

CYBERSEC 2024
臺灣資安大會

5/14_{Tue} — 5/16_{Thu}
臺北南港展覽二館

**Generative
Future**

Fraud Forum

亞洲數位詐欺研究報告2024

台灣數位信任協會 召集人

劉彥伯 Paul Liu




劉彥伯 Paul Liu


台灣數位信任協會 | 召集人


遠見雜誌專欄 | 104人力銀行 未來領袖計畫 提攜人
微軟TechDay講師 | CLOUDSEC 企業資安高峰論壇 | 台灣駭客年會
台灣資安大會 | 育秀盃創意獎評審 | DCN Global 論壇講者

 台灣數位信任協會
Digital Trust Association in Taiwan

 社群召集人


 全球消費產品開發暨市場營運協理

 資深策略經理

 三星全球戰略與創新中心經理 (APEC)

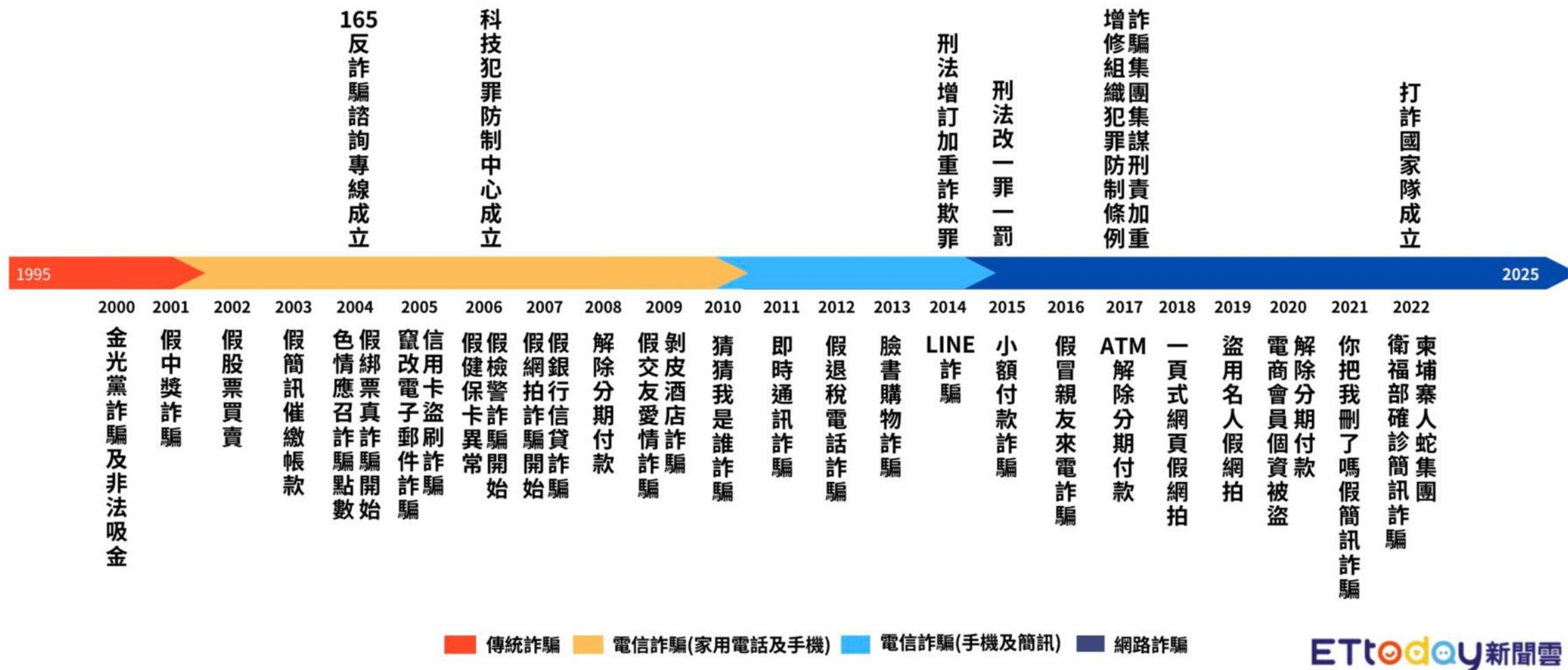
 產品行銷經理
技術經理

 資訊部主任

 網站工程師

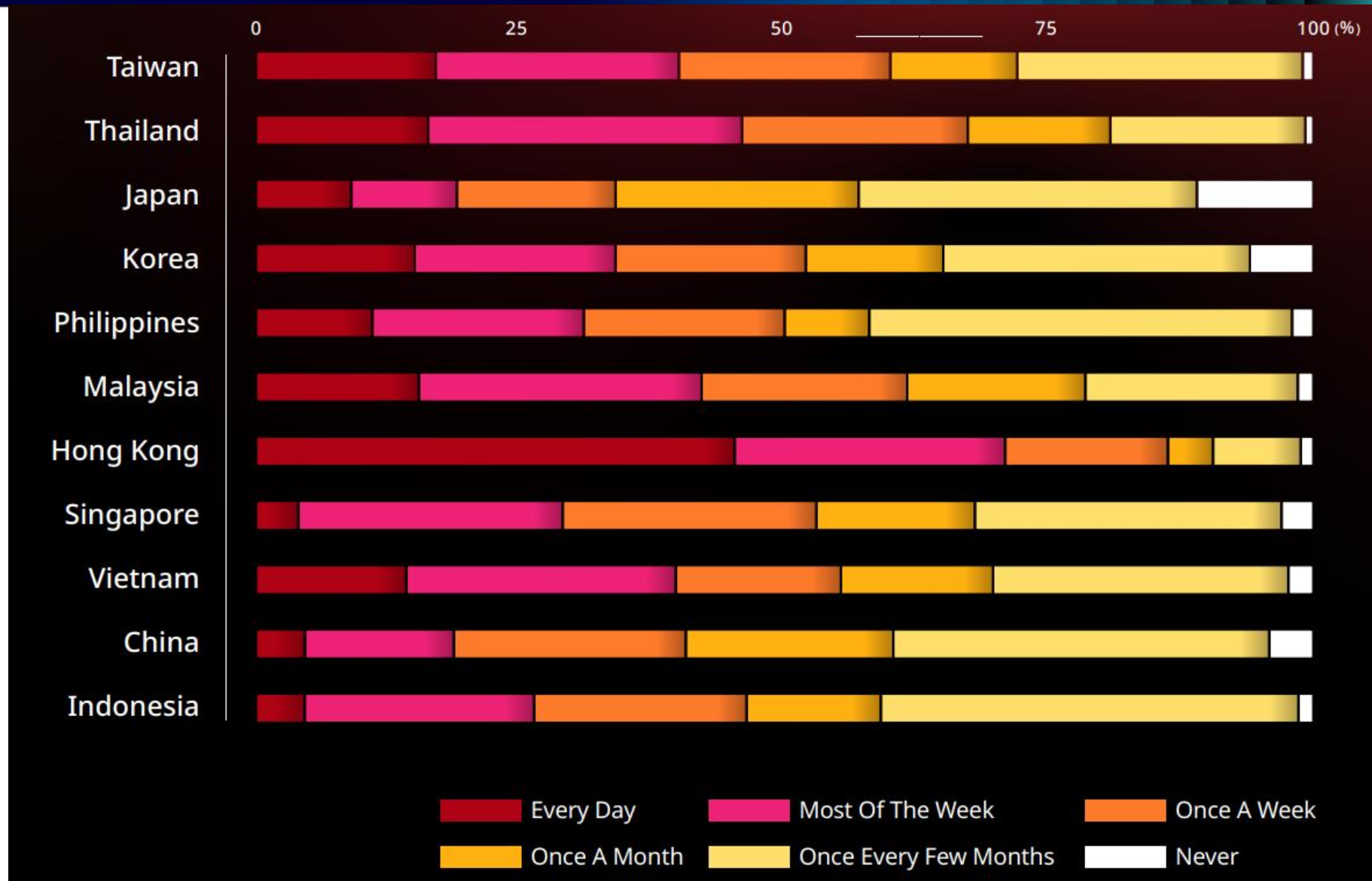
台灣詐騙手法演變

Generative
Future



ETtoday新聞雲

亞洲6成民眾每週會接觸到一次詐騙事件



亞洲各國常見的詐騙

Taiwan

1st 22.2% Identity Theft

2nd 13.4% Bill Payment Scam

3rd 11.7% Shopping Scam

4th 11.6% Investment Scam

5th 9.7% Gov/Bank Scam

Thailand

1st 17.9% Shopping Scam

2nd 15.2% Identity Theft

3rd 9.1% Investment Scam

4th 9.1% Bill Payment Scam

5th 8.8% Gov/Bank Scam

Japan

1st 30.0% Identity Theft

2nd 21.7% Investment Scam

3rd 20.8% Family/Relatives Scam

4th 17.4% Lottery Scam

5th 16.1% Shopping Scam

Korea

1st 13.3% Investment Scam

