FINANCIAL SERVICES DEVELOPMENT COUNCIL 香港金融發展局

業界人士講座系列 報告發布網上研討會

《香港金融服務業的網絡安全策略》

二零二一年六月十日

網絡安全 - 日益嚴峻的重大全球議題

- 網絡攻擊導致各項成本不斷增加，促使世界各國更加關注網絡安全議題。
- 新型冠狀病毒疫情爆發，令世界各國對網絡安全的需求更為迫切。
- 金融服務業在本質上特別容易受到網絡風險影響。行業一直是網絡攻擊的主要目標，並因此蒙受巨大的經濟、監管及聲譽損失。

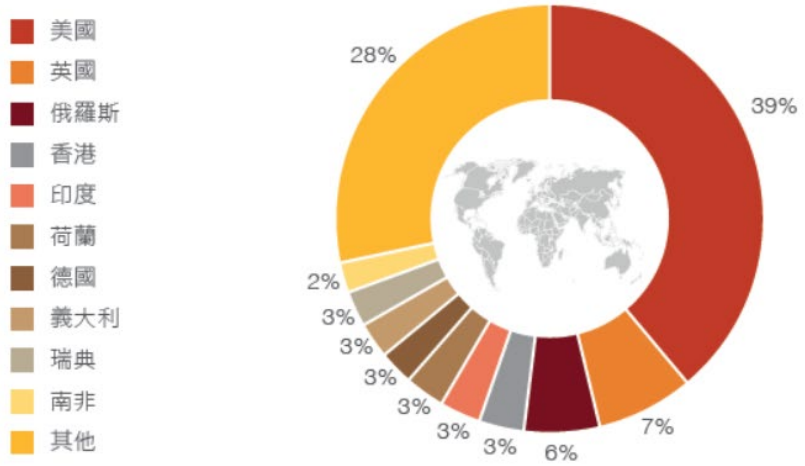
資料來源：財富雜誌, 美國戰略與國際研究中心, 邁克菲

資料來源：國際商業機器公司

香港是否明顯的攻擊目標?

- 香港作為國際金融中心，是網絡攻擊的誘人目標，而網絡犯罪所帶來的經濟損失近年來呈上升趨勢。香港各行業的網絡安全準備水平參差不齊，其中金融服務業的表現最爲優秀。
- 隨著人工智能的廣泛應用，網絡攻擊將變得更為普遍，而未來的網絡世界亦將變得更加複雜。建立一個穩健網絡安全架構的價值主張不單有助預防及抵禦網絡攻擊，亦可以作為金融服務業開拓商機的基礎。

針對不同地區金融機構的網絡攻擊分布（佔總體%）



資料來源：ORX News 及國際貨幣基金組織工作人員計算

為甚麼網絡安全與香港金融機構息息相關

資料來源：弗若斯特沙利文, 微軟, 香港生產力促進局, 香港電腦保安事故協調中心, 世界經濟論壇, 畢馬威

政策建議

政策建議

建議

政策層面

- 為香港制訂專門的網絡安全路線圖並配以政策重點

法律及監管層面

- 立法保護網絡空間
- 統一各項金融業的規例

運作層面

- 促進人才發展；及
- 透過整個業界的壓力測試及加強資料復原措施，令業界能在營運層面上應對網絡風險
  - 壓力測試
  - 資料復原

建議一 (政策層面)
為香港制訂專門的網絡空間安全路線圖並配以政策重點

- 將網絡空間安全元素納入整體智慧城市藍圖對香港而言是良好開端。然而除現時每年更新工作計劃外，香港亦需擁有專門的網絡空間安全路線圖，以制訂更明確的短期、中期及長期優先事項及可行項目。
- 制訂更長遠、更清晰的工作計劃及政策重點，有助香港的不同持份者（包括商界）相互協調並作出相應貢獻。
- 網絡空間安全是一個跨部門議題並涉及多個政府部門或機構，而建議設立一個負責統籌的管治機構的可行方案包括:

  i) 設立一個獨立委員會 (類似於澳洲信號局 (Australian Signals Directorate) 或 新加坡網絡安全局 (Cyber Security Agency of Singapore))；或

  ii) 設立一個跨局 / 跨部門的工作小組，以統籌監管及執法行動。

建議二 (法律及監管層面)
立法保護網絡空間

- 多個在網絡安全範疇領先的地區都設有綜合的網絡安全/網絡空間保護法例作為網絡安全架構的核心要素。
- 香港應考慮制訂綜合的網絡空間保護條例，條例至少應涵蓋以下目標:
  - 識別及界定「關鍵資訊基建」；
  - 建立問責架構（包括網絡事故的調查、報告及執法，包括民事及/或刑事訴訟程序）；
  - 界定及規定公私營機構之間分享網絡保護資訊的類型（例如有關所面對事件/威脅的類型）； 及
  - 在適當的情況下，為網絡安全服務供應商建立寬鬆的發牌架構。
- 除了建議的綜合網絡空間保護條例外，其他相關法規亦應定期檢討，確保相關法規切合目標並與國際標準保持一致。

