FSDC Paper No.49

FINANCIAL SERVICES DEVELOPMENT COUNCIL
香港金融發展局

香港金融服務業的網絡安全策略

二零二一年六月

目錄

行政摘要

網絡安全，又名網絡空間安全，是一個跨行業、跨邊界的主題，而在不同行業中，金融服務業一直是網絡犯罪分子的主要目標之一。多年來，這些犯罪分子為經濟、監管和聲譽帶來重大損失。香港作為國際金融中心面臨越來越多的網絡罪行，而為了避免、解決和處理網絡風險，金融機構正持續提升其網絡安全的預備。

隨著後2019冠狀病毒病時代的科技迅速發展（包括持牌虛擬金融服務的興起、對雲端及在線協作工具的日益依賴等），未來的網絡世界將越發複雜，而應對網絡風險的需求亦更見迫切。

根據香港與其他地區（包括澳洲、歐盟、日本、中國內地、新加坡和美國）在網絡安全框架上的比較，我們在四個方面總結出香港對比國際的表現：（i）網絡安全政策和策略；（ii）法律及監管框架；（iii）網絡安全文化（和社會）；（iv）網絡安全教育、培訓及技能。

雖然香港在網絡空間安全範疇上跟得上其他地區，卻非獨佔鰲頭。為加强香港應對網絡風險的能力，我們建議：

在政策層面上-

- 為香港制訂專門的網絡安全路線圖並配以政策重點；

在法律及監管層面上-

- 立法保護網絡空間；
- 統一各項金融業的規例；

在運作層面上-

- 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。

在倡議上述建議的同時，我們亦鼓勵公私營界別在過程中積極參與合作，讓香港具備更有效及充分的能力應對網絡風險，成為更具競爭力的國際金融中心。

網絡安全——日益嚴峻的重大全球議題

數據已成為新經濟的重要資產：數據可以買賣及交換，價值不菲，而不同經濟持份者趨之若鶩，各有所圖，好壞不一。不同地區、行業及規模的機構，都致力「*防止、檢測及應對（網絡）攻擊*」，以保護其數據 –「網絡安全」[1]正是本文要探討的數據範疇議題。

由於網絡風險本身難以衡量或量化，因此研究網絡安全存在極大挑戰。**網絡風險大多來源不明，而部分國家或機構就其面對的風險或會諱莫如深，令精準分析網絡風險難上加難。**[2]

縱然網絡安全研究面對重重挑戰，但因着網絡風險造成的危害令人震驚，網絡安全已逐漸成為重點議題。網絡攻擊為害不淺，包括引致各項成本不斷增加，促使各國更加關注相關問題。多年來，網絡攻擊造成的經濟損失激增——早在2015年就有英國保險公司估計，全球網絡攻擊每年令企業蒙受的損失高達4000億美元。[3] 美國智庫機構的研究顯示，截至2018年，網絡罪案造成的損失已高達6000億美元，佔全球國內生產總值的0.8%。[4] 最新數據顯示，截至2019年，全球網絡罪案造成的損失超過1萬億美元，較上一年增加超過50%。[5] 網絡罪案造成的損失增多，有多方面原因，包括網絡犯案愈加容易、跨國網絡犯罪「中心」不斷擴展，以及網絡罪犯出售所盜取資料的手法日益精密。[6]

在公司層面，網絡攻擊造成的損失涵蓋多個方面：既有內部防範措施的成本（例如檢測、調查及復原），亦有外部招致的後果及成本（例如業務中斷、收益損失及資料被竊）；既有直接財務損失，亦有間接損失（例如法律及監管責任，聲譽受損等）。埃森哲與Ponemon在2018年調查不同行業350家公司超過2600名高級專業人士，[7] 結果發現，網絡保安漏洞的平均數目以及網絡罪案引致的平均損失持續均穩步上升，在過去五年分別激增67%（2018年有高達145個漏洞）及72%（2018年損失高達1300萬美元）。根據一家保險公司和律師事務所在2021年所進行的最新聯合調查顯示，受訪的亞太、歐洲、英國及美國董事均認爲網絡攻擊是五大影響其業務的風險之首，其中56%的受訪者表示網絡風險對其業務產生非常或極其重要的影響。[8]

金融服務業是網絡攻擊的主要目標，銀行及保險業所受打擊最大，2018年的平均損失分別約為1800萬美元及1500萬美元。[9] 同樣，IBM發現金融及保險業已連續五年成為受攻擊最多的行業，2020年遭受的網絡攻擊及網絡罪案佔整體數字的23%。[10] 基於上述統計資料，網絡安全已迅速成為眾多金融機構的優先要務。

---

[1] 美國國家標準技術研究所電腦資源中心(National Institute of Standards and Technology)，美國商務部轄下非監管機構國家標準技術研究所所作的定義(“Computer Resources Centre - Glossary: cybersecurity”)。
[2] 美國國土安全部，網絡風險經濟能力差距研究策略(“Cyber Risk Economics Capability Gaps Research Strategy”)，2018年10月。
[3] 財富雜誌，Lloyd’s 總裁：網絡攻擊每年共耗企業4000億美元(“Lloyd’s CEO: Cyber attacks cost companies $400 billion every year”)，2015年1月。
[4] 美國戰略與國際研究中心(Centre for Strategic and International Studies)，網絡罪案的經濟影響達6000億美元而金額正逐步上升(“Economic Impact of
[5] Cybercrime: At $600 Billion and Counting - No Slowing Down”)，2018年2月。
[6] 邁克菲, 網絡罪案的潛在成本(“The Hidden Costs of Cybercrime”)，2020年12月。
[7] 見註腳4。
[8] 埃森哲、Ponemon研究所，第九期網絡罪案損失年度報告(”Ninth Annual Cost of Cybercrime Study”)，2019年3月。
其禮律師事務所(Clyde & Co)及韋萊韜悅(Willis Towers Watson)，“Directors and Officers Insurance (D&O) Liability Survey 2021”，2021年4月。
[9] 同上。
[10] 國際商業機器公司(IBM)，應對X-force威脅能力指數2021 (“X-Force Threat Intelligence Index 2021”)， 2021年2月。

網絡風險成本不斷上升

資料來源：財富(Fortune)
戰略與國際研究中心(Center for Strategic and International Studies)
邁克菲(McAfee)

資料來源：國際商業機器公司 (IBM)

除了令機構成本增加外，網絡風險亦因其本質上是跨國議題而更具威脅性。策動與發動網絡攻擊的罪犯可以身處不同地方，而且可迅速轉換互聯網協定（IP）地址。根據過往經驗，歐美市場是網絡攻擊的常見目標，亦較其他地區更早部署保安防範。隨著針對歐美市場發動攻擊的難度愈來愈大，網絡攻擊的重心逐漸擴展到亞太地區。近年來，亞洲區所受的威脅級別已遠高於世界其他地區。例如，LexisNexis研究報告指出，於2020年上半年，亞太地區的整體網絡攻擊率（3%）高於1.4%的全球平均水平。[11] 鑑於其地域流動性極大，網絡罪案往往難以追踪及起訴。

不同的國家和地區已開始意識到網絡安全的重要性，並相應加強其網絡防衛。正如《2018年全球網絡安全指數》報告指出，[12] 亞洲多個國家在網絡安全方面已達致與歐美國家的水準，在評核所及的五大「支柱」（包括法律措施、技術措施、組織措施、能力建設措施及合作措施）方面積極履行網絡安全承諾。中國（包括香港）、日本及新加坡均被劃分為對五大支柱履行「高度」承諾的三個司法管轄區。同樣，美國智庫[13]報告指出，就行為守則及標準而言，香港及新加坡被視為擁有相對成熟的網絡監管制度。

新型冠狀病毒疫情爆發，令對網絡安全的需求更為迫切。隨著各國政府、機構及個人因應時勢開展實行遙距工作及採用虛擬會議等新的網上活動，全世界的網絡罪犯亦在這場危機中蠢蠢欲動。例如，2020年4月，世界衛生組織宣布其遭受的網絡攻擊數目較上一年同期增長五倍。[14] 一家專項風險保險公司所作的調查報告亦得出類似觀點，結果顯示在2020年有幾乎一半的歐洲和北美企業曾遭受因疫情而變得更為活躍的網絡犯罪分子的攻擊；[15] 而在受訪的8個司法管轄區的6,042家公司中，有43%曾在2020年遭受過網上攻擊，較上一年同期增長38%。[16] 至於金融服務業，多個規管機構已呼籲金融機構加強網絡防衛。其中，打擊清洗黑錢財務行動特別組織（FATF）在其風險及政策回應中指出，社交工程攻擊激增，透過詐騙網站連結或惡意附件盜取客戶的個人付款資料。[17] 遙距交易增加，對網上平台的了解有限以及不受監管的金融服務等因素，都可能令全球金融體系更易受到攻擊。[18]

[11] 律商聯訊風險資訊公司(LexisNexis)，“Cybercrime Report January-June 2020: The Changing Face of Cybercrime”，2020年9月。
[12] 國際電信聯盟(International Telecommunication Union)，全球網絡安全指數2018 (“Global Cybersecurity Index 2018”)，2019年4月。
[13] 美國戰略與國際研究中心，亞太區金融界別網絡安全要求 (“Financial Sector Cybersecurity Requirements in the Asia-Pacific Region”)，2019年4月。
[14] 世界衛生組織，世衛指網絡攻擊錄五倍升幅並促警惕 (“WHO reports fivefold increase in cyber attacks, urges vigilance”)， 2020年4月。
[15] Hiscox, Hiscox網絡安全預備報告2021 (“Hiscox Cyber Readiness Report 2021”)，2021年4月。
[16] 同上。
[17] 打擊清洗黑錢財務行動特別組織，新冠相關的洗黑錢及恐怖分子資金籌集活動：風險及政策回應(“COVID-19-related Money Laundering and Terrorist Financing: Risks and Policy Responses”)，2020年5月。
[18] 同上。

香港是否明顯的攻擊目標？

多年來，各類的研究探討如何評估網絡風險，相應衍生眾多評估標準。然而，部分最廣為採用的標準更適用於評核網絡攻擊的可能性及嚴重性，而鮮能衡量一段時間內可能導致的損失程度。同樣，有研究指出，諸如風險價值之類的市場風險及信用風險指標與網絡安全並無關聯。[19]

儘管缺乏評核網絡風險的公認科學依據，全球商界領袖愈來愈關注網絡安全議題。世界經濟論壇報告指出，[20] 公司高層認為網絡攻擊是世界面對的十大風險之一。

儘管網絡安全在多個行業廣受關注，本文將重點探討網絡安全對整體經濟及金融服務業的影響。本節將審視香港作為區內領先的國際金融中心，是否網絡攻擊的重點目標；屬實的話，香港能否妥善應對。

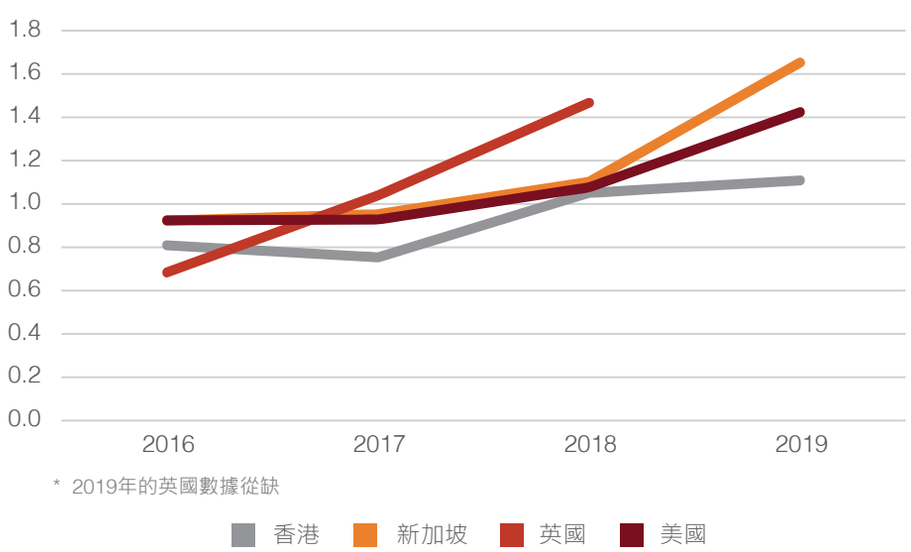
香港的網絡風險水平及其影響

香港面對的網絡風險顯而易見，並且不斷增加。香港電腦保安事故協調中心（HKCERT）的報告，網絡安全漏洞的數量仍然很大。最新公布的數據顯示，單在2020年，香港錄得近39,000個唯一的網絡攻擊數據，涉及惡意程式寄存、釣魚網站和網頁塗改。[21] 而根據香港警務處資料，2019年的科技罪行數目已攀升至8,322宗，按年增長6%。[22]

就香港的網絡風險在國際上處於何種水平，市場意見不一。圖A比較香港與其他幾個發達經濟體的人均科技罪行數目。雖然不同司法管轄區對科技/網絡/電腦相關罪行的定義略有不同，但香港的人均罪行數目與調查所及的其他國家大致相符。與此同時，香港似乎是跨境數碼攻擊的目標之一（見圖B，有關一天內針對香港發起的DDoS攻擊情況的截圖）。

