4月獲得香港保險業監理局發出的一般保險虛擬保險公司牌照。主力險種為寵物險，秉持快速核保/理賠的原則，使用寵物年齡、品種、性別、體重計算保費。理賠方面則與多家獸醫合作，提出由網路獸醫看診最高理賠90%、實體獸醫理賠70%的計畫，最快理賠金兩天就能入帳，減少保戶經濟壓力。

日本

1. 監理機構

日本針對金融業監管採行混業監管，主要監管機關為金融廳。金融廳隊銀行業、證券業、保險業及非金融機構進行全面監管。而純網路保險在日本並無專法特別管理，純網路保險事業許可及監理亦同一般保險公司均由金融廳定之，日本金融廳以「保険会社向けの総合的な監督指針」六大項規定來進行綜合性保險的監理。日本於2006年將小額短期保險（少額短期保険業）納入《保険業法》中規定的保險業務。

2. 案例公司

LifeNet

2006年10月創立，後續獲得三井物產、新生銀行、Seven & I控股、Recruit投資，於2008年3月更名為LifeNet。主要透過網路銷售定期死亡保險、終身健康保險、基本醫療保險等壽險並提供相關資產管理服務，商品特色為簡單、容易理解且低價，並於網站揭露商品附加費用、純保費，利用動畫、視頻等各種網路的方式引導客戶完成投保。

Sony Assurance

1998年6月成立，並於1999年9月更名為Sony Assurance，開始透過網路行銷車險，目前為Sony Financial Holdings Inc. 100%持有。網路銷售車險（含UBI）、火災保險、醫療保險及旅平險，並與Anicom Insurance合作共同販售寵物險。銷售特點為替保戶提供多種保費折扣方式，例如首次購買保險最高折扣10000日圓的網路折扣、續約最高折扣2000日圓；不簽發紙本保單最高折扣500日圓的無紙化折扣；舊有保戶購買新保單最高折扣1000日圓。

新加坡

1. 監理機構

新加坡實施金融監理一元化，保險業與其他金融業皆是接受新加坡金融管理局（Monetary Authority of Singapore，MAS）之監管。新加坡金融管理局並未針對純網路保險公司設立專門監理法規，網路保險公司與一般保險公司相同，同受新加坡保險法（Insurance Act）規範，但2016年11月新加坡金融管理局頒布有關監理沙盒的準則。

2.案例公司

SingLife

SingLife在2017年6月拿到新加坡金融管理局頒布之保險執照，成為自1970年以來，第一家取得執照的保險公司，並於2020年與英國Aviva集團合併。SingLife作為一家新加坡保險科技公司，主要通過網路和行動設備，並善用政府主導的MyInfo平台，成為第一家串接該平台的當地壽險公司，為中小型企業、商家和個人提供全天候的網路保險金融服務，致力於為用戶提供簡單且安全的長期人壽和儲蓄解決方案。主力險種為壽險、癌症險、重大疾病險，並在近期推出儲蓄險。投保過程中只要填寫基本資料，五分鐘內可取得報價；另外只要準備手機、個人證件和信用卡，15分鐘內就可以完成購買流程，所有流程皆在網路上進行。

3. 純網路保險公司的類型

1. 科技團隊導向型

此類公司以科技技術為訴求，創立者大都擁有金融科技專業背景，輔以創新的商業模式或新型態商品，例如美國的Lemonade公司，強調以AI人工智慧增加整體保險購買流程的效率，凡舉投保至理賠，皆包含科技的應用。除此之外，Lemonade公司發展出的回饋機制為一種創新的商業模式，以保險結合慈善是市場上缺少的新概念。

香港OneDegree的商業模式十分相近。OneDegree集團（AI Financial Technology Holding Company）底下的子公司除了虛擬保險公司（OneDegree Hong Kong)為持有一般保險牌照的法律實體，也設有另一家保險科技子公司（OneDegree Global)，專門開發保險科技系統及平台，授權軟體給其他公司。除此之外，OneDegree在販售資安險的同時，不僅是單純將保險商品販售給企業，因為擁有保險科技子公司，可以同時販售資安相關系統，替客戶解決資安方面的問題。

2. 生態圈導向型

此類公司大都已有特定的客戶群，而保險是其中一項待完備生態圈的服務。通常這類型的純網路保險公司背後已有一個完整的生態圈或是基本潛在客戶群作為支持，例如中國的眾安在線股東阿里巴巴是中國最大的電商之一，擁有廣大的客戶資源，這些客戶可以成為眾安在線的消費者。旗下的淘寶更是國內最大的電子商務平台，淘寶交易便是很好的場景，此過程中衍生出大量的保險需求，例如支付安全險，退貨險等等，並且阿里巴巴掌握著大量用戶的交易記錄和信用紀錄，這也成為眾安在線研發新的保險產品的資料庫。這種模式下發展的公司自成立便擁有強大的客戶背景，也為它的發展奠定了基礎。香港的四家虛擬保險公司中，同樣擁有此背景的即為眾安人壽。

3. 傳統保險主導型

此類公司會和傳統保險公司合作，發展新型態保險商品。以香港Bowtie及Avo為例，在此兩家虛擬保險公司的背後都有傳統保險公司的投資，香港永明金融(Sun Life)是在2018年注資Bowtie的大股東，而亞洲金融集團（Asia Financial Group）的普通保險部門亞洲保險（Asia Insurance）擁有Avo 51%的股份，Avo的行政總裁同樣由大股東亞洲保險行政總裁黃子遜兼任。兩家虛擬保險皆有推出新型態的保險商品：Bowtie主打自願醫保而Avo則主推電子錢包險，但和OneDegree不同的是， Bowtie及Avo兩家虛擬保險公司比較不同的是，由於Bowtie是經營長期業務，保監局要求經營長期業務的虛擬保險公司須有一家傳統保險公司做為後備支援。

4. 各國純網保監理制度特色

在監理上，大部分國家對純網路保險公司並無特別規範或禁止事項，純網路保險之監理法規適用一般保險公司之監理法規。以下是幾個有特殊監理措施的案例:

- **日本: 為小額保險降低進入門檻調降設立資本額**
  針對銷售保額較低、風險較小的保險商品，且年保費收入在50億日元以下的小額短期保險公司，訂定較低的

公司成立門檻，其最低成立資本額為1000萬日元，並設立額外監理辦法《少額短期保険業者向けの監督指針》。

- **中國大陸: 為純網保訂定特別規範**
  將純網路保險稱為互聯網保險，並訂定《互聯網保險業務監管辦法》，明確定義互聯網保險公司的業務規則。銷售險種方面中國由銀保監會根據互聯網保險業務發展階段、不同保險產品的服務保障需要，規定保險機構通過互聯網銷售或提供保險經紀服務的險種範圍和相關條件。其他未規範之相關監管規定仍回歸中國保險法規定。

- **香港: 提供虛擬保險公司申請快速通道**
  推出試驗計劃《Fast Track》（快速通道）進行保險業務申請，Fast Track為申請人的新授權申請提供相對其他保險授權申請快速和精簡的流程，申請者必須擁有一套創新和穩健的商業模式，透過數位行銷，於產品開發、行銷、客戶服務和成本效益方面，為香港的消費者帶來益處，其他相關監管規範仍受《保險業條例》規定。

小結

參考各國發展虛擬保險公司狀況，可以發現純網路保險公司的經營模式往往是以客戶需求出發打造產品，發展客製化保險商品，並輔以新技術優化產品，持續增加與客戶之間的互動。金融科技伴隨而來的保險科技，將帶來保險價值鏈重建與用戶自主，以及保險串接裝置和用戶場景，產生了全新的市場需求，對此需要創新的商業模式、金融商品、行銷管道才能滿足，它不但已成為全球性現象，亦成為保險產業組織革新的跳板。

雖然純網路保險公司模式已是各國發展的重點趨勢，但目前受限於公司規模、機構落地服務能力等條件的限制，客戶層面相對仍窄，線上成交的保費規模也比較小，營運模式尚未發展成熟，仍在不斷探索和嘗試之中。以我國開放純網路銀行的例子來說，連線商業銀行與樂天銀行分別擁有通訊軟體LINE與樂天購物之龐大生態圈，同屬於生態圈導向型；而將來銀行則是有傳統金融業如兆豐國際商業銀行及新光人壽作為股東，可以被歸類於傳統保險主導型。可以從純網銀的經驗發現，台灣較缺乏第二類型科技導向型的新創公司。保險若能深入生活，包括支持小眾和未來企業的生存發展，發揮社會保障作用，開放純網路保險公司設立，促進整個保險產業的發展和繁榮，進而建立更全面的風險保障網路，覆蓋更多元的保險場景，實現更為廣泛的普惠金融服務。

金融資通安全

企業多年來一直面臨網路攻擊，加上新冠疫情肆虐，加速全球企業數位轉型、遠距工作和消費者行為的改變，然而同時也使網路威脅遽增。Deloitte《2021年全球風險調查》中，有87%的受訪者表示，在未來兩年內，提高組織的管理網絡安全風險的能力將成為非常重要的優先事項。世界經濟論壇（World Economic Forum, WEF）在其2022 Global Cybersecurity Outlook研究發現，八成的受訪者指出數位轉型是企業架構組織網路韌性的主要驅動力，凸顯數位轉型與資安兩者皆相當重要。

金融業科技發展蓬勃，在提升企業營運效率、強化客戶便利性與體驗的同時，也須一併建構資安體系，金管會在2020年8月發布「金融資安行動方案」，為期四年，期望能建立金融業資安治理能力，確保企業能有保有應變資安攻擊的韌性。然而全球資安攻擊的新聞層出不窮，除了政府政策的推動，企業可以再做哪些投入或投資，減少資安攻擊的影響呢?

1. 數位轉型趨勢和網路風險

企業積極地進行數位轉型和上雲佈局，不僅可以提高效率，隨著資訊與數據在組織間流動，還可以創造新型價值、連接不同的業務和豐富客戶體驗， Deloitte《2021年網路資安調查》中，有94%的受訪者表示正在考慮將其財務系統或企業資源規劃 (ERP) 搬遷至雲端。然而，COVID-19襲捲迅速改變了我們的工作環境，大大小小組織增加網路的運用，也因此擴大網路攻擊的機會。Deloitte《2021年網路資安研究調查》有69%來自不同產業和地區的受訪者表示2020 年初至 2021 年中，網路攻擊對其業務的威脅有顯著增加，高階經理人表示影響企業最大部分是營運中斷(32%)，其次是智慧財產權竊盜侵權 (22%) 和股價下跌 (19%)。

台灣去年(2021)發生16件上市櫃公司資安事件，以產業別進行分析，高科技佔56%，製造業佔25%，零售服務及文創佔6%，金融保險業佔3%，其他產業佔10%[33]。網路攻擊千變萬化，例如透過AI來偽造數位圖像、影像或聲音，並冒充他人的Deepfake，2019年一間英國能源公司被駭客以AI合成的語音，冒充CEO成功詐騙該公司員工電匯22萬歐元給虛構供應商[34]。 雖然Deepfake詐騙目前仍是一個相對較新的威脅，但在 2017年至2019年期間，年成長超過900%，企業在2020年約損失超過 2.5億美元。企業在數位轉型的道路上正面臨重要資安挑戰。

什麼最能滿足當今網路安全的需求？哪些是資安解決方案的最有效投資？儘管許多領導者了解網路安全面臨的風險與威脅，在2015年至2020年間，每年至少有2000件數位信任相關的專利申請，但卻發現領導者很難抉擇適合的解決方案來為企業增強網絡安全措施。

企業營運如履薄冰，踏錯任何一步都將會影響客戶忠誠度、財務業績、品牌聲譽，並最終破壞組織建構和維護信任的能力。Deloitte調查說明81%的消費者在企業發生違規後，會失去對品牌的信任，而25%的消費者則會完全停止使用或購買該品牌服務和產品。隨著疫情大流行，企業加速在數位化基礎設施、推動新興技術安全方案的支出，風險跟著變得更高，因此資安的重要性近年來逐漸提升。

