IBM Cognitive Bank ABCD

解開數位金融 創新密碼

AI 人工智慧超限思維

Blockchain 區塊鏈翻轉交易

Cloud 雲端擴展規模與彈性

Compliance 法遵智慧進化

Cyber Security 資安守護商譽

Data 資料蘊藏無限商機

資訊安全，是金融創新的先決條件
IBM 數位金融資安藍圖

資訊安全是金融業的成功基礎。來到數位金融的時代，面對日新月異的數位科技及多變攻擊模式，資安風險防護更需與時俱進，才能避免惡意攻擊帶來的重大財務與品牌損失。IBM 專為金融業所規劃的數位資安藍圖，將是金融業領導人、資訊長與資安官檢視企業資安風險、完善防護措施的最佳指南。

金融業近年來遭遇幾起重大資安事件如 ATM 盜領、券商 DDoS 攻擊，引發社會熱議與關注。為此，主管機關金管會不僅宣布成立金融業資安資訊分享中心 (F-ISAC)、發展金融監理沙盒機制，更要求本土銀行須於 6 個月內設置資安專責單位與專責主管、金融監理沙盒等機制，循序漸進提升資訊安全管控層級。

此外，為因應做法持續進化的國際金融犯罪，各國反洗錢、金融犯罪的監管法規也日趨嚴格，金融業者不僅要做好組織的資安防禦，更必須與不同機構進行跨組織協作。從預警、監控、應變到協作，未來資安投資只增不減。金融業者必須自問：如何在有限資源內做到最具效益的完整防護，又能兼顧創新？

數位金融兩大資安焦點：資料與人

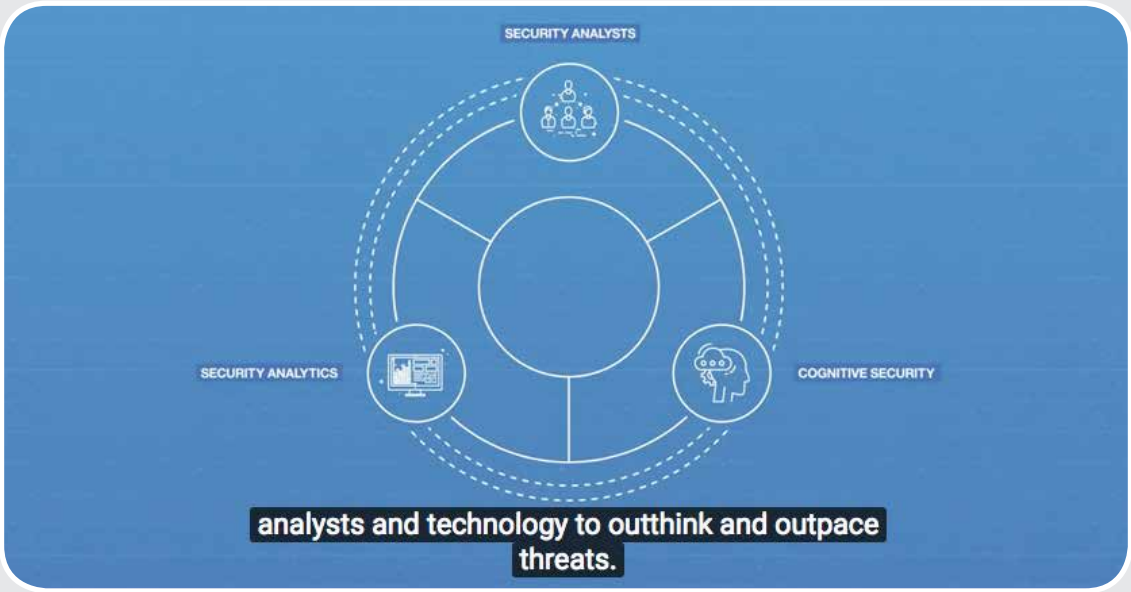
檢視現今的金融資安環境，有兩大資安挑戰必須要克服。首先，是龐大無窮、每天以倍數增加的資安情報量。一家具規模的金融企業每天會發生超過 20 萬次資安事件，數量遠超過任何機構或組織能夠解讀，許多 IT 團隊甚至因為人力不足，不得不直接忽視 50% 的系統安全告警。

然而，這只是資安情報的冰山一角。在冰山之下，資安業界每個月會產出超過 6 萬篇新資安文章、每年發現 7.5 萬個軟體弱點與 1 萬份資安研究報告，加上時事新聞、科技新知、法律與規範等大量非結構化資料，要從中找到能夠有效行動的資安洞察，可說難如登天。

