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

Report on the 2019-20 thematic cybersecurity review of internet brokers

September 2020

Contents

A. Executive summary

1. The Cybersecurity Guidelines[1], which set out 20 baseline requirements including Two-Factor Authentication (2FA), were issued by the Securities and Futures Commission (SFC) in October 2017 and fully implemented in July 2018.

2. The SFC commenced a thematic review in 2019 to examine the systems and related management controls of licensed corporations which engage in internet trading business in Hong Kong and assess their compliance with the Cybersecurity Guidelines and the Code of Conduct[2]. To address reported concerns[3] that some mobile applications might be more vulnerable to hacking risks, the review also focused on security controls for mobile trading applications.

3. The SFC conducted:

   (a) a survey completed by 55 selected internet brokers with diverse backgrounds; and

   (b) onsite inspections of 10 of these 55 firms of various sizes and with different operating business models to review their system controls and other related management controls, supplemented by discussions with several system vendors commonly engaged by internet brokers in Hong Kong to support their internet trading systems.

4. The survey results and inspection findings revealed that most firms complied with the SFC's key regulatory requirements. Nevertheless, the SFC noted deficiencies and instances of non-compliance in the protection of clients' internet trading accounts (including the implementation of 2FA, data encryption and monitoring and surveillance to identify suspicious unauthorised transactions), infrastructure security and user access management as well as cybersecurity management and incident reporting.

5. This report summarises the key findings and observations of the review and provides guidance and reminders on our expected standards. It highlights the deficiencies and instances of non-compliance with the relevant baseline and Code of Conduct requirements noted during the review as well as the good practices adopted by surveyed and inspected firms.

[1] Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading.

[2] These include paragraphs 18.4 to 18.7 of, and paragraphs 1.1, 1.2.2 to 1.2.8, 1.3 and 2.1 of Schedule 7 to, the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (Code of Conduct).

[3] The Hong Kong Wireless Technology Industry Association found in its study in mid-2017 that 44% of the 140 Android applications provided by different financial institutions, including brokers, failed its security test.

B. Overview of the internet broking industry landscape in Hong Kong

6. Based on the 1,372 responses to the SFC's Business & Risk Management Questionnaire submitted by firms licensed for Type 1, 2 or 3 regulated activities from August 2019 to July 2020, 511 firms, or 37%, provided internet trading services to clients. Of these 511 firms:

   (a) 49% derived more than half of their turnover from internet trading;

   (b) 14% allocated more than 30% of their annual financial budget to information technology (IT);

   (c) all 511 firms had implemented 2FA solutions for their internet trading systems and put in place automated client notification controls. However, 12% had not implemented any monitoring or surveillance measures to detect unauthorised access to clients' internet trading accounts;

   (d) 94% used vendor-supplied systems; and

   (e) none reported any hacking of client accounts while 1% reported cybersecurity incidents such as denial-of-service (DDoS)[4] and ransomware attacks and 5% reported unplanned system outages which affected the ability of clients to access their internet trading services.

7. Our survey of 55 selected internet brokers (respondents) provided the following insights into the industry's landscape:

   (a) Turnover

      (i) The monthly turnover of the 55 respondents ranged from $0.4 million to $142 billion for securities and from less than one contract to 1.4 million contracts for futures and options. On average, the monthly turnover of these firms was approximately $16 billion for securities and 150,000 contracts for futures and options.

      (ii) Thirty-seven respondents engaged in securities trading, of which 11 reported that less than 20% of turnover was from internet trading and 12 reported that it was more than 70%. Forty-one respondents engaged in futures and options trading, six of which reported that less than 20% of turnover was from internet trading and 23 reported that it was more than 70%.

   (b) Systems

      (i) The 55 respondents operated a total of 106 internet trading systems:

         - 60 systems only supported securities trading; 36 only supported futures and options trading and 10 supported both securities trading and futures and options trading.

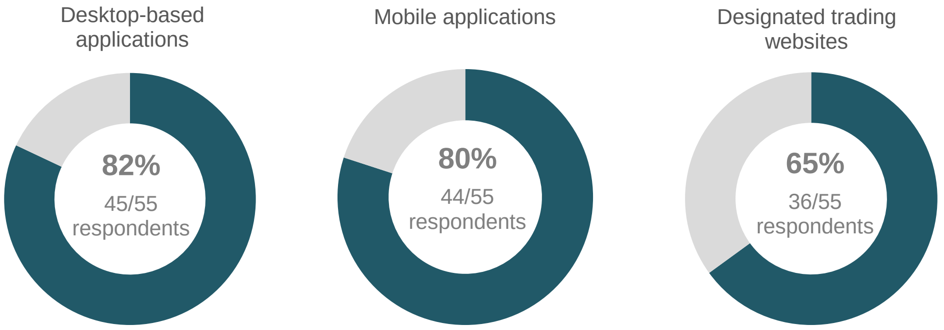
[4] In a DDoS attack, multiple compromised computer systems attack a server, website or other network resource, causing a denial of service for its users.

