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

2019-20年互聯網經紀行網絡保安主題檢視報告

2020年9月

目錄

A. 摘要

1. 證券及期貨事務監察委員會（證監會）在 2017 年 10 月發出並在 2018 年 7 月全面實施《網絡保安指引》[1]，當中載有 20 項基本規定，包括雙重認證。

2. 證監會在 2019 年展開主題檢視，以審視在香港從事互聯網交易業務的持牌法團的系統和相關管理監控措施，及評估這些持牌法團有否遵守《網絡保安指引》和《操守準則》[2]。為處理據報部分流動應用程式可能較容易被黑客入侵的關注事項[3]，是次檢視亦集中於流動交易應用程式的保安監控措施。

3. 證監會進行了以下工作：

   (a) 由背景各異的 55 家選定的互聯網經紀行完成的問卷調查；及

   (b) 實地視察這 55 家公司當中 10 家規模和營運模式各有不同的公司，以檢視其系統監控措施和其他相關管理監控措施，輔以與香港互聯網經紀行通常會委聘來支援其互聯網交易系統的數家系統供應商進行討論。

4. 調查結果及視察所得顯示，大部分公司均遵守證監會的主要監管規定。然而，證監會注意到，在保護客戶的互聯網交易帳戶（包括實施雙重認證、數據加密及為識別可疑的未經授權交易而進行的監察和監督）、基礎設施保安和使用者接達管理、網絡保安管理及事故報告方面存在不足之處及沒有遵守有關規定的情況。

5. 本報告撮述了是次檢視的主要發現和觀察所得，及就本會的預期標準提供指引和提示，並重點闡述本會在是次檢視中注意到的不足之處及沒有遵守相關基本規定和《操守準則》規定的情況，以及參與調查和被視察的公司所採納的良好作業方式。

---

[1] 《降低及紓減與互聯網交易相關的黑客入侵風險指引》。

[2] 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 17.8 段以及附表 7 第 1.1、1.2.2 至 1.2.8、1.3 及 2.1 段。

[3] 香港無線科技商會在其於 2017 年中進行的研究中發現，在由不同的金融機構（包括經紀行）提供的 140 個 Android 應用程式中，44%未能通過其安全測試。

B. 香港互聯網經紀業界環境概覽

6. 根據獲發牌進行第 1、2 或 3 類受規管活動的公司在 2019 年 8 月至 2020 年 7 月期間就證監會的《業務及風險管理問卷》所呈交的 1,372 份回應，511 家公司（或 37%）向客戶提供互聯網交易服務。在這 511 家公司當中：

   (a) 49%有超過一半的成交額是來自互聯網交易；

   (b) 14%將其年度財政預算的超過 30%投放於資訊科技；

   (c) 這 511 家公司全都已就其互聯網交易系統實施雙重認證解決方案，並設有自動化客戶通知監控措施。然而，12%沒有實施任何監察或監督措施，以偵測未經授權而接達客戶的互聯網交易帳戶的情況；

   (d) 94%採用供應商提供的系統；及

   (e) 全都沒有匯報曾經有客戶帳戶遭黑客入侵，但 1%匯報曾發生分散式阻斷服務[4]和勒索軟件攻擊等網絡保安事故，及 5%匯報曾經發生突發系統中斷，因而令客戶無法使用其互聯網交易服務。

7. 本會對 55 家選定的互聯網經紀行（回應者）進行調查，讓我們了解到業界環境的以下狀況：

   (a) <u>成交額</u>

      (i) 55 名回應者涉及證券的每月成交額介乎 40 萬元至 1,420 億元，涉及期貨和期權的每月成交量則介乎少於一張合約至 140 萬張合約。平均而言，這些公司涉及證券的每月成交額約為 160 億元，涉及期貨和期權的每月成交量則約為 150,000 張合約。

      (ii) 37 名回應者從事證券交易，其中 11 名回應者匯報少於 20%的成交額來自互聯網交易，12 名回應者匯報超過 70%的成交額來自互聯網交易。41 名回應者從事期貨和期權交易，其中六名回應者匯報少於 20%的成交量來自互聯網交易，23 名回應者匯報超過 70%的成交量來自互聯網交易。

   (b) <u>系統</u>

      (i) 55 名回應者營運合共 106 個互聯網交易系統：

         - 60 個系統只支援證券交易；36 個系統只支援期貨和期權交易；10 個系統同時支援證券交易及期貨和期權交易。

         - 有關系統在以下平台上提供：

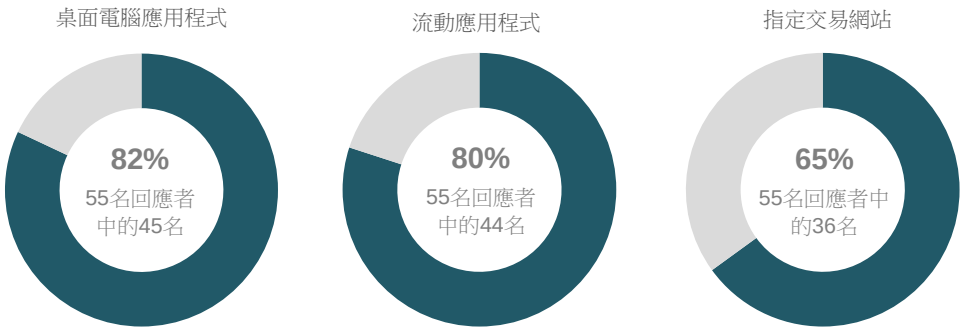
平台	系統數目
所有平台（流動裝置、桌面電腦及指定交易網站）	23

[4] 分散式阻斷服務攻擊指多個受操控的電腦系統一同攻擊某個伺服器、網站或其他網絡資源，導致攻擊目標的用戶被截斷服務。

只限於桌面電腦	23
流動裝置及桌面電腦	21
只限於流動裝置	15
只限於指定交易網站	11
流動裝置及指定交易網站	9
桌面電腦及指定交易網站	4
合計	**106**