2.資安的重要性

網路威脅管理是金融機構的主要優先事項，世界各地的政府和監管機構持續將資訊安全作為重點發展項目。2018年國際貨幣基金組織(IMF)對50個國家的網路攻擊造成的潛在損失進行分析，發現金融機構的年損失可能達到2700億美元至3500億美元，大約是銀行淨收入的50%，並且可能對企業造成系統性的影響。

VMware Carbon Black研究2020年2月至2020年 4 月期間，由於COVID-19許多員工開始遠距工作，發現美國主要金融機構的網路攻擊大幅增加[35]。鑑於與COVID-19爆發相關的網絡犯罪顯著增加，紐約州金融服務署於2020年4月發布了新的通知，強調網絡犯罪顯著增加，應注意危害網路安全的新領域[36]。勤業眾信與

政大金融科技研究中心發布的《2021台灣金融科技趨勢展望》，也有指出提升資安能力是金融科技創新發展的必要條件，例如保險業的遠距視訊核保的需求，隨著企業依賴資訊程度愈來愈高，提升資安勢在必行。

儘管Deloitte《2021年全球風險調查》中有61%的受訪者認為他們的機構在整體管理網絡安全風險方面非常有效，公司仍然高度關注企業的網路安全。87%的受訪企業甚至表示，提高管理網絡安全風險的能力，仍是企業未來兩年內首要進行的事項。另外，商業環境的波動和消費者行為不斷改變的情況下，67%受訪者認為企業在日新月異的業務需求中，想要持續保持產業領先地位相當具有挑戰性。隨著各行各業的公司都在努力保護其營運免受駭客和其他網絡攻擊，金融服務機構與科技公司，甚至其他產業的資安人才競爭極為激烈，有57%受訪者表示延攬資安相關人才是相當大的考驗，從此得知企業在保護自己免受不斷演變的網路威脅面臨多方的挑戰。

3. 國際資安政策

美國和歐盟為了應對大規模資安事件，近年分別籌組跨政府與企業、跨國的合作組織共同打擊網路威脅，還有訂定網路安全相關法令，嚴加規範資通安全。美國網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）於2021年8月宣布成立聯合網路防禦協作機制（Joint Cyber Defense Collaborative, JCDC），由具代表性的聯邦政府單位所組成，包括國土安全部、FBI等，公私部門協力合作，整合網路防禦能力，共同抵禦關鍵基礎設施的惡意網路攻擊[37]。

歐盟執委會（European Commission，EC）於2021年年中提議建立聯合網路機構(Joint Cyber Unit)，成立跨歐盟之資安事件應變團隊，成員國遭受網路攻擊時可以獲得該機構和歐盟的支援，同時也能分享歐盟情資資源[38]。

另外，今年5月歐洲議會於通過歐盟執委會在2020年提出的《網路暨資訊系統安全》（Security of Network and Information Systems）修訂指令NIS 2 Directive，提高網路安全風險管理措施與報告義務的標準，影響產業包含能源、運輸、水力、金融、健康醫療與數位基礎建設等領域，業者必須採取適當的安全措施，並在發生重大資安事件時通報有關單位[39]。

台灣金融業科技與政策發展現況

資料共享

1. 金管會開放銀行與資料共享政策發展

台灣開放銀行於2019年6月啟動，金管會比照香港採用以不修法、不強制的模式，由銀行與第三方業者合作推動，並將推動進程分成三大階段：[40]

- 第一階段：公開資料查詢。目前已開放業者測試，如比價網之類的第三方平台，可透過API串接各銀行的商品資訊，像是定存利率、貨幣匯率、房貸利率等，民眾可直接在網站中，比較各銀行的利率。
- 第二階段：消費者資料查詢。包含帳戶開戶與附屬業務申請、信用卡及附屬業務申請、消費者個人資料查詢等。用戶可以將個人資料打包帶走，例如在A銀行填寫過的個人金融資料，可以直接拿去申請B銀行的戶頭，不必重複填寫資料。
- 第三階段：交易面資訊。包含貸款清償、扣帳授權等。用戶可以透過第三方業者的App，直接連結帳戶扣款、消費支付，以及整合不同帳戶的資金。

為推動開放銀行，金管會委託財金公司，協同銀行和第三方業者參與討論，並交由財金公司制訂API標準，圖 5整理台灣開放銀行推動進程。

圖 5 「開放API」業務推動進程[41]

已完成

- 邀集42家金融機構成立「開放API研究暨應用發展委員會」。
- 完成「公開資料查詢」暨觸及資安標準制定。
- 完成「開放API平台」系統建置。
- 協助金融機構及TSP業者正式營運上線。

進行中

- 偕同「政大金融科技研究中心」及「金融創新科技園區Fintech Space」等新創聚落舉辦多場TSP業者座談會，蒐集TSP業者意見。
- 完成第二階段「消費者資訊查詢」技術及資安標準制定。
- 協助先導銀行辦理業務申請試辦事宜。

規劃中

- 持續觀察國際情勢、蒐集金融機構、產業界及學界需求及意見，滾動式增訂技術規格、完備資安規範及相關作業。
- 配合主管機關核定進程及金融機構與合作TSP業者時程，辦理第三階段標準制定作業。
- 協助金融機構後續「開放API平台」API上架及測試上線作業。

資料來源: 財金公司，2020年5月26日政治大學金融科技研究中心OPEN API 技術合規與測試說明[41]

第一階段的API已在 2019 年 10 月 16 日上線，總計有 25 家金融機構與 7 家第三方服務業者 (TSP) 加入開放。根據財金公司公佈的規格，第一階段開放的API總數有18支，而API類型分成存款、貸款、投資理財、其他銀行服務四大類。而開放銀行第二階段「消費者資訊查詢」，金管會於 2020 年底啟動，核准華銀、元大、中信、兆豐、一銀及國泰世華等六家銀行與集保中心合作案，以及遠東銀行與遠傳電信合作案，由銀行辦理消費者資訊查詢業務，而集保中心和遠傳電信扮演第三方服務業者 (TSP) 的角色。至於第三階段「交易面資訊」，將依時程完成技術與資安標準訂定，持續推動。整體來說，台灣已進入開放銀行第二階段的進程，並朝第三階段開放交易資訊逐步邁進，希望透過讓客戶直接使用 App 連結帳戶扣款、支付帳戶資金，完善金融創新服務的數位生態系。

同時為了降低現行TSP無主管機關監理、金融機構須自行篩選TSP業者的風險，於2018年協調周邊單位針對與金融機構合作的TSP業者建立資訊揭露制度，揭露項目包含TSP基本資料、合作業務項目等，增加TSP業者的透明度，提供外界及其他金融機構參考。

此外，金管會於2021年底頒布之「金融機構間資料共享指引」，其目的主要可分為三個：風險控管、便民以及促進跨業合作，從過去金控與子公司之間的共同行銷模式到現在資料的共享模式，前述三項目的在於深化資料的運用價值及強化未來的客戶體驗。在風險控管中，仰賴著金融機構的內控機制，並規劃在認識客戶(KYC)、洗錢防制(AML)等都能做到控管；在便民服務中，則是希望能透過數位身分認證減少重複簽署的繁瑣程序，並透過建立資料庫與數據中心，進而達到精準的行銷與商品定價；在促進跨業合作的目的中，希望透過不同產業別的資料共享，發展新的商業模式與建立金融生態圈。

目前可以共享的資料範圍，資料共享指引的第六、七點將客戶可同意共享之資料範圍分為九種，客戶可就不同資料來選擇是否共享：客戶基本資料、身分核驗資料、帳戶資料、金融商品或服務的交易記錄、負面資訊、認識客戶 (KYC) 資料及金融機構加值過後的資料、電子通訊歷程記錄 (防詐欺)、其他經客戶與合作金融機構同意共享的資料。

鑒於客戶授權採用逐次同意的方式，因此客戶可就不同類型或不同應用需求的資料形式分別同意授權。另外，金管會為落實金融機構內控制度，在辦理資料共享時不需向金管會申請核准。現今資料共享的開放僅為第一階段，並適用下列三種對象：金融控股公司集團、非屬金融控股公司之金融集團、非屬前兩類之金融機構間，待資料共享的基礎建設、資訊安全及資料授權與使用的信任基礎成熟後，再於第二階段逐步開放金融集團下的非金融機構納入資料共享的對象。

2. 金融機構間資料共享 (跨銀行、保險、證券)

在主管機關頒布「金融機構間資料共享指引」後，金控內應事先取得客戶同意，得以透過指引在金控集團內進行跨子公司的資料共享。從過去金控與其子公司有共同行銷的策略，到現在基於業務合作、便民以及風險控管的目的，有了更明確的資料共享應用目的與架構，然而，各子公司之間的因業務種類不同，且為了降低重複建模資源之成本、增加交查比對之使用性、建立大數據模型以及預先處理風險的效益等，配合現行已發展出可供分享資料卻不違反客戶隱私權之技術，已於金融科技發展路徑圖推動事項2-3中，研擬在子公司管理客戶風險等特定目的下，開放金控與其子公司間得共同建立客戶資料庫及風險評估模型，進而產生金控內資料共享之綜效。

3.金融市場跨機構間資料共享

金融市場跨機構間的資料來源，除來自最廣為人知的銀行、保險公司等大型金融機構外，還有聯徵中心、財金公司等其他特許周邊單位，另外就是來自非金融機構如：金融新創業者、區塊鏈業者、TSP業者，都正在大量快速累積資料。金融服務不再由傳統、單一金融機構提供，跨機構的資料共享不僅能降低機構各自蒐集KYC的成本，也可避免許多非金融機構在資源難以取得的草創階段中，被排除在聯徵中心開放對象外，進而耗費大量蒐集客戶KYC及信用資料之成本。故金管會預計逐步在符合個資法、客戶同意與合理使用目的範圍的前提下，開放可跨機構分享客戶資訊，並為確保風險可控及保障消費者權益，修正相關法規並訂定配套措施。

目前現行法規開放之金融市場跨機構資料共享對象多侷限於金融事業間，如聯徵中心得向金融機構及金融相關事業單位蒐集、處理各類信用資料後，提供予依主

管機關指定之金融相關事業在申請加入聯徵中心會員後查詢使用，然其開放對象尚不包含非金融機構，是備受外界期待主管機關能跨機構資料共享之對象；另外如聯卡中心已建置「信用卡輔助持卡人身分驗證平台」，將研議擴大適用範圍至保險業者及 TSP 業者。

4. 跨產業、跨市場客戶資料共享的相關機制與規範

當金融服務發生的場景不再只限於金融機構，實現場景金融的重要基礎除了金融數據，也需要其他市場的數據加入，包含電信業、醫療業、電商等，才能在各個場域內進一步貼近並滿足消費者的需求，提升整體市場效率與動能，並建立金融場景生態系。因此，日前金管會也依據行政院2019年所推行的「智慧政府行動方案」，與國發會合作，共同推動「數位服務個人化」如Mydata平台並應用於金融領域，使金融市場服務者可以在獲得當事人的同意後，在平台上取得所需之跨市場、跨產業數據，並鼓勵該服務提供者成為平台上的數據提供者。

保險存摺

1. 台灣保險存摺發展背景

2021年立法院質詢金管會推動「電子保單的推動」進度，希望能更快讓民眾可以用更方便、更環保的方式取得保單資訊，壽險公司販售許多保單耗用大量紙張，不僅收納不易還會造成環境資源浪費。此外，考量到民眾可能會有遺失保單的情形，為了讓民眾能運用數位資源更便利地了解自身投保狀況，在金管會的推動下，促成台灣「保險存摺 」制度的誕生。

保險存摺不僅複製了銀行存摺的概念，更進一步彙整客戶在每一間保險公司的投保商品資訊，可讓民眾清楚地看到自己的保單保障內容。保險存摺也代表更彈性的保單存放與讀取服務，透過在公正、獨立的第三方平台上匯集電子保單紀錄，當要保人或被保險人有需求時，即可自行登入平台查詢。此外，過去推行電子保單對於保險存摺有順水推舟的效果，而隨著更多業者皆採用發行電子保單後，保險存摺的便利性也會更加提升。因此，金管會要求所有的保險業者必須於2022年底前開放客戶選擇以電子保單出單。