2nd 9.5% Identity Theft

3rd 7.4% Gov/Bank Scam

4th 5.7% Job Scam

5th 4.9% Family/Relatives Scam

Philippines

1st 35.9% Shopping Scam

2nd 29.0% Investment Scam

3rd 22.9% Lottery Scam

4th 17.8% Job Scam

5th 17.7% Identity Theft

Malaysia

1st 15.7% Identity Theft

2nd 15.3% Shopping Scam

3rd 15.1% Investment Scam

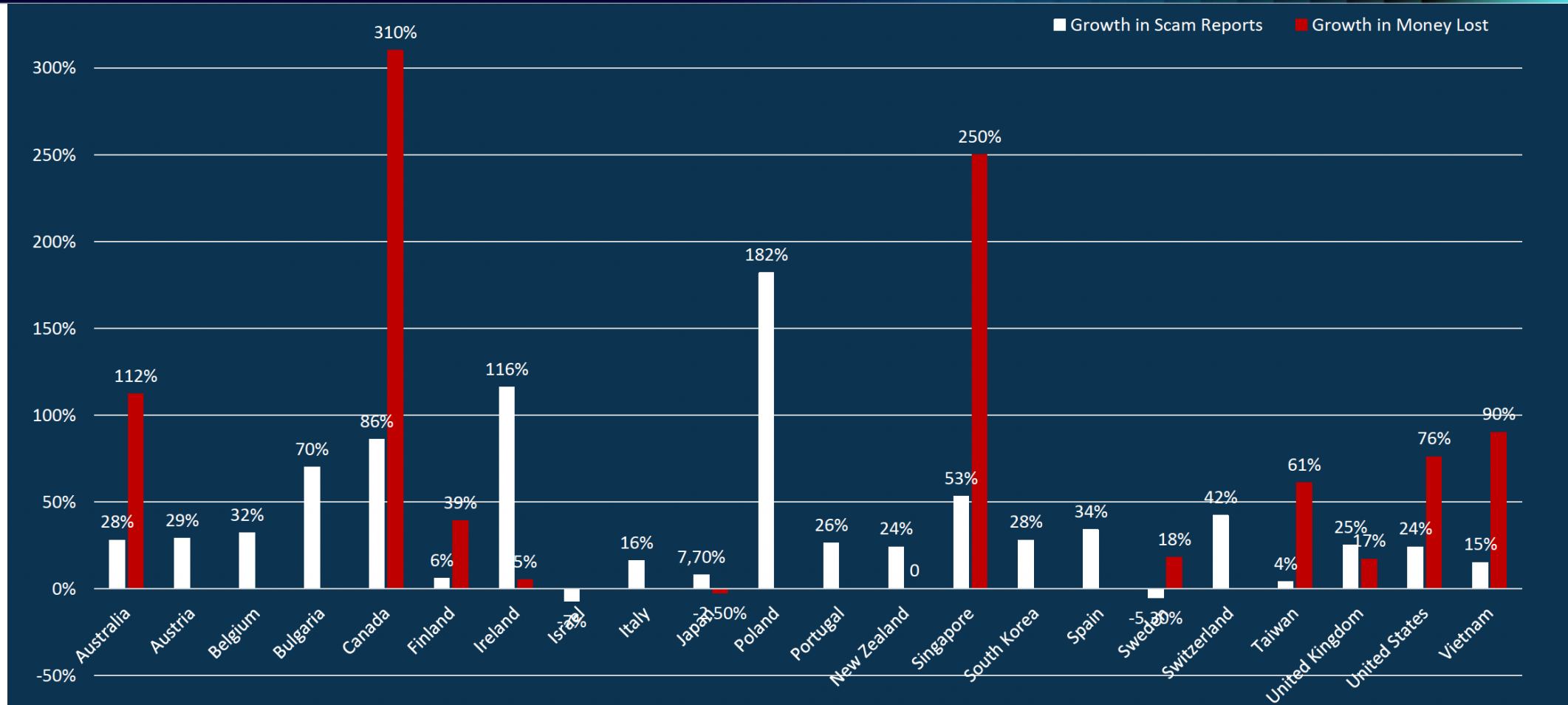
4th 12.3% Gov/Bank Scam

5th 10.7% Job Scam

亞洲各國常見的詐騙



網路詐欺已經成為全球問題



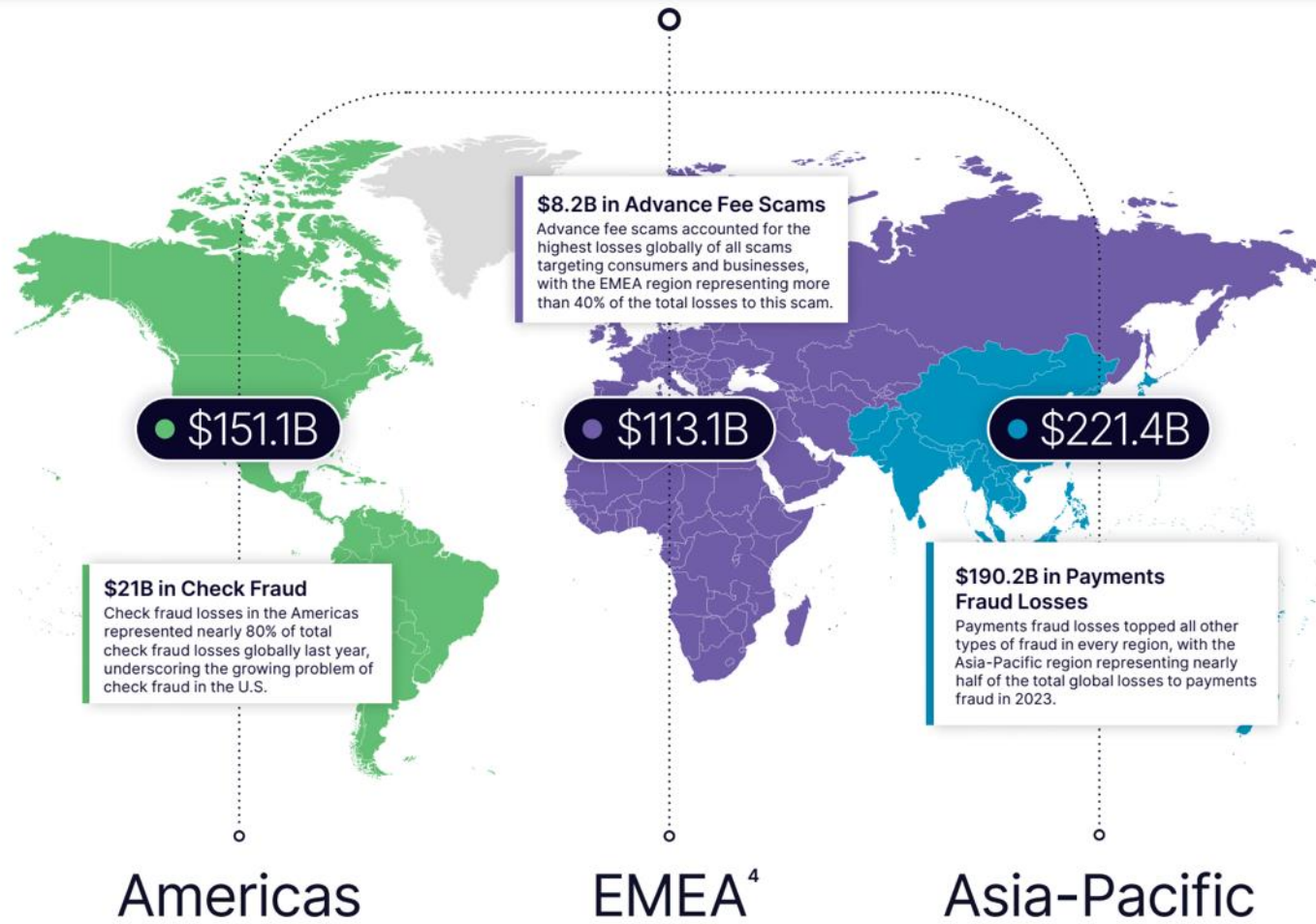
詐騙是繼病毒和網絡釣魚之後的新一波犯罪浪潮。
2021 年全球有2.93億詐騙案件並造成損失553億美元(1.6兆台幣)!

只有 4% 受害者可以拿回被騙的錢

- 全球只有4成受害者回報自身的詐騙經歷，但是有機會將損失金錢要回的人僅有4%。
- 大多數已開發國家中，有20% 到 40% 的犯罪都與網路詐欺相關
- 絕大多數的詐騙者持續逍遙法外中，因為他們可以藏匿於全球各地，但執法部門多數只能在自己的國家執法
- 根據世界經濟論壇的數據，只有 0.05% 的網路犯罪分子受到起訴

	F r a u d	F o r g e r y
Classification	Any kind of practice of dishonesty of a person or a company for financial advantage. Can be performed through the use of objects obtained through forgery.	A common technique in fraud schemes, which utilizes forged documents in order to gain access to information or materials they should not have access to.