- 75 個系統由外間供應商提供及支援；21 個系統由公司內部開發；10 個系統以應用程式服務提供者的模式提供及營運，即應用程式服務及相關基礎設施均由一名外間供應商提供及支援。

(ii) 在 55 名回應者中，大部分都提供桌面電腦應用程式 [5]及流動應用程式，約三分之二提供指定交易網站 [6]：



(iii) 為支援其互聯網交易系統，49 名回應者委聘了第三方服務提供者，例如應用程式服務提供者、數據中心服務提供者及互聯網交易應用程式和軟件的供應商。

(c) 資源

(i) 55 名回應者的年度資訊科技預算介乎 55,000 元至 11 億元；19 名回應者的預算少於 200 萬元。回應者的年度資訊科技預算平均為 800 萬元。

(ii) 46 名回應者將其資訊科技預算的少於 25%投放於網絡保安管理。

(iii) 55 名回應者的資訊科技人員的平均數目為 21。40 名回應者有 10 名或以下人員；六名回應者（不包括在集團公司內另有資訊科技職員的回應者）有兩名或以下人員；一名回應者獲全球 600 名資訊科技人員支援。

(iv) 在 55 名回應者中：

- 兩名屬同一集團的回應者沒有專責的人員或委員會負責網絡保安管理；

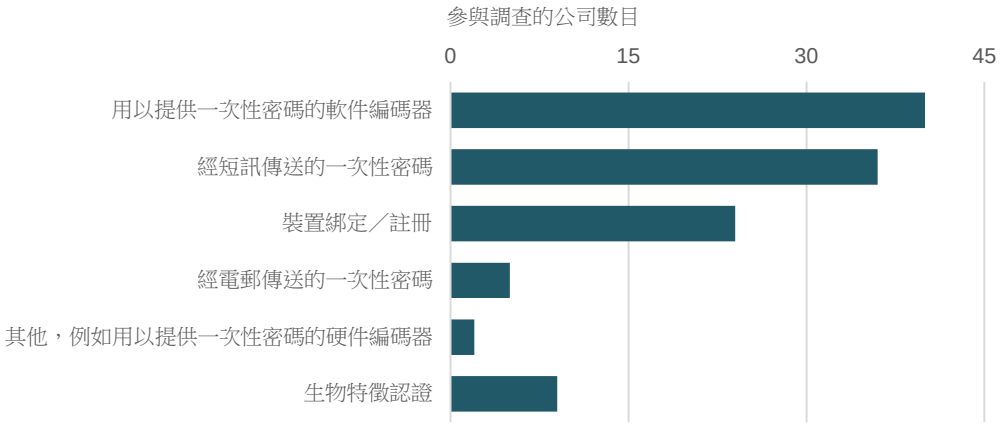
[5] 客戶須在其電腦或裝置上安裝互聯網經紀行的軟件或程式。
[6] 在互聯網瀏覽器（例如 Internet Explorer、Chrome、Firefox 及 Safari）運行的應用程式。

- 兩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 35 名回應者的互聯網交易負責人員在證券或期貨業界具有超過五年的資訊科技管理經驗；及

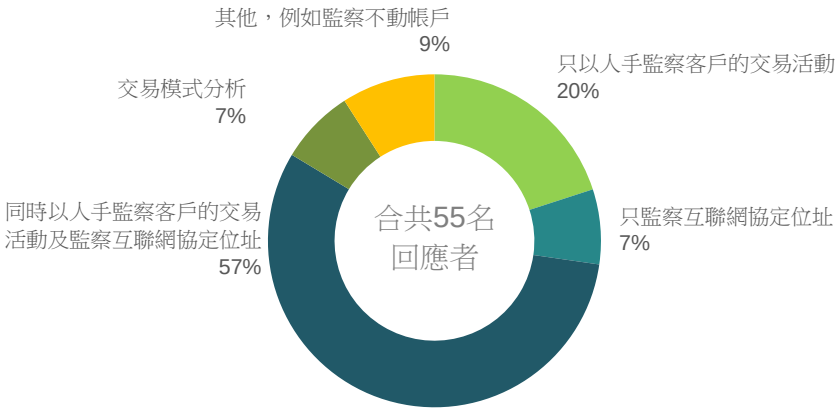
- 22 名回應者的資訊科技核心職能主管具有資訊科技相關資格，而 51 名回應者的資訊科技核心職能主管在證券或期貨業界具有超過五年的資訊科技管理經驗。

