報告題名：

金融科技發展對資安風險發生頻率的影響

The Determinants of Cyber Risks on the Financial Technology Development

作者：孫紫婷、張心柔、林靖雯

系級：財算四

學號：D1082638、D1085023、D1077882

開課老師：陳彥志 老師

課程名稱：金融商品設計與開發

開課系所：財算四

開課學年： 112 學年度 第 1 學期

金融學院

中文摘要

(1) 目的：本研究旨在深入探討金融科技創新對金融機構資安風險事件發生頻率的影響。隨著金融科技的快速發展，金融機構不僅積極提供各種金融科技服務，同時也面臨著日益複雜的資安風險。本研究對象為台灣的銀行和保險公司，研究旨在深入了解金融科技對資安風險的影響，並提供金融業者有效因應和預防資安風險的管理策略。

(2) 過程及方法：研究過程中，我們使用了台灣經濟新報資料庫（TEJ）來收集銀行和保險公司的資安風險事件資料，包括資料外洩、系統中斷以及其他相關事件。透過這些事件資料，我們根據不同類型的金融機構，以探討金融科技發展對資安風險事件發生的影響。針對收集到的資料，我們運用回歸模型進行分析，探討資安風險事件發生的重要影響因子和金融機構實際資安事件與公司金融科技特徵之間的關聯。

(3) 結果：研究結果顯示，保險公司的資產規模與發生資安事件的機率呈正相關，即資產規模越大，發生資安事件的機率越高。此外，研究亦指出，不論是銀行還是保險公司，金融科技的發展都對資安風險事件的發生頻率產生影響，並對公司的獲利性造成一定程度的影響。這些結論提供了金融業者制定資安管理策略的參考，同時也強調了在金融科技創新的過程中，必須謹慎應對資安挑戰，以確保金融體系的穩健運作。

關鍵字：金融科技、金融機構、資安風險

Abstract

(1) Objective: This study aims to delve into the impact of financial technology (fintech) innovation on the frequency of cybersecurity incidents in financial institutions. With the rapid development of fintech, financial institutions are not only actively providing various fintech services but also facing increasingly complex cybersecurity risks. The focus of this research is on banks and insurance companies in Taiwan, seeking to comprehensively understand the influence of fintech on cybersecurity risks and provide effective management strategies for financial industry professionals to respond to and prevent cybersecurity risks.

(2) Process and Methodology: In the research process, we utilized the Taiwan Economic Journal (TEJ) database to gather data on cybersecurity incidents in banks and insurance companies. This included data breaches, system interruptions, and other relevant events. Using these event data, we explored the impact of fintech development on the occurrence of cybersecurity incidents based on different types of financial institutions. For the collected data, regression models were employed for analysis to investigate the significant influencing factors of cybersecurity incidents and the correlation between actual cybersecurity events and the technological characteristics of financial institutions.

(3) Results: The research findings indicate that the asset size of insurance companies is positively correlated with the probability of experiencing cybersecurity incidents, meaning that larger asset sizes are associated with a higher likelihood of such incidents. Furthermore, the study suggests that, whether for banks or insurance companies, the development of fintech has an impact on the frequency of cybersecurity incidents and exerts a certain degree of influence on the profitability of the companies. These conclusions provide reference points for financial industry professionals in formulating cybersecurity management strategies, emphasizing the need for cautious handling of cybersecurity challenges during the innovation of financial technology to ensure the robust functioning of the financial system.

Keyword：Cybersecurity Risks、Fintech、Financial Institutions

目 次

表目錄

第一章　　緒論

第一節　研究動機及背景

全球金融科技 (Financial Technology, FinTech) 快速的興起，新穎的商業模式日新月異，當進入受到高度管制的傳統金融業，對傳統金融業的監理容易造成相當大的衝擊與影響，如果有完善的風險保障，就能降低公司的風險，我們首先想要探討金融科技創新較多的公司跟沒有金融科技創新的公司，在資安風險事件發生的頻率與類型是否存在差異。

近年來，國內外公司都積極將科技運用在各項業務，甚至運用在國家基礎設施上，而過去幾年科技發展也造成資安風險事件頻傳。根據 2014 年統計，全世界中大規模分散式阻斷服務攻擊 (DDoS) 的事件已達平均每小時 28 次，一般針對重要服務和知名網站進行攻擊，如銀行、信用卡支付網等。[1]

其他類型的資安風險，在台灣金融業中，2017 年遠東商業銀行受到北韓駭客組織入侵，盜走 6 千萬美元 (約 18 億元台幣)。[2] 台灣科技業半導體龍頭台積電，也遭遇產線機台及電腦系統中毒，造成台積電機台停擺，震撼全球半導體，認列損失 25.96 億元台幣。[3] 此外，在 2020 年爆發了台灣中油公司及台塑集團遭勒索病毒入侵系統的危機，造成內部網路系統無法正常運作。[4]

台灣是以金融業及科技業為主要發展之行業，金融業也佔有台灣市場很大一部分，若是資安事件發生，皆會影響到台灣整個經濟循環或國安危機，金融機構的資安風險管理相當重要。特別是客戶的信任和忠誠度，以及相對於競爭對手的市場地位已成為金融機構的關鍵戰略重點，金融機構在資安事件發生後對公司聲譽損害以及對民眾信心的影響是相當重要的議題。台灣從 2018 年金融科技的興起後，網路詐騙、資料外洩、挪用公款舞弊事件和系統中斷等事件連綿不斷，造成公司直接與間接損失高達上千萬元同時，也造成民眾對金融機構的不信任。

在數據當道的未來金融中，伴隨著開放銀行的資訊共享、銀行即服務的運用，輔以 AI 模型和金融上雲的科技導入，不僅擴大數據的應用場景，更深化了

[1] 詳細相關資訊可參見，eWeek 報導。檢閱日期：2023 年 1 月 25 日。檢自: https://www.eweek.com/security/ddos-attack-volume-escalates-as-new-methods-emerge/

[2] 詳細事件內容可參見，今周刊(遠東銀行被駭18億元兇找到了)。檢閱日期：2023年1月28日。檢自: https://www.businesstoday.com.tw/article/category/80392/post/201810040003/

[3] 詳細事件內容可參見，聯合新聞網(台積電3天痛失26億)。檢閱日期：2023年1月28日。檢自: https://udn.com/news/story/6839/5995368

[4] 詳細事件內容可參見，YAHOO 新聞(台灣中油遭勒索病毒攻擊 上千加油站系統癱瘓)。檢閱日期：2023年1月28日。檢自: https://tw.news.yahoo.com/%E5%8F%B0%E7%81%A3%E4%B8%AD%E6%B2%B9%E9%81%AD%E5%8B%92%E7%B4%A2%E7%97%85%E6%AF%92%E6%94%BB%E6%93%8A-%E4%B8%8A%E5%8D%83%E5%8A%A0%E6%B2%B9%E7%AB%99%E7%B3%BB%E7%B5%B1%E7%99%B1%E7%98%93-072752446.html