Legal Classification	Class I Felony Fraud Count	Class A Misdemeanor
Fines	up to \$10,000	up to \$10,000
Sentence	up to 3.5 years	average of up to 16 months

2023年因詐欺造成財損達485B美元



Asia-Pacific

- Payments Fraud **\$190.2B**
- Credit Card Fraud **\$11.9B**
- Advance Fee Scams **\$6.2B**
- Check Fraud **\$5.1B**
- Impersonation Scams **\$3.8B**
- Cyber-Enabled Scams **\$1.9B**
- Confidence Scams **\$1.7B**
- Employment Scams **\$0.6B**

2023年全球消費者和企業主要因偽冒、投資、預付費、就業和其他的詐欺類型被騙。並透過現金、支票和信用卡等原因而造成的損失。

- Payments Fraud **\$102.6B**
- Check Fraud **\$21.0B**
- Credit Card Fraud **\$13.6B**
- Cyber-Enabled Scams **\$5.0B**
- Advance Fee Scams **\$4.7B**
- Impersonation Scams **\$1.6B**
- Employment Scams **\$1.6B**
- Confidence Scams **\$0.9B**

- Payments Fraud **\$94.0B**
- Advance Fee Scams **\$8.2B**
- Credit Card Fraud **\$3.1B**
- Cyber-Enabled Scams **\$3.1B**
- Employment Scams **\$1.7B**
- Impersonation Scams **\$1.4B**
- Confidence Scams **\$1.2B**
- Check Fraud **\$0.5B**

