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

SFC
證監會

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總結

2017 年 10 月

目錄

摘要

1. 2017 年 5 月 8 日，證券及期貨事務監察委員會（**證監會**）發出一份《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》（**《諮詢文件》**），邀請公眾就 (a) 對《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》**）的建議修訂及 (b) 建議新訂的《降低及紓減與互聯網交易相關的黑客入侵風險指引》（**《指引》**）（統稱**有關建議**）發表意見。

2. 於在 2017 年 7 月 7 日結束的諮詢期內，證監會共接獲 36 份來自各個業界組織、專業團體、消費者委員會、經紀行、律師事務所、服務提供者及個別人士的書面意見。

3. 證監會已對回應作出詳細考慮，並在諮詢外部網絡保安專家[1]後修訂有關建議。本文件載述證監會對有關建議的總結及就接獲的意見所作出的回應。《諮詢文件》內的主要建議已獲得廣泛支持。鑑於《諮詢文件》所載述的理由及考慮到有關建議獲得大多數的支持，證監會認為只需要作出少許修改或澄清，便能處理以下的關注事項。

   (a) 數名回應者指出，由於建議的監控措施是為較小型互聯網經紀行而設計的基本入行規定，它們可能並不適用於使用非常精密的系統及監控措施的較大型互聯網經紀行。某些回應者亦提議《指引》應減少規範性的條文，並讓互聯網經紀行採納以風險為本的方針，決定哪些監控措施是與他們的網絡保安風險相稱。

   我們維持原有的意見，即這些基本規定對所有互聯網經紀行（特別是較小型互聯網經紀行）來說都是必要的，以降低及紓減黑客入侵風險。儘管如此，我們注意到也許可以採取不同的途徑以達到整體的目標。就此而言，我們在與本總結文件一併發出的有關《指引》的常見問題（**常見問題**）內，指明在特定情況下無須嚴格遵守一項監控措施（詳情請參見下文分段(b)）。

   另外，我們同意《指引》應屬通用性質，使內容不易因科技的發展而變得過時。因此，某些建議的監控措施已作出輕微修訂以提供更大的靈活性。除了一些隨著時間變遷仍持續有效的說明例子外，我們已刪除《指引》內的其他例子。然而，我們已在常見問題中列舉實例，就實施《指引》提供更多的指導。

   (b) 某些回應者提議，隨著在客戶登入互聯網交易帳戶的程序實施雙重認證，客戶應能在每次登入系統時選擇不收取即時通知。儘管我們仍然認為發出通知是有效的偵測性監控措施並應被納入《指引》內，但我們認同若互聯網經紀行能通知客戶不尋常的登入情況（例如某客戶似乎並非透過其慣常使用的裝置登入），則未必需要嚴格遵守每次登入系統時收取即時通知的規定。

   有見及此，我們已在常見問題內載述互聯網經紀行在哪些特定情況下可讓客戶選擇不收取登入系統通知及須符合的條件。

   (c) 我們了解對某些互聯網經紀行來說，六個月可能並不足夠實施全部所需的監控措施。就此而言，互聯網經紀行須在六個月內實施雙重認證，除此以外，他們現獲准以九個月的時間落實其他所有監控措施。

[1] 請參閱《諮詢文件》以了解更多有關外部網絡保安專家的資料。

(d) 我們接獲涉及技術層面的其他意見及提議（例如修補管理及多次嘗試登入後封鎖帳戶），並已按情況所需對建議的《指引》作出修改。

4. 《操守準則》及《指引》的修訂分別載於**附錄 A** 及**附錄 B**[2]內。除了實施雙重認證的規定會於發出本文件日期的六個月後生效外，《操守準則》及《指引》的修訂均會於發出本文件日期的九個月後生效。 我們謹此向所有投放時間和精力審閱有關建議及向我們提供詳盡周全意見的回應者表示謝意。回應者的名單（要求不記名的回應者除外）載於**附錄 C**，而有關意見的全文可在證監會網站 www.sfc.hk 取覽。

接獲的意見及我們的回應

I. 諮詢問題

問題 1：證監會認為應將建議的監控措施訂為基本規定，而這些規定亦將作為潛在互聯網經紀行加入業界所須符合的要求。你是否贊同上述做法？

公眾意見

6. 23 名回應者當中有 22 名回答支持這項建議，而一名回應者偏好以風險為本的做法，讓互聯網經紀行按其網絡保安風險狀況選取他們所需的網絡保安監控措施。

7. 此外，數名其他回應者指出由於建議的監控措施是為較小型互聯網經紀行而設計的基本入行規定，故某些建議的監控措施，特別是對沿用非常精密的系統及牽涉到其他業務的監控措施的較大型互聯網經紀行來說，是過於規範及難以遵循。

