我對金融領域資安的思考

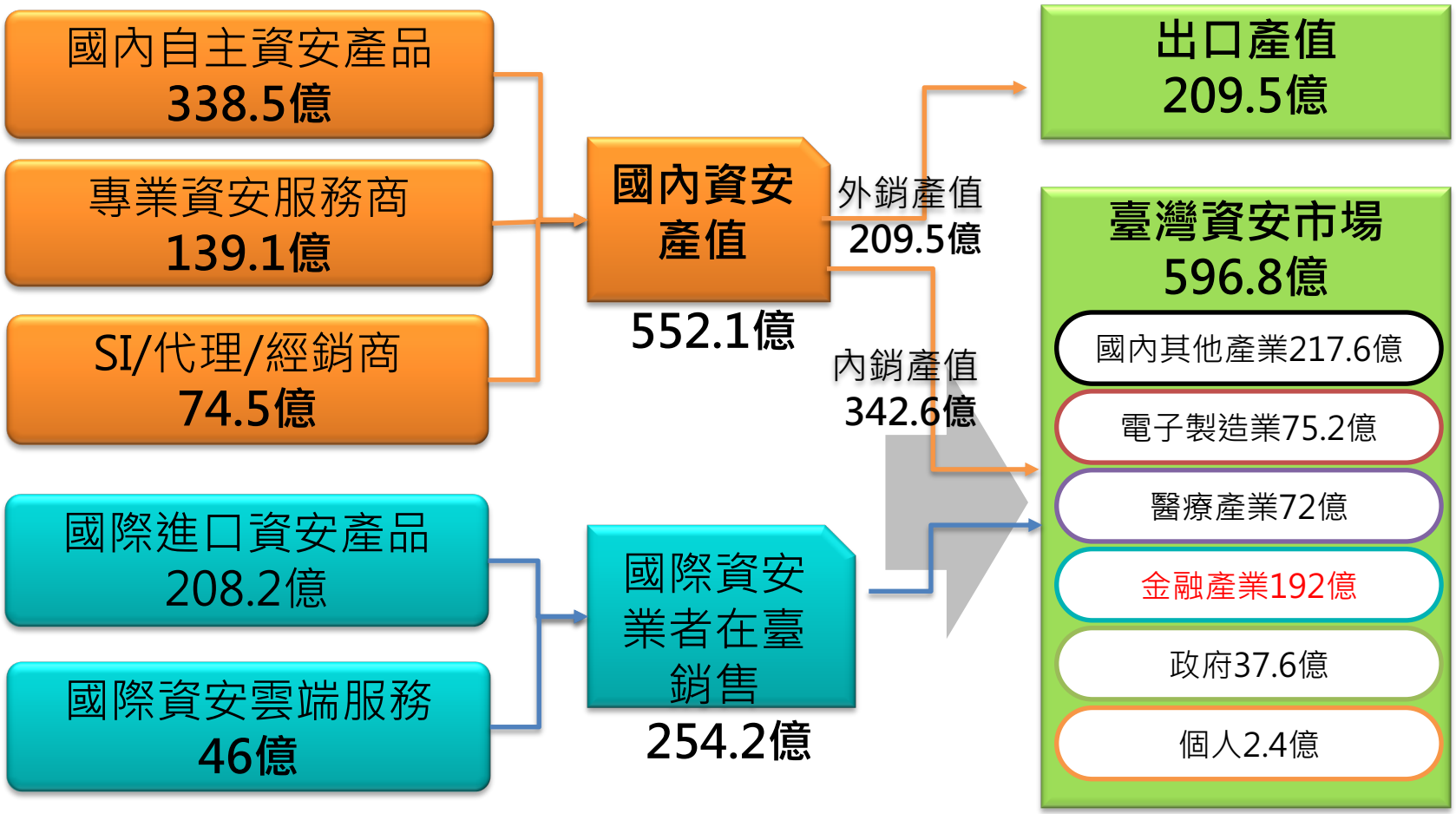
金融監督管理委員會

蔡福隆處長

2021.11.26

2020年國內資安產業與資安市場現況

國內資安市場，金融產業占近1/3



資料來源：海關進出口資料，IDC, 工研院產科國際所

護國神山與護國群山

我們都說台積電是護國神山，台灣需要護國神山還是護國群山？

半導體產業占GDP 16.3%

金融產業占GDP 6.7%

軟體產業占GDP 0.4%

資安長的責任

安例分享：資訊系統升級異常事件
您可能作過很多次演練，也有應變計畫，但是...

