SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

2023/24年持牌法團網絡保安主題檢視報告

2025年2月

目錄

A. 摘要

1. 由證券及期貨事務監察委員會（證監會）於 2017 年 10 月發出的《網絡保安指引》[1]已於 2018 年 7 月全面實施，當中載有 20 項基本規定。

2. 證監會於 2020 年完成了一項主題檢視（2019/20 主題檢視），以審視在香港從事互聯網交易業務的持牌法團（下稱“互聯網經紀行[2]”）的系統和相關管理監控措施，及評估互聯網經紀行有否遵守《網絡保安指引》和《操守準則》[3]（統稱為“網絡保安規定”）。證監會同時將流動保安列為額外網絡保安焦點範疇，並加以檢視。

3. 證監會近期進行了另一項主題檢視，以評估持牌法團在遵守網絡保安規定方面的趨勢。此外，我們亦將仿冒詐騙（或稱網路釣魚）攻擊、採用生命周期結束的軟件[4]、遙距接達、第三方資訊科技服務供應商（第三方供應商），以及在雲端環境中寄存交易和後勤工作系統所出現的新興網絡保安風險和威脅，涵蓋在檢視範圍之內。

4. 證監會進行了以下工作：

   (a) 由規模及業務種類各異的 50 家選定持牌法團完成的問卷調查。有關持牌法團包括證券及期貨經紀行，槓桿式外匯交易商，提供網上分銷平台的基金經理，以及從事多項受規管活動的環球金融機構（統稱“回應者”）；

   (b) 實地視察七家互聯網經紀行，以檢視其系統、程序和監控措施；及

   (c) 與六家擁有環球業務的持牌法團進行深度討論，以深入了解它們採取的網絡保安作業方式。

5. 儘管我們留意到，持牌法團在遵守網絡保安規定若干範疇的情況有所改善，但它們仍應注意在是次檢視中所識別出的監控不足之處及沒有遵守有關規定的情況，包括用於登入系統的雙重認證，系統伺服器和防火牆的保安監控配置，實施由軟件供應商發布的保安修補程式及修正程式，對敏感數據進行加密，以及對使用者接達關鍵系統和數據庫的系統管理帳戶所涉及的問題。

6. 另外，一些持牌法團近年向證監會匯報的網絡保安事故及證監會的視察結果，均顯示有多個保安漏洞。這些事故大多涉及採用了生命周期結束的操作系統和未經修補的虛擬私人網絡（virtual private network，簡稱 VPN[5]）。此外，其中一些事故亦涉及勒索軟件攻擊，這些攻擊可能是由黑客通過仿冒詐騙發起的。持牌法團應檢視並優化（如適用）其網絡保安措施，為它們的業務及客戶提供合理保障，以免因網絡事故而造成任何損失及中斷情況。

---

1 《降低及紓減與互聯網交易相關的黑客入侵風險指引》（《網絡保安指引》）。

2 互聯網經紀行指從事互聯網交易並就以下活動獲發牌的持牌法團：(i)第 1 類受規管活動（證券交易）；(ii)第 2 類受規管活動（期貨合約交易）；(iii)第 3 類受規管活動（槓桿式外匯交易）；及／或(iv)第 9 類受規管活動（提供資產管理），惟以那些以其互聯網為基礎的交易設施分銷所管理的基金者為限。

3 有關規定包括《證券及期貨事務監察委員會持牌人或註冊人操守準則》（《操守準則》）第 18.4 至 18.7 段，以及附表 7 第 1.1、1.2.2 至 1.2.8、1.3 和 2.1 段。

4 生命周期結束的軟件是指其使用期已告結束。該軟件供應商已停止就其提供支援，並且沒有可用的更新保安修補程式及修正程式。

5 VPN 在用戶裝置與企業網絡之間建立加密通道。用戶可透過 VPN 無縫連接至企業應用程式。

7. 隨著數碼化及自動化的程度日益增加，持牌法團委聘第三方供應商提供資訊科技服務，以及在雲端環境中寄存交易和後勤工作系統的情況十分普遍。雖然借助該等供應商提供的技術及服務或有其好處，但它們一旦出現網絡保安漏洞，便可能會產生一連串問題，包括系統中斷、數據外洩和持牌法團未能遵守適用監管規定的情況。因此，我們會在本報告中就第三方供應商管理及雲端保安提供一般指引，以協助持牌法團評估和管理相關風險。

8. 我們亦羅列了被檢視的持牌法團為遵守網絡保安規定及應對新興網絡保安風險和威脅而實施的措施示例。持牌法團在設計其系統和監控措施時，可以參考這些示例。這些示例並非鉅細無遺，持牌法團應檢視自身情況，並採取適當和有效的措施。

9. 現有的網絡保安規定主要聚焦於互聯網經紀行，而此類經紀行往往是網絡攻擊者的目標。儘管如此，隨著所有持牌法團日益依賴科技來進行它們的關鍵業務，即使是從事非互聯網交易業務的持牌法團亦同樣容易受到網絡攻擊。就此，我們計劃於 2025 年全面檢視現行的網絡保安規定及預期標準，並會制訂適用於整個行業的網絡保安框架，向所有持牌法團提供指引，以更妥善地管理網絡保安風險。

B. 香港互聯網經紀業界環境概覽

10. 現時，投資者透過互聯網交易途徑落盤買賣投資產品（包括證券、期貨及槓桿式外匯產品）的情況，在香港相當普遍。這從獲發牌進行第 1、2 或 3 類受規管活動的公司在過去數年呈交的申報表中可見一斑。2021 年有超過 90%的活躍客戶[6]透過互聯網經紀行進行買賣，而這個比例持續上升至 2023 年的 96.9%。

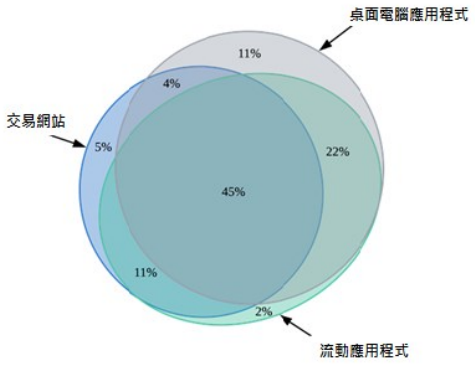
11. 就互聯網經紀行於 2023 年呈交的證監會《業務及風險管理問卷》顯示，92%的互聯網經紀行所實施的互聯網交易系統乃由第三方供應商[7]提供及支援的。此外，當中 70%的互聯網經紀行採用了由五家供應商提供的互聯網交易系統，其中最大供應商所佔的市場份額約為 30%。

互聯網交易途徑

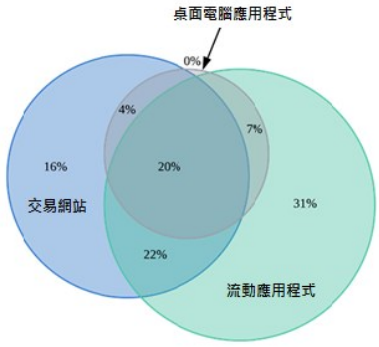
12. 互聯網經紀行向客戶提供的互聯網交易途徑一般包括安裝在客戶電腦的桌面電腦應用程式、交易網站及流動應用程式。互聯網經紀行可能會向客戶提供一種或多種途徑。根據我們為 2019/20 主題檢視而進行的調查，互聯網經紀行所提供的互聯網交易途徑以桌面電腦應用程式最為常見。我們的 2023/24 調查則顯示，流動應用程式已成為最常提供的互聯網交易途徑。

提供互聯網交易的途徑	在 2019/20 主題檢視中互聯網經紀行所佔的百分率	在 2023/24 主題檢視中互聯網經紀行所佔的百分率
桌面電腦應用程式	82%	31%
流動應用程式	80%	80%
交易網站	65%	62%

2019/2020



2023/2024



負責監督互聯網交易系統的高級管理層的經驗

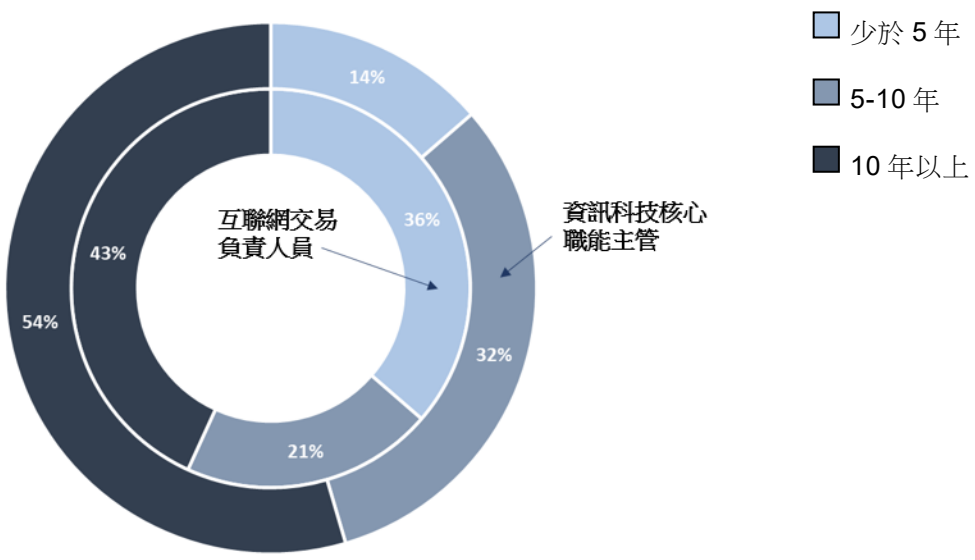
13. 在 50 名回應者當中：

6 活躍客戶指在該年度內完成了至少一項交易的客戶。
7 第三方供應商包括外間供應商及同集團內的聯屬公司。

- 七名回應者有關互聯網交易系統整體管理及監督的負責人員（互聯網交易負責人員）具有資訊科技相關資格，而 28 名回應者的互聯網交易負責人員在證券或期貨業具有五年以上的資訊科技管理經驗；及

- 25 名回應者的資訊科技核心職能主管具有資訊科技相關資格，而 44 名回應者的資訊科技核心職能主管在證券或期貨業具有五年以上的資訊科技管理經驗。

在證券或期貨業資訊科技管理方面的年資
（互聯網交易負責人員及資訊科技核心職能主管）



網絡保安事故

14. 在 2021 至 2024 年間，持牌法團匯報了八宗重大網絡保安事故，其中部分事故造成了嚴重業務中斷，亦有客戶帳戶遭黑客入侵。具體而言，我們留意到：

- 在兩宗個案中，有關持牌法團違反大部分載於本會的《網絡保安指引》及在 2020 年 9 月發出題為“互聯網交易網絡保安檢視”的通函內的基本規定和預期標準。這些漏洞使該等持牌法團面臨重大網絡安全風險，最終導致被勒索軟件攻擊（可能由黑客透過仿冒詐騙所引起），影響全部資訊科技系統，包括互聯網交易系統、交收及後勤工作系統，令業務營運嚴重中斷；

- 在另一個案中，一家持牌法團匯報了一宗事故，指當其供應商的網絡癱瘓時，其後勤服務亦被中斷，而它亦沒有充足的應變計劃；及

- 其中一些個案涉及騙徒透過持牌法團存在的網絡保安漏洞，獲取了其交易系統的接達權限，在未經授權的情況下更改了其客戶數據，繼而控制了受害客戶的帳戶並進行了未經授權交易。