我們的回應

8. 鑑於得到大多數回應者的支持，我們維持原有的意見，即應保留建議的監控措施作為適用於所有互聯網經紀行的基本規定。儘管我們明白以風險為本的做法的益處，但鑑於較小型互聯網經紀行可能沒有資源或能力設立自己的網絡保安風險管理框架，故我們認為向整體互聯網經紀行業以清晰且不含糊的方式闡述我們的期望，更為重要。另一方面，我們知道《指引》內的某些部分可能會為使用截然不同的系統、基礎設施及監控措施的互聯網經紀行帶來實行上的困難，且亦有其他的途徑可達到理想的目標。因此，我們已在常見問題中指明，當符合某些條件的互聯網經紀行在識別到不尋常的登入時（並非在每次登入後）向客戶發出通知的做法是可以接受的（詳見第 40 至 45 段）。

9. 我們謹此重申《指引》的原意只是設立最低標準，並非鉅細無遺。互聯網經紀行的高級管理層應確保所有系統及監控措施與公司的業務營運及需求相稱，並視乎需要實施額外的網絡保安監控措施。如有需要，可尋求解決方案提供商或技術顧問的協助。

[2] 對建議的《指引》內的監控措施所作出的修訂已在附錄 B 以標示形式顯示。

問題 2：《操守準則》第 18 段及附表 7 的適用範圍將擴大至涵蓋就並非在交易所上市或買賣的證券進行的互聯網交易。你是否贊同，建議將監管範圍擴大至互聯網交易是適當的做法？如是的話，建議的用詞是否已夠清晰？

公眾意見

10. 23 名回應者當中有 18 名回答同意就並非在交易所上市或買賣的證券進行的互聯網交易亦應包括在內，原因是這些交易與就在交易所上市或買賣的證券進行的互聯網交易存在著相同的漏洞，一樣容易遭到網絡入侵。

11. 三名回應者因下列原因，對涵蓋就並非在交易所上市或買賣的證券表示關注：

    (a) 黑客在非交易所上市或買賣的證券交易進行市場操控活動（如“唱高散貨的騙局”）的固有風險相對較低；及

    (b) 用作買賣非上市集體投資計劃的帳戶的黑客入侵風險非常低，故可能並不需要涵蓋使用互聯網交易系統讓客戶認購、贖回及轉換集體投資計劃的投資的資產管理公司。

    一名回應者提議應對就並非在交易所上市或買賣的證券進行的互聯網交易，施加能反映其獨特性質及相關風險的其他不同規定。

12. 兩名回應者要求列出有關建議所涵蓋的證券。

13. 此外，四名回應者提議將監管範圍擴大至所有金融產品、業界所用的全部資訊系統或其他類型的電子交易，如直達市場安排及程式買賣。

我們的回應

14. 如在《諮詢文件》所闡述，互聯網交易遭受黑客入侵似乎是本港持牌法團所面對最嚴重的網絡保安風險。因此，我們維持原有的意見，即在設立基本規定時應把焦點放在處理上述風險方面。

15. 我們知道，就並非在交易所上市或買賣的證券進行的互聯網交易遭受黑客入侵的風險和影響可能較低。然而，由於兩者仍面對著相同類型的網絡威脅及漏洞，故我們並不認為把規定局限於在交易所上市或買賣的證券是審慎的做法。

16. 另外，我們認為無需訂立一份名單列出有關建議所涵蓋的證券；有關建議中“證券”的定義應沿用《證券及期貨條例》附表 1 內對“證券”的定義。

問題 3：為了向經紀行提供彈性處理的空間，以便其可針對黑客入侵風險採取額外保障措施，建議的規定不會訂明特定的雙重認證解決方案。你是否同意這是適當的做法？

公眾意見

17. 27 名回應者當中有 22 名回答支持強制互聯網經紀行實施雙重認證。一名回應者認為，證監會把焦點放在多重認證作為一項關鍵的保安監控措施的重要性上是正確的做法；而另一名回應者則相信由於登入程序是對網絡攻擊的第一度防線，故實施雙重認證將大幅加強對客戶的保障。

18. 同一組的回應者支持不訂明特定的雙重認證解決方案，並提出以下的意見：

(a) 這做法既能劃一所有互網聯經紀行的登入保安水平，亦不會為較小型互聯網經紀行在營運及財政上帶來不公平的負擔；

(b) 這做法消除了互網聯經紀行為爭奪尋求方便及快捷地執行交易而不使用雙重認證解決方案的客戶而進行的任何不良競爭。本會提供的靈活性也讓互聯網經紀行選擇最具成本效益及切合他們的業務模式的雙重認證解決方案；及

(c) 從客戶的角度而言，無論他們選擇哪一家互聯網經紀行，這做法都能提供劃一的保安水平。

19. 另一方面，一名回應者提議證監會應訂明使用硬件或軟件編碼器，及三名回應者倡議使用生物特徵識別技術，但對使用短訊傳送一次性密碼，則有保留。詳情請參閱下文第 32 及 33 段。

我們的回應

20. 我們歡迎回應者整體上支持強制使用雙重認證的建議。證監會知道有多種雙重認證解決方案，且各有優點和缺點；當中某些可能會隨著時間過去而變得不合時宜或無效。因此，我們維持原有的意見，即應讓互聯網經紀行根據他們的個別情況自由選擇合適的雙重認證解決方案。為免生疑問，《諮詢文件》的附錄 D 載有的例子僅供參考，而《指引》將不會載述具體的雙重認證解決方案的例子。

