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文件

2017 年 5 月

目錄

序言

證券及期貨事務監察委員會（**證監會**）邀請市場參與者及相關人士於2017年7月7日或之前，就本諮詢文件討論的各項建議提交書面意見，或評論可能對這些建議產生重大影響的相關事宜。任何人士如欲代表任何組織或機構就有關建議發表意見，應提供其所代表的組織或機構的詳細資料。

請注意，評論者的姓名／機構名稱及其意見書的內容，或會在證監會網站及其他由證監會刊發的文件內公開。就此，請參閱本諮詢文件附載的《個人資料收集聲明》。

如你不希望證監會公開發表你的姓名／機構名稱及／或意見書內容，請在提交意見書時明確作出此項要求。

書面意見可以下列方式提交：

郵寄：	香港皇后大道中2號 長江集團中心35樓 證券及期貨事務監察委員會 關於：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
圖文傳真：	(852) 2284 4660
網上呈交：	http://www.sfc.hk/edistributionWeb/gateway/TC/consultation/
電子郵件：	2017_cybersecurityconsultation@sfc.hk

證監會將會考慮在諮詢期結束前接獲的所有意見書，然後才就有關建議作最後定稿，並會在適當時候發表諮詢總結文件。

證券及期貨事務監察委員會
香港

2017 年 5 月 8 日

個人資料收集聲明

1. 本個人資料收集聲明（**本聲明**）是按照個人資料私隱專員發出的指引編寫的。本聲明列出證監會收集你的個人資料[1]的用途、你就證監會使用你的個人資料而同意的事項，以及你根據《個人資料(私隱)條例》（第486章）（**《私隱條例》**）享有的權利。

收集資料的目的

2. 證監會可能會為以下其中一個或以上的目的，使用你就本諮詢文件向證監會提交的意見書中所提供的個人資料：

   (a) 執行有關條文[2]及依據證監會獲賦予的權力而刊登或發表的守則及指引；

   (b) 根據有關條文執行證監會的法定職能；

   (c) 進行研究及統計；及

   (d) 法例所容許的其他目的。

轉移個人資料

3. 證監會就本諮詢文件徵詢公眾意見時，可向香港及其他地區的公眾人士披露其所取得的個人資料。證監會亦可向公眾人士披露就本諮詢文件發表意見的人士的姓名／機構名稱及其意見書的全部或部分內容。證監會可以在諮詢期內或諮詢期完結後，將上述資料刊載於本會網站及由本會發表的文件內。

查閱資料

4. 按照《私隱條例》的規定，你有權要求查閱及修正你的個人資料。上述權利包括你有權索取你就本諮詢文件提交的意見書中所提供的個人資料的副本。證監會有權就處理任何查閱資料的要求收取合理的費用。

保留資料

5. 證監會會保留就回應本諮詢文件而提供予本會的個人資料，直至本會恰當地完成有關職能為止。

---

1 個人資料指《個人資料(私隱)條例》（第 486 章）所界定的“個人資料”。

2 “有關條文”一詞的定義載於《證券及期貨條例》（第 571 章）附表 1 第 1 部第 1 條，指《證券及期貨條例》的條文，連同《公司(清盤及雜項條文)條例》（第 32 章）、《公司條例》（第 622 章）及《打擊洗錢及恐怖分子資金籌集(金融機構)條例》（第 615 章）的若干條文。

查詢

6. 有關就本諮詢文件提交的意見書中所提供的個人資料的任何查詢，或查閱或修正個人資料的要求，請以書面形式向以下人士提出：

   香港皇后大道中2號
   長江集團中心35樓
   證券及期貨事務監察委員會
   個人資料私隱主任

7. 證監會備有本會所採納的保障私隱政策聲明的副本，可供索取。

引言

1. 隨著以科技輔助的業務迅速發展，電腦系統及內部網絡均可透過流動裝置應用程式及互聯網交易平台等途徑以電子方式接達，令業界及其客戶對這些系統及網絡愈加依賴。因此，金融服務業普遍被視為最容易成為不同形式的網絡攻擊（包括黑客入侵、勒索軟件及阻斷服務）的目標。雖然市場對於電子接達漏洞的警覺有所提高，但網絡攻擊亦同時變得更頻繁及精密，令受影響的客戶人數及他們所蒙受的損失大幅攀升。

2. 在本港，香港生產力促進局轄下的香港電腦保安事故協調中心於2016年處理的網絡保安事故增至6,058宗，較2015年上升了23%[3]。 在截至2017年3月31日止18個月期間，有12家持牌法團舉報了27宗網絡保安事故，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，造成了總額超過1.1億元的未經授權交易[4]；另外一些事故則涉及證券經紀行同時遭受針對其網站發動的分散式阻斷服務攻擊[5]及敲詐威脅。

3. 長久以來，我們都十分重視網絡保安管理。我們由2014年1月1日起將《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》**）的監管範圍擴大至涵蓋電子交易，並在當中引入網絡保安管理的規定。自此，我們先後進行了多次主題檢視及向業界發出了多份通函，分享我們的檢視結果及就監控措施提出建議。

4. 鑑於互聯網交易[6]遭受黑客攻擊似乎是本港持牌法團所面對最嚴重的網絡保安風險，我們遂於2016年底在外部網絡保安專家[7]（**外部顧問**）的協助下，就從事互聯網交易的經紀行（**互聯網經紀行**）對黑客入侵風險的抵禦能力進行了主題檢視。該次檢視識別出若干應有助互聯網經紀行降低及紓減黑客入侵風險的基本網絡保安監控措施，當中大部分均為現已在《操守準則》中提及但需作更詳細說明的規定，或屬曾在過往發出的通函中提出的建議。