此外，在某些個案中，相關的持牌法團在其系統和伺服器中採用了生命周期結束的軟件，這可能是這些網絡攻擊事故發生的原因。

C. 發現所得

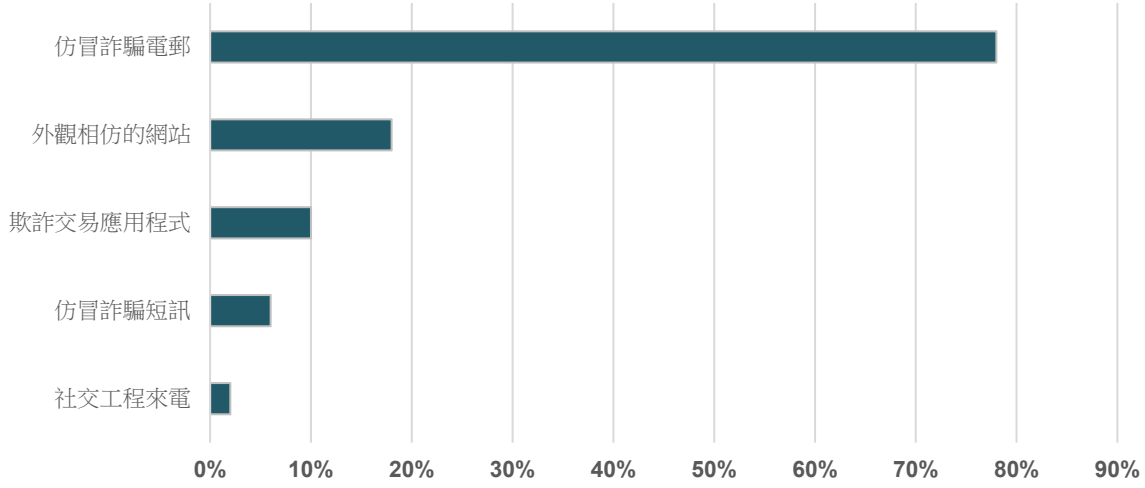
I. 偵測及預防仿冒詐騙

15. 仿冒詐騙攻擊是一種社交工程攻擊，仿冒詐騙者會偽冒成可信的組織（例如金融機構及政府機關）和個人（例如公司高層及相識人士），誘導受害人提供個人和敏感資料，或以惡意程式感染用戶的電腦或流動裝置。

16. 典型的攻擊套路包括仿冒詐騙電郵、仿冒詐騙短訊、假冒互聯網交易網站及欺詐流動應用程式。仿冒詐騙者或會誘使用戶點擊電郵或短訊內的惡意超連結，以引導他們進行交易，提供個人及敏感資料，或開啟受感染的附件。上述行為可能會(i)令系統特權帳戶受到操控；及(ii)藉勒索軟件鎖定用戶裝置及公司系統，繼而導致嚴重的系統中斷、數據遺失及外洩。

17. 根據資訊安全網[8]，仿冒詐騙攻擊仍是近年最常見的網絡攻擊形式。我們的調查亦顯示，大部分回應者曾經歷不同種類的仿冒詐騙攻擊，雖然這些攻擊最終被過濾掉或阻截，並無對回應者的系統及數據造成任何實際影響。

回應者識別出的仿冒詐騙攻擊種類



18. 在其中一宗獲匯報的網絡保安事故中，受害持牌法團所遭受的勒索軟件攻擊似乎源自仿冒詐騙電郵。受害持牌法團遭受攻擊後，其系統及數據被勒索軟件加密，以致無法接達或存取。由於受害持牌法團無法復原其系統及數據，因此需重建整套系統，才能恢復其互聯網交易業務。

19. 持牌法團的客戶亦可能成為仿冒詐騙攻擊的目標，以致他們的個人及敏感資料外洩。

[8] https://www.infosec.gov.hk/tc/knowledge-centre/phishing

主要的觀察所得

20. 某些回應者並無在其交易系統安裝抗惡意程式解決方案，以防範仿冒詐騙攻擊。另外，就其中一宗獲匯報的網絡保安事故所進行的事後檢視顯示，有關持牌法團沒有及時更新抗惡意程式軟件的識別碼檔案，令該檔案過時達一年，這可能是該次事故的成因。在識別碼檔案未及時更新的情況下，抗惡意程式軟件便無法偵測和阻截網絡攻擊者發出的新型惡意程式。

21. 有些回應者將仿冒詐騙相關內容納入了網絡保安意識培訓的範圍之內，當中包括常見的仿冒詐騙種類、潛在影響及防範仿冒詐騙的作業方式。職員如沒有接受有關培訓，或未能識別仿冒詐騙的常見特徵，例如訊息內出現文法或拼寫錯誤，以及可疑連結、附件和網域名稱，繼而可能會無意地點擊可疑連結，下載可疑附件或披露敏感資料。

22. 同樣重要的是，客戶必須對仿冒詐騙電郵或短訊保持警惕。就此，部分回應者向客戶提供了提防仿冒詐騙的貼士及提示。例如，當客戶登入交易應用程式系統或流動應用程式時，便會發出網絡保安提示，或在持牌法團的網站上登載警示訊息。這些措施有助提醒客戶，當開啟據稱來自有關持牌法團的訊息或瀏覽據稱是有關持牌法團的網站時，務必保持警覺。

預期標準

持牌法團應：

(a) 在所有伺服器及工作站（不論所使用的是哪些操作系統）採用抗惡意程式解決方案，並及時更新有關解決方案的惡意程式識別碼檔案；

(b) 避免在發出電子訊息（例如電郵或短訊）時，包含引導客戶到其網站或流動應用程式執行交易的超連結；及避免要求客戶透過超連結提供個人敏感資料，包括登入資料及一次性密碼；

(c) 時刻掌握最新的網絡保安攻擊資訊，並參考由美國國家標準及技術研究院（National Institute of Standards and Technology）[9]等國際標準釐定機構刊發的有關文件，以及善用本地資源（包括守網者[10]及資訊安全網[11]）；

(d) 向全體職員提供定期的網絡保安意識培訓，並應將仿冒詐騙列為培訓主題之一；

(e) 向客戶發送定期的網絡保安警示及提示，包括提防仿冒詐騙攻擊的保安提示；及

(f) 確認其網絡保安事故處理和匯報政策及程序涵蓋各種可能會導致系統全面癱瘓或數據外洩的仿冒詐騙攻擊情境，並具體說明內部上報及對外匯報的程序。

---

9 美國國家標準及技術研究院的提防仿冒詐騙指引（只備有英文版）：https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing

10 守網者的指引：https://cyberdefender.hk/phishing_attack/

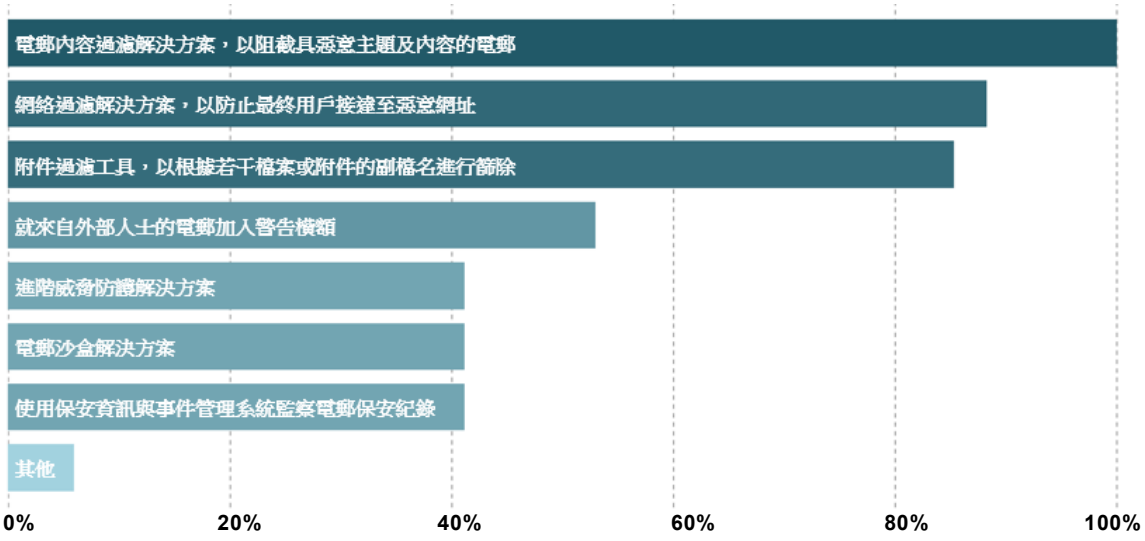
11 資訊安全網知識中心內有關仿冒詐騙的說明：https://www.infosec.gov.hk/tc/knowledge-centre/phishing

持牌法團所實施的措施示例

提防仿冒詐騙的措施

23. 大部分回應者實施了電郵過濾及網絡過濾等提防仿冒詐騙解決方案。舉例而言，由於新開設的仿冒詐騙網站一般都是未經分類，故有少數回應者會利用網絡過濾工具阻截對未經分類網站的接達。另外，部分回應者安排在由公司以外的寄發者發出的電郵中，展示警告訊息。這些解決方案有助紓減主要源自含有惡意超連結的電郵的仿冒詐騙攻擊風險。

回應者為預防及偵測仿冒詐騙攻擊而實施的電郵保安監控措施



24. 一家被視察的持牌法團實施了電郵沙盒解決方案，以分析電子郵件中的任何惡意內容。一旦識別到可疑電郵，便會觸發警示，以便保安運作中心向相關電郵收取人作出跟進。此工具讓該持牌法團能夠及時識別潛在的仿冒詐騙攻擊，並紓減任何潛在後果。

25. 一名回應者與一家電訊公司合作，以識別透過短訊向職員發出的仿冒詐騙訊息，藉此防止他們收到欺詐訊息及保護他們的流動裝置。

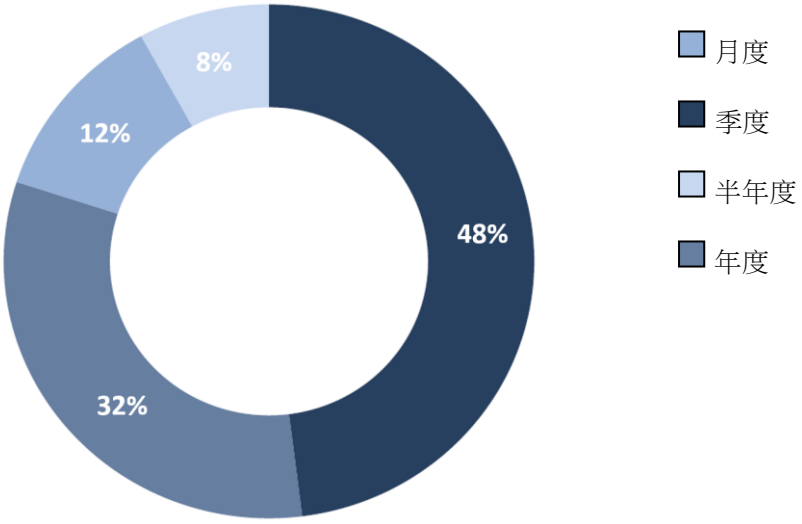
仿冒詐騙模擬演習

26. 定期進行仿冒詐騙模擬演習是測試職員網絡保安意識和應付仿冒詐騙攻擊的有效方法，並且能讓機構評核其職員的整體警覺水平，及評估是否需要額外培訓。

27. 不少回應者進行了定期仿冒詐騙模擬演習，以加強其職員的網絡保安意識。在這些回應者當中，約有半數安排了季度仿冒詐騙模擬演習，而約有三分之一則每年進行該演習一次。

