2010年3月16日

致所有持牌法團的通函
資訊科技管理

證監會最近在監督過程中注意到在資訊科技方面的若干缺失，可能導致持牌法團本身及其客戶承受資訊保安風險。該等缺失包括：

(a) 在沒有足夠的保障及監控措施的情況下使用若干資訊科技系統設施（例如超級用戶帳戶（superuser account）[1] 及測試環境[2]），從而可能助長一些難以偵察的未經授權交易及挪用客戶資產行爲；及

(b) 沒有實施一些簡單的保安措施，如密碼管制（例如強制用戶在初次登入資訊系統時更改密碼，以防止其繼續使用初時編配予所有用戶的普通密碼）、帳戶管理（例如迅速刪除不需要的用戶帳戶）及啓動審計紀錄[3] 等。

證監會謹此提醒持牌法團須：

(a) 設有妥善的內部監控程序、財政資源及操作能力，而按照合理的預期，這些程序和能力足以保障其運作、客戶及其他持牌人或註冊人，以免其受偷竊、欺詐或不誠實的行爲、專業上的失當行爲或不作爲而招致財政損失[4]；及

(b) 制定適當的政策及程序，確保所有與公司業務運作有關的資料，包括以文件及電子方式存儲的數據都是完整、連貫、保密、齊備、可靠和詳盡的。公司的運作及資料管理系統均應配合公司的需要，並在保密及有充分監控的環境下運作[5]。

就此而言，持牌法團的管理層應定期檢討現有的資訊系統、政策及常規，並在有需要時考慮作出改進，以防範有人未經授權而竄改或侵入資訊系統或有關數據。

由於不同的持牌法團在組織架構及所進行的業務活動的性質和範圍方面都有重大差異，因此並不存在一套放諸四海皆準的監控措施及程序，足以確保資訊保安足夠。不過，本通函的附錄載有一些關於以下重要概念的建議監控措施及程序，以便向持牌法團提供更多指引：

---

1 獲授予特許使用權的超級用戶帳戶，可以被用來進行一系列廣泛活動。如以任何不誠實或不當的方式使用超級用戶帳戶，可能導致(i)客戶資料及交易數據被不當修改；(ii)系統的審計紀錄被停止或刪除；及(iii)客戶資產被挪用（例如透過在人頭戶／代名人帳戶內記入欺詐交易）。

2 設立測試環境的目的通常是模擬真實運作環境，以測試系統變更。如不當使用測試環境，可能導致測試數據被利用來捏造客戶資料甚或帳戶結單。

3 審計紀錄旨在記錄用戶接達資訊系統的情況以及在資訊系統內進行的活動等詳情。如沒有妥善管理系統的審計紀錄功能，可能無法追蹤未經授權的接達或不尋常的活動。

4 《證券及期貨事務監察委員會持牌人或註冊人操守準則》第 4.3 段

5 《適用於證券及期貨事務監察委員會持牌人或註冊人的管理、監督及內部監控指引》第 IV 章〈資料管理〉

Tel: (852) 2840 9222 Fax: (852) 2523 4598 Website: www.sfc.hk

(a) 資訊保安政策；

(b) 接達/使用權限管制；

(c) 加密；

(d) 對系統變更的管理；

(e) 對用戶活動的監察；及

(f) 數據備份及持續運作規劃。

如對本通函的內容有任何疑問，請致電2842 7767與薛慕賢聯絡。

證券及期貨事務監察委員會
中介團體監察科

Tel: (852) 2840 9222 Fax: (852) 2523 4598 Website: www.sfc.hk

附錄

持牌法團須考慮的資訊科技管理事宜

A. 資訊保安政策

1) 制定和實施適當的內部資訊保安政策，定期進行檢討，並在有需要時考慮作出改進
2) 按照既定的資訊保安政策進行合規檢查
3) 加強職員對資訊保安重要性的認知
4) 向使用持牌法團所提供的系統服務的客戶發出資訊保安程序／指引
5) 制定和實施實體保安政策，以便在安全穩妥的環境中保護關鍵的電腦設備（包括伺服器及網絡裝置）

B. 接達/使用權限管制

1. 對用戶帳戶及接達/使用權限的管理

   1) 管理層應對新用戶帳戶的建立及接達/使用權限的批授／修改作出適當的批核管制
   2) 按照"需要知道"原則設定接達/使用權限，並確保將互有抵觸的職能分隔
   3) 定期檢討用戶帳戶的有效性及其接達/使用權限的適當性
   4) 刪除或終止不需要的用戶帳戶及其接達/使用權限
   5) 設定獨有的用戶識別碼，輔以適當的認證機制，以確保用戶活動的問責性
   6) 只在管理層作出適當而審慎的考慮後才批准使用超級用戶帳戶

2. 密碼政策及管制

   1) 實施有效的密碼政策，設定（其中包括）最短密碼長度、密碼組合政策及密碼更換周期
   2) 實施充分認證機制（例如規定登入時須輸入用戶名稱及密碼的有效組合，或在必要時考慮附加認證條件）

3. 網絡及系統接達/連接管制

   1) 規定只有獲授權人士方可接達/連接測試環境及真實運作環境，從而將數據被操控及出現未經授權的系統變更的可能性減至最低
   2) 只在有需要時才向外間人士 (例如系統供應商等) 授予遠程接達/連接權，並監察用戶活動以偵察任何不尋常或未經授權的活動
   3) 當不再需要遠程接達/連接時，即時終止該項連接
   4) 除非已實施妥善的網絡保障措施（例如防毒機制及防火牆），否則應避免與外部網絡 (例如互聯網等) 接達/連接

Tel: (852) 2840 9222 Fax: (852) 2523 4598 Website: www.sfc.hk

C. 加密

1) 當敏感資料傳送至安全的內部網絡以外（例如透過互聯網），或儲存於缺乏有效實體／邏輯保護的可攜式儲存裝置（例如USB記憶體、CD／DVD唯讀光碟或軟磁碟），應施以數據加密保護

D. 對系統變更的管理

1) 妥善測試系統變更，例如爲合理地預期將於實際操作時出現的一切情況制訂及執行測試個案
2) 在參照預計及以往的最高數值後，以足夠的數據和交易量來測試系統的容量及表現
3) 爲系統變更及測試結果備存妥善的審計紀錄
4) 將系統變更轉移至真實運作環境之前，須經管理層批准
5) 在測試環境中只准使用測試數據（即非真實數據），以免敏感資料（例如客戶資料）被不當使用

E. 對用戶活動的監察

1) 確保可藉審計紀錄來記錄資訊系統內的用戶活動，並禁止修改審計紀錄
2) 管理層應監察／定期檢討敏感的應用程式及數據庫的接達/連接/使用情況
3) 持續進行系統表現監察，以確保資訊系統可持續提供服務

F. 數據備份及持續運作規劃

1) 定期爲關鍵數據進行備份
2) 規定只有獲授權人員方可接達/連接/使用數據備份媒體
3) 在場外儲存一套備份數據
4) 定期進行從備份復原數據的測試，確保備份數據在緊急情況下可供使用
5) 規定只有獲授權人員方可使用數據復原功能
6) 實施有效的業務持續運作計劃，並根據該計劃制定資訊科技災難復原計劃，確保能恢復關鍵的資訊系統以支援業務運作

完

SFO/IS/004/2010

Tel: (852) 2840 9222 Fax: (852) 2523 4598 Website: www.sfc.hk