5. 本諮詢文件建議將該等監控措施納入將根據《證券及期貨條例》發出的指引內。證監會希望能透過建議的指引加強互聯網經紀行為處理黑客入侵風險及漏洞而採取的監控常規，並向互聯網經紀行更清楚地闡明其在從事互聯網交易時應執行的網絡保安監控措施所須達到的標準等。

黑客事件及可能的根本成因

6. 雖然警方仍在調查持牌互聯網經紀行所舉報的黑客事件，但從警方分享的研究個案得知，黑客是利用受操控的互聯網交易帳戶執行可能造成重大財務損失的“唱高散貨”騙局。該等騙局一般循以下步驟執行：

---

3 香港電腦保安事故協調中心。〈網絡犯罪包辦服務料趨猖獗 勒索軟件事故持續攀升〉。香港電腦保安事故協調中心新聞中心。刊出日期：2017年1月16日。（https://www.hkcert.org/my_url/zh/articles/17011601）

4 證監會統計數據。

5 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。

6 就本諮詢文件而言，“互聯網交易”一詞的涵義與《操守準則》第 18 段所界定者相同，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”。

7 證監會就 2016 年網絡保安檢視和所有於 2016 年之前進行的其他互聯網交易及網絡保安檢視而委任的外部網絡保安專家，是一家跨國專業服務公司，在向金融服務業及監管機構提供網絡保安相關事宜的意見方面擁有多年經驗，並曾就此範疇進行多項行業調查。此公司多年來亦曾向多家本地經紀行提供網絡保安監控及技術評估服務。

(a) 黑客首先取得客戶互聯網交易帳戶（**被入侵的帳戶**）的控制權，讓他們可“正當地”登入該等帳戶以執行未經授權的交易；

(b) 黑客隨後僱用多名人士開設其他互聯網交易帳戶，以囤積細價股；

(c) 黑客繼而盜用被入侵的帳戶中的現金或藉拋售當時在被入侵的帳戶中持有的股票所得的現金，買入該等細價股，以抬高其股價；及

(d) 細價股的價格一經推高，黑客便會大幅拋售該等股份套利，令被入侵的帳戶的擁有人蒙受大額損失。

7. 外部顧問指，該等黑客事件可歸咎於互聯網經紀行的交易系統及網絡保安管理框架存在多項流弊，包括：

(a) **互聯網經紀行的密碼政策寬鬆：**客戶的登入密碼（尤其是其組合過於簡單時）可透過解碼應用程式以反複實驗的方法被輕易破解（俗稱暴力攻擊）。應注意的是，即使實施雙重密碼，亦不能提供充分保障；在某些情況下，黑客仍能入侵須輸入雙重密碼的互聯網交易帳戶。

由此可見，單一認證並不足以保障互聯網交易帳戶不受黑客入侵。

(b) **客戶的網絡保安意識偏低：**客戶可能會因無心之失而被盜取互聯網交易帳戶的登入資料。舉例來說，客戶在使用公共互聯網接達服務（例如設於商業場所的共用電腦）後沒有登出帳戶。此外，社交工程（即透過欺騙或操縱客戶令其披露機密資料）亦會對經紀行的保安程序構成重大風險。

當客戶使用受操控的電子裝置（即已被黑客入侵的電腦、流動電話或其他裝置）接達經紀行的互聯網交易系統時，經由該裝置傳輸的數據（包括客戶使用互聯網交易帳戶所需的登入資料）均可透過存取按鍵紀錄[8]及中間人攻擊[9]等各種黑客入侵技術被盜取。

羅兵咸永道於 2016 年發表了一份資訊保安調查[10]報告，當中指出只有 53%的調查回應者有向其用戶或僱員提供網絡保安培訓及網絡保安意識課程。

(c) **監察及監督機制不足：**經紀行只要及時和及早偵測到有人在未經授權的情況下接達其互聯網交易系統，便能有助防止損失。過去曾有一些經紀行要待客戶發現並向他們舉報未經授權的交易後，才知悉該等交易，結果可能令受影響的客戶互聯網交易帳戶未能及時停用或未經授權的交易未能及時取消，以致未能將有關事故的財務影響減至最低；而有關事故的調查、查找問題及採取適當糾正措施的過程亦可能因而有所延誤。根據上述調查，在調查回應者中僅有 48%有積極監察或分析有關威脅的情報。

(d) **對網絡保安投放的資源不足：**另外，羅兵咸永道在2015年的調查中發現，收益少於一億美元的調查回應者僅將其收益中的0.73%用於資訊保安方面。

---

8 當使用者在某特定應用程式或在某網頁的特定欄目以鍵盤輸入資料（例如密碼）時，惡意軟件可藉由按鍵紀錄取得所輸入的資料。

9 中間人攻擊是指攻擊者能夠攔截、讀取、中斷及修改在兩名使用者或兩個系統之間傳送的訊息。

10 由羅兵咸永道根據超過 10,000 名來自 127 個國家的高層人員所提交的回應意見而擬備的 The Global State of Information Security® Survey。

證監會為處理網絡保安風險而採取的措施

8. 網絡保安管理長久以來都是證監會在監管持牌法團方面的首要工作之一。《操守準則》第18段及附表7載有與網絡保安有關的重要監管原則及規定。有關該等原則及規定的摘要，請參閱附錄A。