2. 台灣保險存摺推動現況

產壽險之保單性質及資料儲存單位本就有所不同，因此保險存摺查詢平台將會分成「人身保險」與「財產保險」兩部分。人身保險的保險存摺早在2020年時就納入由壽險公會統籌建置的「保險業科技共享平台」中，而所謂「保險業科技共享平台」整合了壽險業保險資訊通報系統的資料，以及各式與壽險業相關的便民服務提供一站式服務。而財產保險部分，由於保險事業發展中心(簡稱保發中心)過去是強制汽車責任險資料庫的儲存機構，在具備完備資料量的背景下，由保發中心建置汽機車保險之查詢將會更有效率。因此人壽保險保單歸由壽險公會負責保險存摺服務，財產保險保單則由保發中心辦理。

目前壽險保險存摺由壽險公會推動，規劃以兩種型態推出於大眾面前，第一種的Web網路版本於2022年6月上路；另一種形式為手機等行動裝置APP的軟體服務，規劃於2022年第四季上線。

保發中心因為擁有儲存強制險保單資料的經驗，因此產險保險存摺則由保發中心與產險公會共同推動，產險公司提供保險存摺中的資料，最後由保發中心彙整於保險存摺平台，預計於2022年底前完成建置工作。

今年6月1日「保險存摺」已正式上線，由壽險公會偕同產險公會、22家壽險、14家產險及中華電信、台灣網路認證公司等合作廠商，在現行保險科技運用共享平台的基礎上建置「保險存摺」平台。因此，6月1日以後，民眾透過保險存摺平台可以查詢以本人為要保人或被保險人的所有人身保險已投保狀況，掌握自己投保情形，免除整理、保存的不便，凡已成年具完全行為能力者，均可藉由自然人憑證、晶片金融卡、強化版行動身分識別（即強化版MID）擇一進行註冊成為保險存摺會員。保險存摺又分為普通會員及白金會員，普通會員免費，享有保單總覽功能；白金會員要繳交年費新台幣100元，可瀏覽所有保單資訊，且可於一年內不限次數完整查看所有保單資料，包含保險公司名稱、險種分類、保單險種、商品名稱、保單號碼、契約生效日期、保額以及保單是否有效、要或被保險人資料等，並可下載保單資料PDF檔。

為提供保險存摺白金會員更優質服務，壽險公會表示，預計今年11月將推出保險存摺APP，搭載保險業身分驗證中心功能，屆時白金會員將可透過FACE ID或指紋快速登入，並可介接至線上申請保險理賠、查詢保險理賠聯盟鏈或保險理賠醫起通案件申請轉送進度，提供民眾更便捷的保險服務。

3. 保險存摺功能

以壽險保險存摺為例，民眾從保險存摺平台中可取得資訊包含：要保人、被保人資料、險種名稱、主附約屬性、承保保險公司、保額、保險狀態為有效/失效、契約生效/滿期日期、電子保單存證等資訊。電子保單存證的必要性在於，民眾在遇到保單條款爭議時，無法提供或難以確認保險公司所提供紙本文字。因此，此時由公正第三方單位保存的電子保單，讓民眾即使不信任保險公司，也能逕自申請保單內容。此外當該保單為電子保

單，可獲得區塊鏈存證的Hash值，作為辨認保單真偽的驗證。

由於保單種類繁多，不同類型的商品便會有各式各樣的重要資訊，因此以上揭露的資訊僅涵蓋部分資訊。下一步將再視民眾對於保險存摺的需求、主管機關法令及各保險公司的資料配合情形，再考慮擴充像是保費、保價金等等其他資訊。民眾若要查詢其擁有的保單須付費申請，除本人可查詢外，其他被授權人或親屬也可以查詢。依照目前保險存摺的功能規劃，未來平台上僅容許身為「被保險人」或「要保人」的民眾可以查詢其保單資訊。

又以產險保險存摺為例，以產險公司簽發之財產保險保單為主，被保險人則以自然人為限，查詢險種含括強制汽車責任保險、任意汽車保險、住宅火災保險及其他屬自然人投保之險種，所顯示之查詢結果以保單重要資訊為主，包含投保公司、險種類別、保單號碼、保險標的、保險期間等。平台提供民眾查詢財產保險保單重要資訊，有助於民眾同時掌握於不同產險公司之投保狀況，符合普惠金融之政策目標。

4. 壽險保險存摺之共享平台服務與技術

保險存摺服務設計的核心價值是「簡單」、「直覺」、「服務多元」，視覺設計採儀表板等視覺化圖像讓使用者方便使用。壽險保險存摺的服務包含在「保險科技運用共享平台」中，壽險共享平台提供的平台服務、存證服務和保戶服務的三大類服務如下:

- 平台服務：包括保全/理賠聯盟鏈 (保險同業間的資料互通)，理賠醫起通 (醫院及保險業的資料互通)。
  - 「保全/理賠聯盟鏈」提供一站式變更服務，保戶可透過保險公司網站、APP或行動服務進行單一窗口申請，向任一家投保保險公司申請契約個人資料，以「單一申請，資料互通」的概念，授權受理申請的保險公司透過平台推播至客戶投保之其他保險公司。運用單次理賠申請，完成對所有投保公司相同事項的申請手續， 改變過往必須向各保險公司分別提出申請的程序，增加保戶的便利性。保全聯盟鏈目前可透過兩種方式進行，第一種是透過業務員的協助進行行動保全，第二種是保戶透過官網自主交易。理賠聯盟鏈保戶透過保險公司網站、APP或行動服務進行單一窗口申請，再由保險公司透過聯盟鏈傳送申請資料到共用平台供其他同業使用。
  - 理賠醫起通: 過往保險公司的理賠申請是經由醫院跟單一保險公司串接資料，但由於醫院的意願低，而且建置成本會相當高，現行規劃醫院的資料將跟共享平台直接介接。在民眾授權下，保險公司可以取得就診醫院所開出的診斷證明，加速理賠流程。理賠醫起通服務合作醫院跨及北、中、南且數量超過20家。
- 存證服務：電子保單存證服務自2020年12月起上線。透過區塊鏈與數位簽章等技術建立電子保單存證服務。主要功能是確認保單真偽，經由保險科技共享平台存儲資料在區塊鏈上進行驗證及存證，紀錄投保與異動(保全)歷程。保戶可透過平台驗證確認投保內容，爭議發生時協助釐清事實。
- 保戶服務：蒐集保險業通報資料，建立可信的存摺服務。結合壽險公會通報系統整合保戶電子保單投保資料，保戶可以清楚了解投保資料總覽，協助進行保單檢視，進而了解保障缺口。因此，搭載保險存摺服務的保險科技共享平台除了得以查詢保單，更加入了不少便民的服務。平台將搭載FIDO2的身分辨識技術，而該技術背後有相對應的法規，因此目前並未開放由第三人查詢的管道。但平台也考量到民眾大多會向他人諮詢保險需求，保險存摺會提供經過電子簽章處理的PDF檔下載，本人仍可自平台上將保險存摺單據下載後傳與他人。
- 「保險科技運用共享平台」提供之綜合型服務，目前使用的普及度不是很高。未來運作成功與否關鍵在保戶的數位身分認證流程。共用平台、保險業者、平台上的第三方 (如醫院) 必須能夠提供安全又便捷的數位身分認證機制，例如不需要帳號密碼的FIDO技術 (目前已經考慮使用符合 W3C 標準的FIDO2，FIDO2是FIDO諸多標準中的一種) ，預期金融FIDO技術普及後，「保險科技運用共享平台」的效益將大幅的提升。

純網路保險

金管會2019年開放設立純網路銀行，並發放三張純網路銀行執照，目前純網路銀行都已陸續開業上路。金管會於2021年底再宣布開放設立純網路保險公司，期待能為台灣保險業帶來鯰魚效應。

台灣保險市場特色

1.保險滲透度高

台灣保險市場長期滲透度在世界皆是名列前茅，根據Swiss Re報告顯示，2019年之前台灣的保險滲透度多年高居全球第一，2020年為全球第二僅次於香港。因此，台灣的保險市場已處於成熟狀態，若要開發新客戶，目標客群較可能是在20至35歲間數位原生族群，首次或初期的保險需求者。

2. 網路投保興起但仍非主流

2021年台灣的網路投保有明顯成長，壽險網路保單銷售13.2萬件，產險網路保單銷售287.5萬件，總件數300.7萬件，與2020相比增加56.5%。尤其產險網路保單銷售是同期間壽險的21倍以上成長近64%。另從新契約保費收入來看，網路投保產壽險合計為新臺幣27.78億元年成長約16%；產險業全年新契約保費收入是23億元年成長38%，壽險只有4.78億元年衰退34%[43]。

整體而言，2021年台灣壽險業總保費收入2兆971億元的市場，但網路保險業務僅佔其中的0.07%；產險方面2021年台灣產險業整體簽單保費2,074億元，網路保險業務只佔其中的1%。可見目前台灣傳統投保模式仍佔有絕對的市場地位，網路投保仍處於發展前期階段，預期未來應有很大成長空間。

目前台灣消費型態逐漸走向線上購物趨勢，且手機將成為日後網路購物消費的主流。相關報告指出[42]，有將近60%的保險客戶願意從新保險公司或其他新興通路購買保單，而數位原生代願意轉換通路的消費者比例最大，疫情後更增加到80%以上。相較於傳統保險，純網路保險經營方式及產品特性更具高度的靈活性，預期有機會吸引這群數位原生代填補市場新需求。

3. 傳統保險公司數位轉型仍具挑戰

為因應金融科技潮流，台灣保險業近年來已逐漸展開數位轉型布局，但仍遇到以下的挑戰：

- **創新開發能量不足**
  保險業開發創新產品的能力尚待強化，對既有產品做優化改善的案例較為常見，即使推出全新產品，常因開發週期過長無法因應瞬息萬變的市場需求。
- **行銷通路業務衝突**
  多數保險業者認為既有傳統業務員通路與網路投保通路二者間，存在「此消彼長」的競爭態勢，網路投保因為與龐大業務員通路之間，潛在通路衝突的顧慮，導致傳統保險公司投資數位通路之經營政策受到限制。
- **資料整合與數位化緩慢**
  由於數位轉型不僅需要大量資訊人才與資源投入，更需要組織改變及工作文化轉型意願。相較於國際保險市場，台灣保險業進行金融科技數位化的基礎建設改革速度較為緩慢，加上個人資料保護法令嚴格，導致創新商品與創新客戶服務都不易落實。

台灣開放純網路保險公司之監理方向

金管會公布開放純網保的理由主要有五大項，一、滿足數位時代民眾保險需求。二、推廣創新商品。三、擴大保險保障。四、加速保險產業數位轉型。五、建構直接銷售通路。依據金管會2021年12月發佈規劃，以及金管會後續舉行之純網路保險申設公聽會，相關重要的規範方向如下：

1. 資本額

純網保產險最低資本額要求為10億元；至於純網路壽險則最低資本額要求為20億元。必須依保險法136條例辦理公開發行，除非是單一股東，否則無論公司規模大小都要公開發行。

2. 股東結構

國外金融機構與國外保險公司都可來申請設立純網保，

但須符合外資規範及經投審會核准。發起人條件須有金融科技業股東，但並沒有最低持股限制不過也不可以是零，即一定要有科技業持股，金融業者則必須要持股40%以上、其中一定要有一家保險公司或有保險子公司之金控持股逾25%。

3. 營業方式

純網路保險公司除了總公司及客戶服務中心之外，將不得成立任何其他實體營業據點。客服人員不需有招攬人員身份，可以解說商品但不能招攬。

4. 產品與業務範圍

純網路產險者，業務範圍需以符合消費需求的一年期或短年期創新產品為主，例如共用運輸工具、外送平台等碎片型保險商品；至於純網路壽險的業務範圍，則以不含生存給付或滿期給付的保障型商品為主，純網保壽險保障型商品無年期限制，長照險未含滿期金，純網保亦可銷售。