問題 4：你是否同意，考慮到實際情況，強制要求監察可疑的交易模式並非適當的做法？

公眾意見

21. 22 名回應者當中有 18 名回答同意監察可疑的交易模式應該只納入為行業良好作業方式，而有四名回應者則提議強制要求這類監控措施。

我們的回應

22. 與大多數回應者的看法一致，監察可疑的交易模式將會成為一項良好作業措施。

問題 5：基於成本因素，有關建議並無規定互聯網經紀行須評估及優化其後備設施（即災難復原中心），以在緊急情況下提供互聯網交易服務或接收客戶交易指令的替代安排，從而避免出現不可接受的服務中斷。你是否贊同上述做法？

公眾意見

23. 21 名回應者當中有 16 名回答同意這做法，有一名回應者列舉對後備設施作出全面評估或測試所需投放的精力及開支。另一名回應者認為維持全面運作的後備設施並不符合成本效益。我們亦接獲以下的其他意見和提議：

(a) 鑑於目前的網絡風險環境，訂立健全的後備及復原計劃是非常重要的。如在其他地區所見，若未能確保應變計劃已進行測試及有效，或沒有訂立合適的網絡應對計劃，這對機構及客戶來說都可能是重大的風險。證監會應按照行業良好作業方式提供一系列指引；及

(b) 應強制要求設立基本後備設施及提供處理客戶交易指令的替代安排，尤其是為希望在緊急情況下平倉的客戶而設的安排。

我們的回應

24. 現時在《操守準則》[3]下有規管系統的充足性的規定（包括應變措施）。尤其是，互聯網經紀行須確保定期測試應變計劃，以及有關計劃是可行及足夠的。為了確保應變措施能妥善處理潛在的網絡保安情境，建議的《指引》規定互聯網經紀行須在他們的應變計劃及危機處理程序加入遭受網絡入侵的情境。然而，這並不代表所有互聯網經紀行必須設立一個災難復原中心作為處理客戶要求的替代安排，或應對他們的後備設施作出正式的評估，或進行演習。就較小型互聯網經紀行而言，某些替代安排，例如使用電話熱線處理客戶交易指令和查詢及保留足夠的紀錄以追蹤每項客戶交易指令的狀況，可能已經足夠。

問題 6：你認為，你的服務提供者目前提供的服務水平能否使你遵守建議的基本規定？你預期，與你的服務提供者磋商更高的服務水平會否有任何困難？

公眾意見

25. 18 名回應者當中有 13 名回答確認他們的服務提供者目前提供的服務水平能符合建議的基本規定。一名回應者同意將維修保養及技術協助的可量化規定編纂成為基本規定，以在互聯網經紀行之間營造一個公平的競爭環境。另一方面，少數回應者預期在磋商更高的服務水平時會遇到困難或需支付額外費用。

我們的回應

26. 基於所接獲的回應，我們預期互聯網經紀行將有能力磋商更高的服務水平。然而，業界組織可以考慮利用他們強大的議價能力及以集體方式與服務供應商磋商條款及費用水平。

II. 特定的基本規定

27. 整體而言，回應者對建議的基本規定有不同意見。某些回應者認為建議的監控措施並不足夠，而其他回應者則提議證監會對某些監控措施作出闡明。例如：

(a) 少數回應者表示某些建議的監控措施不夠強大，並提議多項改良措施以加強對黑客入侵風險的防範。某些回應者認為，鑑於適度且健全的後備及復原計劃在緊急情況下是不可或缺的，互聯網經紀行必須評估及改良他們的後備設施（這並非建議的監控措施之一）；及

(b) 在雙重認證解決方案方面，某些回應者倡議使用生物特徵識別技術，並警告避免使用短訊傳送一次性密碼。

鑑於我們即時的目標是設立基本規定，我們擬把這些就改良建議的監控措施而提出的有用提議，反映於我們在日後發出的有關良好作業方式的通函內。

28. 20 項建議的基本規定當中有 11 項接獲極少或並無接獲回應者的意見。其中包括：

- 保護客戶的登入密碼（《指引》第 1.5 段）
- 配置安全的網絡基礎設施（《指引》第 2.1 段）

[3] 請參閱《操守準則》第 18.5 段及《操守準則》附表 7 第 1.2.7 段。

- 使用者接達管理（《指引》第 2.2 段）
- 遙距連接的保安監控措施（《指引》第 2.3 段）
- 端點保護（《指引》第 2.5 段）
- 在未經授權的情況下安裝硬件及軟件（《指引》第 2.6 段）
- 實體保安（《指引》第 2.7 段）
- 網絡保安管理層的角色及責任（《指引》第 3.1 段）
- 網絡保安事故報告（《指引》第 3.2 段）
- 內部系統使用者的網絡保安意識培訓（《指引》第 3.3 段）
- 向客戶發出網絡保安警示及提示（《指引》第 3.4 段）