圖A

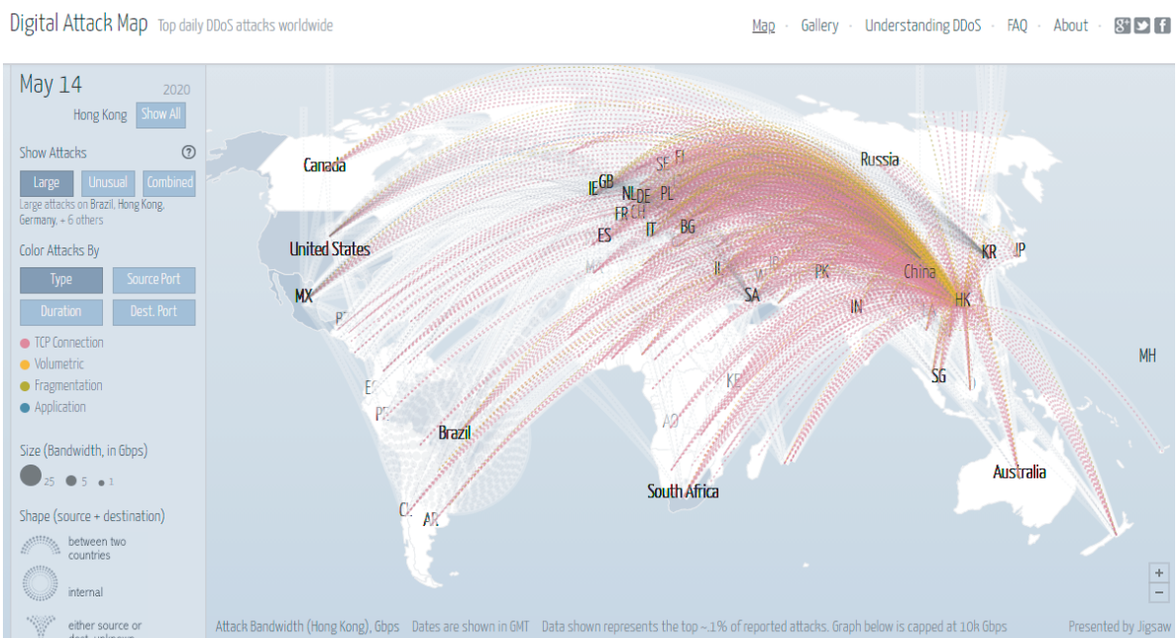
各地區平均每千人的網絡／科技罪案數目



資料來源：香港警務處；新加坡網絡安全局
英國國家統計局
美國聯邦調查局及網絡犯罪投訴中心

[19] Domenic Antonucci，網絡風險手冊：建立及評估有效網絡安全能力（"The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities"）（第67-70頁），2017年5月。
[20] 世界經濟論壇，環球風險報告2021（"The Global Risks Report 2021"），2021年1月。
[21] 香港電腦保安事故協調中心，《香港保安觀察報告（2020年第四季度），2021年2月。
[22] 香港警務處，2019年香港整體治安情況，2020年3月。

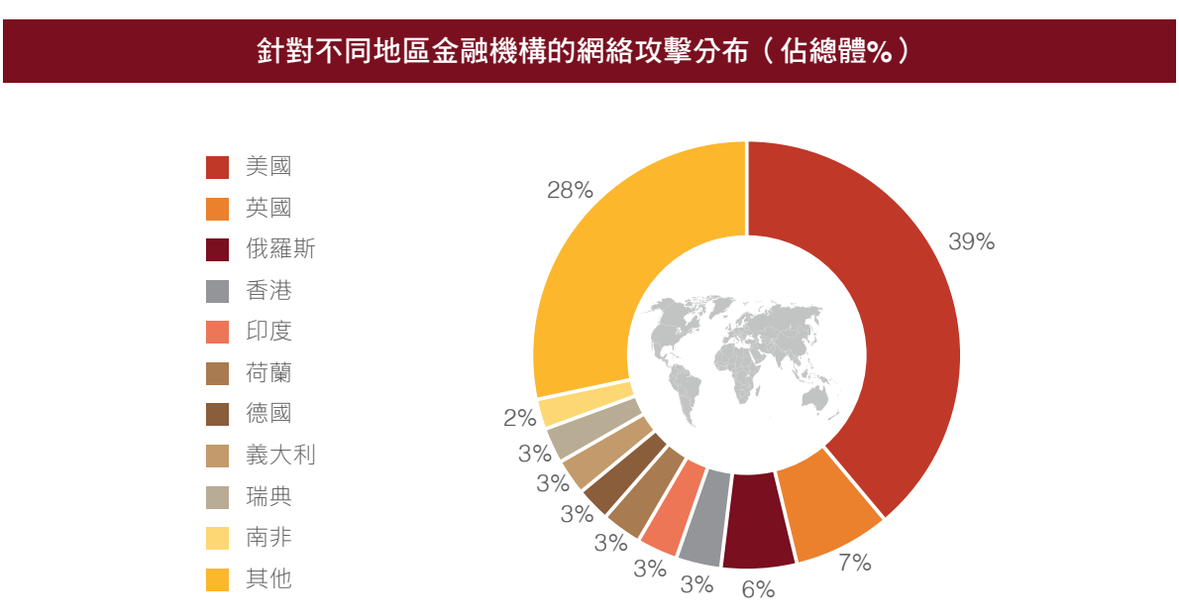
圖B



資料來源：由Google Ideas與Arbor Networks合作構建的數碼攻擊地圖（於2020年5月14日訪問）

香港金融機構面對的網絡風險亦不容低估。根據國際貨幣基金組織職員調查顯示，針對金融機構的網絡攻擊多發生於發達經濟體（包括英美兩地），而香港佔整體3%，與意大利及印度等地相當（見圖C）。[23]

圖C



資料來源：ORX News及國際貨幣基金組織工作人員計算

[23] 國際貨幣基金組織，國際貨幣基金組織工作報告 - 金融界別的網絡風險：量化評估架構（"IMF Working Paper – Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment"），2018年6月。

網絡罪案造成巨大經濟損失，由此亦可見香港所面對網絡風險的嚴重程度。微軟委託Frost & Sullivan於2018年進行的一項研究顯示，網絡安全事件對香港造成的潛在經濟損失可能高達320億美元，約佔香港本地生產總值的的10%。[24] 特別是，大型機構（500名僱員或以上）招致的經濟損失可能高達2,490萬美元，較中型機構（250至499名僱員）的平均估計經濟損失高出超過650倍。[25]

2019年香港公司及居民因網絡罪行而蒙受的實際財務損失超過29億港元（約合3.7263億美元）。[26,27] 例如，在證券經紀行業，在截至2017年3月31日止的18個月期間，證券及期貨事務監察委員會（「證監會」）收到近30宗網絡保安事故舉報，當中大多涉及黑客入侵客戶在證券經紀行開設的以互聯網為基礎的交易帳戶，造成總額超過1.1億港元（約合1,420萬美元）的未經授權交易。[28]

當然，有人可能會辯稱，上述統計數據並不能確切證明香港較其他主要經濟體面對更大的網絡風險，然而，上述網絡罪案的數目及財務損失之大，至少足以表明香港是網絡攻擊的主要目標。正如LexisNexis報告指出，香港已成為網絡攻擊的「主要目標」，因為香港是「*重要的金融中心，人均收入位居全球前列。上述因素，加上較先進的數碼經濟，使香港成為亞太地區網絡罪案的其中一個重點目標*」。[29]

[24] 微軟，網絡安全威脅為香港機構造成320億美元的經濟損失(“Cybersecurity threats to cost organizations in Hong Kong US$32 billion in economic losses”)，2018年6月
[25] 同上。
[26] 香港資訊安全網（政府資訊科技總監辦公室轄下），「電腦相關罪行：統計數字」，最近更新時間為2021年3月。
[27] 對最新數據（資料來源：香港警務處網絡安全及科技罪案調查科）作更深入分析顯示：2019年，一般科技罪案當中的互聯網詐騙案共計5,157宗，佔整體科技罪案總數8,322宗的62%；在2020年上半年，涉及虛擬貨幣的科技罪案數目按年增長1,060%（2020年上半年共58宗），造成的損失總額為2,300萬港元。
[28] 香港證券及期貨事務監察委員會，《有關建議降低及紓減與互聯網交易相關的黑客入侵風險的諮詢文件》，2017年5月。
[29] 見註腳10。

香港的網絡安全應變能力

雖然香港面對的網絡風險日益高漲，令人震驚，但不應因噎廢食，減少採用新科技。相反，我們應著重在網絡安全措施的適用程度與市場/業務發展之間取得平衡。

問題在於，香港是否準備好預防、應對及/或處理其面對的網絡風險。相較於其他經濟體或司法管轄區，對香港整體網絡安全應變能力的研究及調查有限。大多數研究人員或國際機構（例如聯合國轄下的專門機構國際電信聯盟（ITU））均按「國家」編制全球網絡安全指數，對於香港這類的市場通常並無專門得分或排名。儘管如此，有關香港本地各行各業的應變能力仍可作為實用參考。

簡而言之，**香港本地的應變能力水平參差不齊**。香港生產力促進局和香港電腦保安事故協調中心訂立了一個架構，用於編制香港企業網絡保安準備指數，以跟踪本地商界的網絡安全意識及應變能力。2020年，香港企業的整體網絡安全準備指數為46.9（最高100），屬於「具基本措施」級別的較低水平，較上年度下跌2.4。[30] 在研究所及的六個行業中，金融服務業的準備指數得分最高，為62.9，屬於「具管理能力」級別。[31] 而金融業以外的公司，準備指數得分要低得多，具體薄弱環節與非技術解決方案有關（例如培訓、意識建設、流程等）。鑑於網絡風險是跨行業議題，上述情況或會對香港金融機構構成間接威脅——例如竊取所得的私人或機密資料，可用於對個人的金融機構帳戶進行有針對性的攻擊。此外，在指數的四個評估範疇中，人員意識在所有行業都是得分最低的範疇。

香港的網絡安全專家亦深刻意識到網絡安全應變能力參差不齊的情況。2020年5月至6月期間，香港金融發展局（金發局）與本地資深的網絡安全從業人員[32]展開多輪討論，相關人士一致認為香港金融業的應變能力高於其他行業。然而，即使在金融業當中，各個機構的應變能力亦不盡相同，大型機構有能力增撥資源提升網絡安全基建，而小型機構只能守成。同時，公眾通常誤以為網絡安全相當於「科技」，因此個別機構盲目尋求資訊科技相關認證。

根據受訪專家的說法，個人的網絡風險意識普遍較弱，是香港（乃至世界其他地區）面對的主要挑戰。儘管機構往往更重視企業的網絡基建，但「人為因素」通常被忽略。每一個個人——包括金融服務業的每一位用戶以及業內每一位從業人員——都可能在很大程度上影響金融服務業的網絡防衛。事實上，人為錯誤始終是眾多網絡安全漏洞背後的主要原因。出現相關違規行為，原因可能在於人為錯誤（例如配置誤差），或將有關工作外判給對伺服器需求了解不足的第三方所致。特別是，當新的（虛擬）服務供應商嘗試挑戰傳統金融機構以爭取市場份額時，往往會倉促推出新系統，並忽略配置誤差的問題。

[30] 香港電腦保安事故協調中心，SSH香港企業網絡保安準備指數2020調查，2020年4月。
[31] 同上。
[32] 參與討論的從業人員在金融機構、大學及金融科技初創公司從事網絡安全相關工作超過15年。

香港應維持一個網絡安全但對企業友好的環境

如上所述，雖然香港是網絡攻擊的主要目標，但是香港（尤其是金融服務業）已具備一定應變能力，可以應對有關攻擊。然而，未來的網絡世界只會更為複雜，因此網絡攻擊與應變處理之間的攻防戰將會持續發展。

正如世界經濟論壇的職員及其他人士所指出，[33] 網絡攻擊可能會變得更為普遍及複雜。網絡攻擊者透過人工智能（例如Emotet 木馬程式）可以汲取失敗教訓，修改並重新發動可擴展的專門攻擊，令某個行業或金融中心防不勝防。未來威脅網絡安全的可能是注重細節而技術高超的新一代攻擊者。

對於香港這樣的國際金融中心而言，這尤其是一項挑戰，因為金融服務業在本質上特別容易受到網絡風險及其快速擴散的影響。金融機構極大地依賴關鍵的金融市場基建，例如支付及結算系統、交易平台、中央對手方等。當網絡攻擊導致關鍵基建出現單點故障時，漣漪效應便會影響金融體系其他環節。例如，對現金和證券支付結算都非常重要的RTGS及SWIFT系統，兩者都是發生「單點故障」的潛在關鍵基建。[34] 針對此類系統的網絡攻擊不單會影響系統本身及其使用者，甚至可能會影響整個金融市場——例如，假若SWIFT系統由於網絡攻擊而無法提交付款指令，就可能引發廣泛的流動性錯配。[35] 結算週期相對較短的市場（例如，無抵押隔夜貸款市場及回購協議市場）所受影響尤為嚴重。[36]

技術快速發展為企業及個人帶來更多的便利及效益，同時亦令香港網絡安全議題日益複雜。自2018年起，香港引入虛擬金融服務（例如虛擬銀行及虛擬保險公司）。隨著科技發展，線上/遙距虛擬服務的使用量自然增加，網絡安全與金融服務業之間的關係很可能因而變得更加密不可分。[37] 在後疫情時期，金融機構的營運方式正發生變化——透過雲端、在線協作工具等，由傳統的實體寫字樓模式向虛擬/遙距模式轉變。加上第五代（5G）流動網絡覆蓋及其他智慧城市基建，日新月異的科技發展將令黑客及網絡犯罪分子更有機可乘。

如上一段所述，自新型冠狀病毒疫情以來，香港的金融服務機構因應時勢採用更先進的遙距線上商業模式。這在投資產品銷售範疇令人關注。傳統上，開戶、反洗錢調查、適合性評估以及客戶保障工作都涉及當面接觸，而這一定程度上亦有助防範網絡風險。包括證監會、金融管理局（金管局）及保險業監管局（保監局）在內的香港金融監管機構均意識到新型冠狀病毒對其監管對象構成極大壓力，在近年因應金融科技及網上銷售平台的出現而引入相關措施的基礎上，進一步容許金融機構以更靈活方式使用遙距/線上解決方案。[38] 雖然相關措施有助金融業從業員在家工作，維持業界營運，但同時亦令金融機構及其員工面對更大的網絡風險。鑑於遙距辦公的安排日益普遍，證監會在2020年4月29日的通告中明確指出網絡保安風險管理的重要性，並提醒持牌法團「*評估其操作能力，及實施適當的措施以管理與遙距工作安排相關的網絡保安風險*」。[39]