現行保險公司網路投保依據產壽險業務別，開放不同投保險種。壽險開放種類包含旅平險、傷害險、定期壽險、實支實付健康險、傳統年金險、利率變動型年金險、投資型年金、生死合險等險種；產險除傷害險或健康險的綜合險，大多險種已開放，包括汽車保險 (含強制險、任意險)、住宅火險及基本地震保險、旅平險、傷害險、定期壽險、健康保險、年金險等。成立純網路產險者，業務範圍需以符合消費需求的一年期或短年期創新型產品為主，申請設立時就要經金管會核准，與現行保險公司網路投保有差異。而產險業目前要開辦健康險與傷害險，必須有過去一年營運績效，但新設立的純網保公司若要經營健康險與傷害險，保險局承諾會調整法規，不會要求過去經營經績效。

純網保會設投保限額，是因核保、商品及客戶必須限額管控風險，也要查詢通報系統。此外，純網保並未限制法人投保，相對應的法規將視營運模式創新，及對法人身份認證模式是否符合規定。預計修改保險業投資保險相關事業管理辦法，允許純網路保險公司的營業項目中增加技術輸出。

5. 商品審查

台灣的保險商品之審查規定有許多限制。銷售前必須遵守「保險商品銷售前程序作業準則」，無論人身或財產純網保商品皆需要事先送審，若現行保險公司若要作同類商品，也要求採審查制不能採備查。審查內容包含商品名稱、核准方式、費率等等相關規定。純網保的保單附加費用上限可能比現行保單高，主要是純網保沒有業務員銷售，不必給付佣金，但可能需要異業結盟等，在非直接費用上可能比較高，保險局承諾會依商品來審查及調整附加費用規定。

6. 資訊安全

資訊安全無疑是純網路保險公司最該注意的部分。純網保系統可架在雲端，只要符合委外規範、資安風險管理便可辦理。我國保險業資訊安全要求主要規範別明訂於「保險業辦理電子商務應注意事項」、「保險業辦理電子商務自律規範」及中華民國人壽保險商業同業公會與中華民國產物保險商業同業公會聯合頒布之「保險業辦理資訊安全防護自律規範」。

7. 監理規範

其餘風險管控及監理原則，與現有法規及監理要求相同適用[44]。

金融資通安全

台灣資安政策

行政院自2001頒布「建立我國通資訊基礎建設」，並成立資安會報，從政府開始推動安全的資訊通訊環境，每四年做階段性的發展政策，並由政府單位拓展到民間機構和企業，目前2022年為第六期「國家資通安全發展方案」，期望能增強企業與民間韌性能量與資通安全。

金融科技快速發展，數位服務持續地創新與開放，金融監督管理委員會在2020年啟動「金融資安行動方案」計畫，打造金融產業內部資安組織文化，並建立組織資安治理、導入零信任架構和落實資安聯防，建置更完整的情資系統，結合F-ISAC、F-CERT、F-SOC，以期望能達到系統化應變措施和及時間監控能力，深化金融韌性。金管會考量大型或從事電子商務的上市櫃公司資安防護日益重要，在去年(2021年)11月宣布，要求符合一定條件的上市櫃公司須設立資安長、資安主管等，若規模達百億元以上，及主要經營電商的上市櫃公司，皆須在今年底(2022)前設置完成，符合條件的金融機構包含38家銀行、8家保險公司、13家券商、2家期貨商、4家投信都要設資安長[45]。同年2021年12月，證券交易所和證券櫃檯買賣中心發布「上市上櫃公司資通安全管控指引」，並從三大面向著手: 資訊公開、公司治理、及監理協助。隨著近幾年資安事件頻傳，許多單位紛紛發布資安強化政策。

除了政府單位以外，國內14家來自不同產業的上市櫃企業共同宣布成立「臺灣資安主管聯盟」，首任會長為華碩集團資安長金慶柏擔任，主要目標為資安主管核心能力養成、專業資安人才培訓整備、資安產業服務能量鏈結及資安治理合規制度建立[46]。

台灣金融業的挑戰與困難

資料共享

本研究訪談多家金融業者，彙整在「金融機構間資料共享指引」頒布後，業者目前在資料共享的觀察與實務執行挑戰如下：

1.「金融機構間資料共享指引」雖提升客戶便利性但卻降低客戶體驗

若客戶授權金融機構進行資料共享，在目前的資料共享指引下，除改變了資料單向開放的限制，也可以體現在減少客戶反覆輸入資料之方便性。但是，因缺乏金控架構下建置統一資料庫，客戶已在金控下子公司註冊身分後，若欲取得其他子公司業務服務時，客戶就得進行重複的身分驗證、資料輸入與逐次同意，因此客戶體驗的提升依然有限。關於取得客戶同意，如何在充分揭露授權目的的前提下，以淺顯易懂的文字或方式讓客戶同意資料授權，且後續處理逐項同意與否的數據，現行授權的管理模式尚有改善的空間。另外，針對現行客戶授權的作法，現行仍從嚴採逐次同意授權，倘若金融機構遭受到緊急的資料外洩和偵查到客戶有異常的使用行為要對客戶進行身分確認與警示時，逐次同意將會顯得緩不濟急。

2. API的資料流向目前僅為單向且銀行責任過大

目前台灣開放銀行規範的API串接較為單向，且金融機構同業之間沒有一個明確的規範，反映出金融機構/銀行仍多為資料提供者，倘若發生資料外洩或資安事件，金融機構/銀行端需要擔負調查責任，衍生銀行責任過大的問題。另有業者指出，資料的單一流向會使銀行對於中小型新創TSP業者合作意願不高，進而不利於扶持國內新創業者以及國內金融科技的創新。

3. 有設立橫跨銀保證單一客服窗口的必要性

若透過資料共享打通銀保證業務，於金控設立橫跨銀保證單一客服窗口是否必要且可行目前尚待討論。未來在金控下資料共享的串流中，若是基於讓客戶清楚且簡單明瞭自身資料被使用的狀況，和避免窗口重複建置的理由，設立單一客服窗口供客戶查詢確實有其必要性，然而金控不是實質的業務單位，若未來業者有規劃建置單一客服窗口，仍要審慎評估其功能性與定位。

4.金控層級建置資料庫或數據中心之法律合規性

無論依共享指引、共同行銷管理辦法、個資法、或其他金融法規所得為之資料共享共用，在同一金控下為確保同一客戶資料正確性、完整性與運用效率，如果能在金控層級建置資料庫，將可提升跨公司資料共享共用之效率，並強化資料控管之一致性與安全性。93年9月13日由金管會頒布之函令(下稱93函令)明定金控所屬子金融機構得於一定目的範圍內，交付客戶資料予金控公司建立資料庫，但其中又規定金控公司運用資料庫之分析結果或產出表報，如涉及客戶個人資料、往來交易資料及其他相關資料，應僅限於金融控股公司及原提供資料之子公司使用，且不得揭露予其他子公司或第三人；前述規定係為保護客戶個人資料隱私權，惟亦應尊重客戶對其個資之自主運用權，參考GDPR所規範之資料可攜權概念，就金控資料庫所分析之結果，如經客戶同意，亦應允許揭露予其他子公司或第三人，以強化資料之可運用性，並同時兼顧客戶隱私權與促進客戶便利性。

台灣保險存摺推動之挑戰

1. 資安與使用者體驗取得平衡不易

保險存摺之運作涉及個資監理、資安與使用便利三者之考量，要取得平衡著實不易。目前開放註冊的媒介僅有自然人憑證、晶片金融卡以及MID三種方式。為了提高MID的安全性，目前也開發強化版的MID，當民眾在註冊時，會將確認身分流程串接到內政部戶政司比對國民身分證領補換資料的正確性。

在資安的議題上，壽險公會於110年11月經由台灣檢驗科技股份有限公司 SGS進行資安認證，最終「保險科技運用共享平台」通過了「ISO/IEC 27001資訊安全管理系統」、「ISO/IEC 27701隱私資訊管理系統」與SGS A級等多項資安肯定。「ISO/IEC 27701隱私資訊管理系統」認證涵蓋個資隱私的國際標準，過程中強化了個資隱私之保護。

在保險存摺服務中，由於安全考量僅有留存資料加密後的Hash值，儘管區塊鏈相當安全，但仍有被破解的風險，因此真實資料的交換採取API(Application Program Interface，是一種應用程式的程式碼，使兩種不同的軟體程式互相連結，並使用雙方的數據及功能，為程式之間的接口)傳送，並採用VMware的API解決方案，確保數十間保險公司的資料交換能無縫整合。而資料「軌跡」則是採用聯盟鏈的形式進行，此外，由於聯盟鏈預計涵蓋所有壽險業者的資料，資料隱私水準相當高，在建置時間極短、牽涉多家同業合作、系統整合複雜度又高的狀況下，部署難度是相當高的。因此以VMware NSX Advanced Threat Prevention協助防止針對聯盟鏈的惡意攻擊朝橫向擴散，並嚴格保全文件交換的絕對安全性。

2. 個人資料管理限制

為了確保資料是由保戶同意，也會在每個環節上確保資料都是有進行勾選授權，未來相關的聲明也必須確保使用該資料是經過客戶本人同意的。以上繁複的同意程序，必須要有完善便利的流程配套才不會造成使用者體驗不佳的問題。

開放純網保對保險市場的影響

1. 促進產品與服務創新

從國外的經驗可以看出，純網路保險公司主打三項特質：便利、迅速、有競爭力的費率，而純網保的成立將有助於推動保險市場產品與服務創新。就便利來說，因為純網路保險公司主要透過網路或數位工具進行交易與服務，可不受時間空間的限制，在便利性與可及性上，會比傳統保險公司更方便。就速度而言，由於不透過業務員或人員客服或是紙本流程，自然減少許多文書紙本的傳送與審核，不論在投保、保全或是理賠服務上，都會比傳統保險公司快速。而在成本優勢上，因為大部分都採用數位或自動化方式進行，可以不用負擔高昂的銷售佣金或人事成本，相對有優勢。

2. 促進普惠保險的發展

純網路保險公司因為經營模式以數位為主，可以承保傳統保險公司不願意承保或無法承保的商品，一些保額低、保費少、保障特定範圍與保障期間很短的商品，因為傳統保險公司無法涵蓋到所有消費者，純網路保險公司則能大幅降低每次作業的變動成本，因此可以推出較為特殊與有特色的保單，加強對各承保對象層的滲透，加速促進普惠保險的實現。

3. 加速保險業數位轉型

雖然金管會2021年宣布開放純網保，但新的純網路保險公司成立營業最快也會在2023年中，正式開始運作產生影響可能已是2024年以後，對市場要產生明顯衝擊則需要更久的時間。現在台灣保險市場已經非常競爭，純網路保險公司設立後，要直接面對既有保險公司的強大競爭，勢必又是一場生存挑戰賽，但是這次開放預期會刺激現有保險公司的數位轉型，假以時日，隨著數位化交易習慣的普及，純網路保險公司的影響將會更加明顯。未來傳統保險公司無法完全複製純網路保險公司的商品，雖然相同商品條款可能相似，但技術、資料串接及銷售場景等合作模式皆不相同。例如生物辨識這種保險科技的應用是需要特定門檻，投入的資金及公司內部資訊核心系統也必須與生物辨識的系統可以作介接，傳統保險公司若要模仿，速度也無法快速跟上。

4. 純網保對業務員是個潛在威脅

對業務員或保經代公司而言，純網保可能會帶來一個負面的衝擊，因為規定不能透過實體業務員進行銷售。純網保勢必在通路上會有所創新與突破，未來將吸引更多客戶透過網路購買保險，長遠對於過去實體通路與業務行銷方式，可能會產生競爭與壓縮的效果。