為了協助金融業克服資安情報爆量的挑戰，IBM 於 2016 年派出 IBM Watson for Cyber Security 認知運算平台到 40 家全球百大金融機構學習解讀資安情報。結合金融業者的每日資安工作，IBM Watson for Cyber Security 大量吸收內外部情報，以人類的邏輯思維

來勾勒事件輪廓：分析與推理異常事件，找到關聯影響範圍與隱藏的聯繫，交叉比對數十萬筆資安資訊，推論出事件的完整邏輯與洞察，並建議解決之道。憑藉強大的認知運算能力，IBM Watson for Cyber Security 賦予金融業界前所未見的速度與規模，有效應對各種威脅。

觀賞影片：https://youtu.be/MYZOIdK4o1M



Watson for Cyber Security in Action

人性，是永遠的弱點

第二項挑戰是則是「人」的管理。自從有資訊安全的概念以來，好奇、偷懶、疏忽、貪婪等人性特質就是攻擊者最常利用的弱點。尤其在數位金融環境中，資安威脅牽涉到的人不僅有 IT 管理者、員工、協力廠商，還有數以百萬計的使用者。金融業者不僅要持續培養資安意識、強化管理措施，更需要系統性的解決方案，來彌補永遠不完美的人性。

舉例來說，金融創新為提升便利性、讓消費者有感，必須採用更直覺快速又確保安全的身分認證機制，因此結合臉部與聲紋辨識等不可逆生物特徵的「行動多因子認證」(Mobile multi-factor authentication, MMFA) 成為主流。IBM 提供超過 60 項認證因子，助金融業者為客戶設計便捷又安全的金融新應用。

企業內部的人員管理，除了透過教育訓練來強化資安素養，更應主動監測分析異常行為，才能及時避免損失。QRadar User Behavior Analytics (QUBA) 是 IBM QRadar SIEM 免費提供的行為監測系統，可全面分析每一位內部員工的數據使用行為，如果有異常行為如：瞬間移動到沒去過的地點、IP 變換速度太快、存取敏感資料、使用未授權外部裝置等，系統會計算其安全指數，超過安全閥值就立即通報管理者進行深入調查。IBM QRadar 不僅可預防惡意者，亦能找到在無意間被滲透或操控的設備，避免使用者因疏失成為攻擊跳板。

此外，自動化、強制性系統修補更新可減少終端裝置的安全漏洞；行動裝置管理平台可在員工自帶裝置 (Bring Your Own Device, BYOD) 時確保存取安全，遺失時也能立即鎖機或刪除敏感資料。