瞬息萬變的網絡環境對金融中心而言確實是一大挑戰，既要確保網絡安全，又要避免預防（或監管）措施窒礙市場進一步發展而適得其反。在保障網絡安全的同時亦要維持良好營商環境，這是一場舉步維艱的硬仗。香港需要與時並進，制訂清晰的網絡安全政策方向。

---

[33] 世界經濟論壇，人工智能改變網絡攻擊的三個方式 (“3 ways AI will change the nature of cyber attacks”)，2019年6月。
[34] 世界經濟論壇，了解影響全域的網絡風險 (“Understanding Systemic Cyber Risk”)，2016年10月。
[35] 同上。
[36] 同上。
[37] 科技亦可納入金融服務的其他環節，例如「了解您的客戶」（KYC）流程。金發局正就相關議題進行研究。
[38] 香港保險業監管局，《有關延長第二階段臨時便利措施以應對2019冠狀病毒疫情的通函》（只備英文版本），2020年2月、3月及6月（容許個別類型保單採取非親身銷售方式）；香港金融管理局，通告——《新型冠狀病毒疫症與打擊清洗黑錢及恐怖分子資金籌集措施》（暫時只備英文版本），2020年4月（鼓勵充分利用可靠技術作數碼化開戶）；及香港證券及期貨事務監察委員會，通函—《有關在新冠疫情下順延監管要求的實施期限及提醒業界注意記錄交易指示規定》，2020年3月，（可選用替代方案來收取和記錄交易指示）。
[39] 香港證券及期貨事務監察委員會，通函—《與遙距工作安排相關的網絡保安風險管理》，2020年4月。

香港的網絡風險防禦：有危亦有機

建立穩健網絡安全架構的價值主張不單旨在發揮防禦（或保護）作用，亦可以作為金融服務業開拓商機的基礎。

網絡保險市場的發展良機處處。全球網絡保險市場迅速擴張，按年增長率約為20%-25%。[40] 2019年，網絡安全保險市場規模為73.6億美元；而到2025年，預計將達270億美元。[41] 常規的網絡保險產品（例如承保資料外洩、勒索、網絡罪案及詐騙等的保險）主要側重於保護數碼資產免受網絡風險造成的損失，而未來的網絡保險市場可能會擴展至承保無形資產（如加密貨幣及其他數碼資產）的網絡風險。[42]

全球對網絡保險的需求正在增長，但購買情況不一。現時最大的網絡保險市場在美國，而提供相關服務的保險公司亦大多位於美國。[43] 根據一家專項風險保險公司於今年4月所作的調查顯示，三分之一的受訪美國公司擁有獨立的網絡保險。[44] 同時，歐洲的相關業務亦有增加：例如總部位於德國的兩家知名保險公司於2021年3月宣布，與一家主要的雲端服務提供商合作，將其特定的雲端保安專業知識與風險轉移專業知識相結合。香港亦有類似需求。單在2018年，香港發生超過7800宗網絡罪案，造成超過27億港元的財務損失。[45] 有大型保險公司所做的另一項調查顯示，2019年香港有76%的中小企發生網絡事故，其中約三分之一的公司在事發後並未採取進一步行動。有見及此，幾家在港的國際保險公司正發展相關業務，為此類保障不足的客戶提供服務，希望更好地為客戶衡量、減輕及轉移日益增加的網絡相關風險。[46,47]

對網絡安全公司的風險資本投資以及併購活動亦有增加。風險資本投資者愈來愈意識到網絡安全產品及應用可以帶來的商業潛力，例如透過機器學習開發安全解決方案以提升客戶體驗。他們亦不斷發掘網絡安全業務的廣度及深度。畢馬威的數據顯示，2018年，網絡安全公司獲得總計64億美元的風險投資。[48] 截至第三季，2019年內對網絡安全公司的風險投資共有388宗交易，總投資額達58億美元。[49] 大部分交易目標來自以色列及歐洲。此外，併購已成為眾多網絡安全初創企業普遍選擇的退市策略。例如，於2019年第三季，總部位於美國的網絡安全公司Palo Alto Networks收購了容器保安公司Twistlock，以擴展其雲端保安業務。[50]

為應對日益嚴峻的網絡風險，同時發掘網絡安全範疇的潛在商機，香港應致力不斷改進及完善其網絡安全架構。

為甚麼網絡安全與香港金融機構息息相關

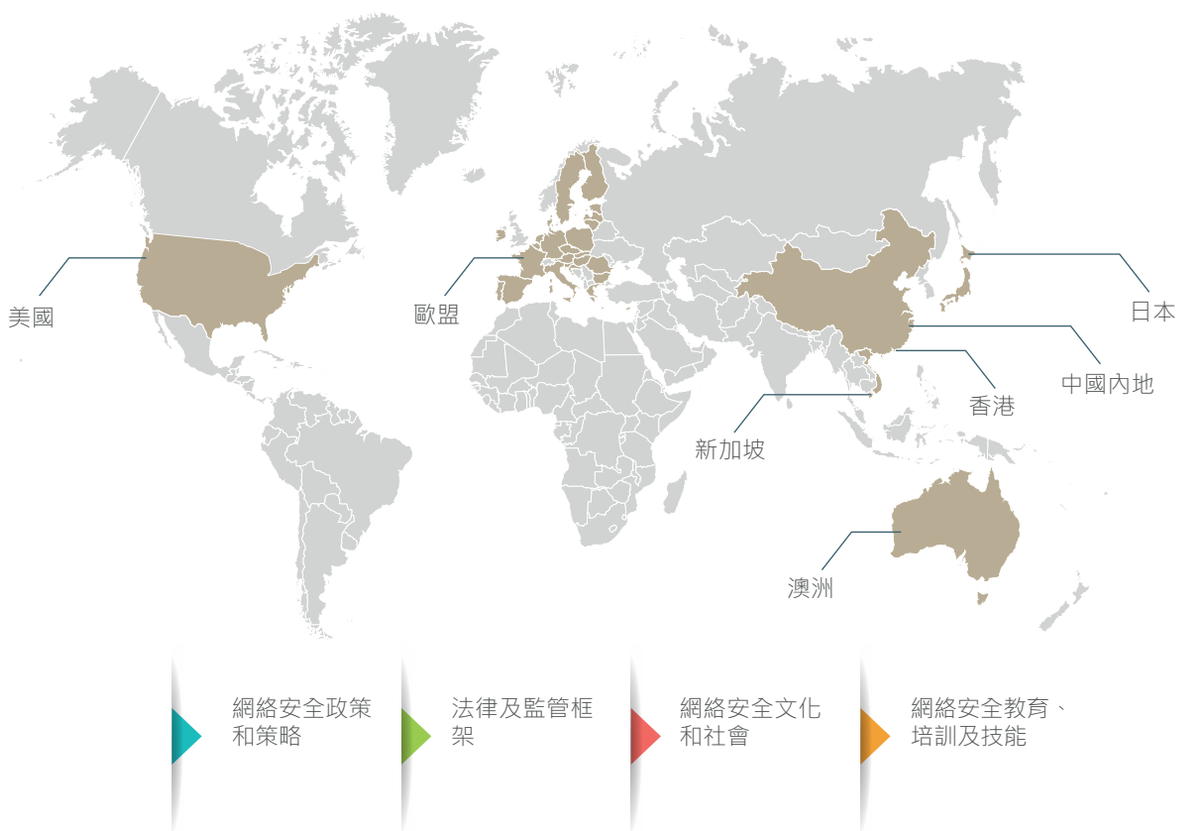
資料來源：弗若斯特沙利文(Frost & Sullivan)、微軟(Microsoft)、香港生產力促進局(Hong Kong Productivity Council)、香港電腦保安事故協調中心(HKCERT)、世界經濟論壇(World Economic Forum)、畢馬威(KPMG)

[40] 畢馬威，把握網絡保險機遇（"Seizing the cyber insurance opportunity"），2017年7月。
[41] Sjouwerman, S. (2020). Cyberheist: The biggest financial threat facing American businesses since the meltdown of 2008. Clearwater, FL: KnowBe4.
[42] Lloyd's， Lloyd's為Coincover推展加密貨幣錢包保險服務（"Lloyd's launches new cryptocurrency wallet insurance solution for Coincover"），2020年2月。
[43] 見註腳40。
[44] 見註腳14。
[45] 見註腳25。
[46] 蘋果日報，《QBE：網絡保險查詢大增》，2019年6月。
[47] 明報，《網絡保險興起 AIG：保費年增四成 亞洲網絡攻擊風險高 市場潛力大》，2018年12月。
[48] 畢馬威，"Venture Pulse Q3 2019"，2019年10月。
[49] 同上。
[50] 同上。

香港緊跟步伐，卻非獨佔鰲頭

如上所述，網絡安全是一個棘手議題——網絡風險難以衡量或量化，特定地點的網絡防衛亦也難以衡量或量化。整體而言，雖然網絡安全範疇尚無一枝獨秀者，但可以公平地說，有些司法管轄區被視為較其他司法管轄區「相對發達」。多項研究指出[51]，澳洲、歐盟、日本、中國內地、美國及新加坡通常被視為具有先進網絡安全架構的司法管轄區。有見及此，我們以司法管轄區作為單位，對香港的網絡安全架構進行調查，並與上述五個司法管轄區逐一比較。[52]

借鑒牛津大學全球網絡安全能力中心構建的國家網絡安全能力成熟度模型，[53] 我們以司法管轄區在四個關鍵層面上的做法作出比較，包括(i) 網絡安全政策和策略；(ii) 法律和監管架構；(iii) 網絡安全文化（及社會）；以及(iv) 網絡安全教育、培訓和技能。以上述方法進行比較，並非要分出孰優孰劣，但至少可以為香港提供有用的參考，使香港在網絡安全架構方面可以拉近與其他領先司法管轄區之間的距離。



[51] 本文綜合參考不同研究，例如《經濟學人》就「數碼安全」編制的「2019年安全城市指數」。
[52] 選定司法管轄區與香港網絡安全架構的主要特徵如***附件***所示。
[53] 這是一個「首創」模型，用於檢視五個關鍵層面的網絡安全能力成熟度，以便各國政府能夠「自我評估，作基準比較，更好地規劃投資及國家網絡安全策略，並制訂能力發展的優先重點」。

網絡安全政策及策略

其他市場網絡安全架構的共同特徵是專為網絡安全制訂統一的策略或政策方向；**而在香港，網絡安全政策方向是融入更為廣泛的「智慧城市藍圖」之中。**作為智慧城市基建的一部分，政府的願景是加強網絡安全能力，以「應對新的保安風險，並促進各持份者之間的協作，提高社會對網絡安全的認知及應變能力」。為此，政府定期發佈有關網絡安全的政策及指引，培養和吸引網絡安全人才，並參與全球及地區性的網絡安全組織以加強資訊交流。香港採取多方參與策略去增強自身網絡防衛。換言之，與網絡安全相關的工作或職責由各政府部門及機構負責。

相比之下，調查所及的部分司法管轄區選擇專門就網絡安全相關事務制訂統一策略。例如，歐盟於2020年12月更新其網絡戰略，闡述在諸如提高關鍵公共和私營部門網絡防衛及增強營運能力以減少網絡犯罪（包括建立新的聯合網絡加強歐盟及其成員國之間的合作）等優先範疇下的各種策略。同樣，緊接美國國家網絡戰略（建基於歷屆政府的早期網絡安全計劃）於2018年完成更新，並且在經歷史無前例的SolarWinds網絡攻擊後，美國新一屆政府班子在上任後迅速規劃其網絡戰略，以達到「將網絡安全視為重中之重，以增強我們在網絡空間中的能力，戰備狀態和應變能力」。[54] 而澳洲政府亦於2020年更新其網絡安全戰略，以取代早期的2016年版本。修訂後的戰略比之前更著重威懾和安全，並計劃在10年內投資合共16.7億澳元以增強網絡防衛和安全。新加坡也在2020年宣布《更安全網路空間總體規劃》(Safer Cyberspace Masterplan)。該規劃以2016年的網絡安全戰略為基礎，並集中保障核心數字基礎設施和保障市民的網絡空間活動。

法律及監管架構——金融業特定情況

在整體網絡安全立法方面，相較於其他司法管轄區，**香港並無單獨的網絡安全法例或獨立的執法機構**，而只有適用於網絡或電腦事故的若干條例。各個行業的監管機構，尤其是金融業監管機構（例如金管局、保監局及證監會），已就相關行業引入網絡安全規例及其他措施，惟其監管方式有較為溫和及著重微觀。 此外，香港有《個人資料（私隱）條例》提供的個人資料私隱及保護架構。

歐盟、日本、中國內地及新加坡都有獨立的網絡安全或網絡空間保護立法（作為制訂其他規例或措施的綜合法例）以及專為金融業而設的規例/指引。除了單獨的網絡安全法規外，這些司法管轄區大多數還設有資料私隱及保護的法例。特別是，歐洲和新加坡的法定框架規定了在數據隱私/數據保護權利受到重大侵犯的情況下（例如由大規模黑客事件所導致），企業必須作出強制性違規通知。

[54] 美國白宮，臨時國家安全戰略方針，2021年3月。

就金融業而言，**香港金融業有關網絡安全/網絡空間保護的規例及指引是與特定行業相關。各個監管機構往往會為各自權限下的認可金融機構制訂相關規例/指引。**部分主要規例/指引包括：

- 證監會《降低及紓減與互聯網交易相關的黑客入侵風險指引》鼓勵透過雙重認證程序、監察機制[55]、即時客戶通知、數據加密及嚴格的密碼政策，[56] 保護客戶的互聯網交易帳戶；就新型冠狀病毒，證監會於2020年4月發佈通函，提醒持牌法團須評估其操作能力，及實施適當的措施以管理與遙距工作安排相關的網絡保安風險；[57]