(d) 雙重認證

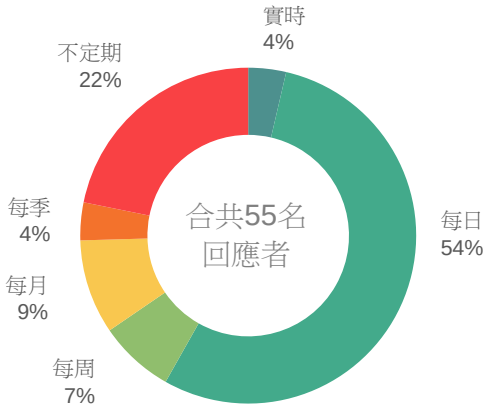
這 55 名回應者所營運的 106 個系統全都採納了使用者名稱及密碼作為“客戶所知的”元素，及以下各項作為使用者認證的第二元素：



(e) 監察及監督機制



相隔時間



8. 根據在 2016 年至 2019 年期間向證監會匯報的網絡保安事故及是次調查的結果，在基本規定生效後並無任何客戶帳戶遭黑客入侵的報告。只有三家互聯網經紀行向證監會匯報分散式阻斷服務或勒索軟件攻擊。在 55 名回應者中，九名回應者曾經在截至 2019 年 7 月 31 日止年度匯報網絡保安問題，其中六宗事故涉及系統中斷，三宗與虛假網站有關。

9. 本會從對有關調查和《業務及風險管理問卷》的回應可觀察到以下情況：

(a) 超過三分之一獲發牌進行第 1、2 及 3 類受規管活動的公司向其客戶提供互聯網交易服務；

(b) 互聯網經紀行在規模、營運模式及系統監控措施方面有極大的差異；

(c) 絕大部分互聯網經紀行都依賴外間供應商開發及支援其互聯網交易系統；及

(d) 在 55 名回應者中，雖然提供桌面電腦應用程式仍然是最常見的情況，但流動應用程式及（在較低程度上）指定交易網站亦已變得更為普遍。

C. 不足之處、沒有遵守基本規定的情況及良好作業方式

保護客戶的互聯網交易帳戶

雙重認證

> 基本規定——第 1.1 段
>
> *持牌人應就客戶的互聯網交易帳戶的登入程序實施雙重認證。*
>
> *持牌人應評估及實施與其業務模式相稱的雙重認證解決方案。*

10. 雙重認證意指使用以下任何兩項元素的認證機制：客戶所知的、客戶所有的及客戶是誰。

    (a) 就“客戶所知的”而言，互聯網經紀行一般採用使用者名稱及密碼；

    (b) 就“客戶所有的”而言，互聯網經紀行一般採用以下一個或以上的解決方案：

        (i) 一次性密碼是透過短訊服務傳送到客戶的指定流動裝置，或由客戶的指定裝置上所安裝的應用程式所產生；

        (ii) 一次性密碼是由提供予客戶的硬件編碼器所產生；及

        (iii) 裝置的綁定或註冊，即客戶在公司的互聯網交易系統內綁定或註冊某台電腦或其他裝置，使有關的電腦或裝置可藉其獨有的裝置資料（例如媒體存取控制（Media Access Control，簡稱 MAC[7]）位址及國際流動設備識別（International Mobile Equipment Identity，簡稱 IMEI[8]）號碼）而被辨識。

    (c) 就“客戶是誰”而言，互聯網經紀行採納生物特徵認證——將客戶的生物特徵數據（例如指紋及人臉識別）比對儲存在其流動裝置的生物特徵數據的加密版本來進行驗證的保安程序。

不足之處及沒有遵守有關規定的情況

A. 經電郵傳送的一次性密碼

11. 有兩家被視察的公司採納了經電郵傳送的一次性密碼作為其第二認證元素，即“客戶所有的”。這做法並不可靠，原因是登入的人不一定是實際的客戶，理由如下：

    (a) 經電郵傳送的一次性密碼可被發送至多部裝置，例如同時發送至流動電話及電腦，以及可被這些裝置上的多個應用程式取用或讀取；

    (b) 經電郵傳送的一次性密碼可能未必由客戶本人讀取，原因是客戶電郵帳戶的登入資料可由多人共用；及

[7] MAC 位址是在用作傳訊的網絡上為識別電腦裝置而設的獨有硬件識別號碼。
[8] 流動裝置的 IMEI 號碼是其獨有的識別號碼或序號。

(c) 電郵帳戶的安全保障不足，例如電郵的轉寄功能可導致不慎將一次性密碼與他人分享。

12. 另外，一些互聯網經紀行可能同時經短訊及電郵傳送一次性密碼。儘管經短訊傳送的一次性密碼有效的第二認證元素，但鑑於上述理由，經電郵傳送一次性密碼仍存在風險。互聯網經紀行***不應***經電郵傳送一次性密碼。

B. 解除雙重認證功能

13. 一家被視察的公司容許客戶解除系統登入的雙重認證功能。鑑於雙重認證是強制性的，因此互聯網經紀行***不應***容許客戶解除此功能。

C. 裝置的綁定或註冊

14. 一家被視察的公司因其互聯網交易的應用程式出現技術性保安漏洞，導致公司為其客戶電腦而設的裝置資料可被複製，讓黑客可藉此登入客戶的互聯網交易帳戶。這個保安漏洞令裝置的綁定或註冊失去作為第二認證元素的功用。互聯網經紀行***應***定期進行技術評估，以識別保安漏洞並立即加以糾正。

15. 另有一家被視察的公司沒有就客戶可綁定或註冊的裝置數目設立上限，並容許有關裝置並行登入（concurrent login）帳戶。這做法並不理想，因為無論是綁定或註冊的裝置還是並行登入帳戶的裝置如數目過多，都會增加黑客入侵的風險，而這樣可能會有更多的裝置成為目標及被黑客入侵。互聯網經紀行***不應***容許客戶就其互聯網交易帳戶綁定或註冊過多裝置，並***應***就並行登入實施監控措施。舉例說，