數據所提供洞察預測的能力。然而，伴隨著科技的發展，金融業也帶來不同的資安風險，例如網路銀行的線上交易模式引起駭客入侵、詐欺、盜刷等問題，以及未來開放銀行的開放應用程式介面 (Open API) 使用者介面資訊透明化。

不可否認的，金融科技雖然帶給傳統金融產業巨大的衝擊，但也創造出新的產業生態和全新的商業模式。最後，在 FinTech 蓬勃發展的同時，為了讓新興的產業模式與客戶之間達成平衡及有效預防不可預期的風險，因此，對於資安風險發生頻率的影響因子是我們想要進一步深入探討分析的，此外，我們也希望思考發展金融科技創新的同時，如何降低公司資安風險發生的機率以及維護聲譽，並且讓客戶對其產生信賴。透過我們的發現也希望建議金融機構該如何做好資安風險管理，並能提供相關資安風險保險的建議，帶給公司完善的保障。

第二章　　文獻探討

1. 金融科技與資安風險介紹

金融科技廣泛的定義是金融服務創新，泛指一群企業運用科技手段，使金融服務變得更有效率，而形成的一種經濟產業。金融科技可分為人工智慧、區塊鏈、雲端運算和大數據四大範疇。目前普羅大眾的使用，主要是在支付上，例如：悠遊卡、信用卡、Apple Pay、Line Pay、網上投保、第三方支付和行動支付等。此外金融科技的應用範圍還有加密貨幣、財務大數據、網路購物、網路銀行、純網銀等多種領域。然而，除了網際網路、資訊安全外，在技術上也運用人工智慧及區塊練技術做為基礎。[5]

目前許多先進國家也已設立相關資訊安全政策，讓金融科技受到保障。例如，保護資訊資產的機密性、完整性與可用性，而資訊安全管理系統利用營運風險方案為基礎，以建立、實施、操作、監督、審查、維持及改進資訊安全，避免遭受各種威脅及降低損害規模。[6] 對應金融科技發展，資安風險對金融機構的影響也逐漸增加，從巴塞爾協議 III 來看，資安風險做為作業風險的其中一樣樣態，如何進行監管也變得越來越重要。[7]

2. 金融科技發展與資安風險

科技對金融服務的影響，來自於行動通訊、社群媒體、雲端服務、大數據分析等。由於技術的快速發展，網路攻擊、數據欺詐和盜竊的事件已成為個人和企業面臨的常見危害。[8] 目前新興金融科技應用主要附加在銀行、保險、資產管理、資本市場等產業金融服務 (蔡福隆與張偉郎 2016)。然而，隨著金融科技發展，企業的資訊安全管理作法繁多，針對公司風險進行分析、建立風險評估模式以及對各種產業的資訊風險分析 (陳志誠等 2009)。因此，資安風險包含哪些類型，若是從巴塞爾協議 III 下作業風險的分類來看，可能包括 (1) 外部詐欺中的駭客攻擊與駭客竊取資料造成之財物損失。(2) 營運中斷與系統當機。(3) 執行、運送及作業流程之管理中的資料外洩事件。[9]

若是從實際案件與資安風險的型態來看，近年來科技使我們更方便、快速的達到目的及資訊，金融業也逐漸從 Bank 1.0 發展至 Bank 4.0。資安風險的態

[5] 詳細說明介紹可參見，什麼是金融科技（FinTech）？為什麼金融科技能給投資人創造翻倍的報酬？檢閱日期：2023年2月5日。檢自：https://startingedu.com/what-is-fintech/

[6] 詳細說明介紹可參見，如何擬定資安策略－從潛藏的資訊風險來看。檢閱日期：2023年2月8日。檢自：https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=5662

[7] 詳細說明介紹可參見，巴塞爾協議 III 更具彈性的銀行和銀行系統的全球監管框架。檢閱日期: 2023年2月5日。檢自：https://www-bis-org.translate.goog/publ/bcbs189.htm?_x_tr_sl=en&_x_tr_tl=zh-TW&_x_tr_hl=zh-TW&_x_tr_pto=sc

[8] 詳細說明介紹可參見，世界經濟論壇發布「2020全球風險報告」。檢閱日期：2023年2月8日。檢自：https://proj.ftis.org.tw/isdn/Message/MessageView/212?mid=57&page=1

[9] 詳細說明介紹可參見，TEJ 金融業作業風險資料庫模組說明。檢閱日期：2023年2月5日。檢自：https://www.tej.com.tw/webtej/doc/woprisk.htm

樣也變得日新月異，從 Bank 2.0 的 ATM 開始，國內外就有許多資安風險案件。例如，國外哈比銀行 (Habib Bank) ATM 盜卡事件損失 140 萬美元、台灣的第一銀行遭駭客入侵 ATM 盜走約 200 美元。[10]

Bank 2.0 的線上銀行服務，不只會帶來外部資安事件如 (釣魚程式)，還有內部資安事件 (自身系統中斷或網路更新)，例如，國泰世華銀行的網銀系統升級維護不當，造成客戶登入網銀延遲，ATM 及信用卡服務也須暫停使用，不但造成損失還可能危及客戶信用。[11] 跟著時代進步，智慧型手機的問世也帶動了 Bank 3.0，隨時隨地可以用手機做所有金融服務，如轉帳、支付、線上貸款及股票買賣等，但也成為網路犯罪的目標。例如，2021 年台灣證券業遭駭客攻擊，使用密碼撞庫方式，盜用客戶資料下單股票買賣，導致 6 家證券商受害，損失約 2000 萬元。[12]

隨著科技的發展，金融業正邁向 Bank 4.0，讓金融服務無處不在，也使台灣企業遭勒索攻擊間接不斷，這些警訊正提醒著我們，資安風險很重要，不只企業需要思考，個人與國家也需要共同面對這個未知風險。這也是商業與數位轉型科技迅速融合之下，所產生的商業風險。因此，對金融科技帶來的風險，政府也提出金融科技創新實驗辦法，一般也常被稱為監理沙盒，讓金融機構與監管機構也可以透過金融科技創新實驗，評估可能存在的資安風險 (李瑞倉 2017)。

而金融機構對應資安風險，金融機構可以如何因應，四大會計事務所也有分享如何建立策略和方案，避免資安風險事件造成的損害。例如，安永 (EY) 提供商業和 IT 間，資安風險評估與簽證服務，協助企業決策者。[13] 勤業眾信 (Deloitte) 成立網路安全團隊，提供全方位之物聯網裝置檢測、網路安全威脅分析和網路安全鑑識調查等服務。[14] 資誠 (PwC) 選擇適切的車載資安國際標準。[15] 另外，近期掀起一股熱潮生成式 AI，所衍生出的深假 (Deepfake) 危機，對此安侯建業 (KPMG) 建議三大策略，一、透過人工加工人智慧的打假工具協助工程師。二、建立智慧型主動式的防護能量和 MFA 多因子認證，讓消費者透過兩種以上的認證機制，才能取得授權。三、使用零信任資訊架構，依據不同服務風險等級、搭配多次且不同方式驗證，降低單一識別方法失效的損失。[16] 考量到