- 金管局制訂「網絡防衛計劃」（CFI），其中包括：(i) 網絡防衛評估框架（C-RAF）（由兩部分組成的自我評估，以及以風險資訊主導的網絡攻防模擬測試（iCAST），有助認可機構評估其網絡防衛）；(ii) 專業培訓計劃（PDP）（為網絡安全專業人士而設的認證及培訓計劃）；及 (iii) 網絡風險資訊共享平台（CISP）；[58,59] 以及

- 保監局《獲授權保險人的公司管治指引》（第7.17條）要求獲授權保險人識別來自網絡、電郵及相關裝置的網絡安全威脅，[60] 其《網絡安全指引》則訂明獲授權保險人在網絡安全方面應達到的最低標準。[61]

內地的做法與香港類似。中國證券監督管理委員會、中國銀行保險監督管理委員會以及其他機構都有各自的網絡安全規例及指引。

相比之下，其他司法管轄區設有超級監管機構，就金融業的網絡安全規例較為整全。例如，適用於新加坡金融機構的主要網絡安全規例是新加坡金融管理局制訂的《科技風險管理指導原則》(已於2021年1月進行更新以反映快速變化的網絡威脅情況) 以及相關的通函和通知。日本在這方面的規例和指引主要由金融廳制訂。

---

[55] 香港證券及期貨事務監察委員會，《降低及紓減與互聯網交易相關的黑客入侵風險指引》，2017年10月。

[56] 香港證券及期貨事務監察委員會，《致所有持牌法團的通函 勒索軟件威脅警報》，2017年5月。
證券及期貨事務監察委員會，《致從事互聯網交易的IT風險管理和網絡安全良好行業規範的持牌公司的通函》，2017年10月。

[57] 香港證券及期貨事務監察委員會，《致持牌法團的通函 與遙距工作安排相關的網絡保安風險管理》，2020年4月。

[58] 金管局於2016年推出網絡防衛計劃（CFI），以提升香港銀行系統的網絡防衛。金管局近日完成對CFI的檢討，並於2020年11月推出增強版本（CFI 2.0）。重大改進包括在網絡防衛評估框架（C-RAF）中納入國際上有關網絡事件應對及復原的最新穩健手法，並擴展專業培訓計劃（PDP）之下的認證清單，將主要海外司法管轄區的同等資歷納入其中。

[59] 香港金融管理局除引入CFI外，亦於2016年12月推出「銀行專業資歷架構——網絡安全」（於2019年1月修訂），以推動人才培養，促進網絡安全從業人員的專業水平及能力建設。金管局於2017年10月向認可機構的行政總裁發出通函，促請他們採納證監會《降低及紓減與互聯網交易相關的黑客入侵風險指引》。此外，金管局透過現場審查、非現場審查及審慎監管會議，對認可機構的資訊系統進行監管。 金管局採用風險為本的合規監督方法，因應機構的不同風險取向，就其基準及檢討週期作出不同要求。

[60] 香港保險業監管局，《獲授權保險人的公司管治指引》，2016年10月。

[61] 香港保險業監督局，《網絡安全指引》，2019年6月。
未能遵從相關指引本身不會令獲授權保險人在任何司法或其他法律程序中被起訴。然而，在根據《保險業條例》於法院進行的任何法律程序中，有關守則及指引可獲接納為證據。保監局在採取紀律行動時亦會考慮相關守則及指引。

網絡安全文化

人為錯誤是造成網絡安全事件的主要原因之一，因此，培養個人及企業的網絡安全意識已成為日益關注的範疇。如以上幾段所述，**香港商界對網絡事故的應變能力正在提升，但各個行業的應變能力仍然不均衡**。為鼓勵各機構改善網絡安全防禦能力，創新及科技局（創科局）自2016年11月起推出科技券計劃，資助各類規模的企業制訂網絡安全措施（須滿足特定條件）。[62] 該計劃更側重於技術服務及解決方案的層面，而非個人用戶/從業人員。為培養網絡安全合作的意識，香港政府推出網絡安全資訊共享夥伴計劃（Cybersec Infohub），讓不同行業及企業可以共享網絡安全資訊。[63] 就更廣泛的個人資料處理而言，香港公眾作為資料當事人，在提升網絡安全意識方面的參與度相對較低。

文化的培養需要時間，而歐洲在此方面一直處於領先地位，自1998年起便實施數據保護的法例。根據2016年生效的《通用數據保障條例》（GDPR），歐盟的數據主體在處理個人資料方面享有一系列權利，包括訪問、更正、刪除及拒絕他人處理個人資料的權利。[64] 歐盟的數據主體行使GDPR提供的上述數據保障權利的步伐較快。[65] 例如，有航空公司因安全違規行為造成的非重大損毀而在英國法院面對5億英鎊的集體訴訟。[66] 此外，英國資訊專員辦公室宣布，有意對違反GDPR規定洩露資料的一家酒店集團及一家航空公司 處以罰款。[67,68]

美國則另闢蹊徑，例如透過紐約於2017年啟動名為「Cyber NYC」的一億美元公私營投資計劃，旨在將紐約變成網絡安全之都——培養未來的網絡人才並催谷新的十億美元規模企業。

至於澳洲，2018年的行政總裁調查指出，有89%的澳洲受訪者表示擔心網絡威脅（上一年度為80%）；不過只有44%的受訪者表示正加大對網絡安全保護的投入，以建立與客戶的互信。[69]

[62] 局方亦與香港互聯網註冊管理有限公司合作，為中小企提供免費網站掃描服務。局方設立網絡安全資訊共享協作平台，讓不同機構共享網絡安全資訊。相關鼓勵措施亦包括由香港電腦保安事故協調中心提供24小時免費熱線服務，記錄各機構舉報的網絡安全事故並提供應對建議。

[63] Cybersec Infohub是一項跨行業的公私營合作夥伴計劃，旨在推動本地各行業的資訊保安持份者更緊密的協作，共享網絡安全資訊，攜手防禦網絡攻擊。截至2021年1月，已有來自多個行業超過360個機構參與計劃。

[64] 另外，香港的《個人資料（私隱）條例》訂明要求查閱個人資料及要求更正個人資料的權利。

[65] The Law Reviews, "The Privacy, Data Protection and Cybersecurity Law Review (Edition 6) - European Union Overview", 2019年10月。

[66] 同上。

[67] 英國資訊專員辦公室，聲明：擬向Marriot就其違反GDPR外洩個人資料事故罰款多於9900萬英鎊("Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach")，2019年7月。

[68] 英國廣播公司（BBC），英航因資料外洩面臨1億8300萬英鎊罰款 ("British Airways faces record £183m fine for data breach")，2019年7月。

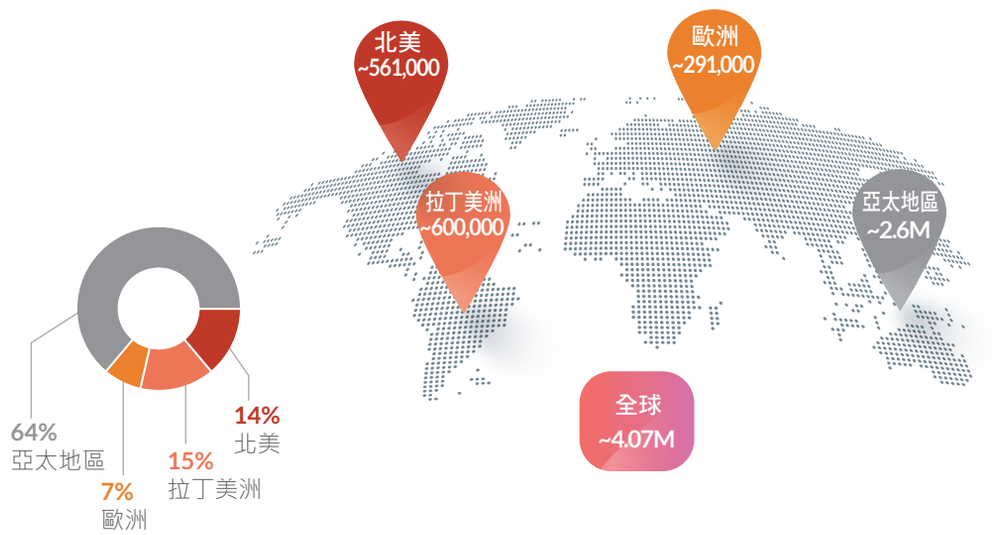
[69] 普華永道，澳洲企業的網絡關注度 ("Infographic: How cyber aware is Australian business?")，2018年3月。

網絡安全教育、培訓及技能

長期以來，網絡人才一直短缺。根據一個名為（ISC）2的國際資訊系統安全認證聯盟的數據，全球網絡安全專業人員的缺口接近430萬，而網絡安全就業人口需要大幅增長145%才能應對激增的需求。[70] 在機構層面，約65%的受訪機構表示存在網絡安全人員短缺的問題。至於地區層面，亞太地區的人才短缺最為嚴重，缺口約為260萬（見圖D）。**2018年香港的資訊科技僱員達98,780人，但當中只有1.2%專門從事資訊科技保安工作。**[71]

圖D

不同地區的網絡安全人才缺口



資料來源：網絡安全勞動人口調查2019, (ISC)²

歐洲的人才缺口相對較小，原因有多方面。正如有網絡安全專家指出，歐洲各國的國防訓練已非常重視網絡安全，一定程度上有助這些國家培養持續不斷的網絡安全專業人才。此外，歐洲的網絡安全教育及培訓策略架構清晰、條理分明，故頗具成效。歐盟網絡安全局（ENISA）是歐盟專門負責網絡安全的機構，透過多項措施提升網絡安全意識及提供相關培訓，包括編制有關網絡安全培訓的材料，以及訂立歐洲網路安全技能架構以改善私人機構的網絡安全文化。為提升從業人員的能力，歐洲已制定多項網絡安全認證計劃，旨在提供一套全面的規範、技術要求及標準，以評估計劃參與者的知識水平。

相比之下，亞洲推行網絡安全相關能力建設計劃的時間較短。

在香港，政府支持的網絡安全資訊站及Cybersechub.hk是主要的網絡安全工具。前者為中小企及其他一般用戶提供意見及循序漸進的指引，就電腦、流動通訊設備及網站進行安全檢測，並學習在防禦網絡攻擊方面的相關貼士及技巧；[72] 而後者是不同行業及企業共享網絡安全資訊的平台。[73] 政府及私營機構定期舉辦研討會及工作坊，並推行其他措施，以提升商界及公眾對網絡安全的認識。[74]

---

[70] （ISC）²，網絡安全勞動人口調查2019（"Cybersecurity Workforce Study 2019"），2019年11月。另外，各個市場已就人才短缺問題展開研究及評估。根據美國政府參與的國家網絡安全教育計劃所支持的CyberSeek計劃指出，在截至2018年8月止12個月內，美國有超過30萬個網絡安全職位空缺。另一方面，英國政府於2020年3月發表研究報告，指出在2016年9月至2019年8月三年內，英國共發佈近40萬個與網絡安全相關的職位空缺。

[71] 香港立法會，《培育網絡保安人才》（ISE15/20-21），2021年1月22日。

[72] 香港網絡安全資訊站，關於我們，最後更新於2020年9月。

[73] Cybersec Infohub，關於我們，最後更新於2019年11月。

[74] 除了透過研討會及工作坊鼓勵及支持業界舉辦資訊安全培訓外，政府亦與專業團體合作，在資訊科技從業人員中推廣資訊安全專業認證，並鼓勵專上教育機構在相關學科提供更多資訊安全課程。

儘管如此，**香港並無專門提供網絡安全培訓的教育機構**，相較於其他司法管轄區有進步空間。例如，澳洲於2016年成立了網絡安全卓越學術中心（Academic Centres of Cyber Security Excellence），鼓勵更多學生學習網絡安全及相關課程，藉此解決全國高技能網絡安全專業人員短缺的問題；[75] 中國內地計劃到2027年開辦4-6所網絡安全學院；[76] 而新加坡已設立網絡安全技術及夥伴計劃（Cyber Seucirty Associates and Technologists Programme），以培訓初級及中級ICT專業人員並提升其技能，填補網絡安全職位空缺。[77]

香港現時就特定行業的培訓較為零散。**從積極的方面看，「銀行專業資歷架構——網絡安全」對銀行業而言是良好開端。**由金管局及業界其他持份者開發的架構有助從事網絡安全職責的銀行業員工提升專業能力。銀行可以參考金管局的指引，包括當中詳列的資歷架構、認可證書及持續專業發展要求，使相關員工具備適切的技能、知識及行為。[78] 至於其他金融行業（例如證券業及保險業），機構可參考各類網絡安全工作坊，例如由證監會、香港警務處及香港電腦保安事故協調中心合辦的網絡保安工作坊，從宏觀層面了解關鍵議題（例如網絡罪案預防小貼士）。由於這些行業並無金管局的同類指引，很大程度上倚賴金融機構或員工主動參加相關培訓以實現高水平的能力監管要求。

在專上教育及持續教育方面，香港在亞洲區內較早將網絡安全的職業訓練元素納入大學課程（例如推出網絡安全理學碩士）。不過，金發局跟資深網絡安全從業人員的訪談獲悉，有能力聘用網絡安全人員的企業更青睞資深員工而非應屆畢業生。另一方面，小企業往往將資訊技術及網絡安全混為一談，認為兩者並無差異，由此進一步收窄網絡安全專業人士的就業市場。[79] 鑑於上述因素，網絡安全範疇的應屆畢業生缺乏入行機會，通常會考慮轉行。