29. 因此，除了《指引》第 3.3 段的輕微修訂之外，上文其他規定內的用詞將不作更改。《指引》第 3.3 段的修訂為培訓課程將涵蓋的範疇提供更大的靈活性，同時清楚說明互聯網經紀行在設計有關課程的內容時，應考慮他們所面對的網絡保安風險的類型及水平。

30. 下文將會討論就其他建議的基本規定所接獲的意見及證監會的相關回應。

1. 雙重認證（《指引》第 1.1 段）

公眾意見

31. 如上文第 17 段所述，大部分回應者都支持強制實施雙重認證的建議。然而，一名回應者認為，雙重認證可能會對客戶造成不便，例如有些客戶沒有智能手機或無法接收短訊（這是使用某些雙重認證解決方案的必要條件），並建議讓客戶可以在了解並確認相應風險的前提下，選擇不採用雙重認證。

32. 一些回應者認為，互聯網經紀行需要證監會提供清晰且可量化的指引，連同網絡保安行業提供的技術選項和情報。有三名回應者對使用短訊傳送一次性密碼的安全問題表示關注。其中一名回應者亦提到，曾有海外黑客假冒受害人以更改他們的短訊設定（例如與電信服務提供者設置短訊轉發），從而偷取一次性密碼短訊。

33. 此外，一名回應者提議生物特徵（即“客戶是誰”的雙重認証原則）的解決方案。另一名回應者指出，特定硬件的需求對有關方案並不會造成阻礙，因為現時已可透過流動裝置的前置相機，或筆記本電腦的網絡攝錄器，經面部識別進行可靠的認證。流動裝置上的指紋讀取器亦越來越普遍。

我們的回應

34. 我們知道雙重認證解決方案並非萬無一失，也會注意黑客誘騙客戶披露其登入資料的風險。此外，我們了解到使用者體驗的重要性，並在政策審議中對其加以考慮。由於雙重認證被廣泛認為是防止黑客入侵的有效認證機制，所以我們不贊同讓客戶選擇不進行雙重認證。證監會一直與投資者教育中心緊密合作，推出一系列網絡保安意識計劃，包括與實施

雙重認證有關的推廣活動。例如，我們於 2017 年 9 月在傳統及網絡媒體上刊載了一篇題為《保密不足招黑客》的文章[4]。

35. 鑑於(i)互聯網經紀行的規模、營運模式和財務能力各異；(ii)可供選用的各類雙重認證解決方案（例如可能由互聯網經紀行自行開發的硬件編碼器、軟件編碼器、一次性密碼短訊、生物識別裝置或等同裝置）在複雜性和價格方面亦各不相同；及(iii)科技迅速發展，故證監會仍然認為，應由互聯網經紀行自行選擇，採取那些匹配其安全基礎設施，及適合用來實現其風險紓減目標的解決方案。

36. 然而，根據公眾的意見，我們在常見問題中：

(a) 提醒互聯網經紀行在選擇雙重認證解決方案時，應評估及衡量不同雙重認證解決方案的特點、局限性和漏洞，並按情況所需制訂監控措施以作彌補。如有需要，應尋求解決方案提供者或技術顧問的協助；及

(b) 建議使用一次性密碼短訊的互聯網經紀行告誡其客戶不要設定短訊轉發。

2. 實施監察及監督機制（《指引》第 1.2 段）

公眾意見

37. 沒有回應者反對實施有效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的建議規定。然而，四名回應者對建議的《指引》中舉例的監察互聯網規約（internet protocol，簡稱 **IP**）地址的營運挑戰和有效性發表了意見，並建議不強制執行這項特定的監控措施。上述回應者解釋，多名客戶從同一個 IP 地址登入，可能是因合理理由所致，例如當他們為同一家公司工作並且共享一個外部 IP 地址以接達互聯網。

我們的回應

38. 證監會理解，監察 IP 地址與交易後的監督性監控措施類似，兩者都可能產生真實警示和虛假警報，但它仍可能是協助互聯網經紀行識別出明顯的違規行為以作跟進的有用工具。

39. 我們應當澄清，上述例子僅以提供說明的目的而被列入建議的《指引》中，並且已從《指引》中刪除。

3. 即時通知客戶（《指引》第 1.3 段）

公眾意見

40. 兩名回應者的意見指，當強制要求就系統登入實施雙重認證時，為每次系統登入發出額外通知的做法可能沒有必要。有人擔心客戶在收到太多通知的情況下，可能會失去警覺性甚至對通知視而不見；有些人甚至可能視它們為垃圾訊息。有人提出了替代方案，即客戶只會在互聯網經紀行留意到不尋常的登入情況（例如，並非透過客戶慣常使用的裝置登入）時才會收到系統登入通知。

41. 關於就“向第三方轉移資金”向客戶發出通知的建議規定，一名回應者認為，如客戶已就資金轉移的目的與其互聯網經紀行登記第三方帳戶，便無需實施這項規定。

[4] http://www.thechinfamily.hk/web/tc/tools-and-resources/hot-topics/keep-details-passwords-safe.html