9. 自2014年以來，我們在外部顧問的協助下進行了多次互聯網交易及網絡保安檢視，並發出了多份通函[11]，提醒業界注意我們所發現的常見缺失及漏洞。我們曾建議實施多種不同的監控措施（包括自我評估問卷），以補充現時在《操守準則》中所訂的原則及規定。在上述檢視中，最近一次是2016年網絡保安檢視，當中以與互聯網交易相關的黑客入侵風險為探討焦點。

10. 除了對選定經紀行的互聯網系統在網絡保安方面的特點和業界對黑客入侵風險方面的整體抵禦能力進行評估外，2016年網絡保安檢視旨在就降低及紓減該等風險的監控措施提出建議，而這些措施可成為適用於互聯網經紀行的基本網絡保安規定。雖然建議的監控措施主要是為了降低及紓減黑客入侵風險而設計的，但亦可用於處理與其他網絡攻擊有關的風險。舉例來說，安裝防毒或抗惡意軟件的程式並更新病毒識別碼，可有助防範勒索軟件。

建議的基本規定

整體框架

11. 2016年網絡保安檢視包括：

    (a) 就25家經紀行的互聯網交易系統在網絡保安方面進行實況調查；

    (b) 對五家經紀行進行現場視察，以對其資訊科技及其他相關的管理監控措施進行檢視，和評估其系統在防止和偵測網絡攻擊方面的設計和成效；

    (c) 對比本地[12]與海外[13]的監管規定和金融機構市場作業方式的異同；

    (d) 與選定的系統供應商進行討論，以衡量不同網絡保安解決方案的可行性、成本及效益；及

    (e) 對證監會在現行規例及該等通函中提供與網絡保安有關的指引進行檢討，以評估是否有需要詳加說明或提供額外指引。

---

[11] 有關通函分別為：(i) 日期為2017年1月26日的《網絡保安威脅警報》；(ii) 日期為2016年3月23日的《網絡保安》；(iii) 日期為2016年1月29日的《有關保障網上交易帳戶安全的提示》；(iv) 日期為2015年6月11日的《互聯網交易－互聯網交易自我評估查檢表》；(v) 日期為2014年11月27日的《緩解網絡保安風險》；(vi) 日期為2014年11月26日的《互聯網交易－資訊保安管理及系統的充足性》及；(vii) 日期為2014年1月27日的《互聯網交易－減低互聯網遭黑客入侵的風險》（統稱為“該等通函”）。

[12] 即本港銀行業。

[13] 包括新加坡、英國、美國、日本、澳洲及南韓。

12. 參照2016年網絡保安檢視的結果及外部顧問提供的意見，我們建議引入《降低及紓減與互聯網交易相關的黑客入侵風險指引》（**指引草擬本**），當中載有多項建議的基本規定（請參閱附錄B）。該等規定旨在：

    (a) 加強監控常規，以處理已知的威脅及漏洞；

    (b) 將本地常用的網絡保安監控常規標準化並編纂為指引條文，以供業內各互聯網經紀行劃一採納；及

    (c) 就證監會在網絡保安監控措施方面的期望，向互聯網經紀行提供明確而實用的指引。

13. 在編撰指引草擬本時，我們已考慮到(i) 本地及海外市場的作業方式和監管規定；(ii) 有關監控措施的成效和適切程度；(iii) 實施成本；及(iv) 對使用者體驗的潛在影響。我們建議，有關基本規定將適用於所有互聯網經紀行，而不論其營運規模及業務模式。

14. 建議的基本規定共有20項，其中17項為現時在《操守準則》中提及但需詳加說明的規定，或屬過往曾在該等通函中提出的建議。指引草擬本現將該等規定及建議集中起來並加以說明。剩餘的三項屬全新規定，並在下文載述。該等基本規定將以根據《證券及期貨條例》第399(1)條發出指引的方式實施。

15. 必須強調的是：

    (a) 建議的監控措施僅可降低及紓減與互聯網交易相關的黑客入侵風險，但不能將該等風險根除。舉例來說，社交工程之所以屬真正的威脅，是因為經紀行即使盡力提供網絡保安警示及提示，客戶仍有可能遭到黑客蒙騙或操縱；

    (b) 建議的規定一般並無指明要採取何種方式來實施該等規定。實施方式應由互聯網經紀行經顧及其本身的情況（例如營運規模、依賴互聯網來接受客戶交易指令的程度、客戶狀況、預算及資源限制、未來目標及策略規劃）後自行決定；

    (c) 建議的規定屬證監會所期望的最低標準。互聯網經紀行（尤其是有大量客戶經常進行互聯網交易的經紀行，及互聯網交易活動在其成交量中佔有甚高比重的經紀行）應自行酌情決定是否要制訂及實施額外監控措施以加強保障；及

    (d) 建議的規定是為了處理迄今所知的黑客入侵風險而制訂，並非詳盡無遺。

> 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？

適用範圍

16. 現時，與網絡保安有關的主要監管原則及規定均收錄在《操守準則》第18段及附表7內。這些規定適用於就在交易所上市或買賣的證券及期貨合約進行的電子交易，而“電子交易”是指

以電子方式進行的證券及期貨合約交易，包括互聯網交易、直達市場安排及程式買賣。該等監管原則及規定目前適用於證券交易商、期貨交易商、槓桿式外匯交易商[14]及基金經理[15]。

17. 部分互聯網經紀行或會就並非在交易所上市或買賣的證券（例如認可單位信託及互惠基金）進行互聯網交易。由於透過互聯網交易系統就該等產品進行交易，與透過互聯網就在交易所上市或買賣的證券進行交易所涉及的風險相同，故我們建議將《操守準則》第18段及附表7的適用範圍擴大至涵蓋該等活動。就此，我們建議對《操守準則》第18.1段（及附表7的引言）作出下列修訂：