金融資通安全

2021年Deloitte網路調查全球CIO和CISO在管理企業面臨的網絡風險，前四大挑戰分別是: 轉型和混合 IT (41%)、網路衛生 (Cyber Hygiene) (26%)、資安人才缺乏 (20%)和Shadow IT (13%)。根據世界經濟論壇 (World Economic Forum, WEF) Global Cybersecurity Outlook 2022調查，50%的受訪者表示當涉及到網路威脅時，勒索軟體是他們第一擔心的問題; 社交工程攻擊位居第二；第三是惡意內部威脅，此為組織的現任或離職員工、承包商或受信任的企業合作夥伴濫用其對重要資產的使用權限。種種的威脅會阻礙企業數位轉型的速度，因此我們必須構建安全架構，維持不斷增長的科技轉型速。

本報告研究台灣金融產業資安相關單位，認為在接下來1-2年內可能會遇到的前五大挑戰如下:

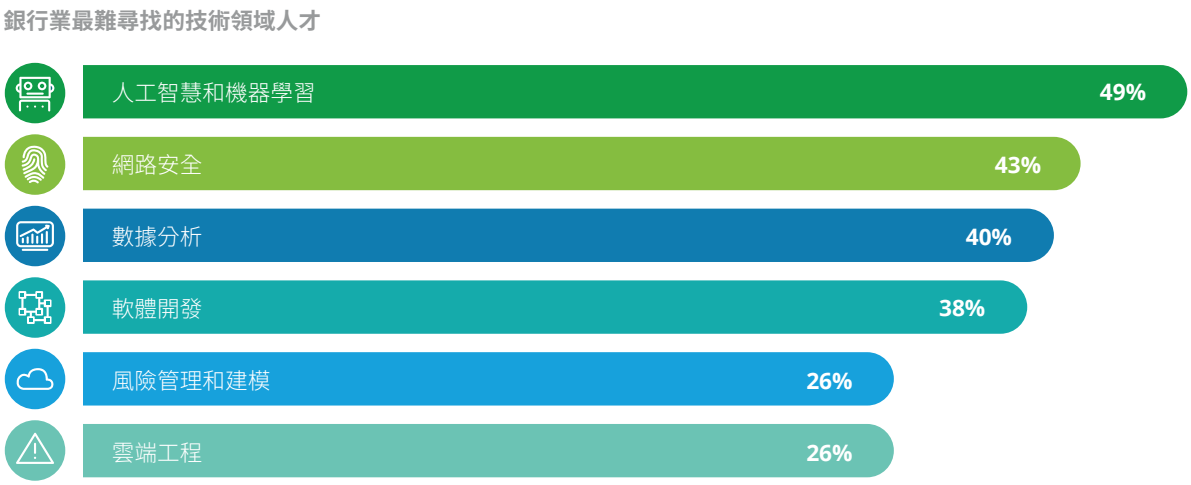
一、 資安人才嚴重缺乏
二、 因實施遠距工作，員工個人或家庭的通訊設備防護程度不一，對於企業可能會形成破口
三、 企業和消費者被勒索軟體和釣魚攻擊
四、 企業對雲端技術的依賴加重，防護性可能不足
五、 第三方供應商或TSP的資安防護

資安人才嚴重缺乏

全球資安專業人力其實相當缺乏，國際資訊系統安全核準聯盟 (ISC)² 2021年網路安全勞動力研究報告，指出過去一年，全球網路安全專業人員數量從312萬減少至272萬，為了有效保護企業或組織的關鍵資產，減少網路攻擊，人力需要成長 65%。[47] Deloitte《第12版全球風險管理調查》指出，57%的受訪者表示，僱用或獲得熟練的網絡安全人才極具挑戰性或非常具有挑戰性。針對金融業的部分，Deloitte 2022年的銀行與保險業的全球調查，資安、機器學習等利基技術領域的人才，仍面臨供不應求的處境。

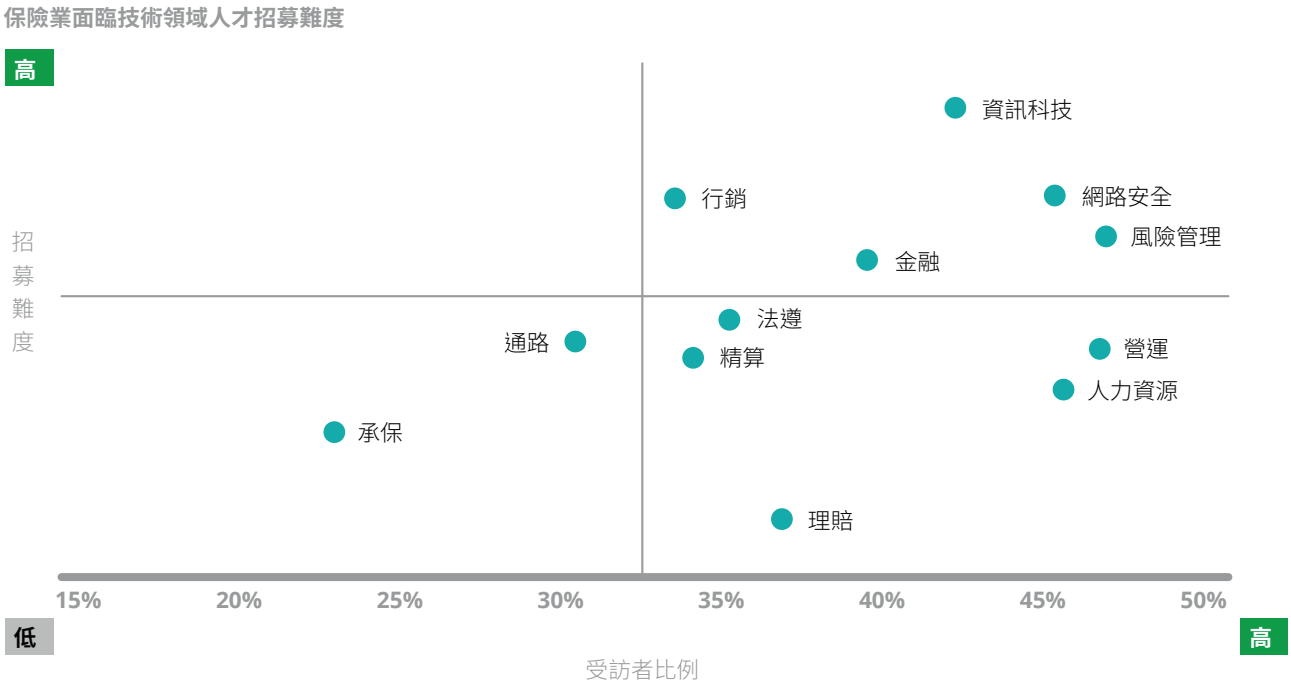
台灣金融企業相當重視台灣資安的人才缺口，不僅如此，金管會要求符合一定條件的上市櫃公司須於2022年底前設立資安長、資安主管等職位。由於各個產業目前對資安普遍都有大量的人才需求，企業也開始競相以高薪挖角，想要找到符合相關能力的員工卻不是這麼容易，原因為稀缺性與專業性，除了人才培育量能不足之外，尚需具備豐富經驗、專業技術，或是取得政府認可的國際資安相關證照。除了招聘專業人力，強化專業團隊以外，如何有效地培育現有的人才，也是企業面臨的一大挑戰。

圖6 Deloitte 2022年銀行全球調查



資料來源: Deloitte Center for Financial Services Global Outlook Survey 2021

圖7 Deloitte 2022年保險業全球調查



資料來源: Deloitte Center for Financial Services 2022 Insurance Outlook Survey

勒索軟體(Ransomware)與魚叉式網路釣魚(Spear Phishing)攻擊

勒索軟體是最流行的網絡威脅之一。勒索軟體主要是在突破企業傳統作業連續性的漏洞、災難復原和資安解決方案。當防護控制功能失效時，傳統備份可能會在檔案中留下未被檢測到的惡意軟體。Sophos的《2022年勒索軟體現況》報告，有66%的受訪企業在2021年遭到勒索軟體攻擊，高於2020年的37%，且有越來越多的受害者支付贖金[48]。此攻擊的破壞性與威脅成長飛快，還有「勒索軟體即服務」(Ransomware-as-a-Service)的出現，降低駭客的進入門檻並允許更多攻擊者進行攻擊，使許多企業措手不及。

美國聯邦調查局 (FBI)警告說現在有100種不同的勒索軟體在全球流通，2021年每個組織平均有270次攻擊，比 2020年增長31%。勒索軟體的威脅持續增加，許多網路科技先進強調，勒索軟體的不斷演變也會對公共安全會造成更多的危險和威脅。

魚叉式網路釣魚即「鎖定目標攻擊」，駭客利用人性弱點，針對特定個人、組織或企業，以電子郵件或數位通信方式誘騙使用者的機敏性資料，或是在使用者的設備上植入惡意程式。

組織耗費在解決資安攻擊的成本相當高昂，平均每事件約360萬美元，而且公司需要約需280天來對網路攻擊進行辨別和反應。網路威脅的快速演變，在安全漏洞工具和系統上發布的新型惡意軟體速度也將會讓駭客和企業之間的競賽受到更大的影響。

遠距工作與雲端技術運用增加風險

由於物聯網設備種類的增加，使企業或家用網路環境變得更多變化，另外也讓資產保護與威脅監控更具挑戰性，物聯網裝置或設備可能成為資安防護的破口，導致營運中斷或機敏性資料被盜取等。新冠疫情以及其他因素使得企業與社會大眾轉為遠距工作，員工使用家用或是私人的通訊軟體，而防毒軟體或其他防護功能可能不及公司強健，駭客因此藉此趁虛而入，並針對企業的敏感資料進行勒索，甚至還追蹤供應鏈以及公司與合作夥伴，使攻擊範圍擴大，更具破壞性。回顧全球所有產業在2021上半年遭遇的網路攻擊事件，較去年同期增加29%，主因便是勒索病毒攻擊事件暴增。

《2021台灣金融科技趨勢展望》調查，有四成的受訪金融機構指出雲端是金融應用的核心關鍵。金融機構漸漸轉移業務到雲端上，無論是未來的開放銀行資料共享，或是法遵的即時監控、大數據的整合與分析，都會以雲端發展，然而機敏資料越多，駭客攻擊的可能性就越高，因此資安防範也隨之重要，應將隱私及資料安全放在首位，企業有責任保護顧客的個資，並採用適當的安全與使用權限控制措施以保護資訊與應用程式。

第三方合作夥伴與供應鏈風險

本報告調查，台灣金融企業擔心合作之第三方業者或TSP資安強度不一定足夠，駭客會尋找供應鏈中防禦能力較弱的攻擊目標，若遭受攻擊，可能會產生連帶影響，另外有鑑於台灣開放銀行Open Banking朝向第三階段邁進，金融業者資料共享機制運行，因此金融業必須調整風險管理和資安的策略。另外，值得注意的是，第三方廠商可能會反過來將一些工作外包給其他公司，因此企業可能也需深入了解由第四方關係造成的額外風險。

Deloitte 2021年全球風險調查中有許多企業指出，他們尚未建立全面性的第三方風險的管理計劃，64%的受訪者表示，優化第三方風險管理為未來兩年內優先執行項目。例如，明確服務級別協定(SLA)與標準合約語言(standard contract language)，和確定角色與職責是企業都應積極建立的基礎，67%受訪企業已經建立了標準合約語言和SLA，而有22%的企業表示目前仍正在進行中。台灣金融產業業者表示為減少攻擊所造成的損害，因此針對TSP業者或委外商，會進行相關資安的盤點與查核。

資安防禦責任需要金融機構與供應商一起承擔，雙方要共同訂定安全責任模型，明瞭彼此的權責範圍。企業也須有效管理第三方合作商，企業必須努力讓其供應商的風險管理流程達到與自身企業標準類似的程度，包含網路安全或營運韌性，因此第三方關係帶來了獨特的挑戰，在評估自身企業營運韌性時應包括第三方關係可能帶來的影響。有效的第三方風險管理方式需要訂定標準化流程，結合技術與數據資訊，並加以分析，且流程與決策能力盡量有一致的標準。