42. 至於就“更改客戶和帳戶的相關資料”向客戶發出通知的建議規定，一名回應者認為有關通知的範圍可能過於廣泛（例如，涵蓋更改首選語言在內的非重要更改），並建議僅限於在更改用於接收保安相關資料的聯絡方式時才發出通知。

我們的回應

43. 雖然雙重認證被用作為主要的預防性監控工具，但它並非萬無一失；即時通知客戶是有效的偵測性監控措施，可與雙重認證互相補足。因此，我們維持原有的意見，即將即時就某些活動通知客戶的規定納入《指引》內。我們亦明白客戶不應收到太多通知，因此互聯網經紀行可向客戶提供不收取交易執行通知的選擇。

44. 關於系統登入通知的問題，根據向證監會匯報的黑客事件，有客戶在沒有登入系統的情況下卻收到系統登入通知，並就事件向互聯網經紀行發出警報，使經紀行能夠及時採取行動，防止黑客進行未經授權的交易。該做法是應被納入《指引》內的有效偵測性監控措施。然而，我們贊同，客戶如果收到不尋常登入的通知，便可能無需就每次系統登入收取通知。我們現已在常見問題中解釋，符合以下規定的互聯網經紀行讓客戶選擇不就每次系統登入收取通知，是可接受的做法：

(a) 互聯網經紀行有能力識別不尋常登入及就不尋常登入即時通知客戶；

(b) 互聯網經紀行向客戶作出了充分的風險披露，而客戶已確認他們了解選擇不就每次系統登入收取通知所涉及的風險；及

(c) 客戶沒有選擇不收取執行交易的通知。

45. 我們同意規定就“向未經登記的第三方轉移資金”發出通知，但我們不同意客戶只應在更改用於接收保安相關資料的聯絡方式的情況下接獲通知。就客戶和帳戶的相關資料（例如銀行帳戶詳情和個人資料）的更改通知客戶亦非常重要。

4. 數據加密（《指引》第 1.4 段）

公眾意見

46. 兩名回應者尋求釐清“端對端加密”和“內部網絡”的涵義，尤其是隔離區是否被視為內部網絡的一部分。

47. 四名回應者建議採用一些先進的加密解決方案，例如對登入密碼進行鹽值及單向散列加密，最好使用慢散列函数的加密程式來阻止暴力破解攻擊。

我們的回應

48. 證監會謹此澄清，就數據加密的規定而言，隔離區被認為是內部網絡的一部分，而這已被列入常見問題內。此外，經過進一步審議，我們將要求互聯網經紀行在內部網絡與客戶裝置之間傳輸敏感資料時，使用強效的加密程式將該等資料加密，並從建議的《指引》中刪除了“端對端加密”一詞，以避免混淆。

49. 證監會對與加密解決方案相關的建議，表示歡迎。根據《指引》，互聯網經紀行須“使用強效的加密程式”，並可根據情況自由決定使用哪種加密技術。我們會在日後的通函中建議採納一些先進的加密解決方案作為行業的良好作業方式。

5. 嚴格的密碼政策及網頁超時監控措施（《指引》第 1.6 段）

公眾意見

50. 所有回應者都承認需要設立嚴格的密碼政策及網頁超時監控措施。他們亦理解，建議的《指引》沒有指明最長的超時期限，互聯網經紀行可根據其業務模式和運作情況設定網頁超時限制。

51. 另一方面，兩名回應者提議從建議的《指引》中刪除“最長的密碼有效期限”的政策。一名回應者進一步辯稱，頻繁更改密碼可能迫使客戶將密碼寫下，從而增加資料洩露的風險。這名回應者建議制訂政策提醒長期未更改密碼的客戶更改密碼作為替代方案。另一名回應者指出，一些國際技術標準已不再建議採用此類監控措施。

52. 此外，一名回應者認為帳戶封鎖機制可能會助長分散式阻斷服務攻擊[5]，因此，強制採用“多次嘗試登入無效後封鎖帳戶”的密碼政策是不合適的；該名回應者轉而建議採用替代方案，例如增加無效登入嘗試之間的時間。

我們的回應

53. 我們接納上述兩項建議，並對《指引》作出以下修訂：

(a) 以“向長期未更改密碼的客戶發出定期提示”的政策取代“最長的密碼有效期限”的政策；及

(b) 以“針對無效的登入嘗試採取適當監控措施”的政策取代“多次嘗試登入無效後封鎖帳戶”的政策，以便互聯網經紀行可以設置自己的政策和監控措施，防止有人在未經授權的情況下接達客戶的互聯網交易帳戶。

6. 修補管理（《指引》第 2.4 段）

公眾意見

54. 回應者對執行保安修補程式或修正程式的建議時間表表示關注：

(a) 兩名回應者覺得一個月的時間不夠，特別是在測試和執行工作涉及第三方的某些情況下，例如當測試需要連接香港聯交所，或需在全球廣泛配置基礎設施且涉及在不同地點使用伺服器時。