建議三 (法律及監管層面)
統一各項金融業的規例

- 鑑於金融體系內不同行業之間的聯繫，某個行業面對的網絡事件很容易對其他行業造成溢出效應。有效的網絡安全架構需要各個金融監管機構互相協調。
- 就網絡安全而言，香港已制訂多項監管指引。金管局、保監局及證監會各有其相關指引/通告，協助其監管的持牌/認可機構處理網絡安全問題。但儘管各監管機構之間存在有限度的協調，但進一步的協調政策應對工作卻仍未展開。
- 其中一個有待協調/統一的範疇是偵測到網絡事件時的報告時間。
- 跨機構督導小組是實現協調的一種有效方法

建議四 (運作層面)
促進人才發展

- 隨著金管局推行專業資歷架構，市場普遍留意到銀行業的網絡防衛得以改善。。然而，鑑於各個金融行業之間關係密切，若其他行業未能表現出相應的防衛能力，銀行業的進展可能會受到影響。
- 我們建議證監會及保監局等其他金融監管機構攜手合作，在金管局專業資歷架構基礎上，發展並建立具有專業分支的統一架構，以滿足不同行業不斷轉變的監管要求。
- 針對目前金融機構可能仍然不願意投放大量資源提升網絡防衛，解決這個問題的其中一個方法是由香港政府提供誘因，例如為參加監管機構認可/批准的網絡安全認證計劃的合資格員工或機構提供培訓資助。
- 長遠而言，香港可參考其他地區（例如澳洲、中國內地及新加坡）的做法，建立一個網絡安全培訓機構。然而，這項建議有待政府作出更深入的可行性研究。

建議五 (運作層面)
業界在營運層面上應對網絡風險的能力

- 為評估香港抵禦及承受網絡攻擊的能力，我們建議政府對金融服務業進行一系列網絡壓力測試。鑑於不同金融服務行業之間的關係日益密切，而網絡攻擊複雜多變，我們建議整個行業的不同界別都應參與壓力測試。
- 我們期望金管局、證監會及保監局通力合作，(並在財庫局的引導下) 優先制訂相關壓力測試。在籌劃整個業界的壓力測試時，香港的金融業監管機構可負責籌劃演練，或鼓勵金融機構各自籌劃及進行行業演習。
- 面對日益頻密及嚴重的網絡威脅及事件，世界各地的金融機構、政府和監管機構都在探討最佳的資料復原方法。現時，香港的金融機構主要依靠自身的基建儲存及復原資料，在發生網絡事件時盡量減少業務中斷及資料遺失。考慮到所涉資料的性質及數量，業界主導的措施至少在短期內是較為實際的選項。

結語

- 網絡攻擊對全球政府及企業造成巨大的經濟、監管及聲譽損害, 而金融服務業是網絡犯罪分子的主要目標。
- 香港作為國際金融中心正面臨愈來愈多的網絡罪案。就此，金融機構不斷提升其防止、應對及處理網絡風險的整體應變能力。
- 為配合國際網絡安全標準，香港應參考被公認為首屈一指的司法管轄區的網絡安全架構。
- 本文提出一系列建議，以作爲香港加強其網絡安全架構的關鍵步驟。鑑於呈現、解決和處理網絡風險的緊迫性，文內所述的建議可以同步進行。
- 然而提升香港網絡安全水平的措施最終能否成功，實有賴公私營機構的充分參與及合作。

討論環節

各地區網絡安全架構比較 - 網絡安全政策及策略層面

香港

- 雖然香港沒有一份獨立的網絡安全文件，但網絡安全政策方向已納入香港「智慧城市藍圖」。
- 香港政府亦定期發布有關網絡安全的政策及指引，並參與國際性及地區性的網絡安全組織以加強資訊交流。
- 香港已成立政府資訊科技總監辦公室 (資科辦) 及其他由政府資助的機構，以防禦及應對網絡威脅及事故。
- 金融監管機構已率先制訂適用於金融服務行業的網絡安全計劃。

歐盟

- 歐盟網絡安全策略於2013年首次公布，並於2020年作出最新修訂。
- 歐盟網絡與信息安全局 (ENISA) 在2020年7月公布其全新的網絡安全策略。

美國

- 美國國土安全部的國家網絡安全策略於2003年公布。
- 《關於加強聯邦網絡安全及主要基建的行政命令》於2017年頒布。
- 《2018年網絡安全與基礎設施安全局法案》於2018年簽署。