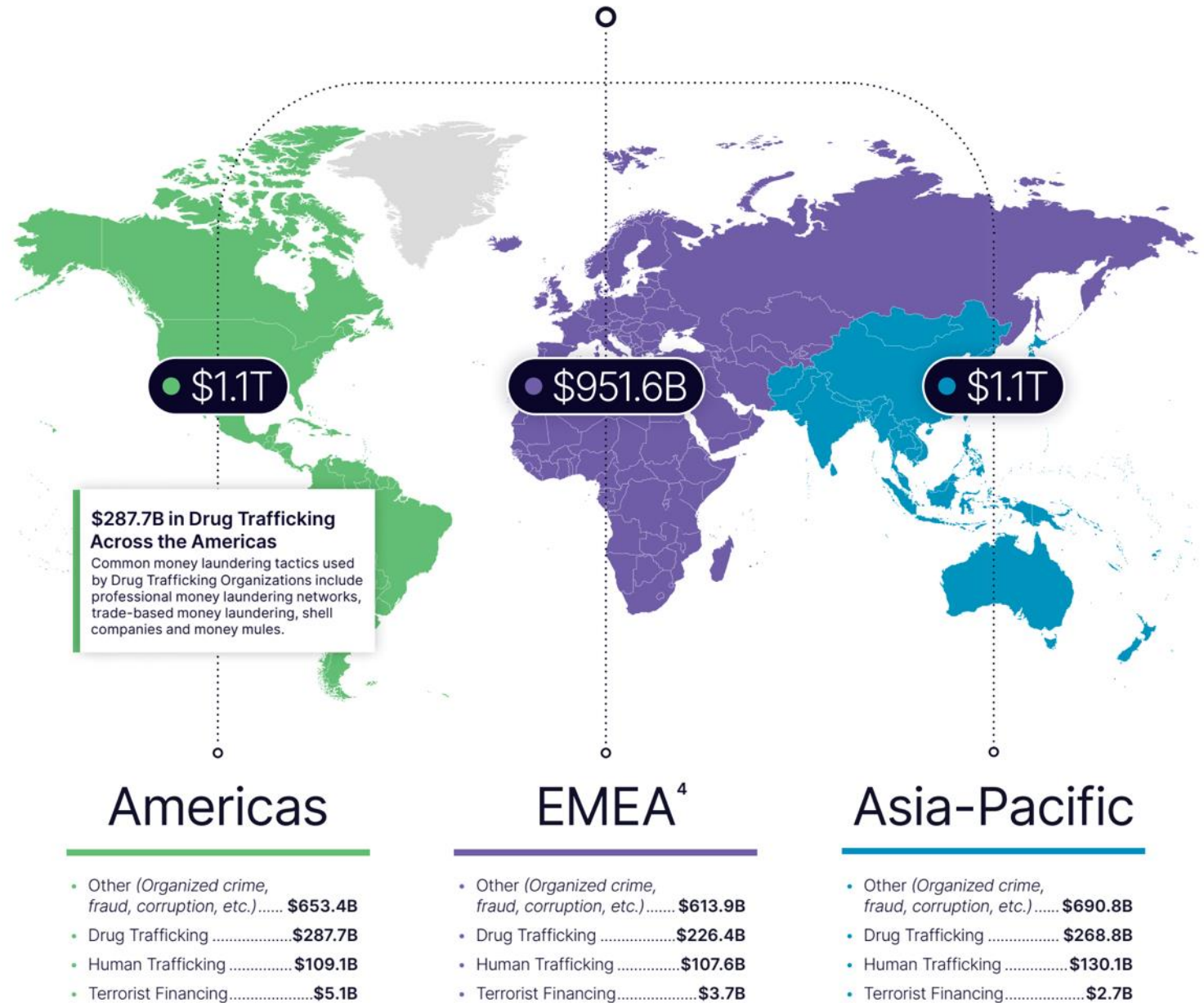
- Payments Fraud **\$190.2B**
- Credit Card Fraud **\$11.9B**
- Advance Fee Scams **\$6.2B**
- Check Fraud **\$5.1B**
- Impersonation Scams **\$3.8B**
- Cyber-Enabled Scams **\$1.9B**
- Confidence Scams **\$1.7B**
- Employment Scams **\$0.6B**

詐騙損害已經超過恐怖主義和人口販運

2023年，全球估計有超過3.1兆美元的非法資金流經全球金融系統。
其中包括：

- 7,829億美元的毒品走私活動
- 3,467億美元的人口販運
- 115億美元的恐怖主義資助

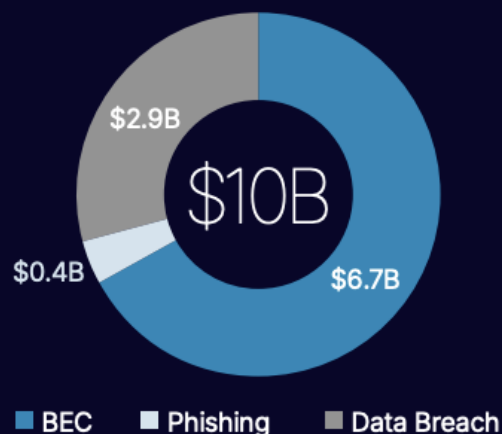
其中「全球詐騙的所得」總額達到了4,856億美元。



對準公司組織 BEC依舊是主流

Banking on Deceit

\$10B in Losses to Cyber-Enabled Scams



In 2023, 67% of cyber-enabled scam losses were a result of Business Email Compromise.



11% of Survey Respondents Ranked Business Email Compromise As a Top Concern.