"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。"

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？

18. 客戶透過不同途徑（包括電腦或流動裝置）接達經紀行以互聯網為基礎的交易設施。為免生疑問，我們亦希望趁此機會對《操守準則》第18.2(f)段作出下列修訂，闡明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：

"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。"

19. 為免生疑問，鑑於《操守準則》適用於註冊人及持牌人，建議的規定亦將適用於從事互聯網交易的銀行。

建議的規定

20. 指引草擬本將多項建議適用於互聯網交易的網絡保安規定歸入以下三個類別：

(a) 保護客戶的互聯網交易帳戶；

(b) 基礎設施保安管理；及

(c) 網絡保安管理和監督。

---

[14] 就槓桿式外匯交易合約的買賣而言，"電子交易"指透過互聯網交易以電子方式買賣該等合約（《操守準則》附表6第66段）。

[15] 為免生疑問，現時與電子交易有關的監管原則及規定（載於《基金經理操守準則》第9段）僅在基金經理代表所管理的集體投資計劃就在交易所上市或買賣的證券及期貨合約進行電子交易的情況下，才適用於該基金經理。此外，凡基金經理是透過以互聯網為基礎的交易設施從事集體投資計劃的網上分銷，該等有關互聯網交易的規定亦將適用。

21. 就本諮詢文件而言，現將該等規定可分為以下三類：

(a) 預防性監控措施－旨在保護互聯網經紀行的內部網絡及互聯網交易系統和客戶帳戶不受網絡攻擊；

(b) 偵測性監控措施－旨在偵測懷疑黑客活動並及時給予互聯網經紀行和客戶警示，以紓減該等活動的影響和減輕財務損失；及

(c) 其他監控措施（包括管治、政策及程序）－旨在加強互聯網經紀行的整體網絡保安管治及管理，以及提高經紀行及其客戶的網絡保安意識。

接下來，我們會詳細討論建議的規定。

(I) 預防性監控措施

(i) 雙重認證（指引草擬本第 1.1 段）

22. 現時，互聯網經紀行須採取可靠措施，藉以認證或核實使用者的身分及權限，確保只有獲核准且有需要的人士方可接達或使用系統[16]。以可靠的技術認證或核實每個互聯網交易系統使用者的身分及權限，是保證只有獲核准人士才可接達系統的關鍵所在。因此，認證是防範網絡攻擊的其中一項最重要的保安監控措施。

23. 最常用的客戶身分認證方法，是要求客戶使用密碼登入系統。根據2016年網絡保安檢視，25家參與調查／接受視察[17]的經紀行全部均在客戶登入其互聯網交易系統時，實施單一或多重密碼認證。然而，從近期舉報的黑客事件看來，即使實施了嚴格的密碼政策及網頁超時監控措施，單靠密碼始終不能提供充分的保障。相反，至今尚未有舉報，指黑客入侵的事件在實施雙重認證的情況下發生。

24. 雙重認證指使用下列任何兩項因素的認證機制：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）。規定使用兩項獨立的認證因素，可增添黑客入侵的難度，從而大大提升保安防護的作用。舉例來說，黑客即使盜取了某人的密碼，亦須掌控第二項因素（例如實際取得硬件編碼器或流動電話以收取一次性密碼）。

25. 在25家參與調查／接受視察的經紀行當中，有八家表示計劃在未來12個月內實施雙重認證。由於雙重認證將要求客戶採取額外步驟，故未必一定受到歡迎，該等經紀行因而擔心其客戶可能會轉向不選擇採取雙重認證的經紀行，繼而造成客戶流失。有意見認為，證監會應強制業界全面實施雙重認證，以確保競爭環境公平。

26. 就監管規定而言，香港金融管理局（**金管局**）及新加坡金融管理局早已強制要求在執行預先定義為高風險的活動（例如涉及將資金轉移至未經登記第三方的活動）時執行雙重認證。自2016年12月起，新加坡金融管理局甚至進一步規定所有金融機構一律為客戶（機構投資者除

---

16 《操守準則》附表7第1.2.4(a)段。

17 我們向 25 家經紀行進行了調查，並同時對其中五家進行了視察。

外）的網上交易帳戶設置雙重認證。與此同時，金管局現正就銀行客戶進行網上證券交易前強制實施雙重認證進行諮詢。

27. 眾所周知，沒有單一個保安解決方案可完全抵禦黑客，而雙重認證是目前被視為能有效預防黑客入侵的認證機制。經考慮各種因素後，我們建議將客戶登入時的雙重認證訂為基本規定。為免生疑問，我們建議將雙重認證訂為適用於客戶登入（而非每次發出交易指令）時的強制規定，因為雙重認證或會對能否及時執行交易指令造成影響，未必符合客戶的最佳利益。

28. 我們已識別出較常見的雙重認證監控措施（即一次性密碼短訊、硬件編碼器、軟件編碼器及數碼證書），並對這些措施的實施成本、對使用者體驗的影響、優點及缺點進行了分析（請參閱附錄D）。建議的規定不會硬性訂明任何特定的雙重認證解決方案，而經紀行可選用任何其認為適當的雙重認證解決方案（不論是否附錄D所列者）。