全組織的應變計畫
對媒體的溝通
客戶權益的保障

經濟日報 > 金融 > 金融脈動

ATM事件連環燒 國泰世華銀行滅火後給金融業的一堂課

本文共2833字

2021/10/28 12:51

經濟日報 記者葉憶如／台北報導

讚 1

國泰世華銀上周ATM升級出包，連二天當機，民眾遭無故扣款、轉帳失敗、領錢卻拿不到鈔票。國泰世華銀董事長郭明鑑、副董事長蔡宗翰等高階主管26日一字排開，親上火線召開線上記者會，向社會大眾解釋說明並道歉，甚至祭出補償措施，再掀市場一波熱烈討論，也是金融業不得不正視的一堂課。

金融資安人才的培育

大家都說人才很重要，人對了、事情就對，但金融界需要作樣的資安人才？

理論面：鼓勵取得國際證照

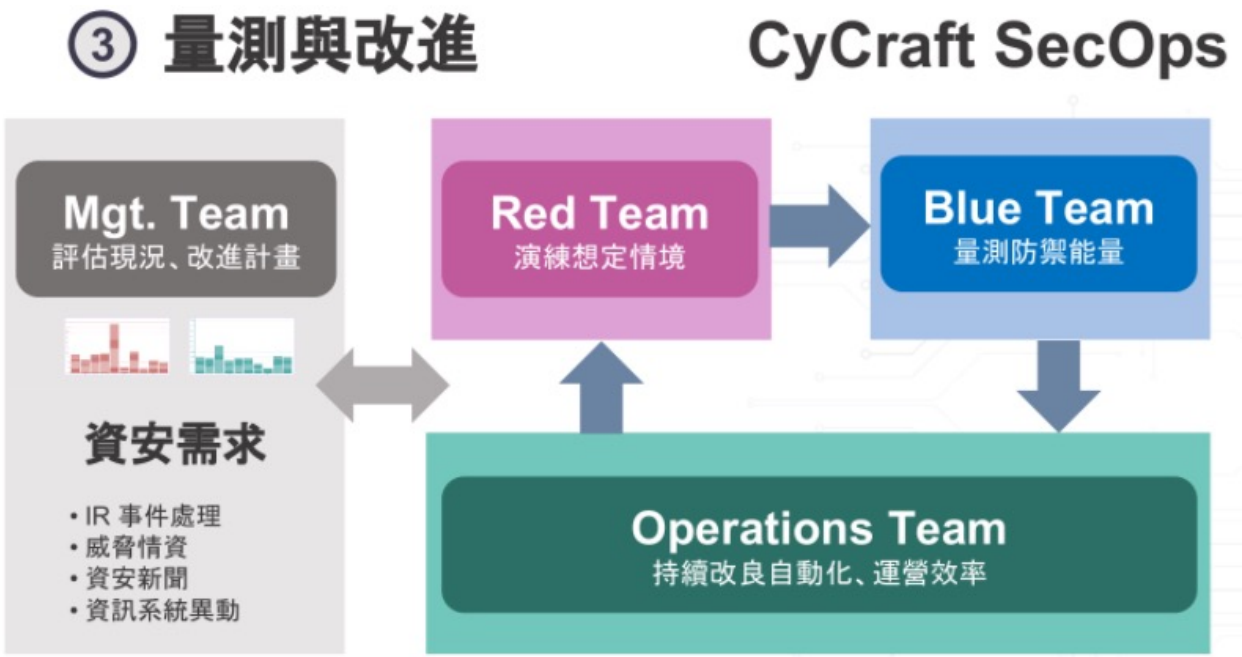
實務面：對現有的資安設備充分掌

以戰代訓：紅軍演練、藍軍演練

金融資安學院 vs. 數位金融學院

資安成效的評量

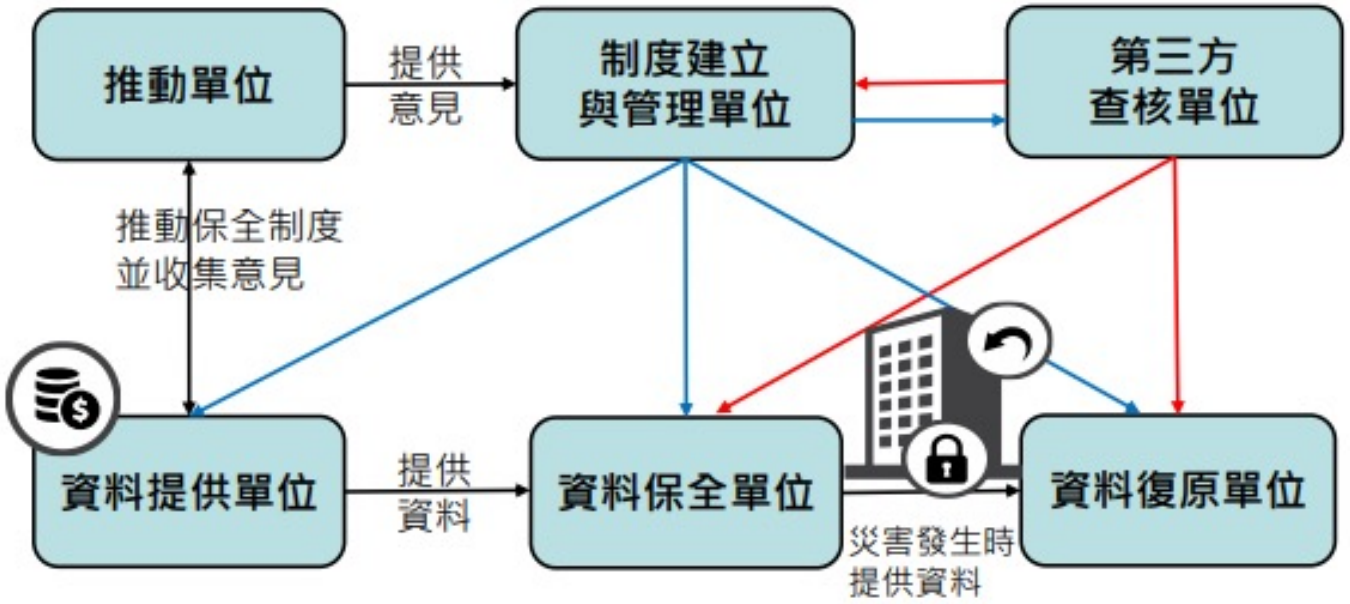
大家都說資安只有投入，無法評量成效。如果不知道目前的情況，也無法評量這次投資的效益，如何說服老闆支持您的計畫？



資料來源：奧義，邱銘彰