[10] 詳細事件內容可參見，駭客攻擊金融機構的手法和技巧(含歷年重大攻擊事件表）。檢閱日期：2023年2月5日。檢自：https://blog.trendmicro.com.tw/?p=59601
[11] 詳細事件內容可參見，國泰世華銀行系統頻出包 金管會年底前開罰 。檢閱日期：2023年2月5日。檢自：https://www.cna.com.tw/news/afe/202212050348.aspx
[12] 詳細事件內容可參見，「1125密碼撞庫攻擊」資安事件。檢閱日期：2023年1月17日。檢自：https://www.ctwant.com/article/154713
[13] 詳細事件內容可參見，科技風險。檢閱日期：2023年2月8日。檢自：https://www.ey.com/zh_tw/consulting/technology-risk-services
[14] 詳細事件內容可參見，資安時代來臨，勤業眾信搶商機。檢閱日期：2023年2月14日。檢自：https://www.chinatimes.com/realtimenews/20220214004659-260410?chdtv
[15] 詳細事件內容可參見，接軌車輛網路安全國際標準，降低資安風險。檢閱日期：2023年2月8日。檢自：https://www.pwc.tw/zh/news/press-release/press-20221215.html
[16] 詳細事件內容可參見，生成式 AI 恐引發資安危機 KPMG。檢閱日期：2023年2月14日。檢自：https://ctee.com.tw/news/policy/807265.html

不同會計事務所顧問部門所提供的種種建議，本研究也會探討簽證會計事務所對資安風險事件發生率是否有影響。

3. 資安風險與保險相關文獻

本研究為什麼針對金融機構的資安風險進行分析，主要的原因是金融機構的風險管理受到監管機關的特別重視，監管機關特別要求銀行和保險公司進行風險資本額的計算，其中也包括資安風險。然而，資安風險事件可能會對受影響的企業造成相當大的後果。根據安聯集團的報告，業務中斷是其中一種重要的資安風險，因此，對於了解資安風險顯得格外重要。[17]

本研究主要參考，Gatzert and Schubert (2022) 所做的研究，Gatzert and Schubert (2022) 使用文字探討分析，建構金融機構資安風險意識評分，根據公司的資安風險管理進行分類，探討決定因素和價值相關性。估計企業持續改進資安風險管理 (CyberRM) 分數探討對資安事件發生的影響。

另外過往關於資安風險的研究主要集中在數據、資訊和互聯網的市場反應，或者特定的攻擊方法、網路攻擊對公司的聲譽、風險管理以及傳染效應的影響。除了探討資安風險管理的應用外， Camillo (2017) 提出資安風險保險的重要。面對資安的新興風險，發現資安風險保險的商品主要針對資料外洩造成的損失與成本來做補償，讓保險公司能夠將其部分風險轉移到再保險 (保險公司的保險) 和資本市場 (通過巨災債券等工具)。目前資安保險的功能有第一方和第三方風險，包括數字資產丟失、數據恢復、業務中斷、通知成本、數據洩露責任、員工不誠實、網絡勒索和監管防禦成本。而從保險業來說，目前在資安風險管理上做得比其他機構來的更好。

若是要發展資安保險，就需要建構資安風險模型，Eling and Wirfs (2019) 考慮整個資安風險，提出從作業風險資料庫中挑選資安損失事件，如數據洩露和丟失的記錄數量以及實際損失的資訊，並使用極值理論中的峰值超過閾值方法來識別日常生活中的資安風險。因此，除了了解整個資安風險範圍外，還需知道公司資安風險實際損失金額，才能作為保險公司估算保費的數據資料。Eling, Jung and Shim (2022) 利用分位數回歸，以便在投保人之間提供適當的資安保險定價，並計算與數據洩露事件相關的索賠成本。

另外，Erola et al. (2020) 提出一個計算資安風險價值 (CVaR) 的系統。CVaR 是資安事件損失的概率密度函數，適用於任何給定的利益威脅和風險控制，然而，資安風險模型必須考慮資產、攻擊者概況和漏洞，所以需要資安風險評估 (CRA) 領域的結合，才能讓 CVaR 產生實際財務損失預測、提供資安保險公司使用以及推斷特定風險的設置對該公司資安風險有無降低。Chen and Leong (2022) 使用資料外洩資料庫，分析不同行業的資安風險，估算損失模型並評估

[17] 詳細說明介紹可參見，2020年安聯風險晴雨表。檢閱日期：2023年2月8日。檢自：https://www.allianz.com/en/press/news/studies/200114_Allianz-risk-barometer-2020.html

風險管理措施對資安風險保險的效益，發現無論是內部和外部資安風險，保險業在風險管理上都有較低的損失頻率與幅度。

目前尚不清楚是什麼那些因素會導致資安風險事件，為了更深入地了解資安風險的性質，探討對其損失模型是否也可以應用於資安風險。過往許多文獻先針對資安風險建模進行討論，再進行後續探討，例如，Malavasi et al. (2022) 針對資安風險的類型進行分析，探討不同類型的資安風險在損失頻率與損失幅度之間是否有差異，也探討不同類型資安風險的可保性。 Pollmeier, Bongiovanni and Slapničar (2023) 設計量化模型協助銀行評估資安事件的直接與間接成本，也發現間接成本包括商譽損失的估算非常困難。

雖然本研究並非針對資安風險管理的做法進行研究，但是還是發現有許多文獻針對資安風險管理的做法進行介紹。Marotta and McShane (2018) 提出一種主動網路防禦技術蜜罐(honeypot)。蜜罐是一種偽裝的電腦系統，做為吸引駭客入侵的技術，能夠主動網絡防禦及掌握攻擊者的信息，順勢推進網絡威脅情報，以及提供法庭認可的取證證據，並且可以檢測內部和外部攻擊。然而，面對資安事件的發生不只需要網路技術上的改善和開發，我們也需要為資安風險進行了解、分類及分析，讓整個資安保護更加完善。