(b) 一名回應者建議將時限延長至兩個月；及

(c) 另一名回應者強烈建議，在就不同漏洞的修補程式制訂執行時間表時，應根據與漏洞和資產類型（例如，業務關鍵系統和不太關鍵的系統）相關的風險，靈活地安排優先次序；此舉能適當分配資源於執行關鍵的修補程式，而不是用於修補低風險的漏洞。

我們的回應

55. 時間是有效修補管理的關鍵所在。以 WannaCry 為例，相關的修補程式於 2017 年 3 月發布，其後 5 月份爆發危機，意味著僅有兩個月的時間來評估和執行修補程式。但是，我們

[5] 如果實施帳戶封鎖，黑客可能會透過反複嘗試錯誤密碼的方式蓄意封鎖大量帳戶，從而導致服務中斷。

也認識到需要預留時間以進行必要的測試。因此，我們已對《指引》進行修訂，現在明確規定互聯網經紀行應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保安修補程式和修正程式。

56. 另外，由於有關建議已就在評估相關影響的前提下執行保安修補程式或修正程式作出規定，互聯網經紀行可根據評估結果自由制訂其執行時間表。

7. 系統及數據備份（《指引》第 2.8 段）

公眾意見

57. 兩名回應者提到，由於運作及資源方面的問題，每天將業務紀錄、客戶和交易數據庫、伺服器及證明文件在離線媒體進行備份存在困難。此外，有人就“離線媒體”的涵義提出疑問，以及建議允許對重大系統變更進行還原。

我們的回應

58. 證監會維持原有的意見，即每天在離線媒體進行備份對數據及業務恢復而言非常關鍵。我們已在常見問題中澄清，離線媒體是指磁帶或任何其他類型的媒體，包括與生產系統安全隔離的遙距備份伺服器。然而，我們注意到大型機構在重大系統變更之前及之後執行全面備份時，會遇到實際困難，故同意應減少規範性的條文，轉而要求互聯網經紀行採用適當的恢復方法，使重大系統變更得以成功還原。

8. 網絡保安情境的應變計劃（《指引》第 2.9 段）

59. 就處理分散式阻斷服務攻擊而言，兩名回應者詢問為何在基本規定中要求應變計劃須涵蓋分散式阻斷服務的情境，但互聯網經紀行卻無須購置反分散式阻斷服務解決方案。

60. 一名回應者強調，互聯網經紀行應進行定期的災難復原測試。

我們的回應

61. 如《諮詢文件》第56段所論述，根據經紀行的回應及外部網絡保安專家的意見，價格較易負擔的分散式阻斷服務解決方案在出現大規模的分散式阻斷服務攻擊時並不一定有效。平衡利弊之後，我們認為專注於制訂健全的應變計劃及危機管理程序似乎是更合適的做法。雖然購置反分散式阻斷服務解決方案不是必需，但在應變計劃中涵蓋分散式阻斷服務的情境卻很重要。

62. 如第 24 段所論述，對較小型互聯網經紀行而言，設立接收客戶指令及提供指令狀態信息的替代安排便可能足夠。有鑑於此，我們不會將進行定期的災難復原測試列作一項基本規定。

9. 第三方服務提供者（《指引》第 2.10 段）

公眾意見

63. 僅有五名回應者對此項建議的監控措施提出意見。他們都同意互聯網經紀行應與第三方服務提供者訂立正式的服務協議，而這些協議應定期予以審視，並在適當時作出修改。

64. 一名回應者尋求釐清其他並非以互聯網交易業務為主的外判活動是否涵蓋在內。

我們的回應

65. 就《指引》而言，“互聯網交易”一詞的涵義與《操守準則》第 18 段所界定者相同。因此，《指引》第 2.10 段僅涉及與用於向互聯網經紀行傳送交易指示的互聯網交易設施相關的外判安排。

執行時限

66. 一些回應者關注到，六個月的執行時間對互聯網經紀行而言，未必足以對其內部程序及資訊科技系統作出必要的變更。由於部分互聯網經紀行以大型及高度複雜的系統連接其互聯網經紀與其他業務，這個時限對他們來說可能尤其緊迫。

67. 我們理解，對一些互聯網經紀而言，用六個月的時間來執行全部所需的監控措施可能過於緊迫。然而，鑑於雙重認證是降低及紓減黑客入侵風險的主要預防措施，我們認為必須在切實可行的情況下盡快執行這項監控措施。因此，《指引》中關於實施雙重認證的新條文將在本文件發出日起六個月後開始生效，而所有其他規定，則在九個月後方會生效。

68. 證監會期望所有互聯網經紀行立即開始檢討其互聯網交易系統，並與第三方服務提供者及客戶（如適用）進行溝通，以確保符合新的監管規定。證監會強調，設立六個月及九個月的執行期，主要是為了切合部分互聯網經紀行儘管已盡最大努力，但在變更其互聯網交易系統時仍會遇到技術困難。我們期望互聯網經紀行應能夠在生效日期之前完成其他非系統相關的措施。

未來路向

69. 網絡保安的格局隨著時間而急速變化，證監會將繼續監察網絡保安的發展和新冒起的威脅。我們預計日後可能需對政策作出進一步的微調及修訂相關的規則，以便在市場創新與投資者保障之間維持適當的平衡。本會亦打算不時按需要提供額外指引，以便對《指引》進行補充。