> 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？

(ii) 有助防止未經授權的入侵及網絡攻擊的保安監控措施（指引草擬本第 2.1、2.4、2.5、2.6 及 2.7 段）

29. 互聯網經紀行明白到保障其關鍵系統免受未經授權的入侵或網絡攻擊的重要性。因此，在2016年網絡保安檢視期間參與調查／接受視察的經紀行均實施了各種保安監控措施。我們現建議將相關的現行網絡保安監控常規編纂為指引條文，並訂為建議的基本規定。

30. 根據建議的基本規定，互聯網經紀行應：

(a) 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[18]；

(b) 及時執行並更新防毒或抗惡意軟件解決方案，以偵測關鍵伺服器及工作站內的惡意應用程式及惡意軟件[19]；

(c) 實施監控措施，以防止硬件及軟件在未經授權的情況下被安裝[18]；及

(d) 訂立實體保安政策及程序，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[19]。

31. 互聯網經紀行亦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。從2016年網絡保安檢視可見，參與調查／接受視察的經紀行執行保安修補程式或修正程式所需的時間，由一星期至六個月不等，當中有超過半數能在一個月內執行該等程式。這段時間亦與我們在

[18] 此規定旨在加強該等通函所述的同一項監控措施。
[19] 此乃新規定，未曾在該等通函提及。

對比海外情況時所留意到海外金融機構的作業方式相符。在有關建議下，持牌人或註冊人應視乎對保安修補程式或修正程式的影響進行的評估，在一個月內執行該等程式[20]。

(iii) 系統及網絡接達（指引草擬本第 2.2 及 2.3 段）

32. 為加強互聯網經紀行對系統接達的監控，我們建議互聯網經紀行應增設政策及程序，以確保只容許有需要的使用者方可接達系統。此外，互聯網經紀行應至少每年進行檢視[21]，以確保只有獲核准且有需要的人士方可接達或使用其系統。

33. 職員及第三方服務提供者遙距接達互聯網經紀行的內部網絡，可能會增加網絡攻擊的風險。首先，遙距接達一般經互聯網進行（與經租用線路進行的專線連接不同），而互聯網經紀行一般沒有對外間網絡實施任何保安監控措施。其次，如從咖啡店等公眾場所進行遙距接達，黑客可能會竊聽敏感數據，以及截斷和更改通訊。

34. 因此，我們建議互聯網經紀行應只容許有需要的人士（例如內部職員或第三方服務提供者）遙距接達其內部網絡。另外，互聯網經紀行應就從外間網絡遙距接達[18]內部網絡的情況，實施保安監控措施。

(iv) 數據加密（指引草擬本第 1.4 段）

35. 互聯網經紀行現時須實施可靠的防禦性措施，以保障敏感資料（例如客戶數據檔案、密碼等）[22]。然而，有些經紀行關注到，如將整個數據庫（包括交易數據及客戶資料）加密，會嚴重削弱其互聯網交易系統的表現。雖然數據加密是該等通函內載述的監控要求，但我們謹此澄清，經紀行只須將系統內儲存的客戶登入密碼加密。

36. 另外，由於確保內部與外間網絡之間傳送的資料的保密性及完整性非常重要，及為了向業界提供更清晰的指引，我們建議，互聯網經紀行亦應將敏感資料（包括交易數據）在內部網絡與客戶裝置之間傳輸時加密（即端對端加密）。

(v) 客戶密碼及網頁超時監控措施（指引草擬本第 1.5 及 1.6 段）

37. 客戶密碼是最常用作認證使用者身分的方法之一。因此，在啟動帳戶及重設密碼的過程中，密碼應在安全的環境下發送給客戶[18]。

38. 此外，由於密碼是第一道防線，互聯網經紀行應在其互聯網交易系統內設立嚴格的密碼政策[18]（例如最短的密碼長度及最長的密碼有效期限），以防密碼輕易被黑客猜中或破解。另外，由於網頁超時監控措施[23]能限制黑客可發動攻擊的時間，互聯網經紀行應實施適當的網頁超時監控措施，以降低黑客入侵風險[18]。市場一般把網頁超時的時限設定為兩至五分鐘不等。

---

20 保安修補程式或修正程式的執行時限屬新規定，過往未曾在該等通函中提及。

21 該等通函已載述進行使用者接達檢視的規定， 不過本諮詢文件將有關規定擴闊至指明進行檢視的頻率。

22 《操守準則》附表 7 第 1.2.4(b)段

23 就本諮詢文件而言，“網頁超時監控措施”指在互聯網交易系統內實施的監控措施，以追蹤閒置時段及在持續閒置一段時間後自動將使用者重新導向至登入頁面。此規定旨在加強該等通函所述的同一項監控措施。

(II) 偵測性監控措施

(i) 監察及監督機制（指引草擬本第 1.2 段）

39. 雖然防禦性監控措施可被視為最重要的第一道防線，但監察及監督控制措施亦有著關鍵作用。隨著網絡攻擊越趨精密，相關的問題並非會否而是何時會出現網絡攻擊。健全的偵測性監控措施對於迅速地上報網絡攻擊和採取補救行動十分重要。因此，經紀行必須能夠偵測對其網絡或互聯網交易系統發動的網絡攻擊。

40. 我們觀察到，在多宗獲舉報的黑客入侵事故中，經紀行透過嚴密的監察機制，成功偵測到未經授權而接達客戶的互聯網交易帳戶的情況及未經授權的交易。在這些個案中，經紀行能夠停用受影響客戶的互聯網交易帳戶及／或解除未經授權的交易，從而減低財務影響，以及向警方舉報有關事宜，讓警方及時進行調查和採取行動。