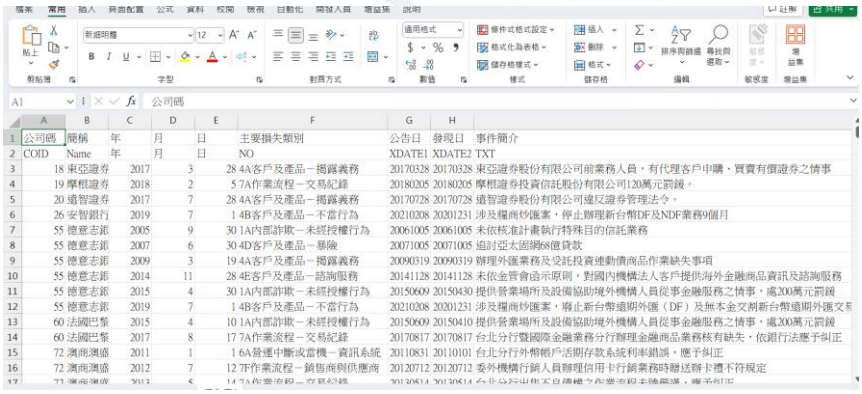
第三章　　研究設計與實施

第一節　資料蒐集

探討近年來金融科技發展對資安風險事件造成的影響，本研究主要以台灣銀行業、人壽保險業進行研究，同時結合 TEJ 金融資料庫中公司的報表資訊以及作業風險資料庫中的資安風險事件，其中 TEJ 金融業作業風險資料庫根據 Base1 III 規範下，根據不同類型的作業風險損失事件型態作為分類，包括以下幾種類型，內部詐欺、外部詐欺、僱用慣例、工作場所安全、客戶、產品、營業行為、人員或資產損失、營運中斷與系統當機以及執行、運送及作業流程之管理。

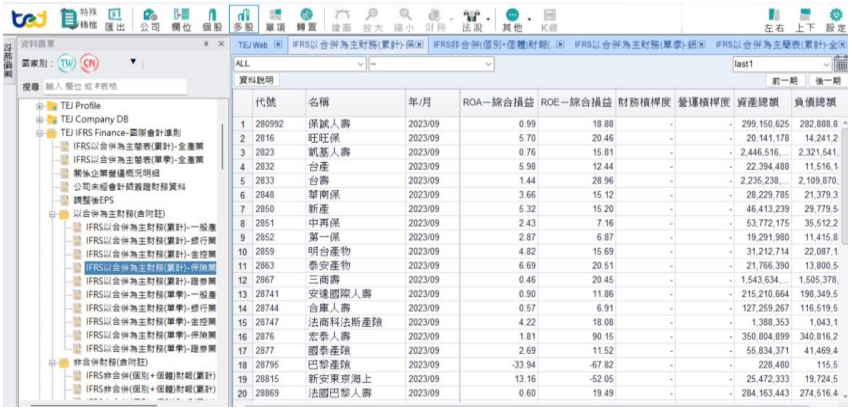
TEJ 金融業作業風險資料庫資料期間包括自 1984 年至今台灣金融機構的作業風險事件，資料來源包括金管會重大裁罰公告、證期局違規案件查詢、證交所&櫃買中心公告、公開資訊觀測站、TEJ 新聞資料庫、公平交易委員會。我們從 TEJ 金融業作業風險資料庫的損失事件型態裡，選取外部系統-系統安全、營運中斷或當機-資訊系統之管理中的資料外洩事件做為資安風險事件的主要研究對象，並從中觀察事件介紹，將事件介紹中有關系統安全地列為資安風險事件。選取原因為外部詐欺可能因為科技發展而增加，包括駭客攻擊、竊取資料造成之財物損失、公司網路系統更新及中斷所導致損失和公司資料外洩事件增加之情形，本研究預計選取台灣本國銀行、純網路銀行、人壽保險公司(圖一)。

另外我們也使用(圖二)TEJ 金融資料庫，蒐集銀行、保險各公司基本面資訊，抓取的資料為各公司的 ROA-綜合損益、ROE-綜合損益、資產總額、負債總額、會計事務所及公司成立年月。



公司碼	簡稱	年	月	日	主要損失類別	公告日	發現日	事件簡介
COID	Name	年	月	日	NO	XDATE1	XDATE2	TXT
18	東亞證券	2017	3	28	4A客戶及產品－揭露義務	20170328	20170328	東亞證券股份有限公司前業務人員，有代理客戶中購、買賣有價證券之情事
19	摩根證券	2018	2	5	7A作業流程－交易紀錄	20180205	20180205	摩根證券投資信託股份有限公司120萬元罰鍰。
20	遠智證券	2017	7	28	4A客戶及產品－揭露義務	20170728	20170728	遠智證券股份有限公司違反證券管理法令。
26	安智銀行	2019	7	1	4B客戶及產品－不當行為	20210208	20201231	涉及權商炒匯案，停止辦理新台幣DF及NDF業務9個月
55	德意志銀	2005	9	30	1A內部詐欺－未經授權行為	20061005	20061005	未依核准計畫執行特殊目的信託業務
55	德意志銀	2007	6	30	4D客戶及產品－暴險	20071005	20071005	追討亞太固網68億貸款
55	德意志銀	2009	3	19	4A客戶及產品－揭露義務	20090319	20090319	辦理外匯業務及受託投資連動債商品作業缺失事項
55	德意志銀	2014	11	28	4E客戶及產品－諮詢服務	20141128	20141128	未依金管會函示原則，對國內機構法人客戶提供海外金融商品資訊及諮詢服務
55	德意志銀	2015	4	30	1A內部詐欺－未經授權行為	20150609	20150430	提供營業場所及設備協助境外機構人員從事金融服務之情事，處200萬元罰鍰
55	德意志銀	2019	7	1	4B客戶及產品－不當行為	20210208	20201231	涉及權商炒匯案，暫止新台幣遠期外匯（DF）及無本金交割新台幣遠期外匯交易
60	法國巴黎	2015	4	10	1A內部詐欺－未經授權行為	20150609	20150410	提供營業場所及設備協助境外機構人員從事金融服務之情事，處200萬元罰鍰
60	法國巴黎	2017	8	17	7A作業流程－交易紀錄	20170817	20170817	台北分行暨國際金融業務分行辦理金融商品業務核有缺失，依銀行法應予糾正
72	澳商澳盛	2011	1	1	6A營運中斷或當機－資訊系統	20110831	20110101	台北分行外幣帳戶活期存款系統利率錯誤，應予糾正
72	澳商澳盛	2012	7	12	7F作業流程－銷售商與供應商	20120712	20120712	委外機構行銷人員辦理信用卡行銷業務時贈送辦卡禮不符規定