28. 為提高仿冒詐騙模擬演習的成效，許多回應者為未能通過該演習的職員安排了跟進培訓。對於連番未能通過該演習的職員，少數回應者會對他們採取紀律行動，包括薪資檢討，甚或在極端情況下將他們解僱。另一方面，一小撮回應者會獎勵在仿冒詐騙模擬演習中表現優秀及曾匯報仿冒詐騙的職員。這種“賞罰分明”機制能提高仿冒詐騙模擬演習的成效。

仿冒詐騙模擬演習的頻密程度

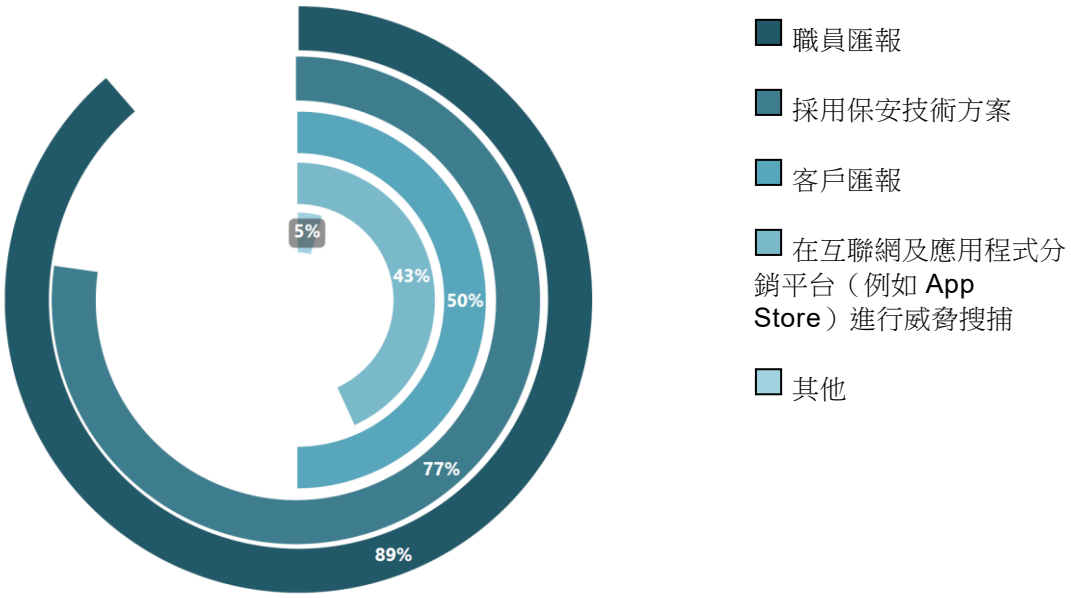


29. 一家被視察持牌法團會將仿冒詐騙模擬演習的結果發送給全體職員。有關結果顯示了點擊仿冒詐騙超連結的職員人數，以及曾在仿冒詐騙網站輸入登入資料的職員人數。該持牌法團亦隨同該演習結果發送一些貼士，提醒職員如何識別仿冒詐騙電郵及保持警惕。此舉有助提高職員對仿冒詐騙攻擊的警覺，並加強機構的保安文化。

識別及匯報潛在仿冒詐騙攻擊

30. 大部分回應者透過職員或客戶的匯報和利用保安技術解決方案（例如電郵內容及網絡過濾解決方案），識別及偵測仿冒詐騙攻擊。由此可見，提高職員及客戶的網絡保安意識和實施適當的技術保障措施相當重要。

回應者識別及偵測仿冒詐騙攻擊的方法



31. 一家被視察的持牌法團鼓勵職員匯報仿冒詐騙攻擊，並提供了特設匯報途徑（例如供匯報仿冒詐騙的專用電話號碼及電郵）。明確的匯報途徑能確立有效的仿冒詐騙攻擊處理程序，以便及時將事故直接交由專責團隊調查和跟進，藉此減低不利影響。

32. 為了保護客戶，大部分回應者進行了定期搜查，以識別涉及它們公司的假冒或可疑網站或流動應用程式。其中一名回應者運用了自動化解決方案，以主動監察及識別模仿其公司登入版面的仿冒詐騙網站，而一些回應者則採用供應商服務，以監察涉及它們公司的欺詐網站。一旦識別到欺詐網站，有關公司(i)會要求網域服務供應商將有關網站下架；及(ii)在它們的社交媒體上及時刊登警示訊息，提醒客戶對有關仿冒詐騙網站及騙局保持警惕。除了保障客戶外，上述措施亦有助維護公司的品牌及聲譽。

33. 一些持牌法團參與了短訊發送人登記制，使來自持牌法團的短訊消息可通過以“#”開頭的已登記的短訊發送人名稱加以區分。這有助於客戶核實短訊發送人的身分，從而防止詐騙者冒充成合法公司。

II. 對生命周期結束的軟件的管理

34. 資訊科技資產的生命周期管理指對有關資產進行端對端追蹤和管理，以確保公司所用的每項資訊科技資產都在其生命周期結束時得以妥善地識別、維護、升級和處置。生命周期結束是軟件生命周期中的一個階段，此時軟件供應商不再為特定版本的軟件提供技術支援和維護服務，包括更新保安修補程式或修正程式、增強功能及修復錯誤。

35. 生命周期結束的軟件面臨重大的網絡保安風險。當未經修補的軟件存在漏洞，而這些漏洞成為攻擊者利用的目標時，網絡保安風險便會增加。攻擊者可能會以這些漏洞作為切入點，藉以進入受害人的資訊科技環境，並獲得關鍵系統和數據的接達特權。這情況可能會導致資料外洩和系統中斷。因此，持牌法團須對生命周期結束的軟件實施穩妥的管理，以確保使用中的軟件是最新和安全的。

主要的觀察所得

36. 雖然大部分回應者已制定有關資訊科技資產管理的政策及程序，但其中某些回應者沒有明確地將對生命周期結束的軟件的管理涵蓋在內。此外，一些大型持牌法團沒有設立任何有關資訊科技資產管理的政策，情況引起了關注，並令人懷疑它們是否可妥善地管理生命周期結束的軟件。

37. 另外，調查發現半數回應者正在其資訊科技環境內使用生命周期結束的操作系統[12]。在一宗極端的個案中，一名回應者報稱當時正使用六項生命周期結束的軟件，而同樣令人嚴重關注的是，當中大部分操作系統已遠超其生命周期結束的日期。這些安排都大大增加了該持牌法團遭受黑客攻擊的風險。

38. 事實上，根據數家持牌法團所提供的網絡保安事故事後報告，它們全部都在本身的伺服器及工作站內使用生命周期結束的操作系統（例如微軟 Windows Server 2008 和 Windows 7），這些薄弱的系統都容易被黑客乘虛而入。

[12] 例子包括 Windows Server 2008 或之前的版本，Windows 7 或之前的版本，CentOS 8，CentOS 6 或之前的版本，Ubuntu 21.10/21.04/20.10/19.10/19.04/18.10，Ubuntu 18.04 LTS，Ubuntu 17.10 或之前的版本，RHEL 6 或之前的版本。。

預期標準
持牌法團應： (a) 制定有關資訊科技資產管理的政策及程序，當中涵蓋（除其他事項外）就使用中的軟件識別和監察生命周期結束或接近結束的情況，軟件升級或遷移策略，及在管理過時軟件方面的相應補救計劃（如適用）； (b) 備存一份完整的資訊科技資產庫存清單，並至少每年一次對該清單進行檢視，以確保其完整性； (c) 持續監察現有軟件的有效性，例如適時地從軟件供應商的官方來源收集生命周期結束的相關資料[13]； (d) 就所有相關的資訊科技資產備存一份完整且最新的生命周期結束清單，並積極地就替換或升級生命周期結束或接近結束的軟件進行規劃（如適用）；如持牌法團需要更多時間來處理技術相容性問題或業務營運方面的關注事項，並因此未能在軟件的生命周期結束前將其更新或替換，有關法團便應採取向軟件供應商訂購額外支援服務的策略性措施，以確保有可用的保安修補程式或修正程式；及 (e) 在所有關鍵系統伺服器和數據庫上，包括面向互聯網的伺服器（例如，網頁伺服器）和與交易相關的伺服器及數據庫，終止使用生命周期結束的軟件。持牌法團亦應適時地升級或替換其他生命周期結束的軟件（即那些不在關鍵系統伺服器和數據庫上的軟件），除非有關法團可妥善地紓減相應的網絡保安風險，則另作別論。

持牌法團所實施的措施示例

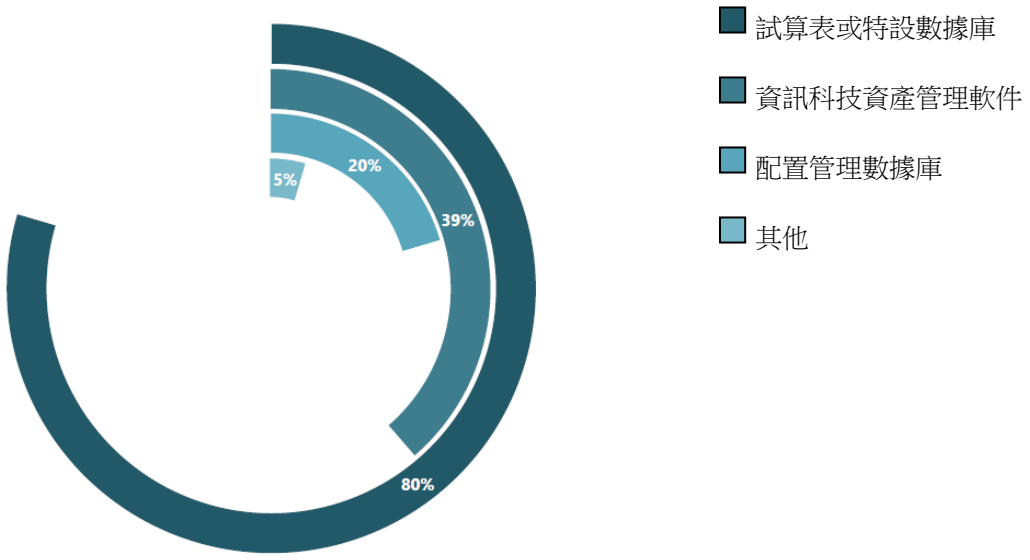
識別軟件庫存

39. 本會的調查結果顯示，所有回應者均至少使用一項軟件或工具來管理資訊科技資產，藉以利便有關工作的進行。其中，試算表或特設數據庫是最常用的工具，其次是資訊科技資產管理軟件和配置管理數據庫[14]。