附錄 **A**

對《證券及期貨事務監察委員會持牌人或註冊人操守準則》的修訂

第 **18** 段 — 電子交易

18.1 適用範圍

本段適用於就在交易所上市或買賣的證券及期貨合約進行電子交易或就並非在交易所上市或買賣的證券進行互聯網交易的持牌人或註冊人。

18.2 釋義

(f) 就本段而言，“互聯網交易”指透過持牌人或註冊人以互聯網為基礎的交易設施向該持牌人或註冊人傳送交易指示的安排。以互聯網為基礎的交易設施可透過電腦、流動裝置或其他電子裝置來接達。

附表 **7** — 對就進行電子交易的持牌人或註冊人的額外規定

引言

《操守準則》第18段訂明適用於就在交易所上市或買賣的證券及期貨合約進行電子交易或就並非在交易所上市或買賣的證券進行互聯網交易的持牌人或註冊人的一般原則。本附表就此列明具體規定。

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

SFC
證監會

附錄 **B**

《降低及紓減與互聯網交易相關的黑客入侵風險指引》

目錄

引言

1. 本指引由證券及期貨事務監察委員會（證監會）根據《證券及期貨條例》第 399 條發表，當中載明了有關降低或紓減與互聯網交易相關的黑客入侵風險的基本規定。

2. 本指引應連同（除其他條文外）《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、附表 7 第 1.1、1.2.2 至 1.2.8、1.3 及 2.1 段一併閱讀。就本指引而言，“互聯網交易”一詞的涵義與《操守準則》第 18.2(f)段所界定者相同，即“透過持牌人或註冊人以互聯網為基礎的交易設施向該持牌人或註冊人傳送交易指示的安排”。

3. 本指引適用於從事互聯網交易，並就以下活動獲證監會發牌或註冊的人：

   - 第 1 類受規管活動（證券交易）；
   - 第 2 類受規管活動（期貨合約交易）；
   - 第 3 類受規管活動（槓桿式外匯交易）。為免生疑問，本指引只適用於獲證監會發牌的槓桿式外匯交易商；及／或
   - 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。

4. 本指引並無法律效力，亦不應以任何方式被詮釋為可以凌駕於任何適用法律、守則或其他監管規定的條文。然而，任何人如未能遵從本指引的精神，則可能對其適當人選資格造成負面影響。

5. 本指引訂明的監控措施僅可降低或紓減與互聯網交易相關的黑客入侵風險，無法消除有關風險。必須強調的是，該等監控措施只是持牌人或註冊人應達致的最低標準，及並非詳盡無遺。持牌人或註冊人應實施與其架構、業務運作及需要相稱而足夠及有效的措施。

1. 保護客戶的互聯網交易帳戶

1.1. 雙重認證[1]

持牌人或註冊人應就客戶的互聯網交易帳戶的登入程序實施雙重認證。

持牌人或註冊人應評估及實施與其業務模式相稱的雙重認證解決方案。

1.2. 實施監察及監督機制

持牌人或註冊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。~~舉例而言：~~

- ~~由同一個互聯網規約（internet protocol，簡稱**IP**）地址登入多個客戶帳戶；及~~
- ~~接達同一個客戶帳戶的IP地址在短時間內改變（例如由香港變為倫敦）。~~

1.3. 即時通知客戶

持牌人或註冊人應在客戶的互聯網交易帳戶內出現某些客戶活動後，立即通知有關客戶（例如透過電子郵件、短訊服務或其他推播通知）。這些活動至少應包括：

(a) 登入系統；

(b) 重設密碼；

(c) 執行交易；

(d) 向第三方帳戶轉移資金（除非該等帳戶在資金轉移前已就轉移資金目的向該持牌人或註冊人進行登記）；及

(e) 更改客戶和帳戶的相關資料。

向客戶發出通知的途徑，應與登入系統時所使用者不同（如第 1.1 段所述）。

客戶只可選擇不收取“執行交易”的通知。在此情況下，持牌人或註冊人應向客戶作出充分的風險披露，及客戶應簽立一份聲明，以確認其明白不收取有關通知所涉及的風險。

1.4. 數據加密

持牌人或註冊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~~（即端對端加密）。~~；及

[1] 雙重認證指使用以下任何兩項元素的認證機制：客戶所知的~~（例如密碼）~~、客戶所有的~~（例如硬件編碼器、在短時間內失效的一次性密碼）~~及客戶是誰~~（即生物特徵）~~。

(b) ~~持牌人或註冊人亦應使用強效的加密程式，來~~保護儲存於其互聯網交易系統的客戶登入密碼。

1.5. 保護客戶的登入密碼

持牌人或註冊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或註冊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，持牌人或註冊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。

1.6. 嚴格的密碼政策及網頁超時監控措施

持牌人或註冊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~~（除其他措施外）~~：

(a) 最短的密碼長度；

(b) ~~最長的密碼有效期限~~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) ~~多次嘗試登入無效後封鎖帳戶~~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。