金融資料保全的機制

數位化後，大家的資產都在磁碟上，金融機構也都有本地、異地備援，但天災人禍如此頻繁，萬一...



零信任戰略

美國聯邦政府提出零信任戰略，我們的金融零信任策略呢？

美國聯邦零信任戰略草案五大願景

面向	願景
識別（Identity）	讓機構工作人員在工作中，須使用企業級的識別來存取應用程式，並且使用可防釣魚的多因素驗證，以保護使用者受到複雜的網路攻擊。
裝置（Device）	機構需要建立完整的裝置清單，包含所有授權於政府使用，且為政府所擁有的運作裝置，並要能夠偵測與回應這些設備上的事件。
網路（Network）	主要重點放在對於環境中加密所有DNS請求與HTTP流量，以及制定網路分隔計畫，同時也將確定電子郵件加密的可行方式。
應用程式（Application）	機構在看待所有應用程式時，都必須將之視為與網際網路連接，並要定期執行嚴格的實際驗證測試，並且樂於接受外部漏洞報告。
資料（Data）	在資料分類與保護方面，機構將有更清晰與共享的路徑，要利用雲端服務與工具的優勢，來發現、分類與保護自身的敏感資料，並需實現全企業範圍的日誌記錄與資料分享。

資料來源:OMB，iThome整理，2021年11月