[13] Linux 及微軟 Windows 的相關資源例子分別包括 https://access.redhat.com/support/policy/updates/errata（只備有英文版）及 https://learn.microsoft.com/zh-hk/lifecycle/overview/product-end-of-support-overview，以供參考。

[14] 配置管理數據庫是一個中央資料庫，用作儲存和管理某機構的資訊科技基礎設施內所有硬件、軟件、網絡組件及其他資產的相關資料。

回應者採用的資訊科技資產管理軟件和工具



40. 為了確保軟件庫存清單是完整、最新且可被妥為管理的：

- 有些回應者採用自動化的軟件識別工具，以定期掃描網絡基礎設施，識別使用中但未在庫存清單上登記或更新的軟件；及
- 一名回應者每季對軟件庫存清單進行評核。

就升級或替換生命周期結束的軟件進行規劃和監察

41. 少數回應者在軟件的生命周期結束日期前 24 個月，就替換或升級軟件的優次處理作出規劃。這個做法令持牌法團得以分配足夠的資源來處理相關的升級或替換工作。

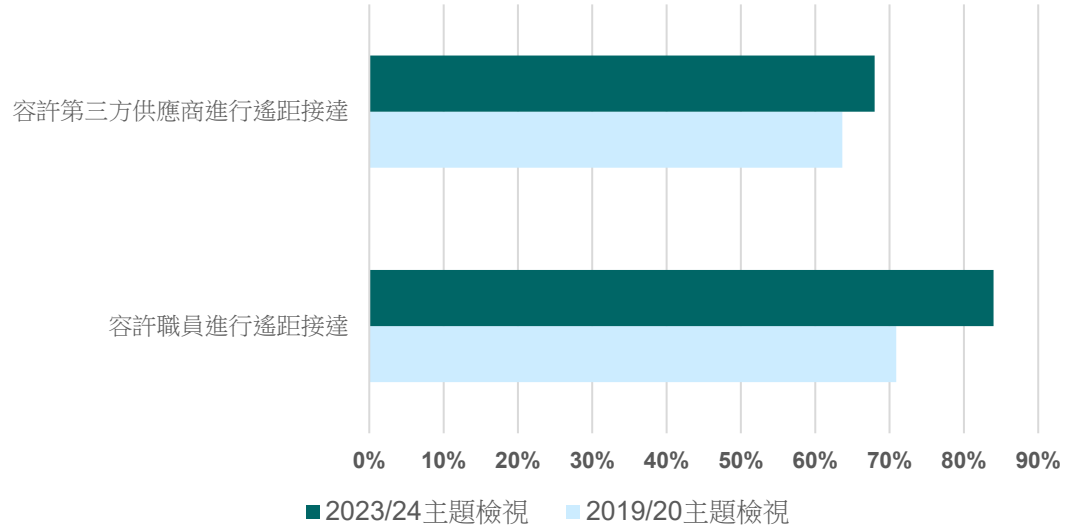
42. 少數回應者使用中央系統來進行軟件庫存管理。該系統會自動向相應的資訊科技負責人發送電郵通知，提醒他們在軟件生命周期正式結束的日期前開始進行生命周期結束規劃和制定補救計劃。

43. 少數回應者開發了儀表板或風險矩陣，以追蹤生命周期結束的軟件的替換和升級情況。這些回應者亦為區域資訊總監和其他資訊科技管理人員安排定期會議，讓他們就生命周期結束的軟件討論最新的補救情況。有關舉措協助高級管理層監督持牌法團的網絡保安風險管理工作。

III. 遙距接達

44. 大部分回應者容許職員和第三方供應商進行遙距接達。本會在比較 2019/20 主題檢視和是次檢視的統計數據後，發現採納遙距接達的情況呈上升趨勢。

採納遙距接達的情況



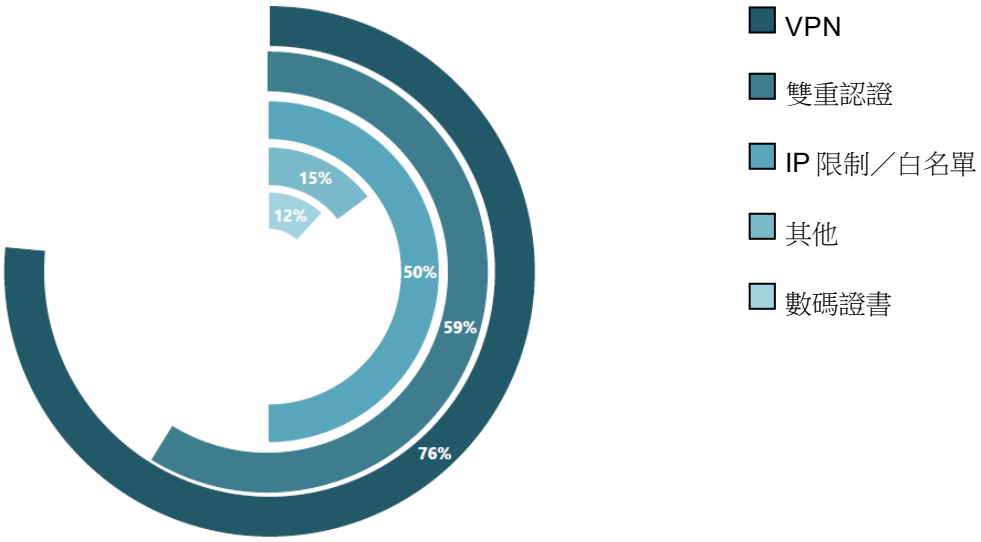
45. 持牌法團增加使用遙距接達方案的情況，造成了新的威脅和漏洞。網絡罪犯（例如勒索軟件組織[15]）正針對薄弱的遙距接達方案，作為入侵內部網絡以及接達系統和存取敏感數據的切入點。近期發生的網絡保安事故，便凸顯了網絡攻擊者可如何利用在未經修補的 VPN 方案和不安全的網絡管理連接埠中存在的漏洞，例如遠端桌面協定（remote desktop protocol，簡稱 RDP）或安全外殼（secure shell，簡稱 SSH）協定的漏洞。

<u>主要的觀察所得</u>

46. 不少回應者使用 RDP 或 SSH 服務來遙距接達內部網絡，以（除其他事項外）對技術問題作出調查和補救。然而，某些回應者沒有同時實施雙重認證或 VPN（或其他提供同等安全保障的技術解決方案）來保障 RDP 和 SSH 連接的遙距接達，令內部網絡面臨保安威脅。

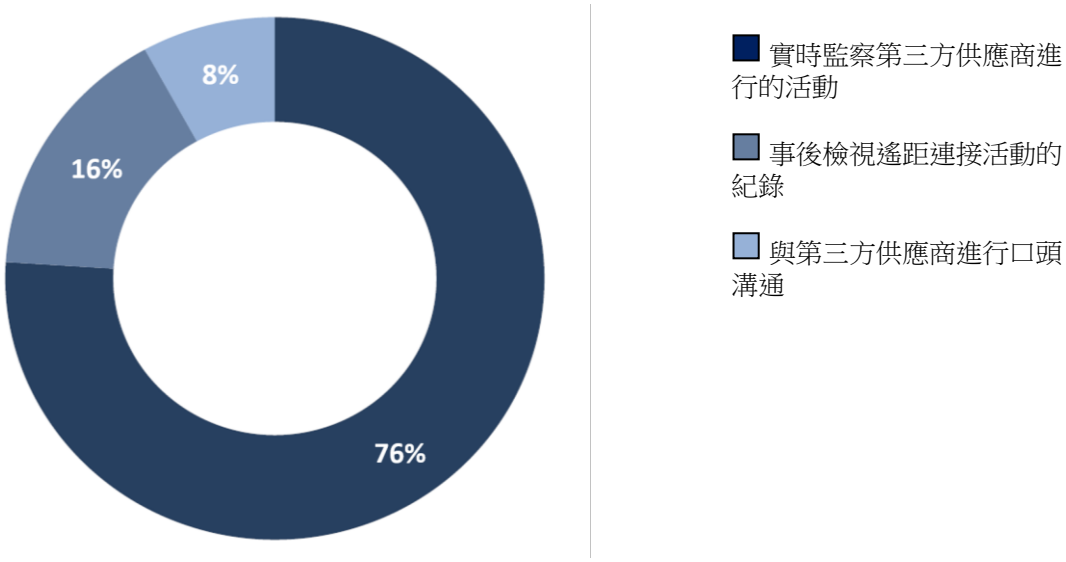
[15] 例子包括 Lockbit，這個勒索軟件組織在 2023 年 11 月利用某遙距接達方案的漏洞，未經授權而接達全球多個大型機構的系統。

為 RDP 和 SSH 連接而設的保安監控措施



47. 為了紓減第三方供應商進行遙距接達的相關風險，大部分回應者實時監察[16]第三方供應商透過遙距連接展開的技術支援活動，以迅速偵測任何可疑行為。某些回應者對遙距連接活動紀錄進行事後檢視，以識別不尋常情況。

有關向第三方供應商提供遙距接達權的保安監控措施



16 資訊科技職員會透過屏幕共享監察供應商的活動，以確保沒有發生未經授權的活動。如偵測到異常情況，他們亦會收到系統警示。

48. 當偵測到多次無效的登入嘗試時，一些回應者沒有相應的監控措施（例如暫停接達）加以處理，導致更易發生未經授權而接達持牌法團內部系統的情況和潛在數據洩漏。

49. 一些回應者的保安修補管理程序沒有涵蓋遙距接達。少數回應者超過一年沒有就 VPN 軟件應用更新的保安修補程式。

50. 一些回應者容許第三方供應商遙距接達它們的內部網絡。然而，其中數名回應者：

- 沒有設立政策及程序以管理有關遙距接達權；
- 在向第三方供應商授出遙距接達權時，沒有要求高級管理層（資訊科技核心職能主管或負責人員）作出書面批准；及
- 向第三方供應商授出永久遙距接達權。

持牌法團欠缺妥善的程序和監控措施，會令第三方供應商對該法團的內部網絡擁有過多接達權（甚或進行未經授權的接達）。有關情況令持牌法團面臨重大的網絡保安風險，並可能會對其系統和營運造成干擾。

預期標準

持牌法團應：

(a) 制定有關遙距接達管理的政策及程序，以涵蓋（除其他事項外）遙距接達的編配、批准和監察要求；

(b) 僅在有需要時予以授予遙距接達權，其權限亦僅限於履行日常職務所需的最小職能；

(c) 適時地移除不必要的遙距接達權，並確保持牌法團的高級管理層（包括資訊科技核心職能主管）或獲其轉授職能的人定期（至少每年一次）檢視獲授遙距接達權的用戶名單（包括外部人士（即業務夥伴和第三方供應商）及合約職員）；

(d) 對其內部網絡的遙距接達實施足夠的保安監控措施，特別是：

- 只容許透過 VPN 或其他提供同等安全保障的技術解決方案進行遙距接達，例如虛擬桌面基礎設施；
- 實施多重認證（至少有雙重認證），以確保只有獲授權的用戶可接達網絡或敏感數據庫；確保用作認證元素之一的密碼遵守《網絡保安指引》內訂明的相同密碼政策；及
- 實施網頁超時監控要求。