未來策略與政策建言

資料共享

透過借鏡國際資料共享實施經驗與分析業者訪談，本研究對台灣資料共享、保險存摺、純網保、資安未來發展提出以下政策建議：

1.建議資料共享指引能擴大適用對象範圍及開放更多客戶資料授權

為擴大金融機構間資料共享指引的效益，並充分涵蓋業務合作、便民以及風險控管的目的，建議主管機關未來可將目前資料共享指引擴大適用對象範圍，逐步開放跨機構和跨產業的資料共享，使金融業甚至跨產業能夠透過資料共享達到更加精準的商品定價、風險聯防和建立金融生態圈。如此，資料共享指引就能在便民的效益之外，也達到業務合作、風險控管等目的。

2.針對重複場景建議可設計共通原則性問卷以簡化客戶授權模式

為強化資安與改善須逐次同意的客戶體驗，若涉及到特定的金融場景或是對客戶有利的情境，在明訂使用目的的前提下可簡化授權。建議未來在同一金控下可採用具共通性且原則性的問卷，透過資料授權行為綁定身分識別，讓客戶簡單明瞭的授權，建議在問卷中可明確訂定客戶授權資料項目、資料使用目的、授權範圍、授權時間，讓客戶了解其授權的資料會在資安、風險控管、防弊或公平待客原則、消費者保護等目的下被使用，以改善因逐次同意受影響的客戶體驗。另外，也可採用資料授權行為綁定數位身分識別的模式，簡化客戶授權程序，可以改善因逐次同意受影響的客戶體驗以及抵禦緊急的資安危機。

此外，基於金融業者風險聯防的理由，針對資料彙總且標籤化進行數據評分，並基於強化消費者保護、資安風險控管、防弊等原則性前提下，可開放不需經消費者同意而進行必要的資料共享，例如：發生資安事件時可以迅速通知其他金融機構，避免客戶損失擴大，類似這樣的情境簡化授權就會有其效益。

3.建議設立橫跨銀保證單一客服窗口

為透過資料共享打通銀保證相關業務，建議於金控設立橫跨銀保證單一客服窗口，並配合中後台的機制，串聯子公司實際業務窗口。另外，可參考國外大型科技公司的做法，除單一窗口外，設立數位看板供客戶查詢資料授權與應用的狀況。

4. 為提升資料共享效率建議未來金控層級應有建置資料庫/數據中心之法源

為避免重複蒐集客戶資料、降低重複業務程序、降低重複建置模組和技術等原因，建議得比照風險控管需要之規定，在法規層面，建議主管機關能夠制定或釐清建置金控公司資料庫的法源依據，以便在金控層級建置統一資料庫進行客戶資料管理。據此金控資料庫的建置，客戶的資料在去識別化後就可以分析並建立風險模型或風險綜合評比，進而讓金控子公司強化跨售的服務模式以及達到更精準的金融產品定價。金控資料庫會依照各子公司不同的資料請求，在消費者同意的前提下共享資料，藉此避免子公司重複蒐集資料、降低營運成本。另外，金控資料庫也可以結合多元身分識別，處理跨金控集團的eKYC、AML，後續資料庫的使用會更加方便。待未來跨機構、跨產業的資料共享成熟，可以討論金控資料庫與金控集團外的TSP、社交平台介接，延伸不同場景的支付與轉帳功能。

5.建議主管機關推動TSP分級制度

為改善現行金融機構的API的資料流向多為單向，與銀行在資料管理上責任過大的問題，建議未來可由主管機關規劃建立獨立管理平台，由信任的第三方機構進行管理，並推動TSP分級制度，對TSP業者開放程度不同的資料，該平台可跟公會、財金公司共同設立單一窗口，處理第三方業主註冊、分級管理、定期稽核等事宜。透過第三方平台的建立，搭配開放銀行的API管理平台，可提升金融業者與新創業者的合作意願並拓展金融業API生態圈。此外，新創公司、Joint Venture等都可以成為第三方平台。建議未來可讓大型金融機構提供模組與技術給其他金融機構，開設跨金融機構的營業項目，進而透過跨金融機構的參與模式將管理成本、合規與稽核成本降低，藉此可提升金融業與新創業者的合作意願。

6.建議現行法規有後續調整的空間並頒布更多指引

由於銀、保、證產業對於資料的要求並不一致，建議主管機關針對現行資料共享法規及指引後續能有適時調整空間，並頒布更多的指引。除金控內資料共享，多數業者也期待在跨機構、跨產業的資料共享、法遵、風險管理能有指引頒布，供業者爰引。

保險存摺

1. 逐步擴大保險存摺揭露資訊

現階段保險存摺所顯示的資訊，是在衡量新系統上線後的資料運作穩定性及取得保戶同意後所決定的範圍，未來可以進一步再視個別險種擴增保單資料，例如對投資型保單的保戶而言，保單價值是隨著市場而浮動的，若保險存摺能夠揭露更多詳細的動態資料，對民眾來說應該會更加便利。因此，建議未來保險存摺的揭露資料項目可以從保單健檢與民眾需求的角度出發更多元擴展，納入更多項目以擴大資料價值。

2. 保險存摺介接第三方資料連接創新服務

從台灣發展開放銀行的經驗可以發現，在客戶同意的前提下，透過資料串接開放第三方業者使用，即能發展出嶄新的場景服務提升消費者的使用體驗。而保險存摺現階段所提供給民眾的服務就好比開放銀行，由第三方服務業者作為仲介人串接保戶於各保單的資訊。然而，由於保險商品設計相當複雜，即使消費者透過保險存摺了解自身投保狀況，在沒有相關知識的輔佐下，要自己做好理財規劃，事實上並不容易。因此，透過保險存摺的使用可對消費整提供更便利的保險服務，逐步建立開放保險的服務架構。未來在保戶同意的前提之下，經由保險科技運用共享平台開放資料，再藉由第三方服務業者與保險公司合作，整合各方保險資訊，可為保險消費者提供創新的服務，如保單健診、專業投保建議、理賠建議、或是保單管理等創新服務。

3. 持續擴大保險科技共享平台的合作規模

在開放金融的架構下，金融業者可以透過開放 API進行資料交換與共享，目前保險存摺的服務已有平台化整合功能雛形，且壽險部分已有區塊鏈技術支持，未來可以將應用與功能持續擴大，例如將保險存摺結合保單健檢功能進行服務整合與推廣，或是讓保險存摺資料平台作為第三方資料管理單位，應可擴大資料共享平台的合作效益，進而達到更精準的保險產品定價與行銷。此外，臺灣的金融產業有許多周邊機構，如財金公司、證券交易所、集保公司、保發中心等都擁有大量的客戶資料，在一站式的金融服務概念與其衍伸的相關APP逐漸被推廣的前提下，金融中介機構間也可以透過API作為資料提供者進行資料共享，若能延伸此種開放資料之應用，台灣將可逐漸走向開放金融趨勢與國際接軌。

4. 確保使用者體驗與資料安全性的衡平

壽險公會建置的保險科技共享平台能協助解決保戶服務痛點，然而社會上有許多人因為年齡、環境等種種因素，導致接觸數位工具的機會不同，自然也會造成使用數位工具的能力落差，所以現實面仍然有部分民眾在數位工具上的使用會有些困難，這部分的配套措施也是未來在服務優化上可納為考量之處。此外，除了提升使用者體驗外，客戶機敏性資料的保護也是相當重要的議題。而現今在追求極大化便民服務與強化資訊安全的角力下，要取得兩者的平衡事實上並不容易。因此，客戶資料的開放與串接也仍須顧慮到法令遵循、資訊儲存的安全性，以及保戶個資保護的問題。

純網路保險

面對金融科技時代的來臨，以及數位網路消費的崛起，傳統的保險經營型態可能已無法滿足所有客戶的需要，純網路保險公司提供快速、好用又便宜的保險，應有一定的發展契機。金管會在觀察消費數位化趨勢及參考國際發展經驗後，發布了「開放設立純網路保險公司的政策目的與規劃方向」值得肯定與支持。

然而，目前台灣產險市場在需求上缺乏消費場景金融，無法與生活作緊密的結合。台灣以中小企業為主，由於過去許多風險大多由政府承擔，企業主較缺乏購買保險的觀念。產險部分，若要開發創新商品亦可能無資料可定價、逆選擇與道德風險也較高；而壽險市場部分，新設純網產公司目前只能販賣保障型，可能因為風險池較小，無法承擔理賠壓力，較無法與現行保險公司競爭。此外，新業務核保、理賠需完全線上快速作業，可能面臨無法區分保戶風險等級，造成大量逆選擇之情況。台灣要發展純網路保險公司仍須許多調適與相關法規配套，經彙整國際經驗與深度訪談保險業界與科技業者等各方意見後，本研究對未來純網保開放提出以下建議:

1. 業務開放應兼顧創新與合理營運空間

開放純網路保險公司，最終目的在於增進消費者的效益，更重要的是提供消費者更多更好的選擇。目前台灣的純網路保險公司必須承受幾乎完全相同的監理條件，在市場競爭條件上，建議監理上應給予新進入純網保業者更合理公平的生存發展空間。

以現行政府開放規劃來看，純網保業務範圍與現有保險業有顯著差別，產險僅限創新型產品，而壽險僅限保障型商品，市場現有產壽險公司業績僅靠這兩大類的業務其實非常有限，建議未來業務規範上可思考採用一定比例的概念，要求產壽純網保的業務，須一定比例承做創新型產品或保障型產品即可而非全部，業者則必須證明有能力開發創新產品與經營模式，作為核准之基礎條件。

此外，目前主管機關規定純網保壽險公司只能賣短期的定期壽險、傷害險、健康險為主，會造成業者經營獲利面的挑戰。分析目前未投保保障型商品的客層，往往可能是風險較高，或需要較高核保技術，且純網保創立前期建置成本高，如財務處理帳務及保險基礎建置屬於固定成本，要在便宜又方便的情況下做到損益兩平有挑戰難度，要擴大規模也有一定的挑戰性。觀察國際上數位保險公司設立經驗，除少數地區如香港規範不得有實體通路外，對於營運模式、通路或商品等大多無特別限制，業者採取創新模式經營是自身策略的選擇並非強制規定。未來可考慮給予純網保壽險業者更合理的發展空間。

2. 調整保險商品審查模式

現行針對網路投保銷售商品的法規，產險為負面表列，而壽險為正面表列。未來純網路保險公司其送審商品卻全部須採核准制，不但與現有制度不同與國際做法也迥異，需要更進一步釐清與變通，若採嚴格的審核標準，則創新商品開發不易。現行商品審查不外乎條款跟費率，在費率面，純網路保險公司未來一樣要適用IFRS17制度，利潤過低的商品不易通過審核。如果定位純網保是小額、以保障為主的商品，建議可以放寬採用備查制而非核准制，將其與現有保險公司的網路投保通路做出區隔。而且，目前監管較難做到很簡單去做新產品和修改產品的方式，例如共享車輛碎片化保險，在消費者使用服務時可直接小額加購，達到一站式消費的目的。此外，未來對於創新型商品以及保障型商品的內容與定義除了應非常明確外，建議商品審查程序也可以給予更多彈性，以兼顧鯰魚創新與新業者業務發展的需求。

3. 監理機關應提供誘因鼓勵保險科技發展

純網路保險公司初期在重重限制下，很難在短期搶占到灘頭堡，因此提升科技力與線上核保能力非常重要，尤其線上碎片化的創新保險產品，保費較低且容易產生道德風險，吸引風險較高的用戶進行投保。且網路投保的核保時間較短，需要處理資訊不對稱的困境，以避免保險詐欺等情況發生。由國外數位保險公司發展經驗顯示，純網保要成功，除了要科技技術、人才與財力支撐外，還有賴保險數位消費客群成熟的程度，以及監理法規是否配合到位等外在因素的配合。因此，主管機關除

