梁嘉麗
香港銀行學會行政總裁

制定風險評估框架提升網絡安全意識

隨着科技的進步，企業如何確保網絡安全已成最重要課題。就銀行業而言，業務發展愈來愈倚靠數據推動，這帶來了更多前所未見的商機，但網絡安全風險也可能對營運造成影響。近年數碼轉型改善包括監管科技的應用，銀行亦積極吸納及培訓相關人才，以加強行業的網絡安全意識。

根據網絡安全解決方案供應商Mandiant本月初公布，於去年8至9月進行問卷調查，訪問對象涵蓋包括香港在內13個市場、過千名網絡保安決策者，結果顯示超過一半受訪本港企業，在一年內曾遭受網絡威脅。44%香港受訪者表示，他們的企業通常在未有深入了解攻擊者背景的情況下，便要就網絡安全決定好對策。

去年8月，阿里雲亦委託市場調研機構Global Data，訪問了主要亞太市場的金融機構，結果顯示82%受訪機構認為數碼科技是促進業務發展的關鍵。隨着數據安全風險上升，全球金融機構將承擔更大的潛在損失，以及對品牌聲譽造成負面影響。故此，網絡安全防範已經被列為金融業的工作重點。

近年不論大型或中小企業的網絡攻擊事件提醒我們，企業必須積極採取措施來保護其業務和客戶的數據安全。否則，公司業績及聲譽可能會因為網絡事故而受到打擊。金融業若遭受到嚴重的網絡攻擊，日常服務亦將受到影響。

因此，企業需要加強網絡安全風險評估和漏洞掃描，以及採用加密和多重驗證等措施。更重要的是，它們需要為員工提供網絡安全培訓和提高其防範的意識，以避免針對電郵系統、社交媒體等攻擊。

為了提高本地銀行業對網絡安全防範的意識，香港銀行學會本月上旬便舉辦了「網絡安全解決方案日2023」。

今年主題為「Smart Cybersecurity Defence for the Future」，獲破紀錄900人出席及支持。在活動當日，來自金融業及資訊科技界的專業人士共同探討新興網絡威脅及相應的解決方案。他們均同意企業必須具備強大的防禦技術和工具，以化解不斷出現的網絡攻擊。

企業應培訓網絡安全人才

在其中一個小組討論環節，講者便就人工智能技術的普及應用，深入分析機器學習所帶來的機會與風險，並提到企業要以更靈活和自動化的方式，來加強應對黑客利用最新科技進行的網絡攻擊，以及掌握雲端安全性、合規及監管要求的發展趨勢。他們強調企業培訓網絡安全人才的重要性，以確保具備制定相關風險評估框架等技能。其實這與我的觀點相若，企業除了要在硬件上持續更新網絡保安系統，同時要確保各階層人員在軟件上的配合，熟習及嚴格執行最新的網絡保安措施。資訊科技部門亦要有一套與時俱進的管理機制，為職員及服務供應商提供適時的指引。

■香港銀行學會本月上旬舉辦了「網絡安全解決方案日2023」。

學會一直有為銀行從業員提供培訓課程，如在「銀行專業會士」和「銀行專業資歷架構」課程中加入網絡安全的內容；還不時舉辦研討會及講座等活動，例如本月中便邀請了香港警務處網絡安全及科技罪案調查科，為會員分析金融業相關網絡安全趨勢。

毫無疑問，隨着金融科技高速發展，網絡安全將愈來愈重要。銀行業界需要密切關注最新趨勢，諮詢服務供應商的意見，加強網絡安全防範工作，並要鼓勵員工積極參加相關培訓和活動，加強本身的網絡安全技能。