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

SFC
證監會

16 March 2010

Circular to All Licensed Corporations on Information Technology Management

In the course of our supervision, it has recently come to our attention that certain deficiencies in information technology ("IT") areas may expose licensed corporations and their clients to information security risks. Such deficiencies include:

(a) Use of certain facilities of the IT system (for example superuser account[1] and testing environment[2]) without adequate safeguards and controls, which may facilitate unauthorized transactions and misappropriation of client assets which are difficult to detect; and

(b) Not implementing simple security measures such as password controls (for example, mandatory change of password for the first time login to the information system to prevent the use of common password initially assigned to all users), account management (for example, prompt removal of obsolete user accounts) and the activation of the audit log[3].

Licensed corporations are hereby reminded that they are required to

(a) Have internal control procedures and financial and operational capabilities which can be reasonably expected to protect its operations, its clients and other licensed or registered persons from financial loss arising from theft, fraud, and other dishonest acts, professional misconduct or omissions[4]; and

(b) Establish policies and procedures to ensure the integrity, security, availability, reliability and thoroughness of all information, including documentation and electronically stored data, relevant to the firm's business operations. The firm's operating and information management systems should meet the firm's needs and operate in a secure and adequately controlled environment[5].

---

1 Superuser account granted with privileged access rights can be used to perform a wide range of activities. Any dishonest or improper use of the superuser account may result in (i) improper amendment of clients' particulars and transaction data (ii) disabling or removing the audit log and (iii) misappropriation of clients' assets, e.g. through the posting of fraudulent transactions in dummy/nominee accounts.

2 Testing environment is usually set-up to simulate the production environment for testing of system changes. Misuse of testing environment could lead to manipulation of testing data for the production of falsified clients' information or even statements of account.

3 Audit log records details such as user access and user activities performed in the information system. If the functionality of audit log is not properly managed, this may result in a lack of audit trail of unauthorized access or unusual activities.

4 Paragraph 4.3 of the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission

5 Part IV – Information Management, Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission

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

In this connection, management of licensed corporations should regularly review their existing information systems, policies and practices and consider enhancement where needed, so as to guard against unauthorized alteration of, or intrusion into, the information systems or the data.

Given the significant differences that exist in the organizational structures as well as the nature and scope of the business activities conducted, there exists no single set of universally applicable control techniques and procedures which will guarantee the adequacy of information security. However, with a view to providing more guidance to licensed corporations, the Appendix has included some suggested control techniques and procedures in respect of the following key ideas:

(a) Information security policy;

(b) Access control;

(c) Encryption;

(d) Change management;

(e) User activities monitoring; and

(f) Data backup and continuity planning.

Should you have any queries regarding the contents of this circular, please contact Coolky Sit at 2842 7767.

Intermediaries Supervision Department
Securities and Futures Commission

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

Appendix

Information Technology Management
Issues to be considered by licensed corporations

A. Information security policy

1) Establish and implement appropriate internal information security policy and perform regular review and consider enhancement where needed
2) Perform compliance checking against the established information security policy
3) Raise staff awareness on the importance of information security
4) Issue information security procedures/guidelines to its clients who access the system services offered by the licensed corporations
5) Formulate and implement physical security policy to protect critical computer equipments (including the server and network device) in a secure environment

B. Access control

1. User account and access rights management
   1) Exercise proper management approval control over creation of new user account and granting/modifying access right
   2) Set access right on a need-to-know basis and ensure segregation of incompatible duties
   3) Review the validity of user account and appropriateness of its access right on a regular basis
   4) Remove or terminate obsolete user accounts and their access rights
   5) Create unique user-identification codes with appropriate authentication mechanism to ensure accountability of user activities
   6) Grant superuser account only after due and careful consideration by management

2. Password policy and control
   1) Implement effective password policy by setting, inter alia, minimum password length, password composition policy, and password life cycle
   2) Implement adequate authentication mechanism (such as login by inputting a valid combination of user ID and password or when necessary consider additional authentication factors)

3. Network and system access control
   1) Access to both testing and production environment should be restricted to

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

authorized parties only so as to minimize possible data manipulation and unauthorized system changes

2) Grant remote access right to external parties such as system vendors only on a needs basis and monitor the user activities to detect any unusual or unauthorized activities

3) Terminate remote access connection immediately when such connection is no longer necessary

4) Avoid access to/by external network such as Internet unless proper network safeguards (such as anti-virus mechanism and firewall) are implemented

C. Encryption

1) Apply data encryption to protect sensitive information transmitted outside secured internal network (e.g. over the Internet) or stored in portable storage devices (e.g. USB memory key, CD/DVD-ROM or floppy disk) without strong physical/logical protection

D. Change management

1) Test system changes properly, for instance, develop and execute test cases which cover all scenarios which can be reasonably anticipated in actual operation

2) Test system capacity and performance with sufficient data and transactions volume with reference to anticipated and historical peaks

3) Maintain proper audit trails for system changes and test results

4) Seek approval from management before system changes are migrated to the production environment

5) Avoid possible misuse of sensitive information (e.g. client information) by only allowing testing data (i.e. not production data) to be used in testing environment

E. User activities monitoring

1) Make sure audit log is available to log user activities in the information systems and audit log should be restricted from modification

2) Management to monitor/regularly review the access to sensitive application program sources and databases

3) Perform performance monitoring on a continuous basis to ensure the availability of information systems

F. Data backup and continuity planning

1) Perform backup on critical data on a regular basis

2) Access to data backup media should be restricted to authorized personnel only

3) Store a set of backup data off site

4) Test restoration of data from data backup on a regular basis to ensure availability of data in case of emergency

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

5) Access to data restoration functions should be restricted to authorized personnel only

6) Implement an effective business continuity plan. Based on the business continuity plan, IT disaster recovery plan should be formulated to ensure critical information systems can be resumed to support business operations

End

SFO/IS/004/2010

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