(a) 若個人客戶要求綁定或註冊超過三個裝置，則互聯網經紀行應了解箇中原因，及評估有關要求是否合理；

(b) 若公司客戶要求綁定或註冊多個裝置，以便獲其授權的人士可操作這些裝置，則互聯網經紀行應提議該公司客戶為那些獲授權的人士開立子帳戶（各自具有獨立的雙重認證）；

(c) 若子帳戶的安排並不可行，則互聯網經紀行應向公司客戶查問獲授權操作其互聯網交易帳戶的人數，並將並行登入的數量限制在有關人數之內。

<u>實施監察及監督機制</u>

基本規定——第 1.2 段

持牌人應實施有效的監察及監督機制，以偵測未經授權而接達客戶的互聯網交易帳戶的情況。

16. 互聯網經紀行可採納不同方法來識別可疑的未經授權交易。舉例說，若某公司只處理數量有限的互聯網交易，並熟悉其客戶的交易模式，則該公司可在收市時就客戶交易是否存在看似不尋常的情況進行人手檢視，從而有效地識別可疑的未經授權交易。在其他情況下，互聯網經紀行可（其中包括）落實使用互聯網協定（internet protocol，簡稱 IP）位址監察工具，以便在偵測到客戶用作登入的 IP 位址在短時間內有異常的變動（例如來自不同國家或城市）時，自動發出警告。

17. 一旦互聯網經紀行偵測到可疑和未經授權的帳戶接達或交易，便***應***即時就異常情況與相關客戶作出跟進以作驗證。迅速採取跟進及補救行動（例如將懷疑被黑客入侵的帳戶暫停）對於控制受損程度而言至關重要。

不足之處及沒有遵守有關規定的情況

18. 在 55 名回應者中，有 11 名只對客戶交易進行人手檢視。鑑於它們當中有些經紀行的互聯網交易客戶眾多，每日均產生重大成交量，故單靠人手檢視並未能有效地識別可疑的未經授權交易。互聯網經紀行***應***顧及其互聯網交易業務的規模，並實施就其業務需要而言屬適當和相稱的監察及監督機制。

19. 55 名回應者中有 19 名只按月、按季或不定期進行監察及監督，這樣做不足以確保能及時偵測和採取跟進行動。互聯網經紀行***應***至少每天進行監察及監督。

20. 有三家被視察的公司在實施自動化的 IP 位址監察時，因網絡閘道器的不當設定而錯誤地將同一個通用的 IP 位址分配給來自不同的流動電話或網絡使用者的所有登入嘗試。互聯網經紀行***應***在實施自動化的 IP 位址監察工具前進行充分的技術測試和使用者測試。

良好作業方式

21. 有四名回應者已就偵測不尋常的作業方式或有問題的客戶交易開發並落實使用電腦輔助監察工具。當預設的參數或門檻被觸發或預設的交易模式（例如沽售客戶投資組合中的所有股票，以及利用沽售股票所得的款項按低於設定水平的價格買入小型股）被偵測出來時，這些工具便會發出實時警報。公司會定期檢視及適當地更新相關的參數及門檻。

22. 43 名回應者實施了入侵偵測系統（Intrusion Detection System，簡稱 IDS）以便監察網絡與系統，並在偵測到潛在威脅時向系統管理員發出警報。此外，一家被視察的公司安裝了可偵測及防止漏洞被利用的入侵防禦系統（Intrusion Prevention System，簡稱 IPS）。

23. 互聯網經紀行***應***考慮上述多項作業方式，藉以適當地改善其互聯網交易系統。

立即通知客戶

基本規定——第 1.3 段

持牌人應在客戶的互聯網交易帳戶出現某些客戶活動後，立即通知有關客戶。除了例外情況[9]外，客戶可選擇不收取“執行交易”或“登入系統”的通知，但不可以不收取重設密碼的通知。

不足之處及沒有遵守有關規定的情況

24. 48 名回應者沒有在客戶的互聯網交易帳戶出現某些行動，如重設密碼後通知客戶。互聯網經紀行須檢視客戶通知所涵蓋的活動，以確保符合《網絡保安指引》第 1.3 段的規定。

[9] 客戶在《網絡保安指引》第 1.3 段所訂明的情況下，可選擇不收取“執行交易”的通知。客戶在符合證監會有關網絡保安的《常見問題》所載的條件後，可選擇不收取“登入系統”的通知：https://www.sfc.hk/web/TC/faqs/intemediaries/supervision/cybersecurity/cybersecurity.html。

25. 另外，在上述的 48 名回應者中，有兩名容許客戶選擇在重設密碼後不收取通知，而其中一名亦容許客戶同時選擇不收取登入系統及執行交易的通知。證監會提醒互聯網經紀行：