（圖一）為 TEJ 金融業作業風險資料庫的損失事件



	代號	名稱	年/月	ROA－綜合損益	ROE－綜合損益	財務槓桿度	營運槓桿度	資產總額	負債總額
1	280992	保誠人壽	2023/09	0.99	18.88	-	-	299,150,625	282,888,8
2	2816	旺旺保	2023/09	5.70	20.46	-	-	20,141,178	14,241,2
3	2823	凱基人壽	2023/09	0.76	15.81	-	-	2,446,516,...	2,321,541,
4	2832	台產	2023/09	5.98	12.44	-	-	22,394,488	11,516,1
5	2833	台壽	2023/09	1.44	28.96	-	-	2,235,238,...	2,109,870,
6	2848	華南保	2023/09	3.66	15.12	-	-	28,229,785	21,379,3
7	2850	新產	2023/09	5.32	15.20	-	-	46,413,239	29,779,5
8	2851	中再保	2023/09	2.43	7.16	-	-	53,772,175	35,512,2
9	2852	第一保	2023/09	2.87	6.87	-	-	19,291,980	11,415,8
10	2859	明台產物	2023/09	4.82	15.69	-	-	31,212,714	22,087,1
11	2863	泰安產物	2023/09	6.69	20.51	-	-	21,766,390	13,800,5
12	2867	三商壽	2023/09	0.46	20.45	-	-	1,543,634,...	1,505,378,
13	28741	安達國際人壽	2023/09	0.90	11.86	-	-	215,210,664	198,349,5
14	28744	合庫人壽	2023/09	0.57	6.91	-	-	127,259,267	116,519,5
15	28747	法商科法斯產險	2023/09	4.22	18.08	-	-	1,388,353	1,043,1
16	2876	宏泰人壽	2023/09	1.81	90.15	-	-	350,804,899	340,816,2
17	2877	國泰產險	2023/09	2.69	11.52	-	-	55,834,371	41,469,4
18	28795	巴黎產險	2023/09	-33.94	-67.82	-	-	228,480	115,5
19	28815	新安東京海上	2023/09	13.16	-52.05	-	-	25,472,333	19,724,5
20	28869	法國巴黎人壽	2023/09	0.60	19.49	-	-	284,163,443	274,516,4

（圖二）為 TEJ 金融資料庫中銀行、保險各公司基本面資訊

另外本研究利用公開資訊觀測站平臺，收集了2012年至2022年間，共11年，銀行和保險公司的年報資料。公開資訊觀測站作為一個提供上市公司相關資訊的公開平臺，為我們提供了各公司完整的年報來源。這些報告包含了公司財務狀況、經營績效以及風險管理等相關信息。使我們能夠方便地獲取並並了解研究期間內銀行和保險公司的年報中對於金融科技及資訊安全是否重視與發展程度。

	證券代碼	年月	是否資安事件	資安事件筆數	是否作業風險	作業風險筆數	Fintech	Cyber	ROA	ROE	BIS	槓桿比率	會計四大	資產規模
12	2801 彰銀	2022	0	0	0	0	11	2	0.11	1.66	14.37	0.00792129	1	9.428920402
23	2807 澄打銀行	2022	0	0	0	0	3	1	0.32	4.72	16.34	-1.239667484	1	8.850503654
34	2809 京城銀	2022	0	0	0	0	7	0	-1.04	-8.24	14.05	-1.116370453	1	8.579768507
45	2812 台中銀	2022	0	0	1	1	0	0	0.5	5.92	15.77	0.275485119	1	8.907391381
56	2834 臺企銀	2022	0	0	1	1	8	2	0.16	3.13	12.48	0.428862053	1	9.316491632
67	2836 高雄銀	2022	0	0	1	1	5	4	-0.39	-6.56	12.36	-2.700022628	0	8.445787274
78	2837 凱基銀行	2022	0	0	0	0	1	0	-0.13	-1.56	14.19	34.79046722	1	8.886459604
89	2838 聯邦銀	2022	0	0	1	1	0	0	-0.38	-4.94	14.59	-1.019363599	1	8.926856675
100	2845 遠東銀	2022	0	0	1	2	8	4	0.26	3.7	14.98	1.706930329	1	8.869548313
111	2849 安泰銀	2022	0	0	1	1	2	0	-0.2	-2.02	16.3	-1.004898099	1	8.542471628
122	2893 新光銀行	2022	0	0	0	0	6	2	-0.5	-9.05	14.38	1.302550226	1	9.083464735
133	2895 陽信商銀	2022	0	0	1	1	4	0	0.21	3.61	13.03	0.634902563	1	8.830814696
144	2897 王道銀行	2022	0	0	0	0	22	2	0.11	1.15	14.49	-1.415045507	1	8.761434005
155	5830 三信銀行	2022	0	0	0	0	7	1	0.39	5.56	13.04	0.394812909	1	8.274056192
166	5835 國泰世華	2022	1	1	1	3	6	0	0.2	2.96	15.05	0.041383946	1	9.589618018

（圖三）為銀行業在過去10年內是否發生資安事件統計

	證券代碼	年月	是否資安事件	資安事件筆數	是否作業風險	作業風險筆數	Fintech	Cyber Risk	資產規模	ROE	ROA	四大會計	RBC	槓桿比率
12	2823 中壽	2022	0	0	1	3	9	0	9.37052879	-2.83	-46.47	1	280.42	21.00530777
23	2833 台壽	2022	0	0	1	3	3	4	9.334275008	-3.04	-51.13	1	275.16	22.07584819
34	2848 華南保	2022	0	0	0	0	0	0	7.38700388	-2.25	-8.47	1	383.03	3.140696364
45	2863 泰安產物	2022	0	0	0	0	9	0	7.35247469	-5.42	-16.62	1	587.67	2.472457638
56	2877 國泰產險	2022	0	0	0	0	7	2	7.782441527	-38.16	-154.77	1	368.76	3.734137278
67	2828 富邦保	2022	0	0	0	0	1	2	8.056295749	-41.08	-198.97	1	-37.25	20.76065298
78	5831 新壽	2022	0	0	1	6	3	1	9.552152279	-1.46	-31.87	1	213.64	24.57352759
89	5834 兆豐保險	2022	0	0	1	1	0	0	7.426175	-41.67	-247.45	1	-8.8	2090.676519
100	5846 國壽	2022	0	0	1	6	4	3	9.912351208	-3.57	-48.03	1	316.46	16.54535878
111	5865 富邦人壽	2022	0	0	1	2	2	3	9.748407469	-5.64	-72.1	1	315.03	19.37309457
122	5873 全球人壽	2022	0	0	1	2	3	0	9.134654933	-2.93	-86.07	1	366.46	51.4417459
133	5874 南山人壽	2022	0	0	0	0	3	4	9.722297463	-4.24	-56.44	1	292.42	17.73705984
144	2850 新產	2022	0	0	0	0	2	0	7.643498936	1.78	5.18	1	432.38	1.927798919
155	2851 中再保	2022	0	0	0	0	0	0	7.701324341	-3.71	-11.04	1	434.86	1.957555789
166	2852 第一保	2022	0	0	0	0	0	0	7.246835275	3.8	8.84	1	867.18	1.334360414
177	2867 三商壽	2022	0	0	1	1	6	8	9.16382698	-1.5	-61.06	1	155.83	49.54840734
188	2816 旺旺保	2022	0	0	0	0	3	0	7.262489344	-7.57	-25.13	1	468.47	2.808984583

（圖四）為保險業在過去10年內是否發生資安事件統計

第二節　研究資料

Pearson 相關係數之大小，可看出兩變項關係的密切程度。相關係數愈高，兩變項之關係愈密切，愈低表示愈不相關。我們採用資安事件比數、作業風險比數、是否發生資安事件及是否發生作業風險事件為被解釋變數，並探討 P-value 數值是否有顯著性，定義P-value大於0.1為有顯著。(圖五)為銀行業皮爾森相關係數；(圖六)為保險業皮爾森相關係數。