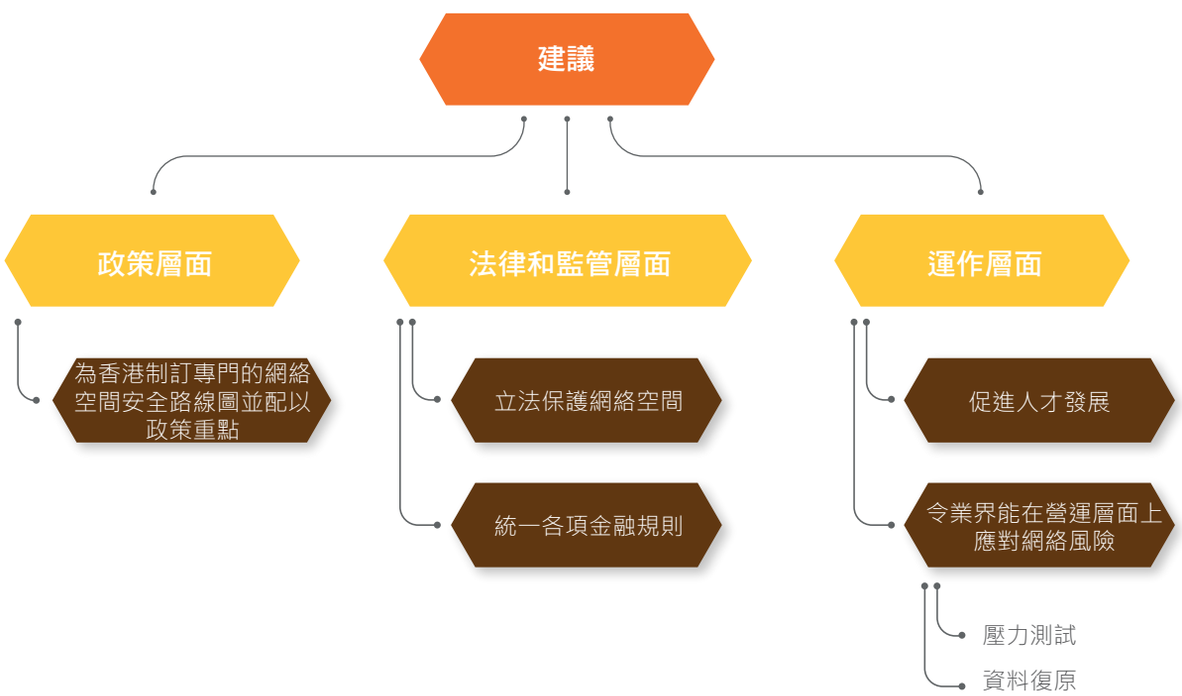
在吸引非本地人才方面，政府的「科技人才入境計劃」透過快速處理安排，為合資格科技公司／機構輸入海外和內地科技人才（包括網絡安全人才）來港進行科技研發工作。此外，政府的《香港人才清單》包括資深網絡安全專才。符合「人才清單」要求的合資格申請人可以透過「優秀人才入境計劃」獲得入境便利計劃的合資格人士在來港前無須事先在港獲得聘用，並可攜同受養人來港定居。

[75] 澳洲網絡安全卓越學術中心（ACCSE），"Program Guidelines"，最後更新於2017年5月。
ACCSE計劃嘉許具備在網絡安全方面具備高水平教育、培訓及研究能力，並與政府和商界緊密聯繫的澳洲大學。
[76] 中華人民共和國教育部，《關於印發<一流網絡安全學院建設示範項目管理辦法>的通知》，2018年8月。
[77] 新加坡網絡安全局，"Cyber Security Associates and Technologists Programme"，最後更新於2020年5月。
[78] 香港金融管理局，"Guide to Enhanced Competency Framework on Cybersecurity"，最後更新於2019年1月。(只供英文)
[79] 根據資深從業人員所講，資訊科技專業人員與網絡安全專業人員所具備的技能組合完全不同——前者擅長「構建」 資訊科技基建，而後者擅長剖析各個組成部分以識別錯誤及潛在風險。

建議

鑑於香港的網絡安全風險以及其他主要司法管轄區的做法，我們提出建議，相信有助增強香港的網絡安全能力，使香港在全球競爭中脫穎而出。作為相關目標的核心，香港需要就網絡安全提出更具策略性的觀點，以反映本地整體需求及其作為領先國際金融中心的地位。

相關建議涉及三個宏觀「層面」：(i) 政策層面；(ii) 法律和監管層面；及(iii) 運作層面。三個層面並非要按次序實施，個別建議所需的推行時間可能較其他建議為長。



政策層面

(1) 為香港制訂專門的網絡空間安全路線圖並配以政策重點

將網絡安全元素納入整體智慧城市藍圖對香港而言是良好開端，有助推動相關政策制定及提升整體網絡安全能力。然而，隨著全球範圍內的網絡威脅持續快速增加，除現時每年更新工作計劃外，香港可能亦需要根據專門的路線圖，以更明確的方式制訂短期、中期及長期的優先事項及可行項目。

現有的公開文件介紹政府已推行的網絡安全措施，但並未詳述政府在該範疇的計劃。例如，我們知道政府及其機構舉辦許多研討會和工作坊，以提升從業人員和社區的能力，然而，市民或業界可能亦有興趣了解香港計劃如何在網絡安全生態系統中擴展優勢，並加強國際對香港完善網絡安全基建的信心。政府在現行的網絡安全工作措施以外，或需讓市場及公眾更了解相關措施，以便他們能因應相關行動而準備並回應。

其他司法管轄區通常會在國家/城市層面制訂系統化的網絡安全策略，訂明一系列內的可行項目，例如在一定時限內引入新法例以加強網絡空間安全管治；承諾將一定比例的政府開支用於網絡安全，以加強政府系統保安。截至目前為止，此類策略在香港公共範疇並不多見，至少在金融服務業鮮有聽聞。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。

除政策重點外，在機構/部門層面作出更明確的授權亦會有所幫助。我們明白網絡空間安全是跨部門議題，涉及多個政府部門或機構，但如果有統籌負責的管治機構及清晰明確的問責機制，相關工作應能更見成效，更為全面。就建議設立的統籌負責的管治機構，可行的方案包括：(i) 設立一個獨立委員會（類似於澳洲信號局(Australian Signals Directorate)[80]或新加坡網絡安全局(cyber Security Agency of Singapore)）；[81] 或 (ii) 設立一個跨局/跨部門的工作小組，統籌監管及執法行動。設立相關機構後，與網絡安全相關的所有工作——包括本地能力建設、基建檢討及國際合作——都可以由單一機構負責。

金融服務業作為香港經濟的主要支柱之一，應在促進制定關鍵政策重點及推動持續公私營合作方面發揮關鍵作用。

[80] 屬法定機構，履行澳洲政府的網絡安全職能。
[81] 屬新加坡總理辦公室轄下機構，由通訊及新聞部管理，負責監察新加坡的網絡安全策略、運作、教育等。

(2) 立法保護網絡空間

如本文所述，在網絡安全範疇領先的多個司法管轄區都設有綜合網絡安全/網絡空間保護法例作為網絡安全架構的核心要素。除了為香港市民及企業提供更明確的法律依據及保障外，全面的網絡空間保護法規亦會就跨境資料處理及傳輸提供清晰資訊。

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。

相關立法可與前文提及的網絡安全路線圖的有效運作同步進行。

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，當中包括涵蓋網絡相關罪案的條例以及涉及其他相關範疇（例如個人資料保障）的立法。

(3) 統一各項金融規例

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。

香港的金融機構通常由相關金融監管機構監管，獲發牌/授權在特定行業從事某類商業活動。此類體制架構的優點是因應特定行業的需求及情況制訂規則及規例，但不同行業對金融規例的不同，或會令市場感到困惑，從而影響香港營商環境。

就網絡安全而言，香港已制訂多項監管指引。如上文所述，金管局、保監局及證監會各有相關指引/通告，協助其監管的持牌/認可機構處理網絡安全問題。各監管機構之間存在協調。舉例而言，金管局於2017年向註冊機構的行政總裁發出通告，要求他們採用證監會《降低及紓減與互聯網交易相關的黑客入侵風險指引》，但令人意外的是進一步的協調政策應對工作仍未展開。

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。現時，證監會要求持牌機構在發生任何重大的網絡保安事故（包括勒索軟件攻擊）時立即向證監會匯報；[82] 保監局則要求保險公司於發生相關事件後「在切實可行範圍內盡快」匯報事件，而且在任何情況下「須在偵測到該事件後的72小時之內」匯報。[83] 雖然各監管機構因應金融服務行業的獨特業務營運及性質採取不同的監管方法具其優勝之處，但部分市場參與者（尤其是直接從事網絡安全工作的人員）表示，單一匯報時間可以減輕金融市場參與者應對多個監管機構的合規負擔。

統一整個金融業網絡安全的監管系統需要各個監管機構共同努力。跨機構督導小組是實現協調的一種有效方法，近期的例子是2020年5月成立的綠色和可持續金融跨機構督導小組，[84] 職責包括協調政策方向，確保香港具備周密全面的綠色和可持續金融策略。如在網絡安全範疇推行類似做法，我們期望相關督導小組至少包括證監會、金管局及保監局。

---

[82] 見註腳54。
[83] 見註腳59。
[84] 該督導小組由金管局及證監會發起；其他成員為環境局、財庫局、港交所、保監局及強制性公積金計劃管理局。

運作層面

(4) 促進人才發展

人才短缺已被視為至關重要的問題，這個問題在亞洲尤其嚴重。從其他市場（例如歐洲）引入人才來解決人才短缺問題是快捷但成本高昂的方法。不過，如前文所述，只有最大型的金融機構才能負擔其高昂的開支。這在某種程度上解釋為何銀行業能擁有比其他行業更高水平的網絡安全能力。

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。因此，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（包括特定行業要求及共同要求），例如首先訂立一系列建議/核准網絡安全認證計劃，讓不同金融行業僱員參與其中，這將會是個好的開始。

由於網絡安全無法直接創造收益，金融機構（尤其是規模較小的公司）可能仍然不願意投放大量資源提升網絡防衛。解決這個問題的方法之一是由香港特區政府提供誘因，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。具體而言，政府可以推行專才資助計劃。政府最近於2020年7月1日為金融科技專才推出類似資助計劃，作為抗疫基金金融科技人才計劃的一部分，鼓勵金融企業在未來12個月開設1,000相關職位。金融企業每聘請一名全職的金融科技專才，就可獲得每月10,000港元的薪酬資助， 為期一年，資助總額達1.2億港元。[85]

較長遠而言，香港可參考其他司法管轄區（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，這個方案需要政府作更深入的可行性研究。

[85] 南華早報， 香港推出1550萬美元資助鼓勵公司增聘1000名金融科技專才(“Hong Kong launches US$15.5 million subsidy plan to encourage companies to hire 1,000 fintech professionals”)，2020年7月。

(5) 業界在營運層面上應對網絡風險的能力

壓力測試

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。

在香港，網絡風險壓力測試的工作一直各自為政，且集中在銀行業。政府資訊科技總監辦公室、香港警務處網絡安全及科技罪案調查科（網罪科）和香港電腦保安事故協調中心一直與不同的持份者緊密合作進行網絡事故演習。舉例而言，在虛擬銀行於2019年11月投入運作之前，網罪科為該等銀行提供網絡安全演習，以提升虛擬銀行對安全攻擊的應變能力及準備。金管局亦推出網絡防衛評估框架(C-RAF)（兩部分組成的自我評估）及以風險資訊主導的網絡攻防模擬測試 (iCAST)，協助銀行機構評估其網絡防衛狀況。在業界主導層面，網絡危機模擬演習(例如行業模擬演習 (Whole Industry Simulation Exercise (WISE))) 為年度活動。最近一次的WISE演習於2019年10月舉行，吸引在港經營的銀行、證券公司、資產管理公司及結算所的代表參加。在監管機構的支援下，[86] 來自40多個金融機構的危機管理團隊參加四小時的模擬演習，其中模擬情景每5至10分鐘轉換一次。[87] 同時參與iCAST及和WISE的銀行都認為兩項演習有助他們評估其網絡防衛能力。他們指出，監管主導及業界主導的計劃各有價值，前者 (iCAST) 受惠於有較為廣泛的業界參與，而後者(WISE) 透過機構特定的機密報告提供寶貴意見，協助銀行在監管審核前，主動識別潛在的弱項。

然而，僅以數個金融行業為重點的壓力測試並不足以體現香港的金融中心地位。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。此外，我們亦期望金管局、證監會及保監局通力合作，例如在財庫局引導下優先制訂相關壓力測試。

相關實例可參考美國的漢密爾頓系列 (Hamilton Series) 演習。該系列演習由美國財政部帶領，模擬針對金融服務業的各類型網絡攻擊，包括對行業各種業務的攻擊（例如股票市場、支付系統及交易所）。測試結果用於改善公私營機構的政策、程序及協調工作。

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（以確保更大參與度），或者鼓勵金融機構籌劃及進行行業演習（例如資助舉行壓力測試的開支）。後者的優點在於金融機構可以在毋須顧慮監管審查的環境下進行演習，但鑒於業界面對的網絡風險性質嚴重，我們建議進行監管機構主導的演習。為保留靈活性，可以採用「基準方法」，（根據iCAST和WISE所述，）當中僅涵蓋關鍵任務系統及互相聯繫的範疇，使各金融監管機構可以因應各自運作考慮因素而作出應急籌劃。

資料復原

香港金融業需要考慮的一個關鍵問題是業界是否已建立適當的網絡事件應對機制，包括有效而全面的資料復原計劃。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。

香港金融業參與者應參考的一個例子是美國的「避風港」(Sheltered Harbour) 計劃。在金融業的推動下，該項計劃允許在發生網絡事件時恢復客戶賬戶資料。參與「避風港」的機構可以直接儲存資料或委託第三方儲存資料。當網絡事件發生，已存儲的資料將透過業界建立的標準統一檔案格式進行驗證、格式化、加密及傳輸，相關資料可以在一周內復原並讓受影響的參與機構存取。避風港的優點在於為金融機構提供多一重保障，而許多市場（包括香港）都缺乏此類保障。英倫銀行最近發表的《金融未來》報告大篇幅提及有關計劃，[88] 表示英國可能考慮採用類似做法。