(a) 不得容許客戶選擇不收取重設密碼的通知；及

(b) 只能在證監會所規定的例外情況下，容許客戶選擇不收取登入系統或執行交易的通知。

數據加密

基本規定——第 1.4 段

持牌人應以強效的加密程式：

(a) 將敏感資料，例如客戶登入資料（即使用者名稱和密碼）及交易數據，在內部網絡與客戶裝置之間傳輸時加密；及

(b) 保護儲存於其互聯網交易系統的客戶登入密碼。

不足之處及沒有遵守有關規定的情況

26. 有七家被視察的公司所實施的數據加密程式並不符合國際保安標準[10]。使用不嚴謹的加密程式增加資料外洩和系統性能受損的風險。互聯網經紀行***應***持續檢視國際保安標準（例如 NIST[11]提供的加密標準），查核其數據加密程式的狀況，及在適當時將其升級。

良好作業方式

27. 19 名回應者在雜湊程式中使用加鹽技術（salting）[12]，為密碼儲存提供額外保障。互聯網經紀行***應***考慮此作業方式，藉以適當地改善其互聯網交易系統。

保護客戶的登入密碼

基本規定——第1.5段

持牌人應訂立並實施有效的政策及程序，以確保在啟動帳戶及重設密碼的過程中，客戶的登入密碼是在安全的環境下產生及發送給客戶的。客戶的登入密碼應由系統隨機產生，及透過不受人為干預及不會被持牌人的職員竄改的溝通途徑發送給客戶。

若客戶的登入密碼並非由系統隨機產生，持牌人應實施足夠的保安監控措施以作彌補，例如強制客戶在啟動帳戶後首次登入時更改密碼。

不足之處及沒有遵守有關規定的情況

[10] 在網絡保安檢視期間識別到的不嚴謹的加密程式的例子包括：
(i) 就數據傳輸而言：SSL 3.0、TLS 1.0、TLS 1.1 及 TLS_RSA_WITH_RC4_128_MD5
(ii) 就數據儲存而言：DES、3DES、RC4、RC5、RSA 1024-bit、Blowfish、Twofish、MD5 及 SHA-1

[11] 美國國家標準與技術研究院（National Institute of Standards and Technology）。

[12] 雜湊程序被加鹽（salt）後會提升雜湊值的獨特性及複雜程度，從而可進一步紓減密碼被攻擊的風險。

28. 兩名回應者並無隨機產生客戶的登入密碼或沒有強制要求客戶在首次登入互聯網交易系統時更改密碼。互聯網經紀行須確保客戶的登入密碼是隨機產生的，或已實施足夠的保安監控措施以作彌補。

<u>嚴格的密碼政策及網頁超時監控措施</u>

基本規定——第 1.6 段

持牌人應在其互聯網交易系統內設立嚴格的密碼政策及網頁超時監控措施，包括：

(a) 最短的密碼長度；

(b) 向長期未更改密碼的客戶發出定期提示；

(c) 最低的密碼複雜程度（即同時包含字母與數字），及重用舊密碼前須更改密碼的次數；

(d) 針對無效的登入嘗試採取適當的監控措施；及

(e) 網頁在閒置一段時間後被設定為已超時。

<u>不足之處及沒有遵守有關規定的情況</u>

29. 六家被視察的公司的密碼政策沒有：

(a) 規定向長期未更改密碼的客戶發出定期提示；

(b) 訂明足夠的密碼複雜程度（即同時包含字母與數字）或有關重用舊密碼的限制；或

(c) 針對無效的登入嘗試設立適當的監控措施。互聯網經紀行須檢視密碼政策，藉以確保符合《網絡保安指引》第 1.6 段的規定。

30. 另外，有九家被視察的公司的網頁超時監控功能可被客戶關掉或其閒置時限可長達 24 小時。這情況並不理想，原因是當攻擊者有無限或過長的時間作出入侵嘗試時，在未經授權下接達帳戶的風險便會增加。互聯網經紀行***應***：

(a) 不容許客戶關閉網頁超時監控功能；及

(b) 限制閒置超時時限（例如在 30 分鐘以內），但須事先作出評估及持續進行監察。舉例來說，進行程式買賣的客戶可能需要交易帳戶處於備用狀態以便隨時執行交易。在此情況下，互聯網經紀行可容許較長的閒置超時時限，但必須更緊密地監察該客戶的登入和登出紀錄及交易活動。

31. 一家被視察的公司因技術性錯誤而導致其網頁超時監控措施無法啟動。客戶的互聯網交易帳戶在超出設定的超時時限後沒有被中斷連接。互聯網經紀行***應***進行充分的測試，以確保網頁超時監控措施妥為設定及運作。

基礎設施保安管理

配置安全的網絡基礎設施

基本規定——第 2.1 段

持牌人應透過妥善的網絡隔離措施（即設有多重防火牆的隔離區）來配置安全的網絡基礎設施，以保護關鍵系統（例如互聯網交易系統及交收系統）及客戶數據免受網絡攻擊。

不足之處及沒有遵守有關規定的情況

32. 兩家被視察的公司將寄存互聯網交易應用程式和其他關鍵系統的系統伺服器和數據庫存置於隔離區內，相對於將伺服器和數據庫中存置於隔離區後的內部網絡而言，這做法較為不安全。此外，有另外兩家公司將一般用作寄存公司網頁或其他敏感度較低的數據的網絡伺服器設置於內部網絡內。互聯網經紀行***應***：

    (a) 將互聯網交易應用程式和其他關鍵系統設置於隔離區後的內部網絡內；及

    (b) 將儲存敏感度較低的數據的伺服器（例如寄存公司網頁的網絡伺服器）寄存於隔離區內。

良好作業方式

33. 全部被視察的公司皆已在網絡基礎設施中，設置不同品牌及型號的多重防火牆。

34. 七家被視察的公司已實施打擊分散式阻斷服務攻擊機制，例如流量清洗服務及打擊分散式阻斷服務攻擊的紓減解決方案。一家公司亦已採用網絡異常偵測（Network Based Anomaly Detection）解決方案，以追蹤關鍵的網絡特徵及偵測異於正常網絡行為基準的事件或趨勢。