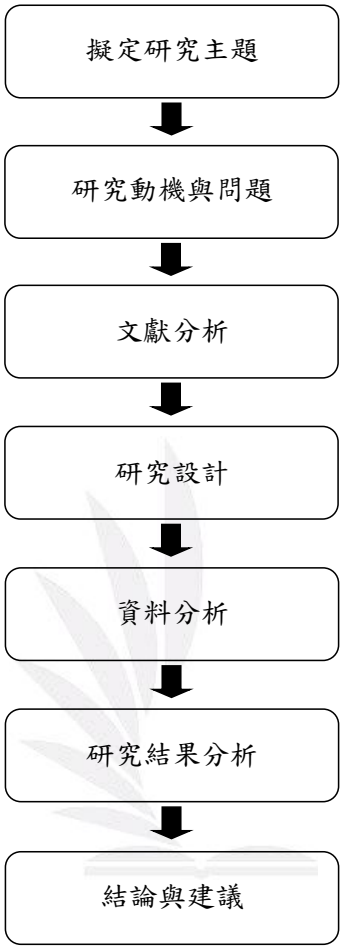
資安事件筆數	Text (Fintech)	Text (Cyber Risk)	Ln(Asset)	ROA	BIS	四大會計事務所	槓桿比率
Cor	0.073	0.106	0.120	0.082	0.023	0.053	-0.014
P-value	0.166	0.044	0.022	0.117	0.665	0.313	0.790
作業風險筆數	Text (Fintech)	Text (Cyber Risk)	Ln(Asset)	ROA	BIS	四大會計事務所	槓桿比率
Cor	0.073	0.106	0.120	0.082	0.023	0.053	-0.014
P-value	0.166	0.044	0.022	0.117	0.665	0.313	0.790
是否資安事件	Text (Fintech)	Text (Cyber Risk)	Ln(Asset)	ROA	BIS	四大會計事務所	槓桿比率
Cor	0.094	-0.027	0.217	0.055	0.071	0.009	0.021
P-value	0.075	0.602	0.00003	0.293	0.180	0.859	0.686
是否作業風險	Text (Fintech)	Text (Cyber Risk)	Ln(Asset)	ROA	BIS	四大會計事務所	槓桿比率
Cor	0.008	0.033	0.155	0.121	0.053	0.023	0.043
P-value	0.886	0.525	0.003	0.021	0.313	0.663	0.409

(圖五)為銀行業皮爾森相關係數

資安事件筆數	Text (Fintech)	Text (Cyber Risk)	Ln(Asset)	ROA	槓桿比率
Cor	0.039	0.094	0.169	0.191	-0.005
P-value	0.576	0.174	0.015	0.006	0.943
作業風險筆數	Text (Fintech)	Text (Cyber Risk)	Ln(Asset)	ROA	槓桿比率
Cor	0.039	0.094	0.169	0.191	-0.005
P-value	0.576	0.174	0.015	0.006	0.943
是否資安事件	Text (Fintech)	Text (Cyber Risk)	Ln(Asset)	ROA	槓桿比率
Cor	0.220	0.009	0.331	0.053	0.001
P-value	0.001	0.893	0.0000009	0.443	0.990
是否作業風險	Text (Fintech)	Text (Cyber Risk)	Ln(Asset)	ROA	槓桿比率
Cor	0.134	0.064	0.193	0.035	0.070
P-value	0.053	0.354	0.005	0.615	0.317

(圖六) 為保險業皮爾森相關係數

第三節　研究流程圖



研究流程圖（圖七）

第四節　研究模型

本研究主要根據 Gatzert and Schubert (2022) 使用的研究方法與模型進行改良，並探討資安發生的決定因素，研究模型如下式：

$$\ln\left(\frac{p(Cyber=1)}{1-p(Cyber=1)}\right)=\beta_1 Fintech+\beta_2 RM+\beta_3\, Size+\beta_4 ROA+\beta_5\, BIS+\beta_6\, Account+\beta_7 Leverage+\varepsilon \quad (1)$$

（公式一）為銀行業的研究模型

$$\ln\left(\frac{p(Cyber=1)}{1-p(Cyber=1)}\right)=\beta_1 Fintech+\beta_2 RM+\beta_3\, Size+\beta_4 ROA+\beta_5 Leverage+\varepsilon \quad (2)$$

（公式二）為保險業的研究模型

（公式一)為銀行業的研究模型，其中 Cyber 為是否發生資安事件的代理變數、Fintech 為金融科技發展程度的代理變數、RM 為公司重視資訊安全程度的代理變數，另外也考量不同簽證會計事務所(Account)、公司獲利能力(ROA)、資本適足度(BIS)、公司規模(Size)、公司槓桿(Leverage)作為控制變數。

（公式二)為保險業的研究模型，其中 Cyber 為是否發生資安事件的代理變數、Fintech 為金融科技發展程度的代理變數、RM 為公司重視資訊安全程度的代理變數，而公司獲利能力(ROA)、公司規模(Size)、公司槓桿(Leverage)作為控制變數。

其中，是否發生資安事件的代理變數，會根據資安保險理賠方法進行定義，包括以下四種資安事件的衡量方式：（1)今年度該公司是否曾經發生資安事件（2）今年度公司是否曾經發生外部事件，例如：駭客入侵造成網路系統更新及中斷或是資料外洩（3）今年度公司是否曾經發生內部事件: 例如：自身網路系統更新及中斷（4）發生資安事件總次數(損失事件型態進行資安風險)。

主要的被解釋變數為公司是否有提供金融科技創新服務以及公司重視資訊安全的程度，Fintech 為公司年報中提到金融科技次數。另外公司重視資訊安全程度的代理變數，則會考量公司年報中提到資安風險次數。

第五節　研究方法

1.我們使用 lm()函式，分別對銀行業和保險業進行分析 ols 回歸模型，被解釋變數有兩個，一是資安事件筆數，二是作業風險筆數，共六條回歸式。下(圖八)為銀行業；(圖九)為保險業。

```
result_bank = lm(資安事件筆數~Fintech+Cyber+ROA+BIS+槓桿比率+會計四大+資產規模,data = bank_all)
result_bank = lm(資安事件筆數~Fintech+ROA+BIS+槓桿比率+會計四大+資產規模,data = bank_all)
result_bank = lm(資安事件筆數~Cyber+ROA+BIS+槓桿比率+會計四大+資產規模,data = bank_all)

result_bank = lm(作業風險筆數~Fintech+Cyber+ROA+BIS+槓桿比率+會計四大+資產規模,data = bank_all)
result_bank = lm(作業風險筆數~Fintech+ROA+BIS+槓桿比率+會計四大+資產規模,data = bank_all)
result_bank = lm(作業風險筆數~Cyber+ROA+BIS+槓桿比率+會計四大+資產規模,data = bank_all)
```