在向第三方供應商授出遙距接達權時，持牌法團：

(a) 不應向有關供應商授出永久接達權限；及

(b) 應就第三方供應商遙距連接該法團內部網絡的情況和所展開的活動進行記錄和監察。

持牌法團應遵守《有關運作上的抵禦能力及遙距工作安排的報告》[17]內所載有關遙距接達的預期標準。

持牌法團所實施的措施示例

51. 大部分回應者容許用戶使用個人裝置來遙距接達它們的內部網絡。為了更有效地：

(i) 保護內部系統和數據：

- 少數回應者禁止在虛擬桌面環境內使用複製和貼上及磁碟機對應功能，以防止數據洩漏；
- 一名回應者可在流動裝置一旦被遺失或破解時，或在僱員辭職後，遙距清除企業應用程式和數據，以防止數據洩漏。此外，該回應者可阻止使用過時操作軟件的流動裝置遙距接達其內部系統和數據；及
- 一名回應者將遙距接達權和無線系統或資源（例如 VPN 伺服器、無線控制器和認證伺服器）存置於隔離區內，而非寄存了業務和客戶敏感數據的內部網絡區段。

(ii) 防止和識別未經授權而遙距接達持牌法團內部網絡的情況：

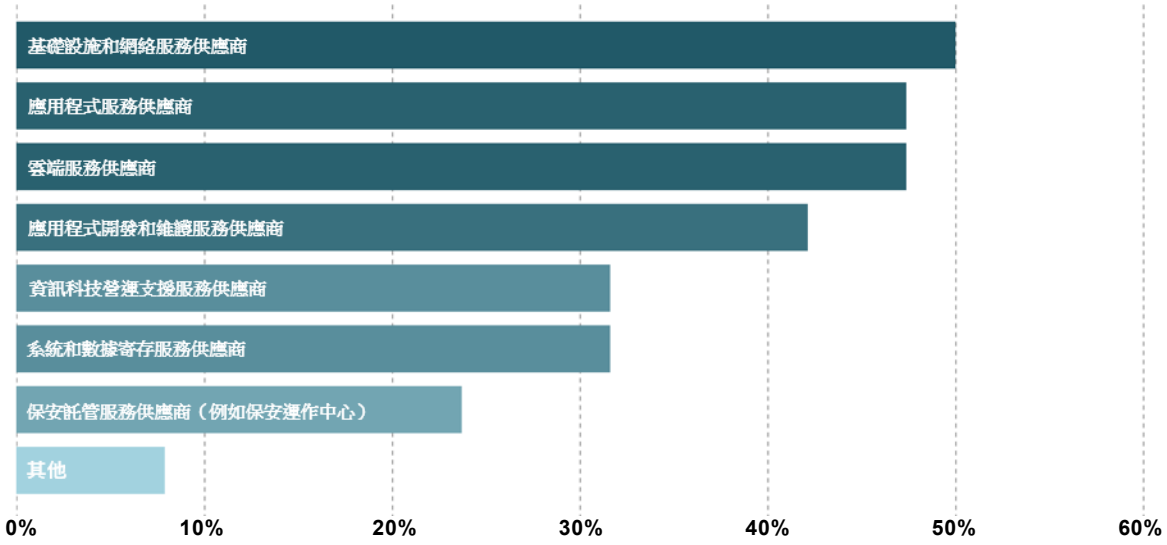
- 一名回應者實施監控措施以阻止來自某些 IP 地址的遙距接達，例如遙距接達來自私人 VPN、受制裁國家和被列入黑名單的 IP 地址，以及用戶登入的 IP 地址定位於短時間內轉為另一國家；及
- 一名回應者就第三方供應商的遙距連接實施 IP 白名單，以便在第三方供應商遙距登入後收到電郵通知，讓該法團能夠即時就任何不尋常的情況進行調查。

IV. 第三方供應商管理

52. 隨著金融業加速數碼化和自動化成為趨勢，持牌法團委聘第三方供應商提供資訊科技相關服務的情況十分普遍。本會的調查顯示，大部分回應者為支持其本身的業務而委聘不同類型的第三方供應商。他們的服務包括應用程式開發和維護服務、資訊科技營運支援服務、雲端服務、基礎設施和網絡服務、系統和數據寄存服務及保安託管服務（例如保安運作中心）。

[17] https://www.sfc.hk/-/media/TC/files/COM/Reports-and-surveys/Report_Operational-resilience-and-remote-working-arrangements_Oct-2021_TC.pdf

回應者使用的第三方供應商的類型



53. 使用第三方供應商所提供的技術和服務可能帶來降低成本、提升營運效率等作用，從而令持牌法團受惠，但與此同時，這些法團必須了解相關的網絡風險。倘若發生服務供應商違反網絡保安的事件，可能會導致系統中斷、數據洩漏、違反適用的監管規定和其他問題。在某持牌法團所匯報的其中一宗網絡保安事故中，該法團因其服務供應商受到網絡攻擊而出現結算服務中斷的情況。

54. 另須注意的是，雖然持牌法團可將實施網絡保安監控措施的工作外判予第三方供應商，但有關法團的高級管理層（即其負責人員和資訊科技核心職能主管）應負責互聯網交易系統的整體管理和監督，界定網絡保安風險管理框架，及確保遵守（除其他事項外）《網絡保安規定 。

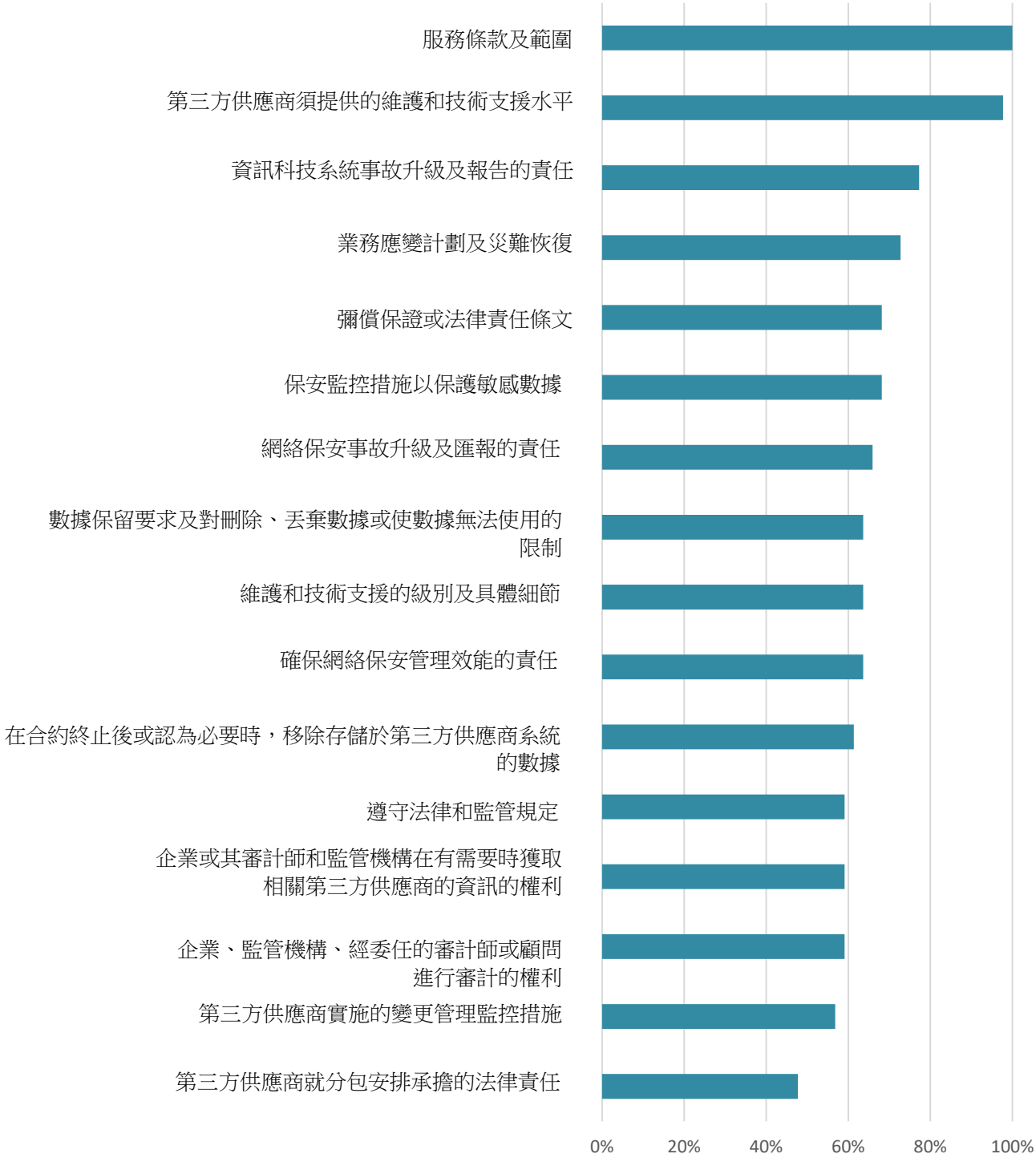
<u>主要的觀察所得</u>

55. 一些回應者沒有就管理第三方供應商設立政策及程序，以全面地識別、評估、監察和紓減與使用該等供應商相關的網絡保安風險。

56. 少數回應者沒有在委任第三方供應商前進行盡職審查。由於沒有妥善的盡職審查，這些持牌法團可能無法選出最合適而又具備適當能力和資源的服務供應商，亦無法評估與委任該等服務供應商相關的網絡保安風險的影響。

57. 所有回應者均與第三方供應商訂立了正式合約或服務水平協議，但這些協議的涵蓋範圍不盡相同。特別是，有些協議沒有指明網絡保安的相關要求和服務供應商的責任，例如有關上報和向持牌法團匯報網絡保安事故的要求和責任。欠缺清晰的條款亦令持牌法團難以妥善地監察這些服務供應商的表現。

服務水平協議內訂明的條款



58. 一些回應者沒有對其第三方供應商的保安監控措施進行定期評估。在另一些個案中，定期評估的範圍並不足夠。舉例而言，一些回應者沒有就第三方供應商是否符合回應者預設的網絡保安相關要求進行評估。

59. 一些回應者沒有在其業務應變計劃中加入第三方供應商相關的網絡保安情境和必要的應變措施，因而妨礙了該等法團有效地應對與服務供應商相關的資訊科技事故，例如系統中斷和數據洩漏。

60. 持牌法團須就在第三方供應商提供的互聯網交易系統內所實施的保安監控配置和參數，向服務供應商作出指示。然而，一些持牌法團未有妥善地做到這一點。舉例而言，一家被視察的持牌法團沒有確保互聯網交易系統內的設置符合多個主要範疇的網絡保安規定，例如容許經電郵傳送的一次性密碼作為雙重認證的元素，及設定過長的網頁超時時限。

預期標準

持牌法團應：

(a) 制定有關管理第三方供應商的政策及程序，包括對第三方供應商進行盡職審查、挑選和批准、合約管理、表現監察、風險管理（包括網絡保安風險管理）、監管規定的合規情況、解決爭議的方式、終止和退出策略以及紀錄備存；