企業郵件詐騙 (Business Email Compromise , BEC) 是一種極其有利可圖的授權推送支付 (Authorized Push Payment , APP) 詐欺 , 詐騙分子將其攻擊對準公司組織 , 並直接攔截和將資金目的轉移。

這類型的詐騙行為特徵：

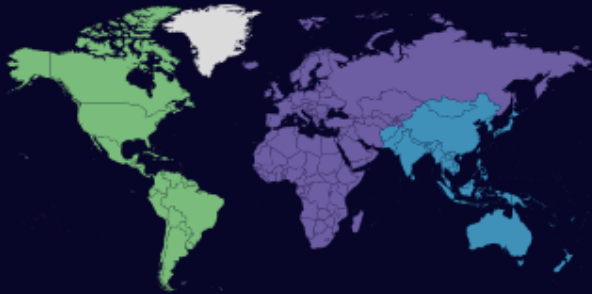
- 假扮成真實受款人 , 說服受害者將資金轉入其控制下的帳戶
 - 詐騙分子通常選擇不可撤銷的支付方式 , 例如電匯
 - 所有組織都是目標。
- 從大型企業到小本經營的企業 , 政府部門、非營利組織、學術機構和品牌公司。

資料來源 <https://nasdaq.com/>



預防授權推送支付騙局

Business Email Compromise
Represented
\$6.7B in Losses



Americas:

● \$3.4B

EMEA:

● \$2.1B

Asia-Pacific:

● \$1.3B



基本原則：

- 始終直接確認(最好是當面或透過電話查核)支付請求，以確認指示真實可信。
- 請勿使用電子郵件中提供的聯繫方式確認付款，請使用您已知的正確號碼。
- 留意電子郵件是否包含異常語句或以異於發件人以往風格的方式撰寫。
- 建立企業內部流程,處理有關支付/授權支付的所有請求。
- 留意付款指示之電子郵件寄件地址是否與真實相符。

資料來源 <https://nasdaq.com/>

資料來源 <https://www.entersekt.com/>

Emotional Exploitation



Romance scams are among the world's **fastest growing fraud trends**.⁹

Romance scams caused

\$3.8B

in estimated global losses with other confidence schemes.



Romance Scams represent a fraction of the losses to consumer scams but the toll on victims is immense.

社群與偽冒詐騙主要在於與受害者建立虛構的關係，通常是通過聊天程式、約會網站或社交平台開始建立關係，但這段關係最終會因對資金的不斷要求，最終導致了巨額金錢損失，另外也沒有統計數據能夠確認到這些受害者所經歷的心理痛苦和情感後果。

社群/偽冒詐騙是增長最快的欺詐之一，其中戀愛詐騙在2023年估計其損失總額高達380億美元。

這類型的詐欺特徵如下：

- 詐騙者會利用PUA的方式一直要求資金，直到受害者無以為繼
- 受害者也可能被利用當作車手，為詐騙分子轉移資金，在不自知地下進行了洗錢
- 即使被警察或金融單位發現了，受害者可能依舊無法接受這是一個騙局
- 社群平台的身份驗證形同虛構
- 生成式AI和Deepfake的發展助長了這類型騙局



資料來源 <https://nasdaq.com/>

利用資訊能力落差來詐欺年長者

Preying on the Vulnerable

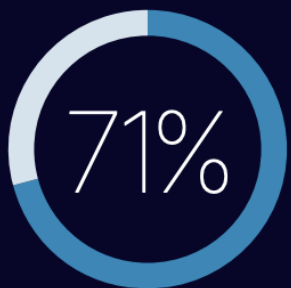
Seniors may be more at risk to fraud.

Of all reported global fraud

\$77.7B

was linked to
elderly victims.

According to Nasdaq Verafin Cloud data



of wire fraud attempts
targeted **people aged 55
or older** in Q2 2023.⁷

針對老年人的金融犯罪被稱為老年金融剝削（Elder Financial Exploitation，EFE）。詐騙集團通常會挑選符合以下條件年長者

- 獨居
- 對技術不太熟悉
- 殘疾
- 公務員

騙子可能冒充信任人士，通常被說服在虛假情境下轉移資金，以換取他們永遠不會收到的利益；或者通過恐嚇手段敲詐資金。

受騙的老年人通常不會報案，原因可能

- 出於羞愧
- 不確定向誰尋求幫助
- 只希望將這一經歷拋在腦後

但失去退休儲蓄及情感傷害，都會帶給老年人長期的創傷。

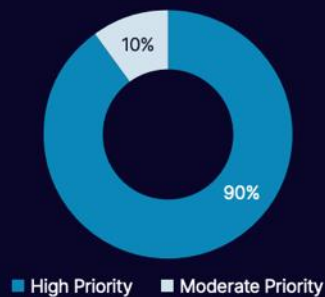
資料來源 <https://nasdaq.com/>



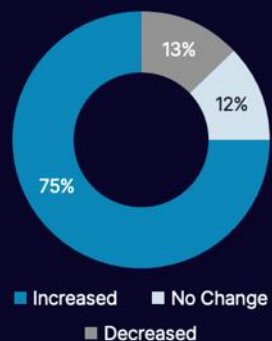
23 unreported
cases of
elder abuse
for each known case.¹⁰

資料來源 <https://nd.nasdaq.com/>

Priority Placed on Financial
Crime Prevention



Anti-Financial Crime Headcount:
2023 vs. 2022



of respondents said they have
adequate resources, including
personnel and technology
to combat financial crime.

在2024年全球金融犯罪報告的調查中可以發現，銀行正在加大對金融犯罪反制的投資，除確保符合監管義務，同時應對不斷發展的詐騙威脅和日益複雜的金融犯罪。

調查報告中也指出

- 近一半的反金融犯罪專業人士指出，缺乏足夠的資源和技術來打擊金融犯罪
- 但與去年相比，在人員投資是有增加的
- 若要解決目前的詐騙問題，必須對目前的系統和流程進行重大改變，現實狀況包含：
 - 若由系統規則來判斷，常會發生誤報的狀況。
判斷是否為系統誤報其實反而需要投入更多人力，另外誤報也可能導致與客戶間的摩擦
 - 手動流程的低效率。
由於金融機構之間的系統和數據源往往是複雜和分散的，日常工作流程往往充斥著手動任務、流程和文檔要求。缺乏自動化可能會影響調查時間、記錄保存、以及其他關鍵的合規流程
- 缺乏成功的衡量標準

台灣近年詐騙財損金額與攔阻

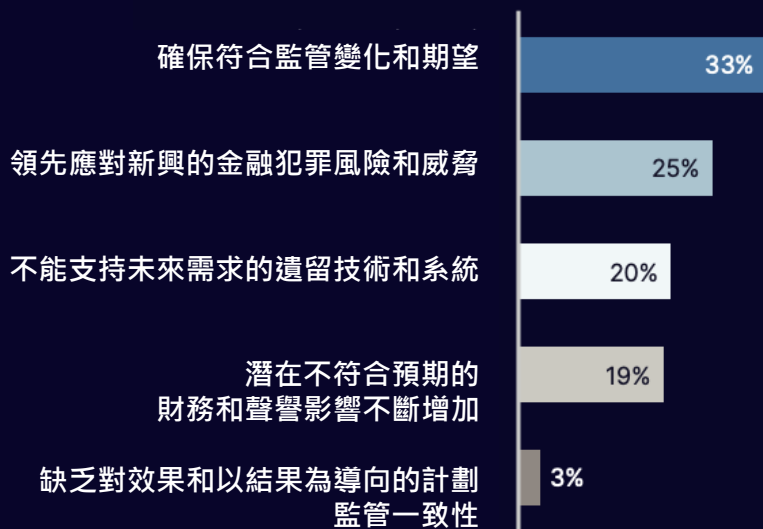
年度	詐欺犯罪件數	詐欺總財損	警方與金融攔阻件數	警方與金融攔阻金額
2018	23,470	39	935	4
2019	23,647	42	1,685	6
2020	23,054	42	2,704	10
2021	24,724	56	4,288	19
2022	29,509	69	7,977	42
2023	37,984	88	(7013 金)	89 (金融64.3)