35. 40 名回應者採納打擊進階持續性威脅解決方案及網絡應用程式防火牆。

36. 互聯網經紀行***應***考慮上述多項作業方式，藉以適當地改善其互聯網交易系統。

使用者接達管理

基本規定——第 2.2 段

持牌人應設有政策及程序，以確保只容許有需要的人士接達或使用系統。此外，持牌人應至少每年檢視使用者有權接達的關鍵系統（例如互聯網交易系統及交收系統）及數據庫（例如客戶數據）的列表，以確保只有獲核准且有需要的人士方可接達或使用系統。

不足之處及沒有遵守有關規定的情況

37. 兩家被視察的公司在接達關鍵系統及數據庫方面，給予了使用者過多的權利。其中一家公司沒有就授予使用者接達權實施足夠的程序，例如負責風險管理的員工獲授予輸入買賣盤功能的接達權。另一家公司容許員工在離職後繼續接達系統。互聯網經紀行須至少每年對使用者接達的情況進行檢視，以確保只容許有需要的人士獲授並保留接達權。

良好作業方式

38. 17 名回應者實施特權身分管理（Privileged Identity Management，簡稱 PIM）或特權接達管理（Privileged Access Management，簡稱 PAM）解決方案，以便管理及監察在資訊科技環境內的高度特權接達的情況（例如超級使用者或管理員）。

39. 一家被視察的公司就使用者接達重新認證實施自動化程序，據此所有使用者接達權每年皆會由業務部門的直屬主管及資訊科技管理員重新認證。

40. 互聯網經紀行***應***考慮上述多項作業方式，藉以適當地改善其互聯網交易系統。

遙距連接的保安監控措施 [13]

> 基本規定——第 2.3 段
>
> *持牌人應只容許有需要的人士遙距接達其內部網絡，並對遙距接達實施保安監控措施。*

不足之處及沒有遵守有關規定的情況

41. 七名回應者向供應商授出隨時適用的永久的遙距接達權。互聯絡經紀行***應***避免向外界人士授出永久的遙距接達權。

良好作業方式

42. 28 名回應者就接達特權帳戶或敏感數據庫的僱員、供應商及使用者的遙距接達實施多重認證（至少有雙重認證）。

43. 42 名回應者只容許經由提供額外保安措施的虛擬私有網絡進行遙距接達。

44. 互聯網經紀行***應***考慮上述多項作業方式，藉以適當地改善其互聯網交易系統。

修補管理

> 基本規定——第 2.4 段
>
> *持牌人應及時監察和評估軟件提供者發布的保安修補程式或修正程式，並視乎對影響進行的評估，在切實可行的情況下盡快進行測試，並在測試完成後一個月內執行該等程式。*

[13] 有關進一步指引，請參閱題為“與遙距工作安排相關的網絡保安風險管理”的通函。有關通函可於以下網頁瀏覽：https://www.sfc.hk/edistributionWeb/gateway/TC/circular/intermediaries/supervision/doc?refNo=20EC37

不足之處及沒有遵守有關規定的情況

45. 六家被視察的公司花了較長時間（即超過六個月）來評估、測試及執行保安修補程式及修正程式，包括被列為關鍵或極度嚴重的保安修補程式及修正程式。一家公司直到 2019 年 5 月才執行於 2016 年至 2018 年期間發布被列為關鍵的保安修補程式。互聯網經紀行***應***盡快識別及執行急需的保安修補程式或修正程式。

46. 另外有兩家被視察的公司每六個月一次，分批進行所有保安修補程式及修正程式的評估、測試及執行工作。這種方式可能導致關鍵的保安修補程式及修正程式被延誤執行。互聯網經紀行***應***只批量執行非關鍵的保安修補程式或修正程式，及至少每季批量執行一次這些程式，除非經評估後斷定該等程式可能與系統應用程式不相容，故無法執行。

47. 此外，有兩家被視察的公司採用了使用期完結的軟件[14]。鑑於供應商不再為使用期完結的軟件提供保安修正程式服務，網絡及系統漏洞可能會遭黑客利用。互聯網經紀行***應***持續和及時監察現有軟件的有效性，並將使用期完結或接近完結的軟件予以替換或升級，藉以確保其使用的軟件獲供應商支援。

48. 持牌人***應***及時評估軟件提供者發布的保安修補程式或修正程式，識別並即時執行那些急需用來處理被列為關鍵或極度嚴重的漏洞及隱憂的保安修補程式或修正程式[15]。持牌人也***應***在合理的時限內，執行並非急需的保安修補程式或修正程式。

端點保護

基本規定——第 2.5 段

持牌人應及時執行和更新防毒及抗惡意軟件解決方案，以偵測關鍵系統伺服器及工作站內的惡意應用程式及惡意軟件。

不足之處及沒有遵守有關規定的情況

49. 四名回應者沒有在所有關鍵伺服器上安裝防毒或抗惡意軟件解決方案，而一名回應者沒有在所有關鍵工作站內安裝抗惡意軟件。本會提醒互聯網經紀行在所有關鍵系統伺服器及工作站內安裝這類解決方案。