（圖八）為銀行業 ols 回歸模型分析

```
Ins_result = lm(資安事件筆數~Fintech+Cyber+資產規模+ROA+槓桿比率,data = Ins_all)
Ins_result = lm(資安事件筆數~Fintech+資產規模+ROA+槓桿比率,data = Ins_all)
Ins_result = lm(資安事件筆數~Cyber+資產規模+ROA+槓桿比率,data = Ins_all)

Ins_result = lm(作業風險筆數~Fintech+Cyber+資產規模+ROA+槓桿比率,data = Ins_all)
Ins_result = lm(作業風險筆數~Fintech+資產規模+ROA+槓桿比率,data = Ins_all)
Ins_result = lm(作業風險筆數~Cyber+資產規模+ROA+槓桿比率,data = Ins_all)
```

（圖九）為保險業 ols 回歸模型分析

2.我們使用 glm()函式，分別對銀行業和保險業進行分析 logistic 回歸模型，被解釋變數有兩個，一是是否發生資安事件，二是是否發生作業風險，共六條回歸式。下(圖十)為銀行業；(圖十一)為保險業。

```
model_bank= glm(是否資安事件 ~Fintech+Cybe+ROA+BIS+槓桿比率+會計四大+資產規模 ,
                family = binomial(link="logit"),data = bank_logist)
model_bank= glm(是否資安事件 ~Fintech+ROA+BIS+槓桿比率+會計四大+資產規模 ,
                family = binomial(link="logit"),data = bank_logist)
model_bank= glm(是否資安事件 ~Cyber+ROA+BIS+槓桿比率+會計四大+資產規模 ,
                family = binomial(link="logit"),data = bank_logist)
model_bank= glm(是否作業風險 ~Fintech+Cybe+ROA+BIS+槓桿比率+會計四大+資產規模 ,
                family = binomial(link="logit"),data = bank_logist)
model_bank= glm(是否作業風險 ~Fintech+ROA+BIS+槓桿比率+會計四大+資產規模 ,
                family = binomial(link="logit"),data = bank_logist)
model_bank= glm(是否作業風險 ~Cyber+ROA+BIS+槓桿比率+會計四大+資產規模 ,
                family = binomial(link="logit"),data = bank_logist)
```

（圖十）為銀行業 logistic 回歸模型分析

```
model_Ins =glm(是否資安事件~Fintech+Cyber資產規模+ROA+槓桿比率 ,
                family = binomial(link="logit"),data = Ins_logist)
model_Ins =glm(是否資安事件~Fintech+資產規模+ROA+槓桿比率 ,
                family = binomial(link="logit"),data = Ins_logist)
model_Ins =glm(是否資安事件~Cyber+資產規模+ROA+槓桿比率 ,
                family = binomial(link="logit"),data = Ins_logist)
model_Ins =glm(是否作業風險~Fintech+Cyber資產規模+ROA+槓桿比率 ,
                family = binomial(link="logit"),data = Ins_logist)
model_Ins =glm(是否作業風險~Fintech+資產規模+ROA+槓桿比率 ,
                family = binomial(link="logit"),data = Ins_logist)
model_Ins =glm(是否作業風險~Cyber+資產規模+ROA+槓桿比率 ,
                family = binomial(link="logit"),data = Ins_logist)
```

（圖十一）為保險業 logistic 回歸模型分析

第四章　實證結果與分析

第一節 ols 回歸模型結果

格式化: 字型: (英文)Calibri, (中文) 新細明體, 字型色彩: 自動, (中文) 中文 (香港特別行政區)

格式化: 內文, 間距 套用前: 0 點, 套用後: 0 點

分別探討年報中提到 Fintech、Cyber Risk 兩個變數於銀行業、保險業，發現資產規模不會受到這兩個 text 變數而改變顯著性。下表1、表2為銀行業與保險業發生資安事件筆數和發生作業風險筆數的顯著因子有哪些。

表1 銀行業研究結果比較（*Table 1*）

	(1) N(CyberEvent)	(2) N(CyberEvent)	(3) N(CyberEvent)	(4) N(OPrisk)	(5) N(OPrisk)	(6) N(OPrisk)
Text (Fintech)	0.002		0.003	0.017**		0.012
	(0.002)		(0.002)	(0.011)		(0.011)
Text (Cyber Risk)	0.016*	0.018*		-0.068	-0.049	
	(0.009)	(0.009)		(0.044)	(0.042)	
Ln(Asset)	0.065**	0.068**	0.067**	0.611***	0.642***	0.601***
	(0.033)	(0.032)	(0.033)	(0.152)	(0.150)	(0.152)
ROA	0.067*	0.062*	0.066*	0.233	0.196	0.234
	(0.037)	(0.036)	(0.037)	(0.171)	(0.169)	(0.171)
BIS	-0.001	-0.009	-0.008	0.016	0.028	0.006
	(0.009)	(0.009)	(0.009)	(0.044)	(0.043)	(0.044)
槓桿比率	-0.0001	-0.0003	-0.0002	0.006	0.004	0.006
	(0.002)	(0.002)	(0.002)	(0.011)	(0.011)	(0.011)
四大會計事務所	0.050	0.050	0.037	-0.442	-0.442	-0.384
	(0.089)	(0.089)	(0.089)	(0.413)	(0.414)	(0.412)
Constant	-0.468	-0.503*	-0.506*	-4.283***	-4.617***	-4.110***
	(0.289)	(0.285)	(0.289)	(1.342)	(1.326)	(1.340)
Observations	363	363	363	363	363	363
R-squared	0.015	0.017	0.011	0.045	0.042	0.041

Note: The dependent variable is total automobile insurance premium. *** indicates significance at the 1% level; ** indicates significance at the 5% level; and * indicates significance at the 10% level.

表2 保險業研究結果比較（*Table 2*）

	(1) N(CyberEvent)	(2) N(CyberEvent)	(3) N(CyberEvent)	(4) N(OPrisk)	(5) N(OPrisk)	(6) N(OPrisk)
Text (Fintech)	0.0007			0.096***		0.093**
	(0.004)		0.002 (0.004)	(0.037)		(0.036)
Text(CyberRisk)	0.021*					
	(0.011)	0.021* (0.011)		-0.070 (0.094)	-0.043 (0.095)	
Ln(Asset)	0.033**			0.552***	0.606***	0.540***
	(0.014)	0.034** (0.014)	0.037** (0.014)	(0.119)	(0.119)	(0.117)
ROA	0.002***	0.002***	0.002***	0.005	0.004	0.005
	(0.0004)	(0.0004)	(0.0004)	(0.004)	(0.004)	(0.004)
槓桿比率	0.0002**	0.0002**	0.0002*	0.001	0.001	0.001
	(0.0001)	(0.0001)	(0.0001)	(0.001)	(0.001)	(0.001)
	-0.255**			-3.338***	-3.597***	-3.256***
Constant		-0.257**	-0.270**			
	(0.119)	(0.118)	(0.119)	(0.977)	(0.985)	(0.969)
Observations	209	209	209	209	209	209
R-squared	0.075	0.070	0.064	0.125	0.100	0.127

Note: The dependent variable is total automobile insurance premium. *** indicates significance at the 1% level; ** indicates significance at the 5% level; and * indicates significance at the 10% level.