詐欺反制的趨勢與困難

目前計劃效力的衡量指標



中長期最令人擔憂的挑戰包括



無論金融業、電信業、社交平台、購物平台等，乃至公部門、一般企業等，甚至資安服務商，在監管機構未提供有關反詐欺犯罪相關準則、優先事項或如何評估效果等的前提下，目前大多業者依舊是以可疑活動報告 (SAR/STR) 的數量視為衡量標準。

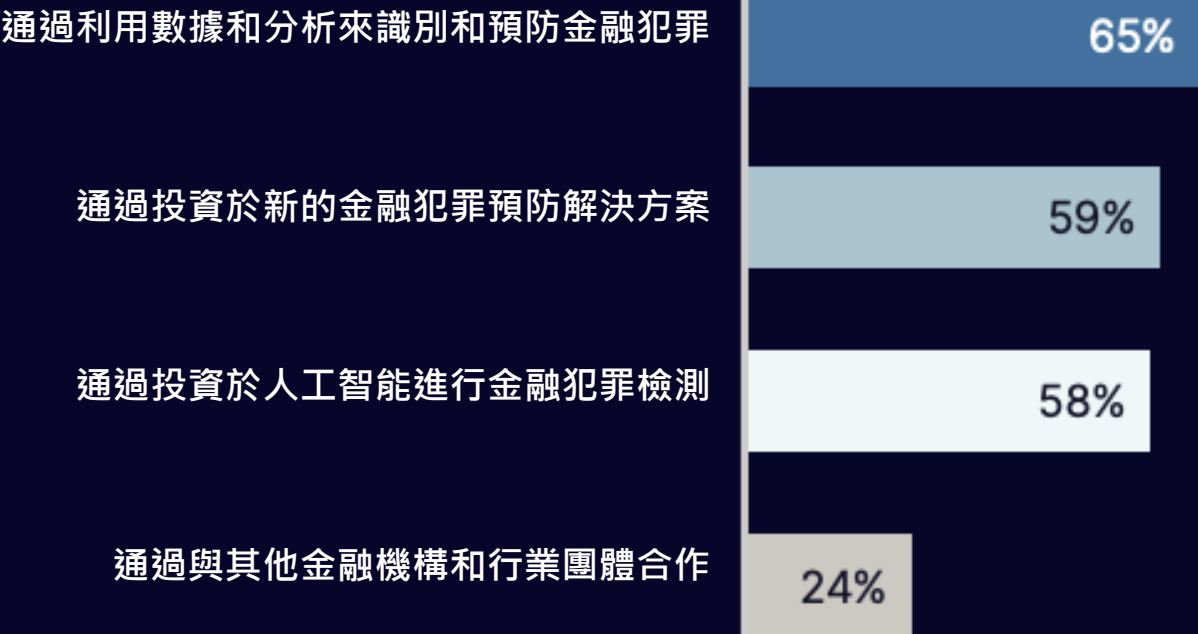
另外還是有幾個需要探討的觀點：

- 公和私部門之間的回報網路，所提交的數據報告，是否能準確反映企業或機構導入反詐欺方案後的真正效果？
- 詐騙的方式變化多端，若只有單一組織或公司的反制成效有限，因此需要多方協助，例如例如跨平台協作、金融單位間合作、執法機關的即時情報、消費者的自覺等，才有機會完全制止。

資料來源 <https://nasdaq.com/>

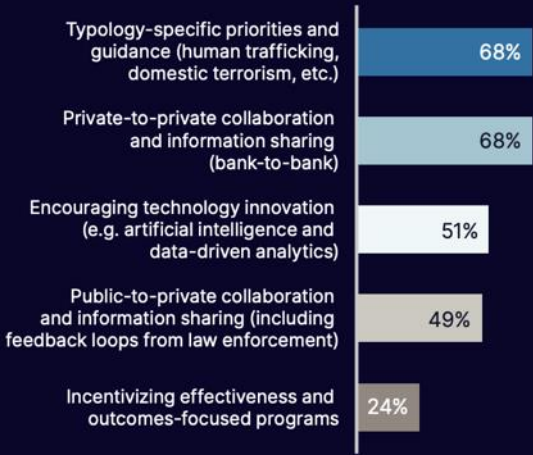
數位金融犯罪下的新機會

為了有效打擊「數位金融犯罪」業界普遍能接受的方式？

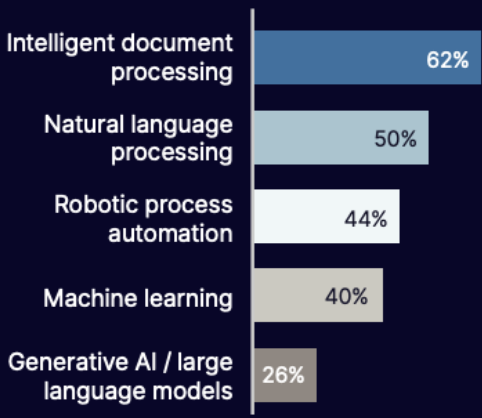


資料來源 <https://nasdaq.com/>

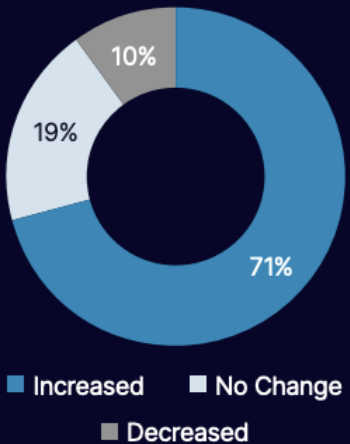
Areas for Improved Regulation



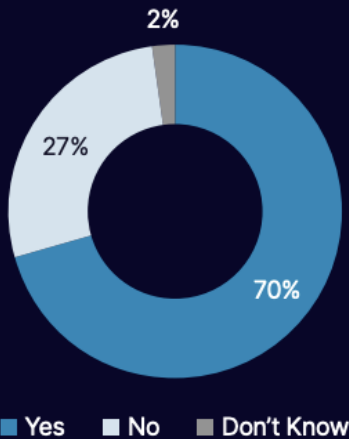
Technologies in Production for AFC Processes



