資安事件案例分析—Google與Facebook一億美元詐騙案

壹、事件背景

一、詐騙手法

根據 Fortune（2017） 的報導，Rimasauskas 透過魚叉式網路釣魚（Spear Phishing） 和 企業電子郵件詐騙（BEC），成功欺騙 Google 和 Facebook 的財務部門。

（一）冒充供應商（Quanta Computer）

Quanta Computer 是一家台灣的電子製造商，Google 和 Facebook 都是其客戶。Rimasauskas 設立了一家與 Quanta 名稱相似 的公司，並開設銀行帳戶。

（二）發送假發票與付款請求

他利用偽造的電子郵件地址，冒充 Quanta，向 Google 和 Facebook 發送「正常業務往來」的假發票，要求支付款項。這些假發票與付款指示看起來與 Quanta 以往的交易模式相符，因此財務部門沒有立即察覺異常。

（三）資金轉移與洗錢

Google 和 Facebook 的財務部門將款項轉入 Rimasauskas 控制的銀行帳戶後，這些款項被迅速轉移至拉脫維亞、賽普勒斯、斯洛伐克、香港等地的銀行帳戶，進行洗錢，以防止被追蹤。

二、Google 和 Facebook 的損失

根據法院文件，Rimasauskas 至少詐騙了 1 億美元（Google 受害金額未公開，Facebook 受害約 2300 萬美元），直到後來發現異常交易才向執法機構報案。

三、事件後續

（一）Rimasauskas 被捕與判刑

2017 年：Rimasauskas 在立陶宛被捕，隨後被引渡到美國。

2019 年：他承認犯下電信詐欺與洗錢罪，被判 5 年監禁，並被要求歸還詐騙所得。

（二）Google 和 Facebook 成功追回部分資金

Google 和 Facebook 表示，他們在發現詐騙後迅速與銀行合作，追回了大部分被騙款項。

貳、分析流程

一、以美國國家標準與技術研究院（NIST）發布的網路安全框架（CSF）2.0 分析

（一）NIST CSF 2.0 介紹

NIST CSF 2.0 提供一個組織管理和降低網路安全風險的框架，包含六大功能：治理（Govern）、識別（Identify）、保護（Protect）、偵測（Detect）、回應（Respond）和復原（Recover）。其對於各式企業與政府機構不僅適用於技術團隊，也能幫助管理層制定網路安全戰略。

（二）分析

▼表 1:NIST CSF 分析詐騙案

核心功能	子類別	Google / Facebook 詐騙案分析	改進建議
治理（Govern, GV）	GV.OC（組織情境）	Google 和 Facebook 供應商多，增加了管理風險的複雜性。	強化**供應鏈管理**，定期審查供應商交易記錄。
	GV.RM（風險管理策略）	BEC 詐騙顯示財務與溝通風險管理不足。	建立 BEC 風險管理計劃，實施**供應商交易風險評估**。
	GV.PO（政策）	付款授權與驗證政策可能執行不力，讓詐騙得逞。	明確**規範付款流程**，對高額交易實施多層級驗證。
識別（Identify, ID）	ID.AM（資產管理）	未充分掌握應付帳款與供應鏈風險，導致財務詐騙成功。	定期評估財務交易與供應商行為，建立**異常檢測機制**。
	ID.RA（風險評估）	對 BEC 詐騙的特定風險評估不足。	增加針對 BEC **的風險評估機制**，識別異常付款請求。
	ID.IM（改善）	事發前未能改善內部財務安全流程。	依據風險評估結果，持續**改進財務與供應鏈交易安全**。
保護（Protect, PR）	PR.AA（身分管理、驗證和存取控制）	員工未能驗證供應商付款請求真實性。	高額支付須經雙人或三層授權，**多因素驗證**（MFA）。
	PR.AT（意識和訓練）	員工可能缺乏 BEC 詐騙識別能力。	定期進行針對 BEC 的資安**訓練**與模擬攻擊**演練**。
	PR.DS（資料安全）	財務流程與供應商資訊未受充分保護。	加密供應商付款資訊，**限制存取權限**。
偵測（Detect, DE）	DE.CM（持續監控）	未能及時監控異常財務交易與可疑郵件。	部署 AI **風險分析工具監測**異常交易與供應商變更。
	DE.AE（不良事件分析）	可能缺乏及時的可疑交易分析能力。	建立**自動異常交易警報機制**，提高檢測效率。
回應（Respond, RS）	RS.MA（事件管理）	Google 和 Facebook 迅速採取行動追回資金。	強化**事件管理計劃**，確保發現異常時能即時處理。

	RS.CO（事件回應報告和溝通）	有效與執法機構合作追回部分資金。	建立**內部回報機制**，確保相關部門快速應對 BEC 詐騙。
復原（Recover, RC）	RC.RP（事件復原計畫執行）	事發後評估影響並加強交易審核流程。	定期**演練復原計畫**，確保未來能快速應對類似攻擊。
	RC.CO（事件復原溝通）	需與內部員工和供應商溝通事件復原情況。	強化內部與外部的**透明溝通機制**，增強信任度。

