# 黑客垂涎金融機構　　提高網絡防衛意識刻不容緩

**香港銀行學會行政總裁梁嘉麗**

*(本文於 2016 年 7 月 15 日刊於《信報財經新聞》)*

借助科技發展，現今金融網絡罪行越發層出不窮，除了漁翁撒網式藉電郵散播帶有病毒的文件或連結，以盜取個人的資料或金錢，亦會鎖定金融機構以提高「回報」。一間國際網絡保安公司的數據顯示，金融機構面對的網絡攻擊是其他行業的三倍。

金融機構匯聚和處理數以億計的資金，擁有數以十萬、百萬計的客戶個人資料，是被黑客青睞的原因。普華永道 2014 年的一項調查顯示，金融業每十名受訪者中，有四人表示曾經遇到網絡罪行，是業內第二常見的經濟罪行。有 41%的金融業受訪者預期未來兩年會有機會遇到網絡罪行，比例較其他行業的 26%為高。在香港，2015 年香港金融管理局接獲 19 宗銀行受分散式阻斷服務攻擊 (DDoS 攻擊)的報告，較 2014 年的 3 宗同類報告大幅增加。

黑客的犯案模式也變得更多元化。他們或發動 DDoS 攻擊，或透過不同的惡意程式軟件入侵銀行網絡。近日，傳媒報道台灣一間銀行疑被植入惡意程式，34 部自動櫃員機自動吐出共值 7000 萬元新台幣的鈔票。事實上，惡意軟件市場相當「蓬勃」，網際網路安全技術廠商賽門鐵克(Symantec)的統計顯示，2015 年共有 4.3 億個新的惡意軟件面世，較前一年多 36%。

黑客挖空心思發動網絡攻擊，背後的目的是直接盜取屬於銀行或存戶的資金，或是盜取存戶的個人資料促成欺詐交易，有的甚至意圖借助銀行系統以促成欺詐交易，或是妨礙銀行完成客戶的指示，以達到犯罪意圖，例如敲詐。

社會大眾對銀行和金融機構抱有很高的期望，事實上，銀行替存戶管理個人財富，所提供的投資及融資服務促進經濟活動生生不息。若網絡攻擊引致銀行營運停頓、癱瘓，或造成金錢損失、個人私隱被盜，受影響的肯定不獨是銀行本身，許多個人和企業也會受牽連，造成廣泛社會影響。

為了提高網絡保安，不少銀行早已投放大量資源提升硬件設施，包括加設多層保安系統，增加黑客攻入的難度； 提升偵測系統，加快發現網絡攻擊的速度。高德納諮詢公司的數據顯示，本年全球用於網絡安全的支出可能高達 770 億美元，較去年多 8%，並估計 2018 年前銀行和其他企業用於網絡安全的開支有機會超過 1000 億美元。

硬件的提升固然重要，但對於銀行業而言，網絡安全和防衛的工作和責任，絕不能單靠負責資訊科技、保安、風險管理等部門的主管和團隊來把關，網絡安全應該被視為銀行業的「通識科」，來自不同業務、崗位和職級的從業員也應接受不同程度的培訓，讓前、中、後台的營運人員也對網絡安全具備一定的專業知識。與此同時，銀行也需要聘任足夠的相關專才去設計、執行網絡安全工作，並同時加強客戶教育，幫助客戶提高防範金融網絡罪行的意識。總括而言，銀行業同步加固硬件和軟件，加上公眾的警覺意識，才能編織一張堅固的安全網，保護整個金融系統，維繫香港作為國際金融中心的聲譽。

隨著越來越多客戶透過互聯網進行交易，銀行與客戶的溝通更多使用電郵，網絡安全的重要性只會有增無減，也是銀行繼續取得客戶信任的關鍵。故此，銀行業在投放資源培訓網絡安全人才時，應設立認證框架，加強專業性，使行業能夠長遠健康發展。

為此，香港銀行學會、香港金融管理局及香港應用科技研究院正在合作，為銀行業推出新的網絡安全培訓及認證計劃，並會參照先進的國際標準設計及制定。這是鞏固香港銀行業網絡安全的重要一步。

銀行業是香港作為國際金融中心的重要支柱，也支撐著社會百業發展。確保銀行服務、銀行體系持續運作，免受網絡攻擊影響是刻不容緩的工作，並極需要持續的資源投入。

完