中國內地

- 《中華人民共和國網絡安全法》自2017年起實施。
- 《中華人民共和國數據安全法》草案於2020年7月公布。
- 《個人信息保護法(草案)》於2020年10月公開諮詢。

新加坡

- 《 更安全網路空間綱要計劃》於2020年公布。

各地區網絡安全架構比較 - 法律及金融監管架構層面

香港

- 並無「綜合」的網絡安全條例或政府部門/監管機構。
- 1993年制訂的《刑事罪行條例》第161條將多項條例下現有的刑事罪行範圍擴大至涵蓋與電腦有關的刑事罪行。
- 《個人資料（私隱）條例》訂明香港的資料私隱及保障架構。
- 證監會已向持牌法團發出一系列與網絡安全風險相關的指引及通告。
- 金管局於2016年推出銀行業的「網絡防衛計劃」。
- 香港保險業監管局要求保險公司識別網絡安全威脅，並發出指引，訂明保險公司在網絡安全方面應達的最低標準。

歐盟

- 《網絡安全法》於2019年實施，以加強ENISA的職權並在歐盟建立網絡安全認證架構。
- 《通用數據保障條例》是歐盟的綜合資料保障法律。

美國

- 並無單獨統一的網絡安全法例。法定架構較為分散，設有適用於特定行業及資訊的規定。
- 美國並無綜合的私隱/數據保護法規。相反，私隱問題受各州及聯邦層面的多項法規規行相關規例。
- 《格雷姆-利奇-比利雷法案》於1999年頒布。
- 美國證券交易委員會亦使用其民事法權力採取與網絡相關的執法行動。

中國內地

- 《國家安全法》將網絡空間和信息安全列入國家安全的重要部分。
- 中國人民銀行於2020年2月公佈新的《個人金融信息保護技術規範》 。

新加坡

- 《科技風險管理指導原則》於2021年作出最新修訂。

各地區網絡安全架構比較 - 網絡文化層面

香港

- 香港企業網絡保安準備指數由香港生產力促進局發布，用於衡量本地的網絡安全意識及企業的網絡是否準備就緒。
- 最新指數於2020年5月發布，並指出本港整體準備水平為46.9（最高為100）。

歐盟

- 歐盟委員會於2020年1月發布有關歐洲人對網絡罪案調查態度的調查報告，指出網絡罪案的意識正在提升，有52%的受訪者表示對網絡罪案頗為了解或非常了解。

美國

- 皮尤研究中心於2017年1月發布的調查報告顯示美國人在日常數碼生活中通常未能達到網絡安全的最佳實踐，例如妥善管理密碼。
- 皮尤研究中心於2019年10月發布的另一份調查報告指出美國人對科技相關議題的理解因主題而異。

中國內地

- 中國政府網絡安全當局在2020年9月進行的一份調查顯示，約88.5%的受訪者指出他們會注意是否同意允許應用程式存取手提電話的傳感器及數據。

新加坡

- 於2019年進行的網絡安全公眾意識調查顯示公眾對網絡事故的關注度為高。

各地區網絡安全架構比較 - 網絡安全教育、培訓及技能層面

香港

- 已建立多個政府支援的平台，提供有關網絡安全的資訊及指引。
- 政府亦已推行多項措施，推動本地各行業的資訊保安持份者的資訊共享及協作。
- 在專上教育及持續教育方面，香港在亞洲區率先將網絡安全的職業訓練元素納入課程。
- 在吸引非本地人才方面，政府的「科技人才入境計劃」為招募網絡安全專業人才提供快速處理安排。

歐盟

- 歐盟網絡與信息安全局實行並支持多項措施，以提升網絡安全議題的意識及教育，包括：公布改善網絡安全文化的指引，舉辦每年一次的「歐洲網絡安全月」等等。

美國

- 國家網絡安全教育計劃是由政府、學術界和私營機構共同成立，目的是滿足公眾意識、教育、專業發展和人才管理等範疇的網絡安全需求。
- 《網絡安全職業和研究國家倡議》是一個網上的國家資源網站，提供網絡安全教育、培訓及就業機會。

中國內地

- 政府計劃在2027年前建立多所世界級的網絡安全學院，以培養強大的專業人員隊伍應對網絡攻擊。截至2019年，11所大學已獲選參與計劃。
- 中央網絡安全和信息化委員會辦公室於2020年9月舉辦國家網絡安全宣傳周。

新加坡

- 網絡安全意識聯盟是由網絡安全局共同主持的公私營合作機構，旨在建立積極的網絡安全文化並提升網絡安全意識。

問答環節