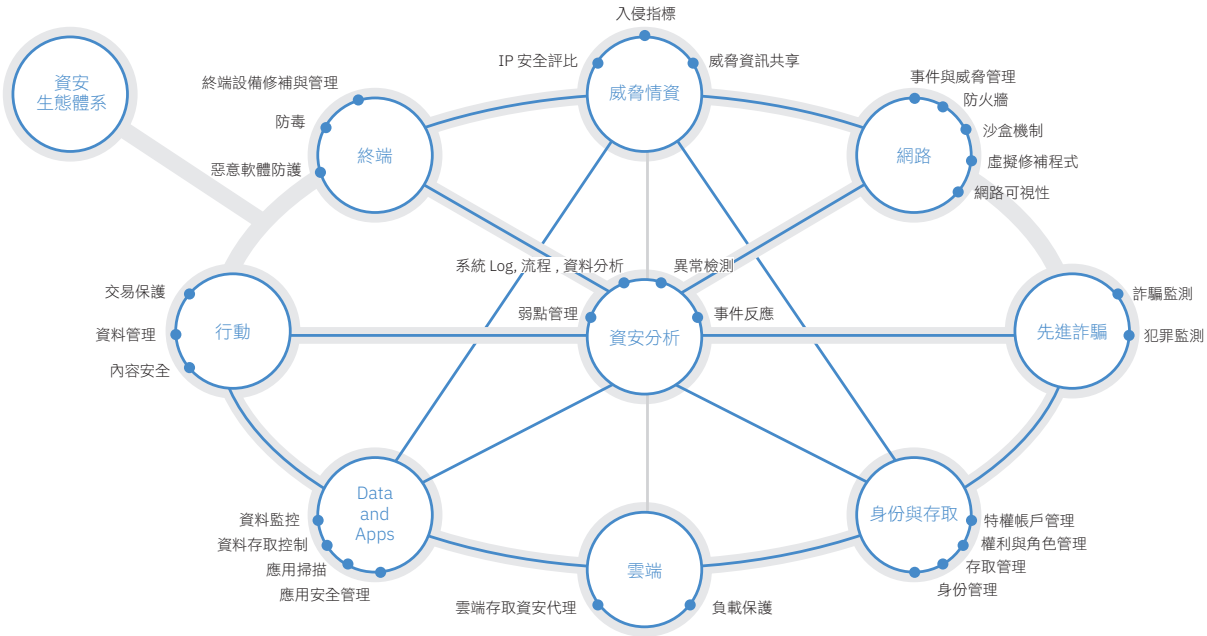
數位金融資安藍圖，實現資安轉型

IBM 是全球金融業最堅實的資安夥伴，憑藉多年來在金融業領域累積的深厚經驗，IBM 為數位金融的未來環境設計了「數位金融資安藍圖」，涵蓋金融業者必須關注的十大資安面向。

資安分析：面對指數暴增的資安情報與威脅告警，多數 IT 團隊與資安系統難以全部消化與處理。IBM QRadar SIEM 能夠整合多來源的資安信息，涵蓋數十億資料點，提供進階威脅偵測與異常行為偵測，並自動實現法規遵循，產生資安報表。

終端裝置：近許多資安事件都是肇因於終端設備的系統更新與修補未能完善，讓有心人有機可趁。除了現有的電腦裝備與 ATM，未來在智慧化趨勢之下，將有更多自動服務裝置或金融機器人加入服務，IBM BigFix 可協助金融業實現終端裝置的自動化更新修補及惡意程式防護，確保終端不再是資安弱點。

行動裝置：行動裝置的惡意軟體與病毒數量與日俱增，當員工使用行動裝置存取公司資料時，必須有完善的惡意軟體保護，否則容易形成風險漏洞。IBM MaaS360 提供企業級行動裝置管理與資安防護功能，讓員工在行動中高枕無憂。



圖一：IBM「數位金融資安藍圖」

資料與應用程式：系統中的資料庫與檔案存取從傳統存取控制與稽核升級到主動掃描、監控與預警。IBM 以 Guardium 來保護與監控資料，並協助金融業客戶加密整體資料庫，AppScan 則可確保應用程式的資訊安全。

雲端資安：在雲端環境中，企業應隨時監控應用程式與使用者的行為模式，偵測異常行為，並限制使用者存取驗證核可的應用。金融業者可採用 IBM Cloud Security Enforcer 雲端資安管理工具，確保在雲端的安全與創新。

威脅情資：資安攻擊手法每分每秒都在進化，跨國、跨企業的資安資訊開放分享將是防止威脅擴散、降低影響規模的關鍵。IBM X-Force Exchange 是開放給全球企業免費使用的資安威脅情報分享平台，X-Force 分析超過 320 億網頁，紀錄 10 萬個資安漏洞、86 萬個惡意 IP，每天監控 2.7 億個惡意軟體端點並管理超過 200 億次資安事件。金融業者能與全球資安工作者一同研究最新安全威脅、彙集可行情報，實現全球協同防禦。

身分與存取：帳戶管理與存取向來是資安重點。數位金融與 Bank 3.0 的創新服務與體驗，牽涉到更多消費者的個人隱私資訊，因此必須導入更安全的多因子認證機制，以確保帳號安全。IBM 提供最先進的多因子認證機制，可兼顧安全與創新。

先進詐欺：IBM Trusteer 主動偵測針對各種金融詐騙與犯罪行為的綜合行為模式，阻絕惡意軟體攻擊。

網路：網路環境除了採用傳統防火牆與事件威脅管理的防護機制，還可引進虛擬修補程式以避免漏洞更新的安全空窗期，以及沙盒機制確保創新應用先經驗證再放行。IBM Network Protection 與 QRadar Incident Forensics 是網路安全保護的最佳選擇。

資安生態體系：積極參與資安生態體系，在符合企業規範的範圍內開放分享資安資訊、威脅事件、威脅特徵、解決方式，不僅有助於避免威脅規模擴散、減少傷害，更能協助業界加速應對資安風險。

先有資安，再談創新

面對高度複雜且持續進化的資安威脅，IBM 專業團隊可協助金融業者依據「數位金融資安藍圖」體檢既有資安架構，以 360 度全方位觀點找出潛在的資安風險並建議有效的解決之道。我們亦建議金融業者針對數位金融資安的「資訊」與「人」兩大挑戰制定策略方案，以確保在金融創新的道路上大步邁進、無後顧之憂。