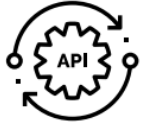
Budget for Financial Crime Compliance Technology (IT & Operations): 2023 vs. 2022



Increase Spending on AI/ Machine Learning Technology: Next 1-2 Years



詐騙預防的產業與服務興起



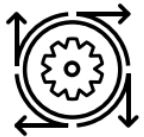
3rd Party API Capabilities



Payment Gateway Capabilities



Operational Support



Machine Learning



Guaranteed Chargeback Liability



ATO Detection Capabilities



Account/Client Management



Device Fingerprint Capabilities



Historical Sandbox Testing



Professional Guidance/Services



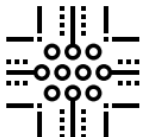
User Behavior Capabilities



Pre-Authorization Functionality



Fraud Engine/Platform Functionality



Non-Production Real Time Rules Testing

3rd Party API Capabilities – The ability to call out via API to third-party vendors for data, device fingerprinting, etc.

Payment Gateway Capabilities – The ability to process payments directly through their own platform or solution.

Operational Support – Provides outsourced operational support, at a cost, for reviewing high-risk transactions and/or managing chargebacks.

Machine Learning – Matching algorithms to detect anomalies in the behavior of transactions or users.

Guaranteed Chargeback Liability – Guarantees merchants do not take fraud losses for vendor-approved transactions.

ATO Detection Capabilities – Using device characteristics to detect account takeover/account penetration.

Account/Client Management – Personnel dedicated to working directly with clients.

Device Fingerprint Capabilities – Built directly into the platform (not a third-party API call).

Historical Sandbox Testing – Ability to test rules against historical transactions in a non-production environment.

Professional Guidance/Services – Provides outsourced support for data analysis, rules-building, and recommended best practices, etc.

User Behavior Capabilities – Built-in (not via third-party) capabilities to capture cursor movements, mouse clicks, and time on a merchant site.

Pre-Authorization Functionality – Ability to score and/or decision a transaction prior to authorization.

Fraud Engine/Platform Functionality – Ability to score/decision a transaction post-authorization.

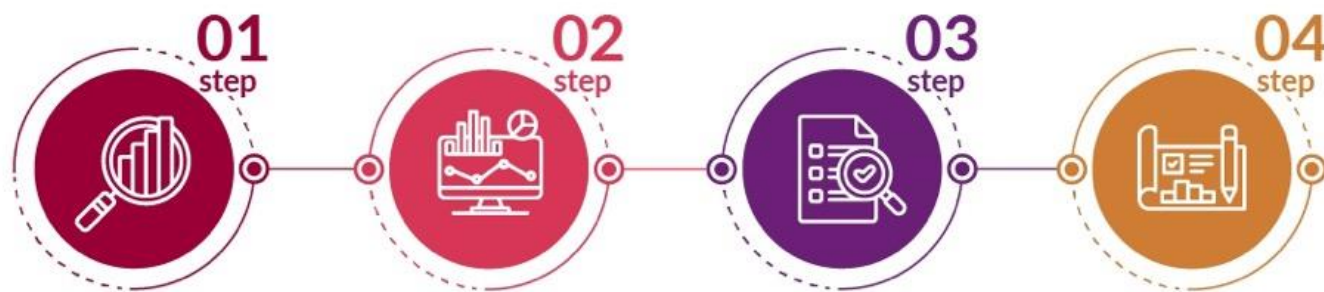
Non-Production Real Time Rules Testing – Ability to test real-time transactions in a non-production environment.

資料來源 <https://go.aciworldwide.com/>

商務案例: Mastercard

Cyber Quant

是一套企業資訊安全風險分析軟體，能夠在資安問題變成大問題之前就看到可能的風險所在。



盤點

建立資訊資產分類與價值判斷標準，並持續更新資訊資產清冊內容，以做為資訊資產存取控管措施選取之基礎。

弱點識別與衝擊分析

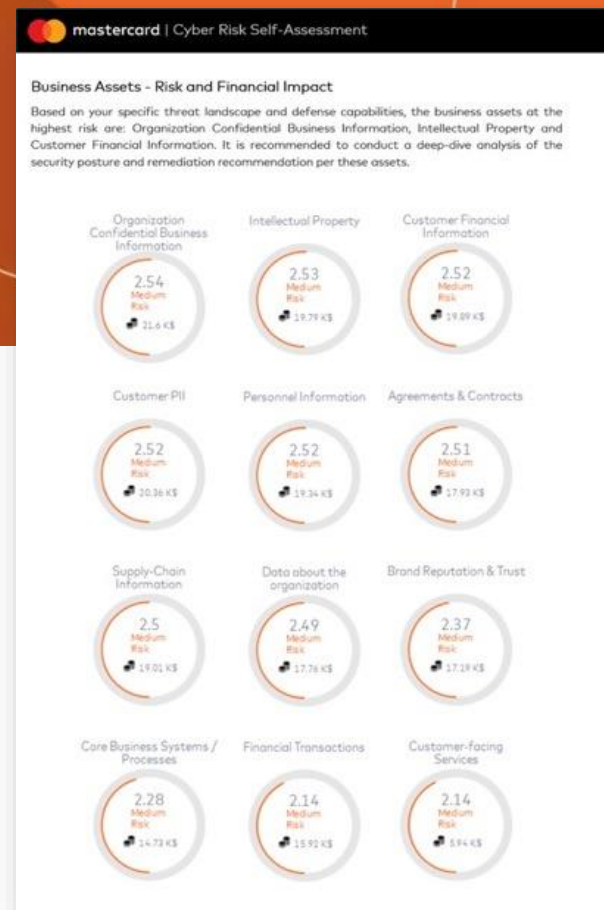
每半年進行資訊資產威脅弱點識別及衝擊分析，並依風險評鑑的結果，評估資訊安全弱點對資訊資產帶來的威脅、影響及發生的可能性，以保護資訊資產的機密性、完整性及可用性。