第二節羅吉斯回歸模型結果

分別探討年報中提到Fintech、Cyber Risk兩個變數於銀行業、保險業，對於資安事件與作業風險事件是否發生使用（0,1）表示，並發現保險業規模越大，出現Cyber Risk次數越多，資安事件反而越多。下表3、表4為銀行業與保險業是否發生資安事件與是否發生作業風險的顯著因子有哪些。

表3 銀行業研究結果比較（*Table 3*）

	(1) CyberEvent	(2) CyberEvent	(3) CyberEvent	(4) OP Risk	(5) OP Risk	(6) OP Risk
Text (Fintech)	0.027		0.035	-0.004		-0.002
	(0.030)		(0.029)	(0.019)		(0.018)
Text (Cyber Risk)	0.126	0.144		0.034	0.029	
	(0.091)	(0.089)		(0.077)	(0.073)	
Ln(Asset)	1.007**	1.035**	1.068**	0.726***	0.718***	0.729***
	(0.480)	(0.489)	(0.494)	(0.252)	(0.249)	(0.252)
ROA	0.934**	0.878*	0.941**	0.680**	0.690**	0.679**
	(0.471)	(0.472)	(0.460)	(0.298)	(0.295)	(0.298)
BIS	-0.145	-0.111	-0.114	-0.003	-0.005	0.002
	(0.145)	(0.136)	(0.141)	(0.072)	(0.071)	(0.071)
槓桿比率	-0.001	-0.004	-0.002	0016	0.016	0.016
	(0.025)	(0.026)	(0.025)	(0.018)	(0.018)	(0.018)
四大會計事務所	14.47	14.45	14.426	-0.337	-0.338	-0.366
	(1190)	(1190)	(1189.686)	(0.658)	(0.658)	(0.655)
Constant	-24.83	-25.34	-25.611	-6.045***	-5.961***	-6.107***
	(1190)	(1190)	(1189.686)	(2.215)	(2.182)	(2.210)
Observations	363	363	363	363	363	363
log-likelihood	-97.097	-97.484	-97.964	-235.093	-235.118	-235.194

Note: The dependent variable is total automobile insurance premium. *** indicates significance at the 1% level; ** indicates significance at the 5% level; and * indicates significance at the 10% level.

表4 保險業研究結果比較（*Table 4*）

	(1) CyberEvent	(2) CyberEvent	(3) CyberEvent	(4) OP Risk	(5) OP Risk	(6) OP Risk
Text (Fintech)	0.039		0.043	0.099*		0.103*
	(0.105)		(0.101)	(0.054)		(0.054)
Text (Cyber Risk)	0.358*	0.363*		0.101	0.128	
	(0.189)	(0.189)		(0.153)	(0.150)	
Ln(Asset)	0.818	0.848*	0.837	0.041	0.1445	0.066
	(0.509)	(0.505)	(0.513)	(0.240)	(0.232)	(0.235)
ROA	0.053***	0.052***	0.048***	0.012**	0.011*	0.011*
	(0.016)	(0.016)	(0.015)	(0.006)	(0.006)	(0.006)
槓桿比率	0.007	0.006	0.006	0.041*	0.035*	0.041*
	(0.006)	(0.006)	(0.006)	(0.021)	(0.021)	(0.021)
Constant	-11.636**	-11.785***	-11.478**	-0.564	-1.158	-0.729
	(4.550)	(4.563)	(4.533)	(1.785)	(1.741)	(1.756)
Observations	209	209	209	209	209	209
log-likelihood	-26.480	-26.547	-27.767	-128.957	-130.756	-129.197

Note: The dependent variable is total automobile insurance premium. *** indicates significance at the 1% level; ** indicates significance at the 5% level; and * indicates significance at the 10% level.

表4 保險業研究結果比較（*Table 4*）

第五章　　結論與建議

第一節　研究結論

我們分別探討年報中提到 Fintech、Cyber Risk 兩個變數，排列組合於每個回歸式中，發現銀行業的資產規模不會受到此兩個 text 變數而改變顯著性，而獲利越高，則越常發生資安事件與作業風險。此外，也發現保險業資產規模越大，年報中提到 Cyber Risk 次數會越多，發生資安風險筆數也越多。

第二節　未來研究方向

未來的研究可以更深入地探究區塊鏈技術、人工智慧、雲端運算，以及資安防範措施在金融科技領域中的應用，並評估這些相關活動的出現次數對資安風險的影響。這樣的研究能夠提供更細緻的分析，深化我們對於金融科技發展與資安風險之間複雜關係的理解。

另外未來的研究可以探討改進研究方法，特別是在分析重視資安風險與金融科技出現次數之間的因果關係時。應考慮采用更精確的統計方法，例如:因果關係的檢核，以區分是金融科技影響資安風險，或是反之。同時，引入固定效果模型和隨機效果模型，以更精確地評估這些變數之間的複雜關係。總體而言，未來的研究可以進一步深化對金融科技發展中各因素之間關聯性的理解。

參考文獻

一、 中文部份

1. 李瑞倉（2017），金融科技發展與監理。*管理與法遵*，第 2 卷 第 1 期，1-20 頁。
2. 陳志誠、林淑瓊、李興漢與許派立（2009），資訊資產分類與風險評鑑之研究－以銀行業為例。*資訊管理學報*，第 16 卷 第 3 期，55-84 頁 。
3. 蔡福隆、張偉郎（2016），金融科技之發展趨勢與因應。*亞洲金融季報*，2016 春季號，37-43 頁。

二、 英文部份

1. Chen, Y. C., & Leong, Y. Y. (2022). The Effect of Cyber Risk Management Services in Insurance Policies. In *Advances in Pacific Basin Business, Economics and Finance*. Emerald Publishing Limited.
2. Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, *2*(1), 53-63.
3. Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events?European Journal of Operational Research, 272(3), 1109-1119.
4. Eling, M., Jung, K., & Shim, J. (2022). Unraveling heterogeneity in cyber riskusing quantile regressions. *Insurance: Mathematics and Economics*, *104*, 222-242.
5. Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L. A., ... & Lin, H. (2019). Cyber risk research impeded by disciplinary barriers. *Science*, *366*(6469), 1066-1069.Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *Journal of Risk and Insurance*, *89*(3), 725-763.
6. Malavasi, M., Peters, G. W., Shevchenko, P. V., Trück, S., Jang, J., & Sofronov, G. (2022). Cyber risk frequency, severity and insurance viability. *Insurance: Mathematics and Economics*, *106*, 90-114.
7. Marotta, A., & McShane, M. (2018). Integrating a proactive technique into a holisticcyber risk management approach.Risk Management and InsuranceReview,21(3),435-452.
8. Pollmeier, S., Bongiovanni, I., & Slapničar, S. (2023). Designing a financial quantification model for cyber risk: A case study in a bank. *Safety Science*, *159*, 106022.