(b) 備存一份完整的第三方供應商名單，包括名稱、聯絡詳情及所提供服務的描述，以利便對第三方供應商的持續管理和監察；

(c) 在委任第三方供應商前對其進行適當的盡職審查，特別是評估有關第三方供應商實施的網絡保安措施是否足夠；

(d) 與第三方供應商訂立正式的服務水平協議，當中指明服務條款和提供者責任，特別是：

- 提供者擬實施的網絡保安措施；及
- 網絡保安事故的匯報程序；

(e) 定期檢視及修訂（如適用）服務水平協議，以反映外判安排或監管發展的任何變動；

(f) 定期監察第三方供應商的表現，從而及時地識別任何違反服務水平協議的情況或不合要求的表現。

(g) 按照相關要求（包括網絡保安規定）設定在第三方供應商提供的系統內的保安監控配置和所使用的參數；及

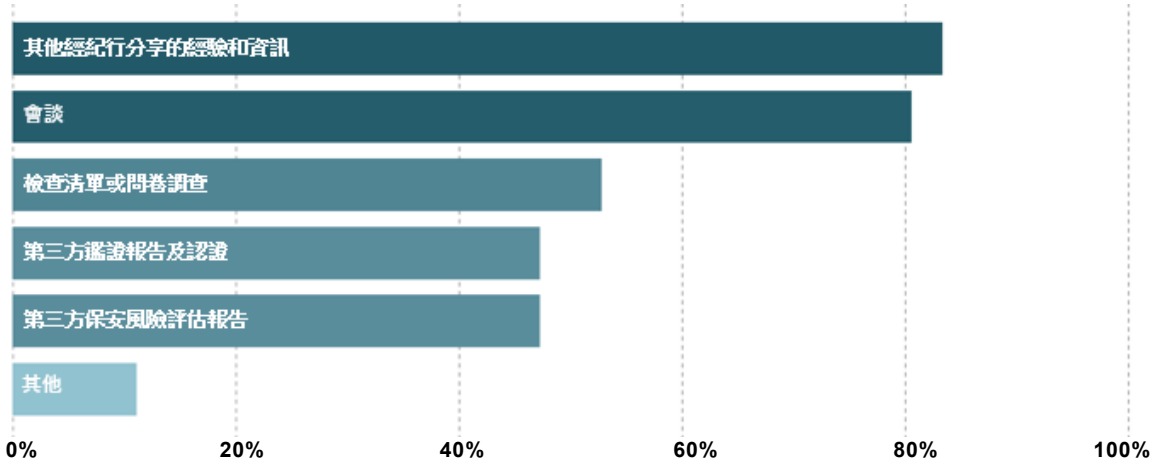
(h) 在其業務應變計劃中加入無法使用第三方供應商所提供的服務的情況，以及相關的網絡保安情境和相應的應變策略。在可能的情況下，持牌法團應聯同這些供應商進行定期的演練和復原測試。

持牌法團所實施的措施示例

挑選第三方供應商

61. 在對第三方供應商進行盡職審查及挑選時，回應者與其他亦有外判這些系統的經紀行交流資訊，與第三方供應商進行會談，要求第三方供應商填妥檢查清單或問卷，以及審閱第三方保安風險評估報告（例如穿透測試及漏洞掃描）和第三方鑑證報告及認證（例如系統與組織監控措施 2（System and Organization Controls 2，簡稱 SOC 2）報告及 ISO/IEC 27001）。

回應者進行第三方供應商盡職審查的方法



62. 具體而言，

- 一名回應者制訂了一份詳盡的問卷來評估第三方供應商的監控環境，當中包括技術評估報告（例如穿透測試報告）、第三方鑑證報告及認證（例如 SOC 2 及 ISO/IEC 27001）、修補管理、加密、身分和接達或存取管理、備份等；及

- 另一名回應者對第三方供應商作出了評估和風險評級，並對高風險的第三方供應商（例如商業關鍵系統供應商）進行了實地測試和驗證，以確保他們的保安監控措施符合其企業標準，並遵從適用的監管規定。

- 某些回應者從其第三方供應商取得了說明文件，以協助他們評估第三方供應商提供的互聯網交易系統的特點可如何讓持牌法團遵守《網絡保安指引》內訂明的規定。

附錄 A 載有某些第三方供應商評估範疇的示例，以供參考。

第三方供應商合約管理

63. 某些回應者制訂了標準合約範本，當中概述了第三方供應商預期應有的網絡保安措施。這使得雙方能了解他們的權利和責任，減低引致不合規情況和潛在糾紛的風險。附錄 B 載有與網絡保安相關的第三方供應商合約條文示例，以供參考。

第三方供應商風險管理

64. 大部分回應者均已設立程序，以備在第三方供應商服務中斷、合約突然終止和清盤的情況下，將有關服務改為在公司內部執行。

65. 大部分回應者均有替代服務供應商，以備在主要供應商服務中斷、合約突然終止和清盤的情況下，更換服務供應商。這些措施讓持牌法團有更周全的準備，能夠在第三方供應商引致服務中斷時維持業務運作。

66. 多名回應者與第三方供應商合作進行演練測試。具體而言，一家被視察的持牌法團每年均與主要第三方供應商共同進行業務修復計劃及復原演練（至少進行桌上演練）。回應者借鑑演練測試中所識別出的缺陷和汲取的經驗，來改善事故發生時的應對程序。

應變計劃

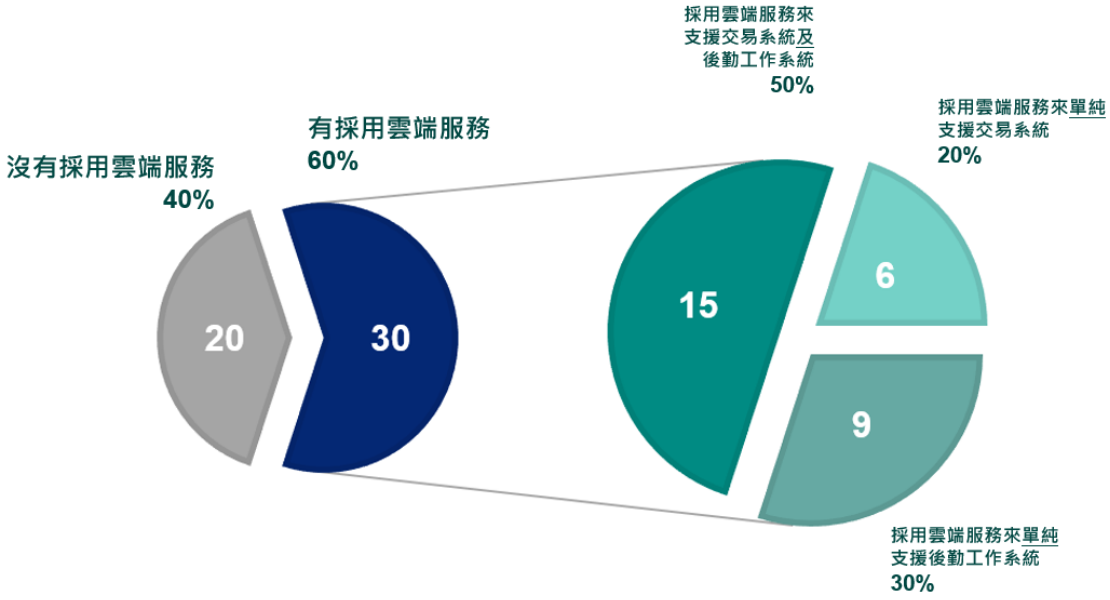
67. 一名回應者在發生了任何重大內部或外部網絡保安事件後，均有進行事後分析來評估潛在影響（包括對第三方供應商所提供的資訊科技服務的影響）和識別所汲取的教訓。在適當的情況下，分析結果將用於檢視和更新應變計劃中的情境分析。

68. 某些回應者備有第三方供應商名單，當中概述了供應商之間的相互關聯。這有助回應者全面識別和評估受影響服務的潛在影響，讓他們能更有效地實施應變措施，以應對網絡保安事故。

V. 雲端保安

69. 近年，金融服務行業使用雲端運算服務的情況日益普遍。許多持牌法團為提高營運效率和節省成本，均將其業務應用程式及後勤工作系統寄存在雲端環境中。

70. 60%的回應者採用了雲端運算服務，當中有半數採用了雲端服務來寄存其交易系統及後勤工作系統。

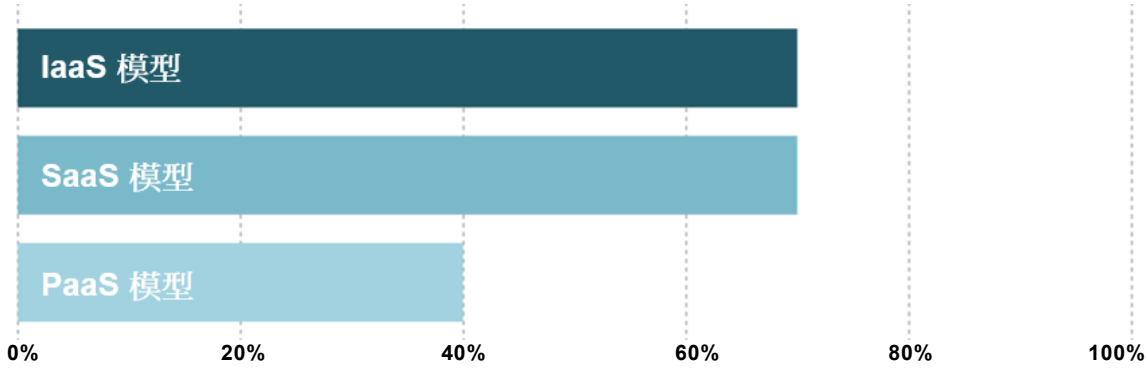


現時，有三種較為常見的雲端部署模型[18]，包括基礎設施即服務（Infrastructure as a Service，簡稱 IaaS）[19]、平台即服務（Platform as a Service，簡稱 PaaS）[20]及軟件即服務（Software as a Service，簡稱 SaaS）[21]。每個模型提供不同程度的控制權、靈活度及對雲端寄存系統和數據的管理。簡單而言：

- 在IaaS模型下，持牌法團負責雲端寄存系統和數據的網絡建設、應用程式系統建設及作業；
- 在PaaS模型下，持牌法團負責應用程式系統建設及作業，而第三方雲端服務供應商則負責提供及維持相關基礎設施；及
- 在SaaS模型下，持牌法團使用應用程式系統，而第三方雲端服務供應商則負責提供及維持相關基礎設施。

這三種模型均獲回應者採用，情況如下：

回應者（合共 30 名）採用的雲端服務模型



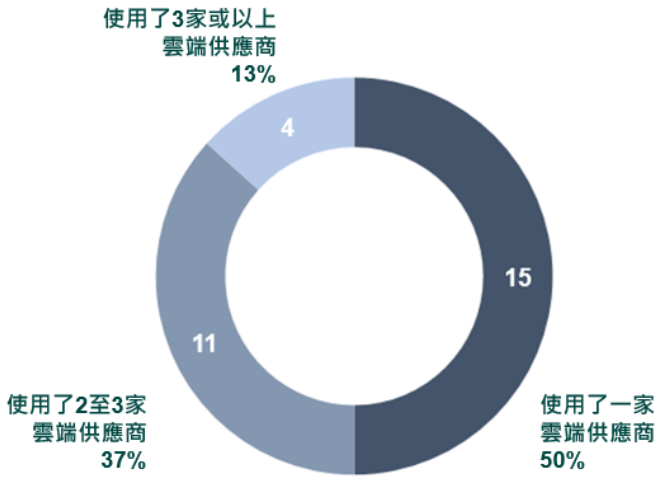
71. 此外，多名回應者採用了多項雲端服務。

[18] 美國國家標準及技術研究院的雲端運算定義提供了三種雲端服務模型。請參閱：https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-322.pdf（只備有英文版）。