---

[86] 金管局在演習過程中就演習情景提出意見，並與參與演習的數家銀行互動，就處理情景練習與銀行的溝通及合作；與此同時，證監會代表以監管及業界支援兼觀察員的身份參加演習。

[87] 路透社，香港銀行以疫情場景進行壓力測試 (“Hong Kong banks compare pandemic stress test with epidemic reality”)，2020年2月。

[88] 英倫銀行，金融未來 (“The future of finance report”)，2019年6月。

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。金融服務業是網絡犯罪分子的主要目標。

作為國際金融中心的香港面對愈來愈多網絡罪案。相應地，金融機構防止、應對及處理網絡風險的應變能力已普遍提升。

隨著後疫情時代的發展 – 包括持牌虛擬金融服務的興起，以及對雲端服務及網上協作工具等的依賴 – 未來的網絡世界只會變得更加複雜，而應對網絡風險的需要也更加迫切。對香港乃至世界其他地區而言，網絡攻擊與應變處理之間的攻防戰將會變得愈來愈激烈。

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。本文根據澳洲、歐盟、日本、中國內地、新加坡及美國採取的不同做法提出一系列建議，香港可加以借鑒，以加強網絡安全架構：

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：

- 加強人才培養；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。

基於需要呈現、應對並處理網絡危機的急切狀況，可同步實施以上建議。我們相信，這些政策建議會為香港帶來更有效、應對網絡風險能力更強的網絡安全基建。然而，提升香港網絡安全水平的措施最終能否成功，亦有賴公私營機構的充分參與及合作。因此，我們鼓勵各方提供意見和合作。

附件——各司法管轄區網絡安全架構調查

層面——網絡安全政策及策略

香港	澳洲	歐盟	日本	中國內地	新加坡	美國
雖然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」。政府也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)以及政府資助的其他機構，以防禦及應對網絡威脅及事故。 資科辦已制訂及維持全面的資訊科技保安政策、標準、指引、程序及有關的實務指引，供政府部門使用。相關程序及指引是根據國際標準、業界最佳常規及專業資源而制訂。 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。	澳洲政府於2020年8月6日啟動《2020年網絡安全策略》(策略2020)（Australia's Cyber Security Strategy 2020），取代《澳洲網絡安全策略2016》(策略2016)（Australia's 2016 Cyber Security Strategy）。在執法、安全和阻嚇方面，由澳洲民政事務署（Department of Home Affairs）修訂的《策略2020》比《策略2016》更穩健，由時任總理製訂的《策略2016》則集中經濟機遇及創新。在《策略2020》下，澳洲政府將在未來10年投資16億7千萬澳元，目標為澳洲創造一個更安全的線上世界。 《策略2020》包括以下目標。 (i) 政府將加強國民、商業、關鍵基建的保護，免受最	歐盟網絡安全策略（首於2013年公布）詳細介紹應對以下五個優先範疇挑戰的行動，包括實現網絡防衛；大幅減少網絡罪案；制訂網絡防禦政策及能力；發展業界及科技資源；以及制訂歐盟的統一網絡空間政策。 2017年9月，歐盟更新其網絡安全策略，以進一步加強保護歐洲的主要基建，增強歐盟對世界其他地區的數碼主張。 最近，歐盟於2020年12月發佈了修訂版的《網絡安全策略》(Cybersecurity Strategy)。連同修訂版的《網絡與信息系統安全指令》(Network and Information Security Directive)的計劃及關鍵實體防衛的建議指令，此策略在法規、投資及政策	根據2014年《網絡安全基本法》於2015年成立的內閣領導網絡安全策略本部負責制訂策略，打擊網絡攻擊並減輕所造成的損害。 內閣官房信息安全中心(The National Center of Incident Readiness and Strategy for Cybersecurity)於2018年7月公布（為期三年的）國家網絡安全策略，確認日本加強網絡安全措施的需求與日俱增。其中包括，改善日本關鍵基礎設施的網絡安全以及鼓勵日本企業實行網絡安全的最佳做法。	中國內地早在2012年底開始制訂網絡安全策略。2012年12月28日，全國人民代表大會常務委員會（人大常委會）通過關於加強網絡信息保護的決定，著重保護「在業務活動中」由「網絡服務提供者」及其他實體收集、處理和使用的個人資料。 人大常委會於2016年11月7日通過《中華人民共和國網絡安全法》，該法律自2017年6月1日起施行。在《中華人民共和國網絡安全法》頒布時，國家互聯網信息辦公室（網信辦）於2016年12月發布《國家網絡空間安全策略》，確定主要任務為：捍衛網絡空間主權；保護關鍵信息基礎設施；以及提升網絡空間防護能力。 習近平主席於2014年	新加坡網絡安全局（CSA）成立於2015年，負責監察新加坡的網絡安全策略、教育和拓展以及行業發展。CSA是總理府的一部分，由通訊及新聞部管理。 CSA於2016年發布《新加坡網絡安全策略報告》，訂明新加坡在網絡安全方面的願景、目標及優先重點。新加坡的網絡安全策略旨在創建一個具防衛能力、可信賴的網絡環境，並以四大支柱作為基礎： (i) 加強新加坡主要資訊基建的防衛能力； (ii) 策動企業及社區創建更安全的網絡空間，應對網絡威脅、打擊網絡罪案及保障個人資料； (iii) 發展活躍的網絡安全生態系統，	2003年，喬治布殊政府公布美國國土安全部的國家網絡安全策略，強調公私營機構合作的作用，就改善企業、教育機構及個人的集體網絡安全提出建議。 2008年，布殊政府啟動《國家綜合網絡安全計劃》(CNCI)。CNCI計劃旨在加強網絡安全教育，在聯邦政府加強部署入侵偵測及預防系統，更妥善協調美國境內的網絡安全研究與發展。 奧巴馬總統意識到加強網絡安全政策的重要性，透過為期60日的網絡政策檢討改善和更新CNCI計劃。其中白宮國家安全委員會及國土安全委員會檢視政府活動及網絡安全計劃，最終提交一份總結報告。然後總統指示行政機構確保對日後的網絡事

香港	澳洲	歐盟	日本	中國內地	新加坡	美國
詳情請參閱層面2。	高級別的威脅； (ii) 商界將採取措施，保障其產品及服務，以及保護客人，避免已知的弱點受攻擊；及 (iii) 公眾將熟習安全的線上行為。 於2014年成立的澳洲網絡安全中心(ACSC)是負責網絡安全的主要機構。ACSC管理遍及全國的聯合網絡安全中心架構，就當前網絡安全事宜與業界、政府及學術夥伴合作。澳洲金融監理署是澳洲主要金融監管機構之一，公佈了新的2020-24年的《網絡安全策略》（Cyber Security Strategy），擬定補完《2020年網絡安全策略》的內容。詳情請參閱層面2的「金融監管」。	建議方面，訂立具體計劃： (i) 在防衛能力、科技主權及領導地位三個範疇，提升公私營行業的網絡防衛能力，以及建立歐盟安全運作中心的網絡； (ii) 培養運作能力，以防止、減少及應對網絡問題，建立全新的聯合網絡組，目標是加強歐盟及成員國的機構間的合作；及 (iii) 透過緊密合作，擴充全球和開放的網絡空間。 歐盟網絡與信息安全局 (ENISA) 是歐盟網絡安全專業知識的中心。該機構支援成員國應對大規模跨境網絡事故，並支持制訂及實施歐盟網絡安全法律和政策（包括歐洲網絡安全認證計劃）。 在2020年7月，歐盟網絡與信息安全局公佈全新的策略，勾畫		成立中央網絡安全和信息化領導小組，奉行網絡安全是國家安全的重要部分的原則。領導小組於2018年改為中央網絡安全和信息化委員會，亦稱為國家互聯網信息辦公室（網信辦）。 《中華人民共和國網絡安全法》頒布實施後，中國內地訂立更嚴謹的新法例和法規，包括不同的國家標準，去規範企業(包括在中國的外國企業子公司)設立雲端基建，包括中國境內的伺服器、虛擬化網絡、軟件及資訊系統。 《中華人民共和國數據安全法》草案於2020年7月公布，是首條相關中國法律的草案，目的是規範國家安全、企業秘密及個人資料的收集、處理、控制及儲存。 2020年10月，《個人信息保護法(草案)》公開諮詢。如草案獲得通過，將會是中華人民共和國首條既全面又達國家級別的保護個人信息法律。	其中包括熟練的技術人員、技術先進的公司及緊密的研究合作，以支持新加坡的網絡安全需求，成為新的經濟增長來源；及 (iv) 加緊建立緊密的國際夥伴關係，以應對國際網絡安全及網絡罪案問題。 此外，CSA每年發布文件，回顧新加坡的網絡生態以及年內為推動新加坡網絡安全策略四大支柱而推行的措施。最新的《新加坡網絡生態2019》於2020年6月26日發布。 2020年2月，新加坡政府宣布將於未來三年撥款10億新元，以加強政府的網絡及數據安全能力，保護公民資料及主要資訊基建系統。 2020年10月，新加坡政府宣布《2020年新加坡更安全網路空間綱要計劃》（Singapore’s Safer	故作出有組織及統一的應對、加強公私營機構合作關係，投入資金進行頂尖的研究與發展，以及提高網絡安全意識及數碼素養。奧巴馬亦設立網絡安全協調員一職。網絡安全協調員將在網絡安全政策的制訂過程中發揮核心作用，向國家安全顧問匯報，並定期與總統會面。（特朗普政府於2018年撤銷有關職位）。 奧巴馬政府亦於2015年發表《網絡安全策略及實施計劃》(CSIP)，旨在識別和縮窄網絡安全差距及新增的優先重點，以加強保護政府系統及資料。CSIP其後於2016年2月發表《網絡安全國家行動計劃》(CNAP)，包括以下措施：擬投入31億美元成立資訊技術現代化基金；設立聯邦資訊安全總監（CISO）；繼續識別及審視最大價值及風險最高的資訊科技資產，以及加強政府各部門就資訊科技及網絡安全的共享服務。奧巴馬總統

香港	澳洲	歐盟	日本	中國內地	新加坡	美國
		出該局的方向，訂立歐盟網絡安全的共同高度。該策略建基於七大策略目標，制訂歐盟網路和資訊保安局的優先次序，包括(i) 提升網絡安全生態系統的社區能力及參與度；(ii) 把網絡安全看作歐盟政策的組成部分；(iii) 在面對大型網絡事故時，促進歐盟內各運作機構的合作；(iv) 培養歐盟內網絡安全高端的能力；(v) 透過安全可靠的數碼解決方案，建立高度的信任；(vi) 洞悉未知的網絡安全挑戰；以及(vii) 高效和有效地管理歐洲的網絡安全資訊及知識。		《中華人民共和國數據安全法》及《個人信息保護法(草案)》一旦正式通過，將與《中華人民共和國網絡安全法》構成中國網絡安全和數據保護制度的全面法律架構。	Cyberspace Masterplan 2020），在《2016年新加坡網路安全策略》（2016 Singapore Cybersecurity Strategy）的基礎上，勾畫出創造新加坡更安全網絡空間的藍圖。此藍圖包括三項策略目標：(i) 確保核心的數碼基建設施、(ii) 保障網絡空間活動，以及(iii) 提升網絡新加坡的人口。	在任期內亦領導其他多項網絡安全相關政策工作，例如軍事網絡運作及國際策略。 2017年5月，特朗普政府頒布《關於加強聯邦網絡安全及主要基建的行政命令》，要求政府機構主管遵守美國國家標準技術研究所（「NIST」）有關改善重要基建網絡安全的架構（NIST網絡安全架構），管理各部門的網絡安全風險。2018年9月，白宮發表《國家網絡策略》，概述政府在相關範疇的計劃，包括保護網絡和系統、發展安全繁榮的數碼經濟，以及增強美國遏止及懲治惡意使用網絡工具的能力。 2018年11月，時任總統特朗普簽署《2018年網絡安全與基礎設施安全局法案》（Cybersecurity and Infrastructure Security Agency Act of 2018），成立網絡安全與基礎設施安全局（Cybersecurity and Infrastructure Security

香港	澳洲	歐盟	日本	中國內地	新加坡	美國
						Agency）。該獨立聯邦機構保護國家的關鍵基建設施，並將國家保護與計劃局（Department of Homeland Security's National Protection and Programs Directorate）重組為網絡安全與基礎設施安全局，並將資源及責任重新分配給此新機構。網絡安全與基礎設施安全局的目標是提升國家能力，免受網絡攻擊；與聯邦政府合作，提供網絡安全工具、事故應變服務及能力評估，保衛支撐政府部門與機構基本運作的「.gov」網絡。 2021年春天，拜登政府宣佈網絡安全與基礎設施安全局於2021年的優先工序，包括(1) 處理勒索軟件，(2) 改善國土安全部的網絡安全訓練，(3)鞏固工業控制系統的防衛能力，(4) 保衛交通系統，(5) 保障投票系統，以及(6)提升國際間網絡安全的能力。更有報導指，在科技供應商太陽風

香港	澳洲	歐盟	日本	中國內地	新加坡	美國
						（SolarWinds）被揭發違反條例，並影響多個政府機構後，拜登政府考慮簽署行政命令，要求軟件違反網絡安全的供應商必須通知聯邦政府。