二、以網路防禦矩陣（CDM）分析

（一）CDM 介紹

當廠商聲稱有一個 100% 防禦無敵的解決方案，企業該如何搞懂實際該方案的適用範疇？戴夫寇爾事業發展經理鍾澤華表示，可借助 CDM 更直觀的檢驗解決方案。

CDM 由前美國銀行首席安全科學家 Sounil Yu 於 2016 年發明，是以 NIST CSF 1.0 的五大功能（識別、保護、偵測、回應、復原）為橫軸，以資產類別（設備、應用程式、網路、資料、使用者）為縱軸的矩陣模型。透過 CDM ，企業可以將其採用的資安解決方案或控制措施對應到特定的格子中，更快速地掌握每個解決方案涵蓋的面向，並找出在不同資產類別和資安功能上的潛在缺口。

（二）分析

▼表 2:CDM 分析詐騙案

CDM 防禦階段	設備	應用程式	網路	資料	用戶
識別	了解供應商設備風險	交易系統風險評估	網路詐騙行為分析	確認財務數據流向	供應商背景調查
保護	強化憑證管理	使用電子郵件驗證技術（SPF/DKIM/DMARC）	監測異常連線	加密付款數據	員工資安意識訓練
偵測	偵測設備異常交易	AI 風險分析	監控釣魚郵件	即時資金流監測	釣魚測試演練
回應	阻斷可疑付款設備	停用可疑帳戶	追蹤可疑資金流	進行交易回溯	通報執法單位
復原	設備強化與補丁更新	增加 AI 風險防禦	加強供應鏈審查	交易系統改進	改善企業內部流程

三、以 D.I.E.（分散、不可竄改、短暫）模型分析

（一）D.I.E. 介紹

D.I.E. 模型是針對下一代網路安全挑戰提出的概念，由 CDM 的發明者 Sounil Yu 提出，強調分散性、不可竄改性與短暫性，尤其著重於提升復原能力。

（二）分析

▼表 3:D.I.E. 分析詐騙案

D.I.E. 原則	目前問題	改善建議
分散（Distributed）	Google 和 Facebook 集中化處理財務交易，易受單點攻擊。	採取**多重驗證與分散式交易**確認機制，避免單一帳戶可授權大量款項。
不可竄改（Immutable）	付款指令可被偽造，且無防範機制。	使用區塊鏈技術**確保供應商資訊不可篡改。**
短暫（Ephemeral）	攻擊者可持續利用相同手法詐騙。	**限制付款請求的有效時間**，超過時間須重新驗證。

參、技術背景需求

一、駭客使用的技術與對應結果

駭客利用了 BEC 和 CEO 詐騙技術，假冒供應商 Quanta Computer，發送偽造的發票與付款請求，同時結合技術與心理操控來發動詐騙。

▼表 4:駭客手法與影響

駭客手法	技術與影響
偽造身份（Impersonation）	創建**與 Quanta Computer 同名的公司**，並在賽普勒斯、拉脫維亞設立銀行帳戶，使其看似合法。
偽造發票（Fake Invoices）	發送**看似來自 Quanta Computer 的付款請求**，誘導 Google 和 Facebook 財務部門轉帳。
電子郵件欺騙（Email Spoofing）	可能透過**偽造寄件人地址、域名欺騙**（SPF、DKIM、DMARC **設定不足**） 使郵件看起來像是真實供應商發送的。
利用供應商關係（Vendor Exploitation）	駭客深入了解 Google 和 Facebook 的供應商關係，針對財務部門進行定向詐騙。
社會工程（Social Engineering）	駭客透過偽造高層指示、施壓付款、模仿內部對話來操控受害者。

二、Google 和 Facebook 可能有的安全措施與漏洞

作為大型跨國科技公司，Google 和 Facebook 理應部署了多層次的網路安全措施，但 BEC 詐騙利用的是管理流程與人員認知的漏洞，而不是單純的技術漏洞。因此，企業需要進一步強化內部審批、交易監控與社交工程防禦，以降低此類詐騙的成功率。