41. 我們在2016年網絡保安檢視中注意到，互聯網經紀行主要採取兩套監察及監督機制來偵測可疑活動：

(a) 監察不尋常的互聯網規約（internet protocol，簡稱**IP**）地址

互聯網經紀行可透過不同方式監察不尋常的IP地址。例如，當同一個IP地址接達多個客戶的互聯網交易帳戶，或者接達同一個客戶的互聯網交易帳戶的IP地址在短時間內出現不尋常的改變（例如由香港變為倫敦）時，可以人手操作（例如就應用程式的接達紀錄作出系統指令或查詢）或透過自動程式（例如批次編程、實時監察系統）即時發出警告。有關監察工作的成效取決於偵察可疑系統活動的頻率及模式。

(b) 識別異常交易模式

互聯網經紀行對客戶的交易活動進行監察，並在出現異常交易活動時[獲適當警示。例如，假設一名客戶的交易紀錄顯示他的交易模式為買入並持有藍籌股，而監察系統偵測到他在一段短時間內沽出現有股票持倉並以所得款項來買入仙股，監察系統應發出警報。這些監察工作可交由人手（即由直接與客戶互動的客戶主任）或系統（即利用使用者行為分析法，以識別異常交易）進行。

42. 根據2016年網絡保安檢視，我們注意到：

(a) 接受視察的五家經紀行中有三家已實施監控措施，以監察(i)IP 地址在短時間內出現可疑的改變；及(ii)以同一個 IP 地址登入多個客戶帳戶的情況。進行監察的頻率為實時以至每日監察不等；

(b) 在基準評價活動所涵蓋的金融機構中，有 60%已實施若干措施，以監察可疑的 IP 地址及交易模式；及

(c) 金管局及新加坡金融管理局等其他監管機構規定金融機構須設有健全的監察及監督機制，以及時偵測任何異常系統活動、傳輸錯誤或不尋常網上交易。

43. 鑑於互聯網經紀行的規模和業務模式各有不同，而且有多種可用的監察及監督機制，我們建議規定互聯網經紀行須實施與其業務模式相稱的監察及監督機制，以偵測未經授權而接達客戶的互聯網交易帳戶的情況，但不會指明要以何種方式達致此目的[18]。

44. 我們曾考慮規定互聯網經紀行須監察異常交易，例如不尋常的交易模式，因為此舉亦被視為是另一種有效的偵測方法。然而，由於透過互聯網交易平台進行的客戶交易，按其性質而言，一般不牽涉客戶主任，故經紀行未必了解其客戶的投資策略和交易模式。要求經紀行以人手檢視大量交易數據是不切實際，而且對大部分經紀行而言，自動化監察客戶的交易模式亦不可行，因為需要投入龐大資源開發才可實施使用者行為分析功能。因此，這項監控措施只會成為良好作業方式的例子，並將會包括在證監會將於適當時候刊發的通函內，但不會是一項基本規定。

> 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？

(ii) 即時通知客戶 [19]（指引草擬本第 1.3 段）

45. 如黑客登入了客戶的互聯網交易帳戶，即時通知客戶可以是有效偵測有關事故的第二道防線。在部分獲舉報的黑客入侵事故中，受影響客戶是在收到登入系統或執行交易的通知後，揭發及向互聯網經紀行報告未經授權而接達並使用互聯網交易帳戶來執行未經授權的交易的情況。

46. 根據2016年網絡保安檢視，我們注意到：

(a) 在 25 家參與調查／接受視察的經紀行中，有兩家在登入系統後向客戶發出通知，14 家在執行交易指令後發出通知及七家在客戶的互聯網交易帳戶中出現其他活動（例如更改個人資料）後發出通知。短訊及電郵是最常用作發出通知的兩個途徑。

(b) 金管局、新加坡金融管理局及澳洲審慎監管局等其他監管機構規定金融機構須將高風險交易（例如付款或資金轉移）即時通知客戶。新加坡金融管理局及澳洲審慎監管局亦規定須透過第二種途徑（即不同於登入系統時所使用的途徑）發出通知。

47. 因此，我們建議互聯網經紀行應在客戶的互聯網交易帳戶內出現某些活動後，立即通知有關客戶。這些活動包括登入系統、執行交易、向第三方轉移資金、更改個人資料及重設密碼。

48. 業界關注，如須透過短訊發出所有通知，可能會產生高昂的合規成本。考慮到業界在這方面的關注，我們建議互聯網經紀行可透過其認為適當的途經發出通知，即電郵、短訊或其他推播通知[24]。然而，向客戶發出通知的途徑，應與登入系統時所使用的途徑不同，以紓減被黑客操控的風險。例如，使用流動電話收取一次性密碼短訊的客戶不應透過短訊收取登入通知。此舉是為了避免出現如客戶的流動電話遭黑客入侵，透過短訊發送的登入通知亦可能被黑客截斷或干擾的情況。

---

[24] 然而，儘快及有效地向客戶發出登入系統的通知是可取的做法。就此而言，透過短訊自動發出登入系統的通知或會獲推薦為良好作業方式。證監會將於適當時候刊發有關作業方式。

49. 另外，業界亦指出，部分客戶（尤其交投活躍的客戶）未必希望收取大量執行交易的通知。因此，我們建議，假如互聯網經紀行已實施充分的保障措施（例如風險披露及客戶確認），客戶可選擇不收取執行交易的通知。然而，客戶不可就任何其他活動（例如登入或向第三方轉移資金）選擇不收取通知。