風險評估彙總報告

透過資訊資產之風險評鑑模型，量化各項資訊資產所面臨之風險程度，做為選擇控管措施之依據。當所有風險權值計算完成後，由風險評鑑執行人員彙總成風險評鑑彙總報告。

風險改善計畫

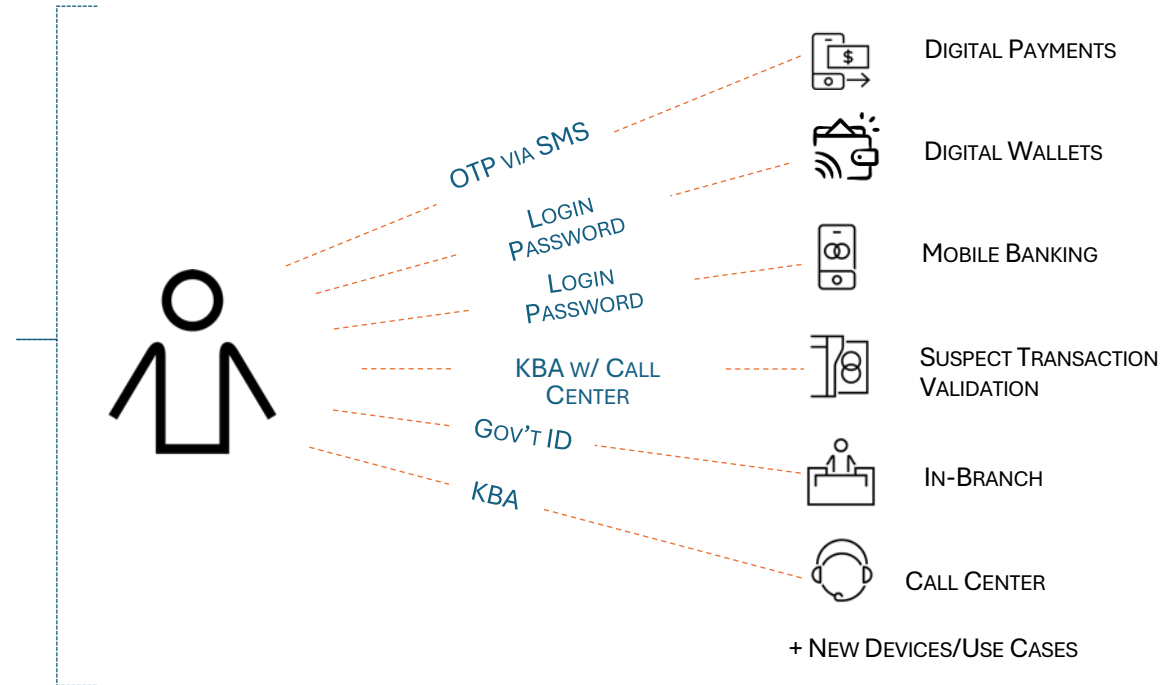
風險權值若高於風險可接受水準，應由資訊治理執行小組協調相關負責單位製作風險處理計畫改善現有控管措施或新增控管措施，直到風險權值降至風險可接受水準為止。



Cyber Quant 可以評估 50 多種網路安全控制措施，以預防關鍵的安全漏洞導致的財務影響，快速確定您可以採取的措施來改善安全狀況。

Portfolio Intelligence Solutions

為發卡機構、收單機構、商家服務提供者以及聯名卡提供強大的支付分析，透過資料分析結果來提升詐欺偵測的應對能力。



關鍵數據集

查看關鍵資料集，包括身分驗證、授權、拒絕、詐欺、退款、交易紀錄。



集中分析

將整個企業的分散式資料集中分析，以獲得單一事實來源。



24/7 監控數據警報

透過系統警報和電子郵件通知監控特定業務確保安全與穩定。

Showing 1-20 of 25 results

☐ Turn job alert on [Share result](#)

Sort by Most relevant

Security and Fraud Analyst

🕒 17 days ago 📍 Cheltenham, Gloucestershire, United Kingdom

🏠 Up to 100% work from home

Security represents the most critical priorities for our customers in a world awash in digital threats, regulatory scrutiny, and estate complexity. Microsoft Security aspires to make the world a safer place for all. We want to reshape security and empower ever...

[See details](#)

Product Manager 2

🕒 Today 📍 Redmond, Washington, United States

🏠 Up to 50% work from home

Microsoft Fraud Protection team is seeking a Product Manager 2 with proven track record of strategizing and shipping great products. Our mission is to help digitally transformed enterprise customers prevent all types of online fraud while keeping friction low ...

[See details](#)

Senior Software Engineer

🕒 10 days ago 📍 Redmond, Washington, United States

🏠 Up to 100% work from home

Security represents the most critical priorities for our customers in a world awash in digital threats, regulatory scrutiny, and estate complexity. Microsoft Security aspires to make the world a safer place for all. We want to reshape

Security and Fraud Analyst

Cheltenham, Gloucestershire, United Kingdom

[Apply](#)

[Save](#)

[Share job](#)

Date posted	Apr 19, 2024	Job number	1700327
Work site	Up to 100% work from home	Travel	0-25 %
Role type	Individual Contributor	Profession	Security Engineering
Discipline	Security Research	Employment type	Full-Time

Overview

Security represents the most critical priorities for our customers in a world awash in digital threats, regulatory scrutiny, and estate complexity. Microsoft Security aspires to make the world a safer place for all. We want to reshape security and empower every user, customer, and developer with a security cloud that protects them with end to end, simplified solutions. The Microsoft Security organization accelerates Microsoft's mission and bold ambitions to ensure that our company and industry is securing digital technology platforms, devices, and clouds in our customers' heterogeneous environments, as well as ensuring the security of our own internal estate. Our culture is centered on embracing a growth mindset, a theme of inspiring excellence, and encouraging teams and leaders to bring their best each day. In doing so, we create life-changing innovations that impact billions of lives around the world.

The Identity security analyst team, IDFIRE, is the premier identity cyber threat hunting and investigation team in the industry. IDFIRE is responsible to identify and understand all novel attacks against user and application authentication by researchers, criminals and nation state actors. We partner with data scientists and

Qualifications

- Experience working with extremely large data sets
- Experience of using tools, Scripting languages or MapReduce solutions.
- Experience in Cybersecurity, and/or Fraud, anomaly detection, software development lifecycle, large-scale computing, or data science
- OR BS Degree in Computer Science, Electrical & Computer Engineering or Mathematics or equivalent experience

CYBERSEC 2024
臺灣資安大會

5/14_{Tue} — 5/16_{Thu}
臺北南港展覽二館

**Generative
Future**

Fraud Forum

謝謝



www.linkedin.com/in/impaul67

劉彥伯 Paul Liu