[19] 美國國家標準及技術研究院將“基礎設施即服務”定義為“向雲端服務客戶提供計算處理、儲存空間、網絡及其他基礎運算資源，使其能夠部署和運行任意軟件，包括作業系統及應用程式”。

[20] 美國國家標準及技術研究院將“平台即服務”定義為“使雲端服務客戶能夠在雲端基礎設施內，部署由雲端服務客戶創建或取得的應用程式，而此等應用程式乃由供應商所支援的程式語言、程式庫、服務及工具所創建的”。

[21] 美國國家標準及技術研究院將“軟件即服務”定義為“使雲端服務客戶能夠使用雲端服務供應商在雲端基礎設施上運行的應用程式”。



雖然採用多雲端策略有助提高系統抵禦能力和減低服務中斷風險，但隨著不同雲端環境的管理愈趨複雜且情形不一，這有可能會帶來額外風險及營運挑戰。例如，在雲端環境之間傳送資料，需要有強效的加密技術保障。

72. 適用於雲端寄存系統和數據的網絡保安管理，可能與傳統部署於本地的資訊科技環境中的網絡保安管理截然不同。有見及此，持牌法團必須了解其所採用的雲端服務模型並實施相應的保安措施，這一點至關重要。如有誤解或認識不足，可能會導致雲端環境的保安漏洞未獲修補，並有可能洩露客戶資料。

<u>主要的觀察所得</u>

73. 某些回應者沒有在雲端內設立隔離區或實施雲端原生的隔離監控措施，令他們面臨更高的黑客入侵風險。在一宗個案中，有一家被視察的持牌法團實施了網絡策略[22]，以控制寄存於同一個網絡叢集（network cluster）內的面向互聯網系統服務與敏感的內部系統組件（包括交易系統）之間的存取情況。然而，由於其網絡策略較為寬鬆，使得面向互聯網的服務能直接與資料庫接達，因而增加了數據外洩的風險。

74. 某些回應者在雲端內儲存了客戶帳戶數據、交易數據及系統配置數據。然而，他們並無設置充分的數據備份程序，因此未必能夠在有需要時復原數據。例如：

- 某些回應者沒有至少每日一次將這些數據備份到離線媒體，亦沒有在獨立於雲端環境的媒體中儲存備份數據；
- 某些回應者沒有在備份程序完成後中斷數據來源。因此，當黑客發動勒索軟件攻擊，破壞運作環境與備份環境之間的連接時，已備份數據可能會被刪除或加密；及
- 某些回應者所採用的雲端備份方案，沒有設立不可更改的數據備份控制（即一寫多讀功能）。

[22] 網絡策略指控制容器叢集內的元素之間的通訊的網絡連接規則。

預期標準

持牌法團應：

(a) 制訂雲端保安管理政策及程序，包括存取認證管理、安全的雲端基礎設施、數據加密、安全紀錄及監控、備份、合規監控、定期審核，以及事故應對和報告；

(b) 對第三方雲端服務供應商進行妥善的盡職審查，尤其是關於該等供應商實施的保安監控措施；

(c) 建設安全的網絡基礎設施[23]，以及將寄存關鍵系統的網絡區段（network segment）或安全性群組（security group），與面臨較高被黑客入侵風險的其他網絡區段或安全性群組[24]分隔開來；

(d) 實施充分的監控措施，以防在未經授權下接達和使用雲端平台的管理者帳戶[25]；並設立充足的監控措施（例如雙重認證及互聯網規約（即 IP）白名單），以防在未經授權下接達和使用此帳戶；

(e) 妥善保管用來進行與互聯網交易系統和數據互動的雲端登入資料，包括應用程式介面（application programming interface，簡稱 API）金鑰和存取權杖；僅在有需要時向登入資料授出指定的存取權，權限亦僅限於其履行日常職務所需的最小職能。持牌法團亦應將這項預期標準，應用於不同雲端的應用程式系統之間（例如交易系統和交收系統之間）的數據存取和通訊；

(f) 定期更改 API 金鑰，及避免使用永久密鑰；

(g) 至少每日一次在離線媒體內備份業務紀錄、客戶和交易數據庫、伺服器及證明文件；同時，確保備份資料“不可更改”（即設有一寫多讀功能）並已設置“網閘”（即於每次備份程序完成後，截斷備份媒體與雲端環境的連接）；及

(h) 與第三方雲端服務供應商合作，在自身的業務應變計劃內，訂定與雲端相關的網絡保安及服務停用情境；及如情況許可，與第三方雲端服務供應商協作進行演練和復原測試。

持牌法團所實施的措施示例

75. 多名回應者設有先進的雲端相關保安工具，以保護寄存在雲端環境中的系統和數據。這些保安解決方案包括雲端存取安全性代理程式[26]、雲端工作負載保護平台[27]、雲端安全性態

[23] 在雲端環境內設計及建設網絡基礎設施來寄存系統和數據，有別於在“非雲端”環境（例如地端數據中心）內建設網絡基礎設施。因此，持牌法團未必會透過設有多重防火牆的典型隔離區部署網絡區隔。他們應使用雲端原生的隔離監控措施，並採用微分隔的方式來細緻地部署網絡區隔，亦即在已分隔的網絡叢集、安全性群組，乃至個別系統服務及組件之間實施存取限制。

[24] 例如，網絡伺服器或利用互聯網的服務。

[25] 雲端運算平台的管理者帳戶是擁有最高權限的帳戶，能夠完全接達和存取雲端環境內的所有系統服務和資源。

勢管理[28]及雲端原生應用程式防護平台[29]。這些方案或可協助應對與雲端配置錯誤和雲端工作負載問題有關的風險，同時改善漏洞管理和接達監控措施。

76. 某些回應者至少每年一次在雲端環境中進行保安技術評估，包括穿透測試及漏洞掃描。他們亦進行了雲端配置檢查，以評估雲端控制平面[30]的保安監控措施是否有效。

77. 為了改善雲端運算平台的保安，某些回應者採用了零信任架構，以在雲端環境內對身分和接達或存取管理執行嚴格的監控措施。

VI. 網絡保安規定的合規情況

78. 根據調查結果，持牌法團遵從了部分網絡保安規定及預期標準，包括監察及監督機制以及流動保安，與 2019/20 年主題檢視的結果相比有所改善。

79. 然而，是次檢視亦發現若干主要監控範疇的規定沒有獲得遵守，例如使用不合規格的雙重認證登入系統，以及未有定期監察保安修補程式更新版本的可用及部署情況。

---

26 雲端存取安全性代理程式（Cloud Access Security Brokers）是一項設置在雲端使用者與供應商之間的保安解決方案，用來執行保安政策及保護往來雲端環境的數據通訊。

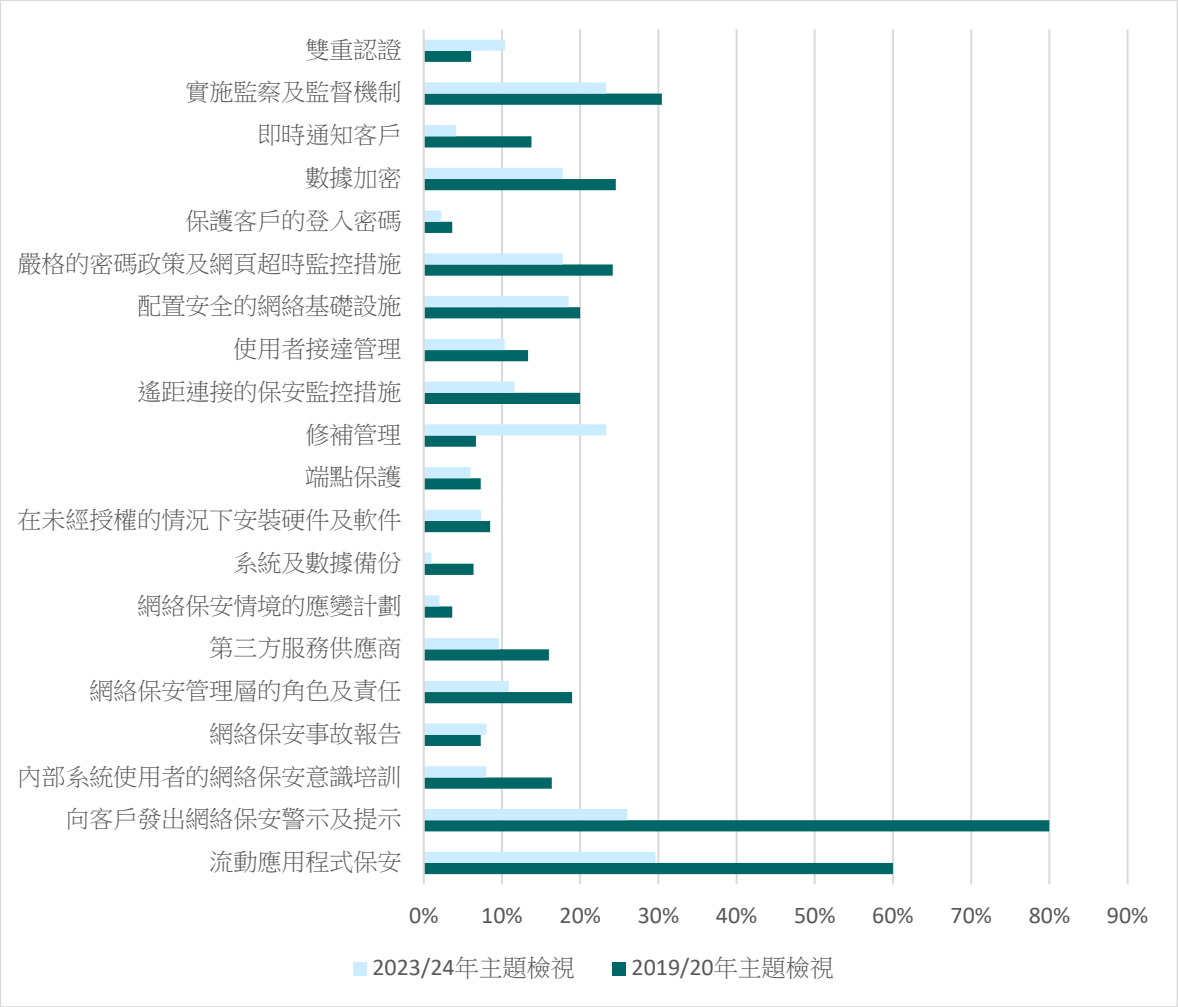
27 雲端工作負載保護平台（Cloud Workload Protection Platforms）是一項保安解決方案，用來保護雲端環境內運行的工作負載，包括虛擬機器、容器、無伺服器運算及運行環境。

28 雲端安全性態勢管理（Cloud Security Posture Management）是一項保安工具及程序，用來識別和糾正雲端環境內的保安風險和配置錯誤。