2. 基礎設施保安管理

2.1. 配置安全的網絡基礎設施

持牌人或註冊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。

2.2. 使用者接達管理

持牌人或註冊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，持牌人或註冊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。

2.3. 遙距連接的保安監控措施

持牌人或註冊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。

2.4. 修補管理

持牌人或註冊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~~保安修補程式或修正程式的~~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。

2.5. 端點保護

持牌人或註冊人應及時執行和更新防毒及抗惡意軟件解決方案（包括相應的定義檔案及辨識檔案）~~應及時予以執行和更新~~，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。

2.6. 在未經授權的情況下安裝硬件及軟件

持牌人或註冊人應實施保安監控措施，以防止硬件及軟件在未經授權的情況下被安裝。

2.7. 實體保安

持牌人或註冊人應訂立實體保安政策及程序，以確保關鍵系統組件（例如系統伺服器及網絡裝置）處於安全的環境下，及防止有人在未經授權的情況下實際接觸寄存互聯網交易系統及關鍵系統組件的設施。

2.8. 系統及數據備份

持牌人或註冊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。~~在任何重大系統變更之前及之後，均應對上述系統及資料進行全面備份。~~

持牌人或註冊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。

2.9. 網絡保安情境的應變計劃

為確保在網絡保安事故發生時可有效執行適當的應變程序，持牌人或註冊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[2]），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。

2.10. 涵蓋互聯網交易的第三方服務提供者管理

若持牌人或註冊人安排將任何與其互聯網交易有關的活動外判給第三方服務提供者，持牌人或註冊人應與有關服務提供者訂立正式的服務協議，當中須訂明服務條款及提供者的責任。尤其是，持牌人或註冊人應確保第三方服務提供者所提供的服務，可使持牌人或註冊人遵守（除其他規定條文外）《操守準則》第18段和附表7以及本指引所載的相關規定。服務協議應定期予以審視，並在適當時作出修改，以反映外判安排的任何變更或監管發展。在可行的情況下，有關協議應以量化方式詳細規定服務提供者需提供的足夠保養及技術協助。

[2] 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。

3. 網絡保安管理及監督

3.1. 網絡保安管理層的角色及責任

負責互聯網交易系統的整體管理及監督的負責人員或主管人員，應設定網絡保安風險管理框架（包括但不限於政策及程序），及列明主要角色及責任。這些責任包括~~（除其他責任外）~~：

(a) 審視及批准網絡保安風險管理政策及程序；

(b) 審視及批准有關網絡保安風險管理資源的預算及開支；

(c) 安排定期就整體網絡保安風險管理框架進行自我評估；

(d) 審視透過網絡保安事故報告機制上報的重大事件；

(e) 審視內部和外部稽查及網絡保安檢視所識別出的重大發現；批准作出補救行動及監察有關工作直至行動完成為止；

(f) 監察及評估最新的網絡保安威脅及攻擊；

(g) 審視及批准業務延續計劃，當中涵蓋網絡保安情境，及為互聯網交易系統而設立的相關應變策略；及

(h) 審視及批准與互聯網交易有關的第三方服務提供者的服務協議及合約（如適用）。

這些責任可以書面形式轉授予指定委員會或營運單位，但整體責任仍由負責人員或主管人員承擔。

3.2. 網絡保安事故報告

持牌人或註冊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或主管人員）和向外（例如客戶、證監會及其他執法機構（如適用））報告。

3.3. 內部系統使用者的網絡保安意識培訓

持牌人或註冊人應至少每年向所有內部系統使用者[3]提供足夠的網絡保安意識培訓。~~有關培訓課程應予更新，以包含最新的網絡保安相關規則及規例，當前及新興的網絡保安威脅及趨勢，以及相應的措施。~~在設計培訓課程的內容時，持牌或註冊人應顧及其所面對的網絡保安風險類別及水平。

[3] 內部系統使用者指任何可接達持牌人或註冊人的內部網絡和系統的常額職員及合約職員。

3.4. 向客戶發出網絡保安警示及提示

持牌人或註冊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，例如登入資料應妥為保管及不能共用。

附錄 **C**

回應者名單

（按英文原文的字母排序）

1. 存款公司公會會員
2. 嶺首有限公司
3. Cheng, Vincent
4. Chow, Chi Fai
5. Chow, Paul
6. 國際合規顧問有限公司
7. 天智合規顧問有限公司
8. 消費者委員會
9. CQG
10. 德勤
11. Dragon Advance Tech Consulting Co. Ltd.
12. Fast Identity Online (FIDO) Alliance
13. 富達基金（香港）有限公司
14. 香港網上經紀協會
15. 香港投資基金公會
16. 香港證券學會
17. Hui, Albert
18. Kwok, Vincent
19. Leung, Frankie
20. Lok, Ka Wing
21. Moy, Eric
22. 柯伍陳律師事務所
23. Post-Quantum (HK) Limited
24. 香港銀行公會
25. 香港律師會
26. 11 名回應者要求在公開其意見書時不要披露其姓名／機構名稱