層面二——法律及金融監管架構

法律架構

香港	澳洲	歐盟	日本	中國內地	新加坡	美國
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，現時並未強制要求在發生資料外洩時通知個人資料私隱專員或資料當事人。然而，2020年1月，個人資料私隱專員指出，資料外洩的強制通知很有可能在修訂《個人資料（私隱）條例》時納入當中，但尚未有時間表。	並無「綜合」的網絡安全法律。 澳洲主要透過《2001年網絡罪案法》修訂的《1995年刑法》，將網絡攻擊定為刑事罪行。 《電訊行業安全改革》（根據《2017年電訊及其他立法修正案》）適用於針對主要基建及特定行業的網絡威脅。 《1988年私隱法》規管私營機構及政府機構處理個人資訊的方式。受《1988年私隱法》規管的實體必須遵守強制性的資料外洩通報機制，並且必須依照《私隱法》附表1中所載的13項澳洲私隱原則處理及使用個人資料。 《2018年關鍵基建安全法》旨在應對外國實體實施破壞、間諜行為及威迫行為等國	《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。 《網絡與資訊系統安全指令》（NIS指令）旨在應對整個歐盟的網絡及資訊安全事故和風險。2020年12月，連同修訂版的《網絡安全策略》(Cybersecurity Strategy)，歐盟委員會採納《網絡與資訊系統安全指令》(NIS2 指令)修訂版的建議。該建議參考和廢除 NIS指令的內容，令現存的法律框架與時並進。此外，它亦要求更嚴格的安全措施和通報責任，以及成員國需為違法行為實施行政罰則，以統一制裁制度。 此外，2020年12月，歐盟宣佈有關關鍵實體防衛的建議指令(CER指令)。建議指令將提升現時歐盟條例	2014年制定《網絡安全基本法》，訂明中央與地方政府在國家整體網絡安全政策中的角色及責任。法律亦規定網絡業務及基建相關企業應採取自願措施加強網絡安全。 2018年12月，日本國會通過一項法案，修訂《2014年網絡安全基本法》，以加強網絡安全，為日本舉辦東京奧運會及殘奧會做好準備。 另有法律（例如《刑法》(Penal Code)及《非法存取禁止法》(Act on the Prohibition of Unauthorized Computer Access)）涵蓋不同類型的網絡罪行及網絡安全。 資料保障方面的主要法例是《個人資料保護法》(Act on the Protection of Personal Information)。2020年	《網絡安全法》於2017年施行，是中國首項應對網絡安全（包括相關數據保障）的全國法律。《網絡安全法》訂明網絡營運者的各項安全保障責任，並對主要資訊基建營運者的安全責任提出更高要求。該法律就舉報或通報實際或可疑的重大個人資料外洩行為訂立一般規定。 《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。 網絡罪案納入《中華人民共和國刑法》。 正如層面1所述，中國的《個人信息保護法》及《數據安全法》的立法程序已進入最後階段。	於2018年8月31日生效的《2018年網絡安全法令》（2018年第9號）是新加坡監督及維護國家網絡安全的法律架構。《網絡安全法令》建立保護主要資訊基建免受網絡安全威脅的監管架構，授權網絡安全局調查及應對網絡安全威脅和事故，並建立網絡安全資訊共享架構。 除《網絡安全法令》外，其他重要立法還包括《2012年個人資料保護法令》（2012年第26號）及《濫用電腦法令》（第50A章）。 《個人資料保護法令》由個人資料保護委員會管理，規管個人資料的收集、使用、披露及管理。具體而言，個人資料保護法令要求機構作出合理的保安安排，保護其管有或控制的個人資	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。涉及電子安全的主要聯邦法規包括： • 《1986年電子通訊私隱法案》（最新於2008年修訂）訂明在傳輸及電子儲存中獲取或使用通信的法律要求，以及違反相關要求的刑事和民事訴訟因由。 • 《電腦欺詐及濫用法案》於1986年首次頒布，最新於2008年修訂，訂明一系列網絡罪案的刑事及民事訴訟因由。 • 《1996年健康保險流通與責任法案》要求醫療保健行業中的承保醫療實體實行技術及非技術保障措施，確保個人「受保護電子健康資訊」的安全。 • 《聯邦貿易委員會

香港	澳洲	歐盟	日本	中國內地	新加坡	美國
	家安全風險。該法案實施的目的是回應與關鍵基建有關的網絡聯繫。2020年11月，政府為了符合新修訂的《網絡安全策略》，提出《2018年關鍵基建安全法》的重要修訂。建議修訂包括(i)如關係到國家利益，政府獲賦予新的權力界入網絡攻擊，並搜集有關關鍵基建實體的資料；(ii) 增加符合「重要基建」行業的定義，包括金融服務業；及(iii) 要求關鍵基建資產的持有者及營運者必須履行安全的責任。	對關鍵基建的廣度及深度，並涵蓋10個行業，包括銀行業及金融市場基建。CER指令也會訂立執法機制，以確保成員國當局有權力實地巡查關鍵基建，以及對違規行為判處罰款。 歐盟將在未來數月嘗試實施新的網絡安全策略。在成員國採納NIS2指令及CER指令前，歐盟機構將進一步審視指令內容。 《通用數據保障條例》(GDPR) 是歐盟的綜合資料保障法律，全面訂明與處理個人資料相關的一系列責任及權利。GDPR普遍被視為資料保障法例的黃金標準，當中包含嚴格的數據外洩通報要求。	6月5日，日本立法機關通過數項《個人資料保護法》的修正案，加強個人資料的保護及要求所有行業在使用個人資料時須履行新的責任。重要的是，如某些資料外洩，便有責任通報給個人資料保護委員會(Personal Information Protection Commission)，通報責任的門檻尚待決定。修正案將於2020年6月5日後的兩年內生效。		料，防止未經授權的存取、收集、使用、披露、複製、修改、處置或類似風險。 2021年1月，個人資料保護委員會宣佈《個人資料保護法2020(修訂)》的部分章節將於2021年2月1 日生效。這包括三大改動: (i) 根據資料外洩的影響程度和範圍，訂立強制資料外洩通報的門檻；(ii) 為個人的個人資料處理失當定上刑罰；以及(iii) 擴大同意網絡。修正案的改動，包括提高企業的罰款將於2021年2月生效。 《濫用電腦法令》是新加坡針對網絡罪案的主要法例，將某些網絡活動（例如黑客攻擊、拒絕服務攻擊以及使用惡意軟件感染電腦系統）定為刑事罪行。該法令亦涵蓋對電腦、電腦資料及電腦服務的未經授權存取、使用或修改。	法案》的第5條禁止實體就公司保護消費者個人資料的虛假陳述，禁止實體作出「不公平及欺詐的行為或常規」。美國聯邦貿易委員會已發布有關保障資料的最佳常規指引，並闡述在網絡安全環境中的執法行動。 • 《2014年聯邦資訊安全現代化法案》要求聯邦政府機構和承辦商制訂及實施網絡安全計劃。因應該法案，美國商務部國家標準技術研究所發布了網絡安全架構。 • 《2015年網絡安全資訊共享法案》加強有關網絡安全威脅資訊的共享。該法案訂明相關流程，使公司在與聯邦執法機構共享有關網絡安全攻擊的資訊時，可以豁免承擔責任及公眾記錄披露。 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

香港	澳洲	歐盟	日本	中國內地	新加坡	美國
						管，非由中央機構執行相關規例。聯邦貿易委員會最近似聯邦私隱執法機構，不過針對網絡安全相關事故的起訴並不常見。至於資料外洩通報，每個州都各有相關法例，對「個人資料」的定義有所不同。

金融監管

香港	澳洲	歐盟	日本	中國內地	新加坡	美國
證券及期貨事務監察委員會（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。主題包括緩減與證券及期貨互聯網交易相關的黑客入侵風險以及提高對勒索軟件的意識。 香港金融管理局（金管局）於2016年推出銀行業的「網絡防衛計劃」(CFI)，其中包括：(i) 網絡防衛評估框架（兩部分組成的自我評估及網絡攻防模擬測試； (ii) 認證計劃及培訓計劃；及(iii) 網絡風險資訊共享平台。加強版計劃（CFI 2.0）於2020年11月推出。 金管局亦推行專業資歷架構，推動銀行業培養網絡安全人才。此外，金管局發出通告，要求註冊機構（即同時在證監會註冊的認可機構）的行政總裁採用證監會的上述指引。為履行監管	澳洲審慎監管局(APRA) 於2019年發布強制性規例（審慎標準CPS 234 – 資訊安全（審慎標準）），旨在確保APRA監管的實體符合特定網絡安全要求，以抵禦新興的資訊安全威脅。根據審慎標準的主要規定，受APRA監管的實體必須： • 明確界定董事會、高級管理層、管治機構及個人與資訊安全相關的角色及職責； • 維持與資訊資產所受威脅的規模和程度相稱的資訊安全能力； • 因應資訊資產的重要性及敏感度實施控制措施，以保護資訊資產；及 • 向APRA通報重大資訊安全事故。 正如層面1所述，澳洲審慎監管局宣佈2020-24年的《網絡安全策略》，以補完《2020年網絡安全策	網絡與資訊安全(NIS)指令旨在確保必要行業的營運商（包括金融市場基建服務供應者）採取適當措施管理網絡安全風險。如上所述，新NIS2指令已於2020年尾建議在涵蓋的行業履行更嚴格的責任。 因應歐盟委員會2018年3月發布的重申網絡安全問題的金融科技行動計劃，歐洲監管機構聯合委員會（包括歐洲銀行業管理局、歐洲證券及市場管理局，以及歐洲保險與職業養老金管理局） 於2019年4月向歐盟委員會提出有關歐盟加強金融業網絡及資訊安全監管的建議。相關措施包括： • 建立歐盟監督架構，監管活躍於金融服務（特別是雲端服務）的第三方供應商；及 • 制訂整個歐盟測試重要金融機構網絡防衛的架構。	個人資料保護委員會及金融廳(Financial Services Agency)發布《金融領域個人資料保護準則》(Guidelines for Personal Information Protection in the Financial Field)。相關準則要求金融機構及其他機構制訂必要及適當的網絡安全管理措施，重點在於預防數據外洩、遺失或損毀。 2018年10月，金融廳發布最新的《加強金融業網絡安全的政策方針》 (Policy Approaches to strengthen Cyber-security in the Financial Sector)，以應對日益增長的數碼化趨勢以及即將舉行東京奧運會帶來的挑戰。 2020年6月，金融廳發佈《金融業網絡安全報告》 (Financial Sector Cybersecurity Report)，描述在監	根據《網絡安全法》，金融機構被視為主要資訊基建營運商，因此需要遵守額外的網絡安全要求。 在金融監管層面，金融機構一般必須對客戶資料保密，並對反洗錢資訊及個人財務資料加強保護。在相關金融監管機構就資訊科技系統開發、外判和營運制訂的法規中，網絡安全也是監管重點之一。 中國中央銀行，即中國人民銀行於2020年2月13日公佈新《個人金融信息保護技術規範》，並即時生效。這業界標準為金融行業機構的個人金融信息收集及處理的周期定下私隱及網絡安全的額外要求。	新加坡的金融機構受新加坡金融管理局監督監管。新加坡金管局的主要監管重點之一是建立金融業的網絡防衛能力。就此而言，新加坡金管局已發布三套以網絡安全為重點的重要通知及指引，包括《科技風險管理指導原則》、《科技風險管理通知》及《網絡衛生通知》。相關通知及指導原則一般訂明金融機構在以下方面的責任：(a) 系統可靠性、可用性及可復原性； (b) 向新加坡金管局通報資訊科技安全事故及重要系統故障；以及 (c) 客戶資訊的安全性，亦訂明關鍵風險管理原則及最佳常規標準，以指導金融機構建立良好穩健的科技風險管理架構。 2021年1月18日，新加坡金融管理局公佈修訂版的《科技風險管理指導原則》 (Technology Risk Management Guidelines)，	1999年頒布的《格雷姆-利奇-比利雷法案》(GLBA) 結合金融服務監管機構發布的實施規例，要求金融機構採取技術、實體及行政措施，保護消費者的非公開個人資訊免受未經授權的存取或使用。各公司制訂的全面保安計劃有所不同，視乎公司規模、公司活動範圍及資訊範圍。GLBA規定進一步要求某些金融機構在非公開個人資訊外洩後通知監管機構及資料當事人。 美國證券交易委員會（SEC）亦使用其民事法權力採取與網絡相關的執法行動。SEC第30條規則適用於根據SEC網絡安全措施而註冊的經紀人、交易商及投資公司。SEC亦於2017年設立執法部網絡小組，主要負責範疇包括受監管實體的網絡安全控制，以及發行人的網絡安全事故和風險披露。SEC發布相關指

香港	澳洲	歐盟	日本	中國內地	新加坡	美國
職能，金管局亦對認可機構的資訊系統進行現場審查及非現場審查。 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到的最低標準。	略》的內容。新策略的三大重點包括： (i) 訂立網絡控制的基線，例如加入不容談判的網絡行為、推動更好的網絡資訊流動和共享及提升事故回報程序的效率； (ii) 讓金融機構的董事局和執行委員監察及糾正網絡風險；及 (iii) 透過網絡評估和保證及統一金融系統的法規和監察，改善金融生態和供應鏈的弱點。 澳洲證券和投資委員會（ASIC）評估金融實體的資訊科技管理系統，並提供有關網絡風險的指引。	2020年9月，歐盟委員會通過數碼金融方案，包括數碼金融策略及加密資產和數碼防衛的立法建議書。歐盟委員發佈《數碼運作防衛法》(Digital Operational Resilience Act) 草案，確保金融行業的訊息和通信技術系統能夠抵禦安全威脅，並監察第三方的信通技術供應商。 如上所述，建議的CER指令要求銀行及金融市場基建業的企業成為關鍵實體，意味著它們需要採取共同匯告措施，包括實體一級的風險評估及事故通報，以及實施其他技術及組織措施。國家當局亦會進行實地巡視。	察施政報告2018(2018 Policy Approach) 的進度文件所發現的現狀及挑戰。除此之外，該報告指出金融機構周邊的網絡危機隨著2019冠狀病毒病及延遲的2020東京奧運會和殘障奧運會而上升。有見及此，金融廳鼓勵中小型金融機構透過業界團體間的合作，保持並提升網絡安全管理系統的基本效能，並從網絡演習中提升事故應變能力。就較大型的企業來說，金融廳鼓勵它們提升集團及全球網絡安全的風險管理能力，並進一步加強網絡安全防護措施。		一併考慮瞬息萬變的網絡威脅環境及金融機構對雲端科技、應用程式介面及軟件迅速發展依賴的增加。新指導原則適用於所有銀行、支付服務企業、經紀及保險企業。	引，幫助投資者免受網絡威脅。 《薩班斯-奧克斯利法案》（Sarbanes-Oxley Act）要求美國上市公司發布年度內部控制報告，以證明公司對財務報告實施充分內部控制，包括確保公司資訊系統安全完整。值得注意的是，公司高層如違例可面臨刑事處罰。 《商品期貨交易委員會規章》要求所有商品期貨交易委員會註冊機構制訂政 策及程序，以行政、技術及實體措施保護客戶資料。 根據《紐約州金融服務管理局網絡安全要求》，受監管的實體須實施及維持符合特定要求的網絡安全計劃，進行定期測試及風險評估，聘用和培訓合資格的網絡安全人員，監察第三方供應商遵守網絡安全控制的情況，並向紐約州報告特定的網絡安全事故。