29 雲端原生應用程式防護平台（Cloud-Native Application Protection Platforms）是一項保安解決方案，透過融合雲端環境內的保安特點（例如工作負載保護、漏洞管理和合規監察）來保護雲端原生的應用程式。

30 雲端控制平面（Cloud control plane）能發出施行指令和控制雲端平台上的所有系統服務和資源。

2019/20 年與 2023/24 年主題檢視發現的不合規情況比較



80. 此外，我們在視察期間注意到，部分不足之處可能使持牌法團面臨重大網絡保安風險，包括鬆懈的系統伺服器和防火牆保安監控配置[31]，延誤執行由軟件供應商發布的保安修補程式及修正程式，對敏感數據使用弱加密算法並對傳輸中的數據及靜態數據加密不足，以及對關鍵系統和數據庫的系統管理帳戶給予了使用者過多權限。

81. 除此之外，在持牌法團匯報的某些網絡保安事故中，我們注意到關鍵系統和伺服器缺乏審計線索。這妨礙了持牌法團進行定期監察並在發生網絡保安事故時進行調查的能力。

82. 本會特此提醒，持牌法團應實施足夠的網絡保安監控措施來保護其系統、客戶帳戶和數據，以及確保遵守網絡保安規定。

持牌法團所實施的措施示例

83. 本節重點闡述回應者和被視察的持牌法團就遵守網絡保安規定所實施的一些措施。持牌法團在設計其系統和監控措施時，可參考這些示例。

[31] 例如，打開了系統伺服器不必要的服務端口，如文件傳輸協定（File Transfer Protocol）和 SSH 協定，並且在防火牆的訪問控制列表中允許了不必要的訪問。

雙重認證

84. 目前，短訊一次性密碼是系統登入和裝置綁定中最常見的認證元素之一。然而，使用此方法存在一些保安方面的疑慮，例如，騙徒可透過安裝於受害人流動電話的惡意程式，截取到這些一次性密碼。為了紓減這些風險，一些回應者已採用更安全的認證方法，例如生物特徵認證（包括容貌識別技術）和軟件權杖。本會特此提醒持牌法團要時刻掌握最新的科技發展，以及檢視使用短訊一次性密碼所帶來的風險，並且鼓勵持牌法團停止使用短訊一次性密碼進行認證，或在適當情況下，實施監控措施以作彌補。

85. 某些回應者使用多種識別碼來綁定裝置。例如，某些回應者在裝置上使用了超過一種識別碼來綁定裝置。這增加了黑客模擬裝置的難度。下表載列回應者在各個平台所使用的識別碼，以供參考。

平台種類	綁定裝置所用的識別碼
桌面電腦應用程式	• 全域唯一識別碼（GUID） • 算法產生的識別碼 • 媒體存取控制地址
流動應用程式	• AndroidID • 客戶裝置公鑰和裝置版本 • 數碼證書 • 供應商識別碼（IDFV） • 廣告識別碼（IDFA） • 由專有算法產生的識別碼 • 媒體存取控制地址 • 開放匿名設備識別碼（OAID） • 通用唯一識別碼（UUID）／唯一裝置識別碼（UDID）
網上交易平台	• 瀏覽器插件及擴充功能 • 瀏覽器種類及版本 • 裝置大小 • 屏幕解像度 • 系統語言 • 時區 • 使用者代理程式字串

註：在網上交易平台用來綁定裝置的識別碼，能為認證檢查提供額外資料，但其強度卻不足以獨一無二地識別各個裝置。回應者除了在網上交易平台採用綁定裝置的做法外，還採用了其他認證元素。

86. 一家被視察的持牌法團在交易網站的登入系統上採用了免卻一次性密碼的認證解決方案。在登入時，交易網站和客戶裝置所綁定的流動應用程式上，均會顯示一組數字代碼。據此，客戶便可透過流動應用程式授權登入。

數據加密

87. 一家被視察的持牌法團能夠透過線上掃描器，自動識別其網絡伺服器所使用的弱加密算法。

修補管理

88. 2024 年 7 月，一項網絡保安解決方案更新異常，引發全球資訊科技事故。該項更新由該軟件供應商推送，並分發給所有客戶作自動更新。某些持牌法團由於暫停了自動更新，因此免受事故影響。這些持牌法團評估了該項更新的潛在影響，及／或在不同的系統組別內分階段進行解決方案更新，以便管理該項更新的潛在問題。

89. 一家被視察的持牌法團在中央系統內存放了所有用作軟件開發的軟件組件和程式庫，使它能夠有效率地監察其保安修補程式是否可用。

90. 一家被視察的持牌法團透過不同途徑（例如香港網絡安全事故協調中心[32]、資訊安全網[33]及網絡安全資訊共享夥伴計劃[34]）訂閱威脅情報，由此得悉最新網絡保安風險趨勢，藉以識別最新發現的漏洞以及保安修補程式的可用情況。

網絡保安情境的應變計劃

91. 多名回應者定期進行涵蓋網絡攻擊情境的演練測試，以驗證其業務應變計劃的成效。他們亦參與整個業界的演練測試，參與者包括金融監管機構及其他業內人士。

92. 一些依賴第三方供應商來提供服務的回應者，會與這些供應商合作進行應變計劃的演練測試，讓他們能夠做好準備，應對第三方供應商服務潛在中斷的情況。

流動應用程式保安

93. 多名回應者定期進行穿透測試，以取得流動交易應用程式的網絡保安鑑證。他們亦定期進行流動交易應用程式的保安原始碼評審，以應對新發現的漏洞。

[32] https://www.hkcert.org/tc
[33] https://www.infosec.gov.hk/tc/
[34] https://www.cybersechub.hk/tc/home/highlights

附錄A —— 第三方供應商評估

評估範疇	描述
聲譽	檢視第三方供應商的聲譽，並以其競爭對手作比較。
風險管理及資訊保安政策	檢視有否制訂風險管理及資訊保安政策和程序，以應付因科技的使用方式而帶來的風險。
職責分隔	檢視有否將其資訊科技職員的職責妥善分隔開來，例如開發人員不得接觸真實運作環境。
真實運作環境與開發環境的分隔	檢視有否將真實運作環境與開發環境分隔開來。
網絡架構設計	檢視是否有關於妥善的網絡區隔、反分散式阻斷服務（anti-DDoS）及可用性方面的結構設計文件
身分和接達或存取管理	檢視有否對帳戶的建立、修改、刪除及重新認證進行妥善管治。
特權接達或存取管理	檢視有否對特權帳戶的使用方式進行妥善管治。
對實際接達、網絡接達及遙距接達的監控	檢視有否對實際接達、網絡接達及遙距接達進行妥善監控。
軟件開發生命周期	檢視有否界定適當的軟件開發生命周期，以及在開發生命周期內有否處理網絡保安風險，例如在有關系統推出至真實運作環境前進行源代碼審查、漏洞掃描及穿透測試。
資訊科技資產的生命周期管理	檢視有否制訂程序以避免採用生命周期完結的軟件及硬件。
變更管理程序	檢視有否對變更管理進行妥善管治。
修補管理	檢視有否對修補管理進行妥善管治，以實施保安修補程式及錯誤修正程式。
抗惡意程式	檢視有否運用抗惡意程式解決方案
電郵保安	檢視有否運用技術監控措施，以降低透過電郵令數據外洩和遭受仿冒詐騙攻擊的風險。
系統配置管理	檢視有否為系統的基本配置制訂標準以應付網絡保安風險，以及有否進行定期檢視，以確保配置仍符合該標準。
加密	檢視所採用的加密算法是否最新版本，經定期檢視，並應用於正在傳輸及儲存於數據庫內的敏感數據。
備份	檢視是否設有妥善的備份安排。
防止數據遺失	檢視有否制訂技術監控措施，以避免敏感資料外洩。
業務延續計劃	檢視有否制訂業務延續計劃，以向客戶提供服務。
事故管理及問題管理	檢視有否制訂妥善的事故管理及問題管理程序。

評估範疇	描述
記載、監察及警示的處理	檢視有否制訂程序以妥善處理記載、監察及警示。
威脅情報管理	檢視是否設有程序，以定期收集、分析及處理從不同來源獲取的威脅情報。
第三方管理	檢視有否制訂第三方管理政策及程序，以妥善管理第三方供應商的供應商所帶來的風險。
雲端運算	檢視有否就雲端服務的使用方式制訂管治及技術標準。
網絡保安意識培訓	檢視有否為其職員安排定期網絡保安意識培訓。
審計及合規	檢視有否進行定期審計工作，以確保有關第三方供應商符合其政策和法律及監管規定。
技術評估報告	檢視技術評估報告，例如 SOC 2 報告、穿透測試報告及漏洞評估報告，以估計第三方供應商的保安措施。
認證	檢視第三方供應商是否持有網絡保安證書，例如 ISO/IEC 27001。

附錄B —— 第三方供應商合約條文示例

合約所載的項目	描述
網絡保安管理作業方式	述明對網絡保安管理作業方式的要求，即有關方式應與 ISO/IEC 27002 或 NIST SP800-53 等國際公認框架相若。
實際接達監控	述明對實際接達監控的要求，以避免未經授權而接達其系統和進入其處所，例如(i)只允許獲授權人員接達安全區域；(ii)使用生物特徵或感應卡的接達篩選方式來限制接達；及(iii)利用保安人員和影像監控持續監察出入口。
邏輯接達監控	述明對邏輯接達監控的要求，以避免未經授權而接達其系統，例如(i)按照最低權限原則設立的接達監控措施；(ii)特權帳戶和經增強及／或系統層面的接達監控措施；(iii)任何系統接達都必須是暫時性和即時的，且授權的職責必須加以分隔；(iv)所有接達和變更必須留有審計線索；及(v)必須在接達後及時進行檢視。
遙距接達	述明對遙距接達連同多重認證和加密的要求，及有關用作遙距接達的裝置的保安監控措施。
軟件開發生命周期	述明對在軟件開發生命周期內進行設計檢討、威脅模型分析、代碼審查和保安測試的要求。
變更管理	述明對適當的變更管理的要求。
抗惡意程式	述明對抗惡意程式的要求。
數據保護	述明對在傳輸、處理和儲存數據時保護數據（例如加密），及防止數據損毀、洩漏和在未經授權下被接達（包括銷毀數據的流程）的要求。
加密	述明對以行業最新的加密算法來加密數據的要求。
數據備份	述明對備份頻率和保留期限的要求。
網絡保安事故的監察、處理和匯報	述明對網絡保安事故監察、處理和匯報的要求和時間表。
業務延續性	述明對維持最新的業務延續計劃和程序的要求。
網絡保安意識培訓	述明對提供予其職員的網絡保安意識培訓的要求，包括入職前培訓和年度培訓。
年度保安審計	述明對由獨立第三方進行年度保安審計以評估網絡保安管理成效的要求。
漏洞掃描	述明對進行定期漏洞掃描和制訂時間表，以解決不同風險水平的漏洞的要求。
穿透測試	述明對進行定期穿透測試的要求。
審計權	述明對審計權，對由持牌法團或獨立第三方進行現場監控評估和核查的要求。

合約所載的項目	描述
遵守法律和監管規定	述明對遵守法律和監管規定的要求。
法律責任、罰則和終止權	述明違反保安事件的法律責任和罰則及有關的終止權。