考量監理安全，更應積極提供誘因刺激保險科技發展。台灣目前對網路投保之相關規範相較國外繁複嚴謹，如果開放程度有限難以滿足時快速的需求變遷，建議未來可放寬網路投保限制，將相關規範採負面表列，給與網路投保更多發揮空間，鼓勵保險科技的發展。

4. 定期盤點法規適時調整加速開放資料共享

台灣目前純網路保險公司原則上適用與一般保險公司相同之監理法規，但因為純網保之型態特殊，其中涉及相關法規與行政規則眾多，未來應定期就現有規範事前加以盤點是否與純網保運作有牴觸之虞，並適時加以調整修改，否則未來純網保開業後法令上若有扞格，屆時再行修法耗日費時，都將造成純網保業務執行上之困難。此外，未來純網保型態可能與異業合作發展生態系，若在平台上販售碎片化保單，還將遇到資料與系統的串接、大數據的資料及數據運用不同於傳統的問題。純網保講究快速，是否可能利用線上即時回饋數據分析，立刻做出產品修正，也是未來監管機關需要思考的問題。建議純網保業務在可承做商品開放程度、異業合作、生態圈的門檻等未來都應注意適時盤點放寬。尤其，未來保險業應加速開放API串接平台與資料共享，因為異業結盟與策略夥伴是保險生態系需求整合平台的關鍵，透過更便捷的資料共享，才能使保險需求與生活情境貼合，並在平台上一次購足，滿足消費者需求。

金融資通安全

1. 建議資安解決方案

儘管多數公司在資安威脅後慢慢恢復，但有部分企業卻面臨結束營運的情況。隨著網路攻擊覆蓋範圍越廣，漸漸在消費者的心中播下懷疑的種子，結果損害公司、機構或個人長期聲譽。因此即使企業從資安事故後恢復，在財務上和聲譽上仍須付出很大的代價。企業又應如何提早佈局與準備?

應對日益嚴重的資安威脅，WEF建議解決方案包括：員工網絡培訓（61%）；離線備份（58%）；和資安保險(57%)。企業應建立一個平台整合所有已知資安威脅的解決方案。越來越多的組織開始接受網絡事件將會層出不窮，駭客與越趨複雜的技術也會越來越多，現在需要的不只是精密的保護，更需要快速反應資安威脅的能力。

資安長與資訊長應建立的企業資安短中長期目標

金管會將金融機構資訊安全納為金融業者內部控制及稽核重點，並要求國內符合一定條件的上市櫃公司在2022年底之前完成設立資安長以及資安專責單位。資安長可說是近期最炙手可熱的高階人才，主要職責是整合企業組織資訊與資料安全，確保企業不受威脅。全球駭客組織的攻擊能力持續精進，資安長尚需組織資安人力、建立組織架構、加強技術能力，引進新興科技來對抗不斷進化的資安威脅。資安團隊需要有快速的應變能力，建立跨機構之資安事件應變體系，更能發揮資安聯防的效益，防止駭客突然的網路攻擊。

全球CISO和CIO們投資於雲端的網絡規模化解決方案、網路韌性、和人工智慧的威脅辨識，來建立企業的網絡防護。本研究訪談台灣金融機構資安長、資訊長、資安相關單位，並認為企業與組織短期與中長期應建立和執行的項目:

短期目標:

1. 檢視現行資安作業，確認資訊程序有效性，確定員工資訊執行正確性的落實
2. 組織人員分工與職掌調整，拓展資安團隊人員
3. 資安教育訓練
4. 確保資安防護作業與應變機制符合新架構的運作
5. 強化網路安全，聚焦關鍵風險，提升網路安全成熟度
6. 將資安內建至商業價值流程，前後台串聯至客戶端
7. 創立資安的共識，訂定未來資安藍圖和政策

中長期目標:

1. 資安藍圖的實行，強化企業資安治理文化
2. 持續強化資安防護縱深
3. 提升資安可視度，落實合規稽核及建立定期檢測機制來提升企業資安韌性
4. 人才持續精進，關鍵資安人才庫的建立
5. 提升系統開發成熟度雲端設備和應用安全
6. 建立主動式防禦策略
7. 零信任架構建立

建置國際網路安全標準檢測認可之設備，導入零信任(Zero Trust)架構

企業應考量選擇國際網路安全標準檢測認可之物聯網裝置，降低聯網設備所帶來的網路安全風險。歐盟積極推動網路安全與隱私保護等國際標準，針對物聯網裝置安全，建議台灣企業應參酌相關國際標準持續評估物聯網裝置安全，並及時取得相關國際標準認證，以持續強化產品安全、維護品牌信譽與提升市場競爭力。

除了硬體設備的安全強化，在運用上也需建立有效的防護機制。零信任不是一種技術或單一的解決方案，它是一基於「從不信任，始終驗證」的原則的架構策略，可信任的連結是建立於內部和外部不斷地重新驗證。NIST（美國國家標準暨技術研究院，National Institute of Standards and Technology）在2020年推出SP 800-207零信任標準後，美國國防部（DoD）接著在2021年二月提出零信任參考架構（Zero Trust Architecture, ZTA）。美國行政管理和預算局（OMB）於今(2022)年1月正式發布新網路安全策略與M-22-09備忘錄，要求政府機關要實施零信任架構，進而影響企業使用零信任抵禦網路威脅。 金管會於2020年發布的金融資安行動方案，其中也指出金融產業需導入零信任架構思維，

來完備資安規範。以零信任之精神建立核心架構，將資安防護意識嵌入各業務中，以全面提昇企業網路安全防護力。

2. 未來資安防護建議與展望

資安產學合作培育相關人才，並建置人才庫

企業建立資安長、資安團隊，除了具備技術的增進以外，團隊也需懂得企業營運價值。資安並非一個人或一個單位的工作，應該要把安全概念部署在公司每個營運單位，讓每個地方都備有了解資安觀念的人。金管會「金融資安行動方案」在強化資安監理職能的策略下，已將資安專業訓練和進修列入規劃，並特別針對中高階主管提供課程。然而資通安全需要更廣泛的推廣給企業員工、民眾、和年輕學子。界定不同產業的所需資安專業項目，從大專院校開始培育人才，開設大學部和碩士班專業課程，輔以與企業合作實地操作演練，建立產學合作札實訓練，協助學生可以順利接軌企業，也幫助企業建立資安團隊與人才庫。對於企業在職員工則可施以資安在職訓練，強化員工安全網路使用方式，鼓勵員工資安專業的學習，建立良好資安治理文化。

對供應鏈採取零信任機制

銀行越來越容易受到來自第三方甚至第四方的網路攻擊，互聯關係的增加導致攻擊機會擴大。零信任（Zero Trust）的「信任始終來自於驗證」，假定所有網路都隱藏惡意軟體，因此限制了網路存取權限，不斷地對身份和憑證進行驗證，以達到實質的防禦作用。網路威脅邁入更新更複雜的層級，組織在面對資安問題應做足準備。另外，對於未來台灣開放銀行的推廣，金融產業會有越來越多的合作TSP業者，除了對TSP業者訂定資安相關規範標準與定期追蹤以外，鼓勵金融產業與TSP業者投保資安保險，降低企業的遭受攻擊的風險。

落實資安治理，增強營運韌性

銀行也應將強化營運韌性列為首要任務。此外，網路風險團隊應迅速對違規行為和事件通知做出反應，而組織的其他成員則需知道如何快速復原關鍵業務流程。在真實或模擬的入侵中，網絡風險部門需儘速就可能在入侵中受損之資產和資料編製詳細報告。在上述一連串機制下，企業應有信心能夠快速偵測出資料損毀、鎖定或破壞事件，並重建散布於雲端和本地設備上的資料。

在這資安危脅環伺的情狀之下，金融機構在發展金融科技的同時，應該從治理面、管理面、技術面等，進行以下資安治理強化措施：

- 將資訊安全管理納入公司治理架構，促使管理階層建立企業資訊安全管理願景、風險胃納以及整體策略方向。
- 新興科技之採用應進行完整之安全評估，以確保可具體風險與既有控制成熟度，並擬訂資訊安全控制計畫。
- 以「風險管理」之角度推行資訊安全控管，定期自我評估資訊安全管理能力，並透過持續優化，形成持續改善與強化之管理循環。
- 建立金融大數據安全管理措施，藉由數據預測分析即時掌握風險，提昇整體業務發展之同時，達到業務與資安控管平衡發展之產業態勢。
- 強化資安事件應變與數位鑑識能力，建立資安事件通報程序與應變計畫，並以資訊安全防駭演練提昇內部人員面臨突發狀況之應變與與協調溝通之能力，避免或降低資訊安全事件帶來的損害。
- 建立資安威脅情資分析與預警機制，透過資安情報的即時分享，提供所需的即時與歷史資訊安全事件資料、報表、及相關情報，協助組織執行資安管理活動。

資安防護不只是資安長、資訊長或是資安專責團隊的工作，公司每位員工都有責任盡一份心力，資訊安全防範需要企業上下共同努力。

參考資料

1. Allied Market Research, (2020). Open Banking Market Size to Reach $43.15 Billion by 2026, at 24.4% CAGR. [online] Available at: https://www.globenewswire.com/news-release/2020/04/13/2015104/0/en/Open-Banking-Market-Size-to-Reach-43-15-Billion-by-2026-at-24-4-CAGR.html [Accessed 02 Jun. 2022]
2. Pandy, S., (2020). Developments in Open Banking and APIs: Where Does the U.S. Stand?. [online] Federal Reserve Bank of Boston. Available at: Developments in Open Banking and APIs: Where Does the U.S. Stand? - Federal Reserve Bank of Boston (bostonfed.org) [Accessed 02 Jun. 2022]
3. The Financial Brand, (2020). U.S. Financial Institutions Now Lead Europe in Open Banking (Here's Why). [online] Available at: https://thefinancialbrand.com/102918/u-s-financial-institutions-now-lead-in-open-banking-api-token-mobile-app-screen-scrape/ [Accessed 02 Jun. 2022]
4. Allied Market Research, (2020).
5. Competition and Markets Authority, (2016). Retail banking market investigation. [online] Available at: https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk [Accessed 02 Jun. 2022]
6. Open Banking Limited, [online] Available at: https://www.openbanking.org.uk/insights/ [Accessed 02 Jun. 2022]
7. Capgemini & BNP Paribas, (2020). World Payment Report 2018. [online] Available at: https://www.capgemini.com/news/press-releases/world-payments-report-2018/ [Accessed 02 Jun. 2022]
8. OECD, (2019). Enhancing Access to and Sharing of Data. [online] Available at: https://www.oecd.org/digital/ieconomy/enhancing-access-to-and-sharing-of-data.pdf [Accessed 02 Jun. 2022]
9. Rogier, B., (2019). Establishing a Durable Environment for Digital Financial Services: Eliciting Design Principles for the Financial Ecosystem to Develop Robust APIs for Open Banking.
10. IBM, (2016). Evolution of the API economy Adopting new business models to drive future innovation. [online] Available at: https：//www.ibm.com/downloads/cas/XG8RYO63 [Accessed 02 Jun. 2022]
11. 資策會產業情報研究所, (2019). 開放銀行發展簡報
12. EBA, (2017). Open Banking: advancing customer-centricity. [online] Available at: https://www.abe-eba.eu/media/azure/production/1355/eba_open_banking_advancing_customer-centricity_march_2017.pdf [Accessed 02 Jun. 2022]
13. Open Banking Limited, Open Data Specifications version v2.4.0. [online] Available at: https://openbankinguk.github.io/opendata-api-docs-pub/v2.4.0/ [Accessed 02 Jun. 2022]
14. Open Banking Limited, Account and Transaction API Profile - v3.1.6. [online] Available at: https://openbankinguk.github.io/read-write-api-site3/v3.1.6/profiles/account-and-transaction-api-profile.html [Accessed 02 Jun. 2022]
15. Vegelius, A. (2020). PSD2 Strong Customer Authentication (SCA) and PCI Multi-factor Authentication (MFA) compliance. Advantio Available at: https://www.advantio.com/blog/psd2-strong-customer-authentication-sca-and-pci-multi-factor-authentication-mfa-compliance [Accessed 02 Jun. 2022]
16. Open Banking Limited, Open Banking Standard. [online] Available at: https://standards.openbanking.org.uk/ [Accessed 02 Jun. 2022]
17. EU, (2015). Payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366 [Accessed 02 Jun. 2022]
18. BIAN, (2020) Build the future of banking service, Available at: http：//bian.org/participate/bian-webinars/bian-apis-future-banking-api-standards [Accessed 02 Jun. 2022]
19. Penser, (2019) AIS and PIS – A status update on open banking licenses issued in the UK, Available at: https://www.penser.co.uk/business/ais-and-pis-a-status-update-on-the-licenses-issued-in-the-uk/ [Accessed 02 Jun. 2022]
20. 薛丹琦, (2019) 開放銀行金融創新之機制研究, 世新大學財務金融學研究所碩士論文
21. Open Banking Limited, Available at: http：//openbanking.org.tw/index.php/foreign_implement
22. Australian Banking Association, Open Banking. Available at: https://www.ausbanking.org.au/priorities/open-banking/ [Accessed 02 Jun. 2022]
23. Consumer Data Standard, Available at: https://consumerdatastandardsaustralia.github.io/standards/#introduction [Accessed 02 Jun. 2022]
24. Apix, Available at: https://apixplatform.com/v3/about-us [Accessed 02 Jun. 2022]
25. Monetary Authority of Singapore, Financial Industry API Register. Available at: https://www.mas.gov.sg/development/fintech/financial-industry-api-register [Accessed 02 Jun. 2022]
26. The Association of Banks in Singapore & Monetary Authority of Singapore, ABS-MAS Financial World | Finance-as-a-Service: API Playbook. p.34-41
27. 谷湘儀, 臧正運 (2019) 變革中的金融科技法制, 五南出版社
28. Financial Data Exchange, (2020) FDX API 4th edition. Available at: https://www.financialdataexchange.org/FDX/News/Announcements/financial-data-exchange-releases-first-major-update-to-fdx-api-makes-fourth-version.aspx [Accessed 02 Jun. 2022]
29. Nacha, Afinis Interoperability Standards. Available at: https://www.nacha.org/afinis-interoperability-standards [Accessed 02 Jun. 2022]
30. IRDA, (2016) Insurance Repository A Step towards world. Insurance Regulatory and Development Authority.