系統及數據備份

基本規定——第 2.8 段

持牌人應至少每天將其業務紀錄、客戶及交易數據庫、伺服器及證明文件在離線媒體進行備份。

[14] 指的是使用期已告結束，並且供應商已停止就其提供支援的軟件（例如 Windows 伺服器 2008）。

[15] 可參考國家漏洞數據庫（National Vulnerability Database），當中載有 NIST 提供的常見漏洞的嚴重程度排序。詳情請參閱 https://nvd.nist.gov/vuln-metrics/cvss。

持牌人亦應採納適當的恢復方法，使重大系統變更得以成功還原。

不足之處及沒有遵守有關規定的情況

50. 根據網絡保安調查結果：

(a) 一名回應者只是每月進行一次備份；及

(b) 六名回應者沒有備份到離線媒體。

51. 本會提醒互聯網經紀行，至少每天將其業務紀錄（除其他資料外）在離線媒體進行備份。

良好作業方式

52. 七家被視察的公司至少每年對備份紀錄進行一次復原測試，以確保數據恢復的有效性。互聯網經紀行*應*考慮這種作業方式，藉以適當地改善其互聯網交易系統。

網絡保安情境的應變計劃

基本規定——第 2.9 段

持牌人應盡一切合理努力，使其業務延續計劃及危機管理程序涵蓋可能出現的網絡攻擊情境（例如分散式阻斷服務攻擊），及業務紀錄和客戶數據因網絡攻擊（例如勒索軟件）而完全損毀的情況。

不足之處及沒有遵守有關規定的情況

53. 兩名回應者的業務延續計劃沒有涵蓋數據洩漏及勒索軟件之類的網絡保安情境。本會提醒互聯網經紀行，應在其業務延續計劃及危機管理程序中涵蓋可能出現的網絡攻擊情境。

網絡保安管理及監督

網絡保安管理層的角色及責任

基本規定——第 3.1 段

互聯網交易負責人員應設定網絡保安風險管理框架（包括但不限於政策及程序），及列明主要角色及某些訂明的責任。

不足之處及沒有遵守有關規定的情況

54. 在 55 名回應者當中：

(a) 兩名回應者沒有任何指定人員或委員會負責其網絡保安管理；

(b) 21 名回應者沒有設定《網絡保安指引》第 3.1 段所規定的全部角色及責任；

(c) 一名回應者指定了負責其網絡保安管理的人員，但沒有設定該人與其網絡保安管理框架有關的角色或責任；

(d) 12 名回應者僅非正式地設定了網絡保安管理框架，但沒有任何文件紀錄；

(e) 11 名回應者僅不定期進行資訊科技審查或網絡保安自我評估；及

(f) 26 名回應者沒有在其資訊科技審計或自我評估中充分涵蓋有關的基本規定。

55. 本會提醒互聯網經紀行清晰地設定負責網絡保安風險管理的指定委員會、營運部門或人員的角色及責任。互聯網經紀行***應***至少每年在其資訊科技審查或網絡保安評估過程中檢視其遵守基本規定的情況。

良好作業方式

56. 24 名回應者在過往的 18 個月內進行了滲透測試（即確定哪些系統和數據可能被黑客透過利用網絡及應用程式漏洞來接達的過程）。

57. 14 名回應者就網絡保安事故投購了保險。

58. 一家被視察的公司建立了保安運作中心（Security Operations Center，簡稱 SOC）[16]，負責所有保安監察程序及技術，並協調有關事故的偵測及處理工作。

59. 另一家公司進行了差距分析，將其全球網絡保安程序及作業方式與基本規定及香港的其他有關規定進行比較。

60. 互聯網經紀行***應***考慮上述多項作業方式，藉以適當地改善其互聯網交易系統。

網絡保安事故報告

基本規定——第 3.2 段

持牌人應訂立書面政策及程序，訂明懷疑或確實的網絡保安事故應以何種方式上報及向內（例如負責互聯網交易的負責人員）和向外（例如客戶、證監會及其他執法機構（如適用））報告。

不足之處及沒有遵守有關規定的情況

61. 三名回應者沒有設立上報及報告懷疑或確實的網絡保安事故的程序。此外，一家被視察的公司的互聯網交易系統曾在整個上午交易時段出現運行中斷的情況。但是，該公司沒有透過電郵或公司網站等方式知會客戶系統已中斷，或在中斷期間可使用的替代交易途徑。

[16] 保安運作中心是集中監察、評估及保衛公司的資訊科技系統和基礎設施，並就網絡保安事故作出應對的部門。

62. 本會提醒互聯網經紀行制定書面政策及程序，以在切實可行的情況下盡快上報事件並向內部及外部各方報告。

良好作業方式

63. 38 名回應者在識別到可能或確實發生了未經授權接達客戶的互聯網交易帳戶的情況後，會暫時關閉客戶帳戶，並通知相關客戶、監管機構及香港警方。互聯網經紀行***應***考慮這種作業方式，藉以適當地改善其互聯網交易系統。

內部系統使用者的網絡保安意識培訓

基本規定第 3.3 段——

持牌人應至少每年向所有內部系統使用者（即，任何可接達該持牌人的內部網絡和系統的常額職員及合約職員）提供足夠的網絡保安意識培訓。

不足之處及沒有遵守有關規定的情況

64. 有兩名回應者沒有提供任何形式的網絡保安意識培訓。有 18 名回應者沒有為其內部系統的所有使用者提供網絡保安意識培訓。另外，有八家被視察的公司的年度網絡保安意識培訓只有部分內部系統使用者參加，並且沒有對未參與培訓的人採取跟進行動。