(III) 其他監控措施

(i) 網絡保安管理層的角色及責任（指引草擬本第 3.1 段）

50. 為強化對網絡攻擊的復原能力，互聯網經紀行應設定適當的網絡保安風險管理框架，包括董事局或高級管理層的明確責任承擔及問責性。我們在2016年網絡保安檢視中注意到，部分經紀行僅非正式地界定網絡保安管理層的角色及責任，例如由不同營運單位（如資訊科技部門）批准的網絡保安政策及程序和業務延續計劃，而沒有就有系統的轉授及匯報作出規定。這導致可能存在沒有人須就一些關鍵的網絡保安風險管理活動承擔責任的情況，因而令經紀行蒙受較高的網絡攻擊風險。

51. 我們建議，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，及列明網絡保安風險管理下的主要角色及責任[25]。然而，這些責任可以書面形式轉授予指定委員會或營運單位，儘管整體責任仍會由負責人員或主管人員承擔。

(ii) 網絡保安事故報告（指引草擬本第 3.2 段）

52. 合適的人員應及時獲報告網絡保安事故，以確保有關問題可迅速及有效地得到處理[18]。根據有關建議，互聯網經紀行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和向外報告。

(iii) 備份和應變計劃（指引草擬本第 2.8 及 2.9 段）

53. 互聯網經紀行現時須設有確保業務紀錄、客戶及交易數據庫、伺服器及證明文件均在離線媒體存有備份的安排[26]。為確保互聯網經紀行在出現危機時能有最新的交易數據以便繼續進行業務，我們建議互聯網經紀行應每天對這些紀錄及數據進行備份。另外，它們應在任何重大系統變更之前及之後，對系統及數據進行全面備份[27]。

54. 2016年網絡保安檢視顯示，大部分參與調查／接受視察的經紀行均設有業務延續計劃，但接近一半的業務延續計劃並無涵蓋網絡保安情境。這個情況並不理想，因為網絡保安情境有別於業務延續計劃所涵蓋的其他情境（例如不能進入辦公室及數據中心的情況），所需的應變安排並不相同。

55. 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，我們建議，互聯網經紀行應盡一切合理努力，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[18]（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。

---

25 該等通函已載述建立網絡保安管理框架的規定。不過本諮詢文件將有關規定擴闊至指明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的角色及責任。

26 《操守準則》附表7第1.2.6(b)段

27 該等通函已載述系統及數據備份的規定，但我們建議指明備份周期並規定須在任何重大系統變更之前及之後進行有關備份。

56. 雖然一些證券經紀行近期遭受分散式阻斷服務攻擊，但我們不建議強制要求購置分散式阻斷服務攻擊解決方案。根據接受視察的經紀行的回應及外部顧問的意見，市場上價格可負擔的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，故此，平衡利弊之後，我們認為專注於制訂健全的業務延續計劃及危機管理程序似乎是更合適的做法。

> 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？

(iv) 網絡保安相關培訓及警示（指引草擬本第 3.3 及 3.4 段）

57. 內部系統使用者[28]在防範網絡攻擊方面擔當重要角色。然而，2016年網絡保安檢視顯示，部分經紀行從未向其內部系統使用者提供任何網絡保安意識培訓，其他經紀行則不定時提供相關培訓。這令人關注到，內部系統使用者是否充分認識不斷演變的網絡保安威脅，以及防範和抵禦潛在網絡攻擊所需的措施。根據有關建議，為提高網絡保安意識，互聯網經紀行應至少每年向所有內部系統使用者提供網絡保安培訓[29]。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（例如偽冒電郵、勒索軟件），以及相應的措施。

58. 另外，為提高客戶的網絡保安意識，互聯網經紀行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[18]。例如，客戶登入互聯網交易系統時，系統可自動彈出網絡保安提示。

(v) 第三方服務提供者管理（指引草擬本第 2.10 段）

59. 許多互聯網經紀行（尤其中小型經紀行）現時均使用由第三方服務提供者提供的互聯網交易系統，亦有部分在向客戶提供互聯網交易服務時，採用應用程式服務提供者的模式。

60. 誠如該等通函所述，如互聯網經紀行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，它們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，互聯網經紀行應確保有關服務提供者所提供的服務，可使它們遵守相關監管規定。此外，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（例如99.9%的系統運行時間或在30分鐘內提供支援服務）。我們建議將以上所述編纂為指引條文，以納入基本規定之內。

> 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？

---

28 內部系統使用者指任何可接達互聯網經紀行的內部網絡和系統的任何常額職員及合約職員。

29 《操守準則》附表 7 第 1.2.4(d)段規定應採取適當的步驟，藉以提升系統使用者對採取保安預防措施的重要性的意識。本諮詢文件旨在將有關規定擴闊至指明進行這些培訓的頻率及培訓內容。

徵詢意見及未來路向

61. 證監會歡迎公眾及業界對本諮詢文件所提出的建議、附錄B內的指引草擬本及附錄C內對《操守準則》的建議修訂發表任何意見。請於2017年7月7日或之前以書面向證監會提交意見。

62. 我們計劃在2017年9月／10月發表諮詢總結，以及敲定《操守準則》的修訂本和新訂的《指引》。為了讓互聯網經紀行有更充足的時間實施基本規定，《指引》會在發表諮詢總結後六個月才生效。

附錄 A

與網絡保安有關的現行監管原則及規定

《操守準則》
[1]第18段及附表7載有就在交易所上市或買賣的證券及期貨合約進行電子交易（其定義包括互聯網交易）的一般原則、一般規定及特定規定。

這些原則及規定有部分亦適用於從事以電子方式買賣槓桿式外匯交易合約的持牌人[2]，及代表所管理的集體投資計劃就在交易所上市或買賣的證券及期貨合約進行電子交易的基金經理[3]。