31. Screwvala backed insurejoy.com becomes the fastest-growing Insurtech Startup (2020) The Economics Times, Available at: https://economictimes.indiatimes.com/industry/banking/finance/insure/screwvala-backed-insurejoy-com-becomes-the-fastest-growing-insurtech-startup/articleshow/91496824.cms [Accessed 02 Jun. 2022]

32. Eling and Lehmann (2018)

33. 2021年國內上市櫃公司至少14件資安事件重大訊息，平均每月一起, Available at: https://www.ithome.com.tw/news/149271 [Accessed 02 Jun. 2022]

34. Catherine Stupp, (2019) Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. WSJ, Available at: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 [Accessed 27 May 2022]

35. Charlie Osborne, (2020) COVID-19 blamed for 238% surge in cyberattacks against banks. ZDNet

36. New York Department of Financial Services Issues New Guidance Regarding COVID-19 Cybersecurity Risks, (2020), The National Law Review, Available at: https://www.natlawreview.com/article/new-york-department-financial-services-issues-new-guidance-regarding-covid-19[Accessed 27 May 2022]

37. 林玉書, (2021) 美國網路安全暨基礎設施安全局（CISA）成立聯合網路防禦協作機制（Joint Cyber Defense Collaborative，JCDC），將領導推動國家網路聯防計畫. 資策會法律研究所, Available at: https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=8711 [Accessed 27 May 2022]

38. 行政院國家資通安全會報技術服務中心, (2021) 歐盟規劃成立聯合網路機構以應對大規模資安事件, Available at: https://www.nccst.nat.gov.tw/NewsRSSDetail?lang=zh&RSSType=news&seq=16574 [Accessed 27 May 2022]

39. Chee, F., (2022) EU governments, lawmakers agree on tougher cybersecurity rules for key sectors. Reuters, Available at: https://www.reuters.com/technology/eu-governments-lawmakers-agree-tougher-cybersecurity-rules-key-sectors-2022-05-13/ [Accessed 27 May 2022]

40. 高敬原, (2019) 開放銀行...怎麼全世界都在熱？圖解全新金融生態系帶來的大變革, 數位時代, Available at: https://www.bnext.com.tw/article/55095/global-open-banking-taiwan [Accessed 27 May 2022]

41. 財金公司2020年5月26日政治大學金融科技研究中心OPEN API 技術合規與測試說明. Available at: http：//www.ftrc.nccu.edu.tw/wordpresseng/?p=10997

42. Bain & Company, (2018) Customer Behavior And Loyalty In Insurance: Global Edition

43. 彭禎伶, (2022) 純網路保險對誰威脅大保險局數字洩端倪, 工商時報 [online] Available at: http：https://ctee.com.tw/news/insurance/598569.html [Accessed 27 May 2022]

44. 吳麟, (2022) 觀念平台－純網路保險會是市場鯰魚嗎？, 工商時報 [online] Available at: https://wantrich.chinatimes.com/news/20220224900219-420501[Accessed 27 May 2022]

45. 魏喬怡, 彭禎伶 (2021) 65家金融機構要設資安長, 工商時報 [online] Available at: https://ctee.com.tw/news/finance/466586.html [Accessed 27 May 2022]

46. 簡永祥, (2022) 台灣資安主管聯盟正式成軍 產官學研界齊讚聲. 聯合報[online] Available at: https://udn.com/news/story/7240/6276321[Accessed 27 May 2022]

47. MoneyDJ, (2022) Fortinet：8成企業因資安知識不足導致安全威脅. [online] Available at: https://www.moneydj.com/kmdj/news/newsviewer.aspx?a=c0252199-b70a-4382-9f88-cb05b64e145e [Accessed 27 May 2022]

48. iThoms, (2022) Sophos 2022年勒索軟體現況報告揭露勒索軟體攻擊多達66%的組織. [online] Available at:https://ithome.com.tw/pr/150762 [Accessed 27 May 2022]

49. Deloitte Insights, (2021) 2021 Future of Cyber Survey. [online] Available at:https://www2.deloitte.com/global/en/pages/risk/articles/future-of-cyber.html

50. Deloitte Insights, (2022) Earning digital trust: Where to invest today and tomorrow. [online] Available at: https://www2.deloitte.com/global/en/insights/topics/digital-transformation/digital-trust-solutions.html

51. Deloitte Insights, (2021) Global risk management survey, 12th edition. [online] Available at: https://www2.deloitte.com/us/en/insights/industry/financial-services/global-risk-management-survey-financial-services.html

52. 行政院 國家資通安全發展方案

53. 金管會 金融資安行動方案

54. World Economic Forum, (2022) Global Cybersecurity Outlook 2022. [online] Available at: https://www.weforum.org/reports/global-cybersecurity-outlook-2022

55. Deloitte Insights, (2021) 2022 Banking and Capital Market Outlook. [online] Available at: https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-outlooks/banking-industry-outlook.html

56. Deloitte Insights, (2021) 2022 Insurance Outlook. [online] Available at: https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-outlooks/insurance-industry-outlook.html

57. 彭金隆 (2021) 保險存摺上路， 保險服務再升級，前瞻保險論壇. [online]Available at：https://www.advisers.com.tw/?p=10260 [Accessed 30 June 2022]

58. Economic Times (2014) E-manage your insurance portfolio.[online]Available at：https://economictimes.indiatimes.com/wealth/insure/e-manage-your-insurance-portfolio/articleshow/29099047.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst[Accessed 30 June 2022]

59. 晴報 (2017) 保險科技App 整合保單看清保障範圍. [online] Available at：https://skypost.ulifestyle.com.hk/article/1632855/%E4%BF%9D%E9%9A%AA%E7%A7%91%E6%8A%80App%20%E6%95%B4%E5%90%88%E4%BF%9D%E5%96%AE%E7%9C%8B%E6%B8%85%E4%BF%9D%E9%9A%9C%E7%AF%84%E5%9C%8D [Accessed 30 June 2022]

60. The Indian Express (2021) Paperless Policies: 'Challenges exist, but e-insurance accounts seeing 100% growth'. [online]Available at：https://indianexpress.com/article/business/paperless-policies-challenges-exist-but-e-insurance-accounts-seeing-100-growth-7141257/[Accessed 30 June 2022]

61. 彭金隆 (2022) 純網路保險公司將帶來什麼改變？Smart [online] Available at：https://smart.businessweekly.com.tw/Reading/WebArticle.aspx?id=7005252[Accessed 30 June 2022]

62. 主筆室 (2022)《工商社論》純網保無利基 欲達的政策效果堪慮，工商時報 [online] Available at：https://www.chinatimes.com/newspapers/20220310000093-260202[Accessed 30 June 2022]

63. 邱金蘭 (2022) 鯰魚？鯊魚？ 場景保險有潛力，經濟日報 [online]Available at：https://udn.com/news/story/7239/6070264[Accessed 30 June 2022]

64. 彭金隆 (2021) 保險鯰魚來了！，聯合報 [online] Available at：https://udn.com/news/story/121739/5984338[Accessed 30 June 2022]

65. 蘇維國 (2018) 臺灣設立純網路保險公司之法制可行性分析.

致謝

感謝金融機構團體與事業單位於疫情期間撥冗接受訪談

國立政治大學金融科技研究中心

政大研究團隊

王儷玲 教授
國立政治大學金融科技研究中心主任
jenwang@nccu.edu.tw

謝明華 教授
國立政治大學數位金融創新實驗室執行長
mhsieh@nccu.edu.tw

彭金隆 教授
國立政治大學保險科技創新實驗室執行長
jlpeng@nccu.edu.tw

王世方 執行長
國立政治大學國際產學聯盟執行長
cicii@nccu.edu.tw

丁伯康 副執行長
國立政治大學國際產學聯盟副執行長
deanting@nccu.edu.tw

徐金聖 專案管理顧問
國立政治大學金融科技研究中心
gn023589071021@gmail.com

胡昱晨 專案研究員
國立政治大學金融科技研究中心
tommyhu@nccu.edu.tw

聯絡我們

勤業眾信金融服務產業服務團隊

吳怡君 資深會計師 Jessie Wu
金融服務產業負責人
jessiewu@deloitte.com.tw

廖哲莉 資深會計師 Cheli Liaw
稅務服務
cheliliaw@deloitte.com.tw

楊承修 資深會計師 Charles Yang
銀行與資本市場產業負責人
charlesyang@deloitte.com.tw

李紹平 資深執行副總經理 James Lee
財務顧問服務
jamesslee@deloitte.com.tw

林旺生 資深會計師 Eric Lin
保險產業負責人
ericwlin@deloitte.com.tw

劉曉軒 資深執行副總經理 Kelly Liu
風險管理顧問服務
kellyliu@deloitte.com.tw

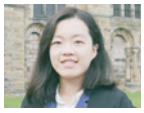
黃秀椿 資深會計師 Kathy Huang
投資管理產業負責人
kathyshuang@deloitte.com.tw

黃志豪 資深執行副總經理 Casper Huang
管理顧問服務
cashuang@deloitte.com.tw

楊清鎮 資深會計師 ChingCheng Yang
不動產產業負責人
chyang@deloitte.com.tw

熊誦梅 副總經理 Sungmei Hsiung
法律諮詢服務
sungmei@deloitte.com.tw

專案聯絡



林孟儒 Karen Lin
金融服務產業專案經理
karenmlin@deloitte.com.tw

謝依倫 Milly Hsieh
金融服務產業專案專員
mhsieh@deloitte.com.tw

MAKING AN IMPACT THAT MATTERS since 1845