▼表 5:安全措施的作用與漏洞影響

安全措施	作用	可能存在的安全漏洞	影響
資安意識培訓（Security Awareness Training）	讓財務部門識別 BEC **詐騙**，降低社交工程攻擊成功率。	**人為錯誤**（Human Error）	財務人員仍可能誤判詐騙郵件，過度信任假發票
電子郵件安全（Email Security - SPF, DKIM, DMARC）	防範**電子郵件欺騙**（Email Spoofing），減少釣魚郵件攻擊。	**電子郵件防禦不足**（Email Security Gaps）	駭客可能利用進階釣魚技術繞過驗證，偽造供應商郵件。
多重驗證（MFA）	保障財務系統登入安全，防止未授權存取。	**財務帳戶存取漏洞**（Financial Account Access Gaps）	若 MFA 僅應用於登入，未涵蓋付款流程，則仍可能遭詐騙。
供應商驗證機制（Vendor Management）	確保供應商資訊真實性，減少冒名頂替風險。	**供應商帳戶驗證不足**（Vendor Authentication Weakness）	可能在**新銀行帳戶變更驗證**方面不夠嚴格，未發現駭客帳戶異常。
財務內部控制（Internal Controls）	付款流程 **多層核查**，降低詐騙風險。	**大額付款審批流程漏洞**（Weak Payment Approval Process）	若缺乏**交叉驗證**，則駭客可能假冒內部高層施壓快速付款。
自動化財務監控（AI/ML Fraud Detection）	利用 AI **偵測異常付款模式**，防範詐騙交易。	**未即時偵測異常交易**（Delayed Anomaly Detection）	若 AI 監測機制未即時啟動，駭客可能在資金轉移前成功逃逸。
即時通報與應變機制（Incident Response）	內部系統一旦發現可疑交易，可立即啟動資金凍結。	**反應時間不足**（Slow Incident Response）	若無**快速通報機制**，企業可能在發現詐騙時已難以追回資金。

肆、心得

這起 Google 和 Facebook 遭遇的一億美元詐騙案，突顯了社交工程攻擊的嚴重性，即使是大型科技公司也可能成為受害者。本案中的駭客透過 BEC 與 CEO 詐騙，利用偽造發票、假冒供應商及電子郵件欺騙等手法，成功誘騙財務部門進行大額付款，表

明供應鏈安全與內部控制的潛在漏洞。這起事件不僅揭露了企業在供應鏈管理、內部審核機制與員工資安意識上的挑戰，也突顯了現有網路安全框架的價值與應用。

一、NIST CSF 與防範措施

NIST CSF 2.0 提供了一個全面的安全框架，包括識別、保護、偵測、回應與復原。在識別（ID）階段，Google 和 Facebook 應加強供應商管理（ID.AM）及風險評估（ID.RA)。保護（PR）方面，應透過多重驗證（MFA)、電子郵件安全（SPF/DKIM/DMARC)、強化財務審核機制來降低風險。此外，持續監控異常交易（DE.CM）及強化事件回應（RS.MA）也至關重要。

二、CDM 與 D.I.E. 框架的應用

CDM 提供不同資產類別的安全評估，例如保護支付流程、偵測異常交易，能幫助企業強化風險控制。D.I.E. 原則則提醒組織應考慮分散式交易驗證、加密簽章與自動化安全審查，以降低人為錯誤與詐騙風險。

三、結論

本案凸顯了社交工程的威脅與供應鏈風險管理的必要性。無論是 Google、Facebook 等科技巨頭，還是中小企業，都可能成為BEC、社交工程與供應鏈詐騙的目標。NIST CSF 2.0、CDM 與 D.I.E. 提供了不同角度的資安防禦策略，企業應透過多層次的資安架構來減少詐騙風險。此外，這起事件也說明，除了技術防禦，員工的資安意識、內部驗證機制與即時交易監控系統，都是防範供應鏈詐騙的關鍵。

伍、參考來源

KnowBe4. (n.d.). *What is social engineering?* KnowBe4. Retrieved March 21, 2025, from https://www.knowbe4.com/what-is-social-engineering

KnowBe4. (n.d.). *Phishing resource center.* KnowBe4. Retrieved March 21, 2025, from https://www.knowbe4.com/resource-center/phishing

KnowBe4. (n.d.). *Spear phishing.* KnowBe4. Retrieved March 21, 2025, from https://www.knowbe4.com/spear-phishing

KnowBe4. (n.d.). *CEO fraud.* KnowBe4. Retrieved March 21, 2025, from https://www.knowbe4.com/ceo-fraud

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Jeff John Roberts. (2017, April 27). *Exclusive: Facebook and Google Were Victims of $100M Payment Scam.* Retrieved from https://fortune.com/2017/04/27/facebook-google-rimasauskas/

U.S. Department of Justice. (2017). *Lithuanian man charged in fraudulent email compromise scheme that led to the theft of over $100 million.* U.S. Attorney's Office, Southern District of New York. Retrieved from https://www.justi

ce.gov/usao-sdny/press-release/file/950556/dl?inline=

iThome. (2023, May 17). 【臺灣資安大會直擊】面對下一個網路安全時代，網路防禦矩陣CDM發明人提出資安防護要有親疏遠近因應之道. iThome. Retrieved from https://www.ithome.com.tw/news/156903

iThome. (2020, September 24). 【用Cyber Defense Matrix搭配資安框架改善資安弱點】資安策略成效要靠真實威脅調整. iThome. Retrieved from https://www.ithome.com.tw/news/140095