與互聯網交易的網絡保安風險相關的主要監管原則及規定可概述如下：

(a) 保護客戶的互聯網交易應用程式及帳戶（《操守準則》第18.5段及附表7第1.2.4(a)、(b)及(c)段）

商號應採取充足及適當的保安監控措施，以保護電子交易系統免被濫用。基本的保安監控措施應包括：

(i) 可靠的技術，藉以認證或核實系統使用者的身分及權限，確保只有獲核准且有需要的人士方可接觸或使用系統；

(ii) 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；及

(iii) 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。

(b) 基礎設施保安管理（《操守準則》第 18.5 段及附表 7 的引言、第 1.2.4(a)、(b)及(c)段、第 1.2.6、1.2.7 及 1.2.8 段）

商號應：

(i) 制訂一份書面應變計劃，以處理與電子交易系統有關的緊急情況及中斷事故；

(ii) 確保定期測試用以處理潛在緊急情況及中斷事故的應變計劃，以及有關計劃是可行及足夠的；

(iii) 及時確保重大系統延誤或故障得以糾正，並通知客戶重大系統延誤或故障的原因或可能原因，及將會如何處理客戶的交易指示（如適用）；及

---

1 《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》**）
2 《操守準則》附表 6 第 66 至 67 段
3 《基金經理操守準則》第 9.1 及 9.2 段

(iv) （如電子交易系統由第三方服務提供者提供）作出適當的盡職審查，以確保其在使用該系統時符合《操守準則》第18段及附表7所載的規定。

(c) 網絡保安風險管理的責任承擔（《操守準則》第 18.4 段、《操守準則》附表 7 第 1.1、1.1.1(a)、1.1.1(d)及 1.2.4(d)段以及《操守準則》第 12.5(e)段）

商號應：

(i) 有效管理及充分監督電子交易系統的設計、開發、應用及運作；

(ii) 有至少一名負責人員或主管人員負責電子交易系統的整體管理及監督；

(iii) 實施管理監控措施及監督管制措施，用以管理與其本身或其客戶使用電子交易系統相關的風險；

(iv) 採取適當的步驟，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；及

(v) 在交易系統或工具在運作或施行上出現任何重大缺失、錯誤或缺陷時，立即向證監會匯報。

附錄 B

建議的《降低及紓減與互聯網交易相關的黑客入侵風險指引》

背景

證券及期貨事務監察委員會（**證監會**）建議了多項適用於獲證監會發牌或註冊並從事互聯網交易[1]的經紀行（例如證券交易商[2]、期貨交易商或槓桿式外匯交易商[3]）（**互聯網經紀行**）的基本規定，以降低及紓減與互聯網交易相關的黑客入侵風險。

我們將根據《證券及期貨條例》第399(1)條發出指引，以訂立該等建議規定。有關規定應連同（其中包括）《操守準則》第18.4至18.7段、《操守準則》附表7第1.1、1.2.2至1.2.8、1.3及2.1段一併閱讀。

基本規定包含20項網絡保安監控常規，可分為以下三類：

- 保護客戶的互聯網交易帳戶；
- 基礎設施保安管理；及
- 網絡保安管理和監督。

必須強調的是，建議的監控措施只可降低及紓減與互聯網交易相關的黑客入侵風險，但無法消除有關風險。此外，這些規定只是互聯網經紀行應達致的最低標準，及並非詳盡無遺。

建議規定的詳情

以下規定將被納入根據《證券及期貨條例》第399(1)條發出的建議指引。

1. 保護客戶的互聯網交易帳戶

1.1. 雙重認證[4]

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：

---

[1] 就本指引而言，“互聯網交易”一詞的涵義與《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”。

[2] 包括那些透過其以互聯網為基礎的交易設施分銷所管理的基金的資產經理。

[3] 為免生疑問，有關基本規定只適用於獲證監會發牌或註冊的槓桿式外匯交易商。

[4] 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）。

- 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) 向第三方轉移資金；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的途徑不同（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）。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；

(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；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，在一個月內執行該等程式。

2.5. 端點保護

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。

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[5]），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。

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；

[5] 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。

(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[6]提供網絡保安意識培訓。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。

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。

[6] 內部系統用戶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。

附錄 C

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。

附錄 D

常見的雙重認證監控措施

在客戶登入互聯網交易帳戶時，應實施雙重認證。

下表概述四類常見的雙重認證監控措施的實施成本、對使用者體驗的影響、優點及缺點，以供參考。

	一次性密碼短訊	數碼證書	硬件編碼器	軟件編碼器
實施成本	低	中	高	低
對使用者體驗的影響	低	低	高	中
優點	(i)市場上現時已有可供選用的短訊服務，及(ii)這個方法已廣為使用者採納	有關技術經過驗證、可靠	使用者無論身在何地及使用何種端點裝置均可進行交易	(i)使用者無須攜帶實體編碼器以作認證及(ii)與電子裝置的相互操作性較佳
缺點	使用者必須處於流動網絡覆蓋範圍；若使用者在海外使用流動數據網絡，可能會產生漫遊費用及延誤	(i)需額外成本來維修保養用以管理電子證書及更新證書的基礎設施，及(ii)並非與流動裝置廣泛相容	(i)實施及維修保養的成本相對較高，及(ii)使用者須攜帶硬件編碼器	需額外成本來維修保養用以管理軟件編碼器的基礎設施