層面三——網絡文化

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，本整體準備水平為46.9（最高100），較2019年的調查微跌，可能是因為企業優先將資源用於應對目前艱難的營商環境。調查亦顯示：

- 除非牟利機構及學校外，所有行業的整體準備指數都較2019年有所下跌；
- 金融服務業的警覺性仍然最高，準備水平達「管理」級別；
- 所有其他行業，如非牟利機構、資訊和通訊科技業、製造業及專業服務業的準備指數水平達「基本」級別；
- 大型企業普遍採取較為全面的網絡安全措施；及
- 2020年，遭受外來

澳洲

澳洲網絡安全中心（Australian Cyber Security Centre）公佈的年度《網絡威脅報告》（2018年7月至2020年6月）在報告期內，發現2,266宗網絡安全事故。

- 當中佔最大部分的是「第5類別–中等事故」(36.5%)，其次是「第4類別–重大事故」(33.3%)；以及
- 最常見的網絡安全事故是「惡意電子郵件」(27%)、其次是「入侵系統」(24.4%)。「入侵系統」是指遭黑客在未經受權的情況下入侵或竄改網絡、帳號、資料庫或網證的事故。

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，較2017年的46%為高；
- 受訪者對確保自身網絡安全的信心愈來愈低：有59%的受訪者認為自己能防範網絡罪案，較2017年的71%為低；
- 超過三分之一的受訪者在過去三年收過要求提供個人資料的詐騙電郵或電話；及
- 有10%的受訪者表示，由於擔心網絡安全問題，他們不大可能網購。

日本

皮尤研究中心 (Pew Research Center) 於2019年7月公布2018年日本公眾意見調查，指出：

- 有81%的受訪者表示，來自其他國家/地區的電腦系統攻擊是對日本的主要威脅，較2016年增加10個百分點；
- 自2016年起，網絡攻擊是日本人每年最擔心的國際議題；及
- 有84%的日本互聯網用戶對網絡攻擊表示憂慮。

中國內地

中國互聯網絡信息中心第44次《中國互聯網絡發展狀況統計報告》（於2019年9月發布）指出：

- 截至2019年6月30日，中國8.54億網民中有99.1%透過手機上網。
- 2019年上半年，有大量互聯網用戶使用網上服務，例如網上訂餐及外賣用戶有4.21億；網購用戶有6.39億；網上支付用戶超過6.33億；網上串流服務用戶超過7.59億；另外近40%的網民使用召車服務。

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。其他研究結果包括有一半受訪者指，他們在首次使用應用程序時或更新前，會

新加坡

新加坡網絡安全局 (Cyber Security Agency) 於2019年進行的網絡安全公眾意識調查（於2020年8月發布）指出：

- 網絡事故的關注度較高；
- 大部分受訪者同意，網絡安全，人人有責；
- 受訪者的網絡衛生仍有進步空間，例如大部分受訪者知道沒有在流動設備上安裝保安程式會有風險，但仍沒有安裝；
- 受訪者認為要辨別釣魚郵件有困難，即只有4%的受訪者能夠正確辨別所有釣魚郵件；及
- 很多受訪者繼續認為網絡事故不會發生在他們身上。

美國

皮尤研究中心 (Pew Research Center) 於2019年10月發布的調查報告指出：

- 美國人對科技相關議題的理解因教育程度及年齡而出現明顯差異；及
- 他們對科技相關議題的理解因主題而異，例如超過60%的受訪美國人正確回答有關網絡釣魚詐騙及Cookies的問題，而只有30%的美國人正確回答有關網址或網站加密的問題。

皮尤中心此前於2017年1月發布的調查報告顯示：

- 美國人在數碼生活中通常未能採取網絡安全最佳實務，例如妥善管理密碼；
- 有64%的受訪美國人曾遭遇重大數據外洩；
- 有相當大比例的公眾不相信主要機構

香港	澳洲	歐盟	日本	中國內地	新加坡	美國
網絡攻擊的企業較2019年為多，其中網絡釣魚電郵是最主要的攻擊類型。				小心閱讀私隱政策。該調查亦顯示77.8%的受訪者同意監管機構應加重違規行為的罰則，而72.2%的受訪者同意為個人數據保護立法。		（例如聯邦政府、社交網站）可以保護個人資料；及 • 美國人在流動安全方面未能時刻保持警覺，例如有28%的智能電話用戶表示並無使用屏幕鎖或其他安全功能，而大約十分之一的人表示從未更新過智能電話的應用程式或作業系統。

層面四——網絡安全教育、培訓及技能

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，包括：

- 網絡安全資訊站；
- 網絡安全資訊共享夥伴計劃；
- 香港電腦保安事故協調中心；
- 政府電腦保安事故協調中心；及
- 香港警務處網絡安全及科技罪案調查科。

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。「網絡安全資訊共享夥伴計劃」是其中一項措施，目的是促進跨部門協作，以更深入了解全球和本地的網絡威脅。該項計劃已經運作超過一年，截至2021年1月，各行各業超過360間公私營機構已加入計劃。計劃為機構提供有關收集網絡安全資訊的參考，並與資訊安全

澳洲

為配合澳洲政府的網絡安全策略，多項措施已經制訂。

- 澳洲網絡安全部門（Australian Cybersecurity Growth Network）及Cyber.gov.au網站採取措施發展當地網絡安全行業及提升網絡安全風險意識；
- 設立網絡安全卓越學術中心，鼓勵更多學生學習網絡安全及相關課程；及
- 正制訂自願網絡安全指引，推動不同機構的網絡安全的良好實務。

此外，為增加熟練網絡安全專業人員的數量，博士山學院 (Box Hill Institute) 在業界支持下制訂兩項全國網絡安全資歷：網絡安全四級證書及網絡安全高級文憑，是澳洲首批獲國家認可的網絡安全職業教育資歷。

歐盟

歐盟網絡與信息安全局 (ENISA) 支持多項措施，提升網絡安全議題的意識及教育，其中包括：

- 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」活動；
- 舉辦針對學生的經常性活動，例如年度《歐洲網絡安全挑戰》；
- 推廣網絡安全教育，解決網絡技術短缺，宣傳與維護網絡安全眾包數據庫有關的教育活動；及
- 訂立適當機制，統一應對網絡事故及處理危機；及
- 設定「歐洲網絡安全技術框架」，以訂立對職責、能力、技術及知識相同的定義，從而解決網絡技術短缺。

歐洲網路資通安全組織(European Cyber-

日本

日本有多個機構（包括政府機構及研究/教育機構）已制訂網絡安全教育及培訓計劃，例如：

- 總務省於2013年發起的網絡防禦計劃(CYDER)，著重處理政府辦公室、行政機構及大型企業面對的網絡攻擊；及
- 日本多間大學聯合推出SecCap計劃，向大學生傳授資訊科技安全工程人員所需的基本技能。

日本防衛省在2021年初宣布舉辦首個網絡安全人才發掘比賽，參加者透過展示網絡安全的認識及應用知識的能力，來勝出比賽。這個比賽是政府發掘人才的其中一環，以提升日本的網絡防衛能力。

網絡安全策略本部推行制訂安全標準、提升安全意識，加強故

中國內地

政府計劃在2027年前建立多所「舉世知名」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。

由中央網絡安全和信息化委員會辦公室發起的2020年國家網絡安全宣傳周包括一系列活動。這個活動的重點包括以網絡安全為主題的論壇，目的是推廣良好做法及提升有關國家網絡安全標準的實施與應用的意識。

業界、學術界與中國政府之間的合作亦有助培養網絡安全人才。

新加坡

新加坡網絡安全局監督網絡安全策略、教育、拓展和行業發展，並在相關範疇與政府機構及私營機構夥伴合作。

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。

網絡安全局亦透過多項計劃及措施推動網絡安全教育，例如：

- 已推出「網絡安全技術及夥伴計劃」以及「網絡安全職業指導計劃」，前者旨在培訓ICT專業人才及提升技能，後者則旨在吸引學生及年輕專才從事網絡安全相關職業；
- ICE71是網絡安全初創中心，透過與高等教育機構、大型本地企業及全球網絡安全加速器建立夥伴關係，促進

美國

國家標準技術研究所(NIST) 是美國商務部轄下機構，是美國領先的教育及外展機構。NIST舉行各類活動和簡報，並發布有關網絡安全及事故應對架構的書面資源，以推動網絡安全解決方案及技術的發展，從而增加美國的安全能力。

作為《國家綜合網絡安全計劃》(CNCI) 的一部分，國家網絡安全教育計劃(NICE) 於2010年由政府、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。NIST負責主導NICE計劃，透過推廣相關措施支援其運作。

2013年啟動的《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。Cyber

香港	澳洲	歐盟	日本	中國內地	新加坡	美國
持份者會面以分享最新安全趨勢及最佳常規。 在行業層面上，銀行業具備卓越的網絡安全資歷架構。 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。「人才清單」亦為網絡安全專家提供入境便利。	政府將於未來十年投資16.7億澳元在《2020年網絡安全策略》，引入多項措施，當中包括： • 加強合作，以建立澳洲的網絡技術渠道； • 透過《聯合網絡安全中心計劃》，建立業界更良好的夥伴關係； • 提供建議給中小型企業，以提升其網絡防衛能力；及 • 提高公眾對網絡安全威脅的意識。	security Organisation)於2016年成立，與歐盟是公私營機構的合約夥伴關係，當中涵蓋2016至2020年度的「展望2020」。歐洲網路資通安全組織舉辦不同活動，目的是建設社區及發展歐洲的工業。	障應對架構以及管理及應對風險的措施。 經濟產業省與日本資訊科技促進局共同發布《網絡安全管理指引》，促請企業認識網絡安全風險並制訂企業防禦措施。		及加快網絡安全初創企業在各階段的發展，從而加強新加坡不斷發展的網絡安全生態系統； • 新加坡網絡女性計劃旨在鼓勵更多女性（包括尚未升讀大專院校的年輕女性）加入網絡安全行業；及 • 網絡安全局網絡安全合作創新與發展基金為解決網絡安全問題的公司提供資助。 CSA的首屆《網絡安全教育研討會》(Singapore Cyber-security Education Symposium)在2020年11月19-20日舉行，是首個區內同類型的研討會，也是《新加坡網絡教育工作者計劃》(SG Cyber Educators)的重點項目之一。研討會的目的是匯集一班熱心的大專、中學教師，以及教育及職涯指導員，讓他們更了解網絡安全，從而指導他們的學生決定在網絡安全發展他們的學業和事業。	Careers.gov提供最新的網絡安全資訊及資源，為聯邦僱員、學生和學者提供支援。 2015年，美國司法部電腦罪行及知識產權組發布「受害者應對及網絡事故舉報的最佳實務」報告，其後於2018年進行更新。該報告就如何合法地防範及應對網絡事故，以及如何充分策劃事故的應對措施，為機構提供指引。 2016年，奧巴馬總統撥款6,200萬美元，在《網絡安全國家行動計劃》（CNAP）下推行以下措施：為有意接受網絡安全教育的美國人提供獎學金；制訂網絡安全教育核心課程；以及加強國家網絡安全學術卓越中心計劃，以增加參與計劃的學術機構和學生的數目。 2017年5月，特朗普政府責成多名內閣部長共同評估美國網絡安全勞動人口教育和培訓的範圍及充分程

香港	澳洲	歐盟	日本	中國內地	新加坡	美國
					CSA宣佈會推出兩個全新的活動，擴展新的領域，培育傑出年輕人才和領袖。這兩個新活動就是《新加坡網絡奧林匹克》(SG Cyber Olympians)及《新加坡網絡領袖》(SG Cyber Leaders)，詳情將會不日公佈。	度，包括與網絡安全相關的教育課程、培訓和學徒計劃。 2019年5月，特朗普總統頒布一項有關美國網絡安全勞動人口的行政命令，為國土安全部及其他機構的網絡安全從業員建立聯邦網絡安全輪調計劃。該行政命令亦推廣將NICE架構用於網絡安全人員的知識和技能要求。

註：以上列表並非詳盡無遺，僅用於說明上述司法管轄區的網絡安全架構特點截至2021年3月的情況。

致謝

金發局感謝以下業界專家的寶貴意見

賴智明先生　陳家敏女士
趙必立先生　何志恒先生
郭儀雅女士　石浩然先生
黃振權先生

關於香港金融發展局

香港金融發展局於二零一三年一月由特區政府宣布成立，為高層和跨界別的平台，就如何推動香港金融業的更大發展及金融產業策略性發展路向，徵詢業界並向政府提出建議。金融發展局會集中研究如何進一步發展香港金融業，促進金融業多元化，提升香港國際金融中心在國家和地區中的地位和作用，並背靠國家優勢、把握環球機遇，以鞏固本港的競爭力。

聯絡我們

電郵：enquiry@fsdc.org.hk
電話：(852) 2493 1313
網頁：www.fsdc.org.hk