65. 本會提醒互聯網經紀行，至少每年為所有內部系統使用者提供一次網絡保安意識培訓。

向客戶發出網絡保安警示及提示

基本規定——第 3.4 段

持牌人應採取一切合理步驟，就網絡保安風險及有關使用互聯網交易系統的建議預防和保護措施向客戶發出提示及警示。

不足之處及沒有遵守有關規定的情況

66. 44 名回應者沒有定期向其客戶提供網絡保安提示。本會提醒互聯網經紀行採取合理的步驟，向客戶提供足夠的網絡保安警示及提示。

良好作業方式

67. 43 名回應者訂閱了網絡保安威脅情報服務，將有關網絡攻擊及漏洞的最新資訊加以分析並與客戶共享。互聯網經紀行***應***考慮這作業方式（如適當），以改善其互聯網交易系統。

D. 流動交易應用程式——遵守《操守準則》規定的情況

68. 我們在網絡保安實地視察中注意到，有十家被視察的公司雖然向其客戶提供了流動交易應用程式，但其中一些公司沒有採取充足或適當的預防或偵測性監控措施來保護其互聯網交易系統。

> 《操守準則》的規定[17]
>
> *持牌人應採取充足及適當的保安監控措施，以保護其使用或提供予客戶使用的電子交易系統免被濫用。保安監控措施應至少包括：*
>
> *(a) 可靠的技術，藉以認證或核實系統使用者的身分及權限，確保只有獲核准的有需要人士方可接達或使用系統；*
>
> *(b) 有效的技術，藉以確保儲存在系統內及在內部與外間網絡之間傳遞的資料的保密性及完整性；*
>
> *(c) 適當的運作監控措施，藉以防止及偵測未經授權的入侵、違反保安事件及對安全性的攻擊；及*
>
> *(d) 適當的步驟，藉以提升系統使用者對使用系統時需採取保安預防措施的重要性的意識。*

不足之處及沒有遵守有關規定的情況

<u>偵測性監控措施</u>

69. 六家被視察的公司沒有在流動交易應用程式中執行任何監控措施，以偵測被破解的裝置（即遭“越獄”[18]或被“root”的流動裝置[19]），並阻止流動交易應用程式在這些裝置中使用。互聯網經紀行*應*偵測並阻止被破解的裝置登入其互聯網交易系統。

<u>預防性監控措施</u>

A. 原始碼

70. 五家被視察的公司的原始碼（涵蓋其流動交易應用程式中所有功能）可輕易地被找到和易於理解。其中一家公司的原始碼亦公開了互聯網交易伺服器的資料。由於此類資料易於取覽，故流動交易應用程式可能遭黑客修改及重新包裝，藉以繞過內置的保安監控程式（例如對被破解的流動裝置的偵測）。此外，經修改及重新包裝的流動交易應用程式可能繼續運行並與這些公司的內部網絡保持連接。黑客甚至可將重新包裝及修改過的應用程式發布到互聯網論壇或留言板以供他人下載。如果客戶下載及使用這些應用程式，所有內置的保安監控程式便

---

[17] 《操守準則》附表 7 第 1.2.4 段。

[18] *越獄*（Jailbreaking）是修改 Apple 操作系統以移除軟件限制，以利便安裝惡意軟件的過程。

[19] 英文是“*Rooting*”，這是一個允許採用Android流動操作系統的智能手機、平板電腦及其他裝置的使用者獲得多個Android子系統的最高權限管控權（稱為“root權限”）的過程。

可能被移除，並且無法安裝最新的保安修補程式或修正程式。互聯網經紀行*應*模糊其原始碼以加強保護，避免其遭到潛在的惡意利用。

71. 三家被視察的公司的流動交易應用程式中存在一些沒有使用的程式碼庫或模組。這增加了緩衝區溢位攻擊的風險，使黑客得以利用程式空間來安裝惡意軟件。互聯網經紀行*應*將沒有使用的程式碼庫或模組從原始碼中清除。

B. 儲存在使用者裝置內的敏感資料

72. 六家被視察的公司的流動交易應用程式中有“記住密碼”、“自動填寫”及“自動完成”等功能，容許客戶的敏感資料被儲存（即緩存）在流動裝置中，而有關資料不會在客戶登出後從系統進程記憶體中被刪除，增加了有關資料被黑客存取以嘗試進行未經授權的登入的風險。互聯網經紀行*應*在客戶一旦離開安裝於其流動裝置內的互聯網交易應用程式或登出其互聯網交易帳戶後，將客戶的敏感資料從這些應用程式中清除。

C. 生物特徵認證

73. 一家被視察的公司的生物特徵認證（包括指紋及人臉識別）不會在客戶多次登入嘗試失敗後被停用。另外，只要在流動裝置的紀錄中添加額外的指紋或更改人臉圖像，便可在沒有妥善驗證的情況下，獲准以生物特徵認證登入。互聯網經紀行*應*收緊保安監控措施，例如：

(a) 若客戶希望添加或修改儲存在其流動裝置紀錄中的生物特徵數據，規定客戶須解除其生物特徵認證，並在經過核實後重新註冊；及

(b) 限制認證失敗的次數。