- Systems were provided on the following platforms:

Platforms	No. of systems
All platforms (mobile, desktop and designated trading websites)	23
Desktop only	23
Mobile and desktop	21
Mobile only	15
Designated trading websites only	11
Mobile and designated trading websites	9
Desktop and designated trading websites	4
Total	**106**

- External vendors provided and supported 75 systems, 21 were developed in-house and 10 were supplied and operated on an Application Service Provider (ASP) model, where an external vendor provides and supports both application services and the underlying infrastructure.

(ii) Most of the 55 respondents provided desktop-based applications[5] and mobile applications, and about two-thirds provided designated trading websites[6]:



(iii) To support their internet trading systems, 49 respondents engaged third-party service providers, such as ASPs, data centre service providers and vendors of internet trading applications and software.

(c) Resources

(i) The 55 respondents' annual IT budgets ranged from $55,000 to $1.1 billion; 19 had budgets of less than $2 million. The average was $8 million.

(ii) 46 respondents allocated less than 25% of their IT budgets to cybersecurity management.

(iii) On average, the 55 respondents had 21 IT personnel. 40 had 10 or less, and six (excluding respondents with separate IT staff within the group companies) had two or less; one respondent was supported by 600 IT personnel globally.

[5] These require clients to install the internet broker's software or programme on their computers or devices.

[6] Applications that run from an internet browser, eg, Internet Explorer, Chrome, Firefox and Safari.

(iv) Of the 55 respondents:

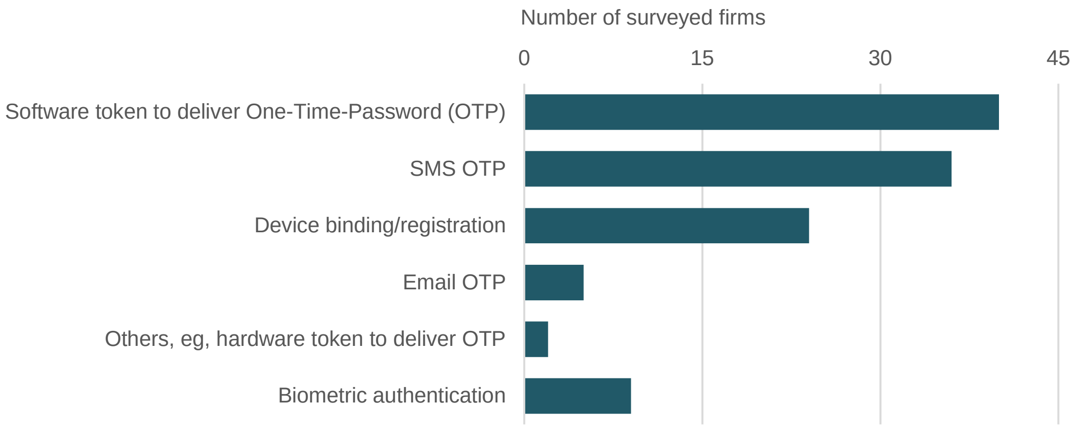
- two respondents, which were part of the same group, did not have a designated person or committee in charge of cybersecurity management;

- two respondents' responsible officers for the overall management and supervision of internet trading systems (RO-Internet trading) had IT-related qualifications while 35 respondents' RO-Internet trading had more than five years of IT management experience in the securities or futures industry; and

- the Manager-In-Charge of IT (MIC-IT) of 22 respondents had IT-related qualifications while the MIC-IT of 51 respondents had more than five years of IT management experience in the securities or futures industry.

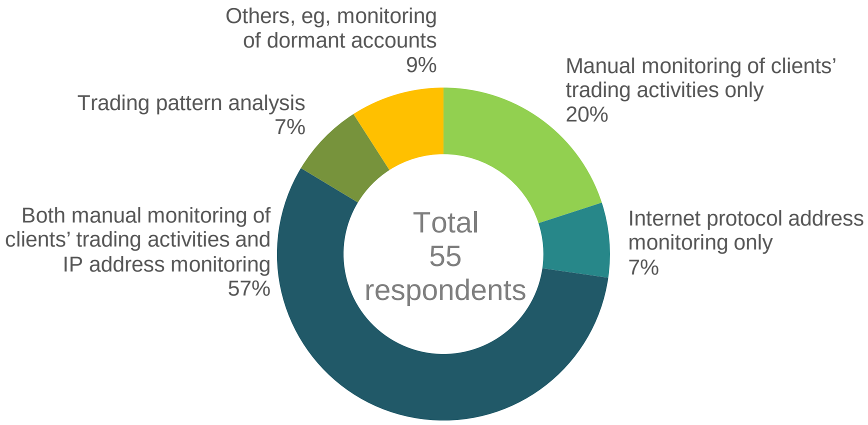
(d) 2FA

Of the 106 systems operated by these 55 respondents, all adopted user ID and password as "what a client knows" as well as the following as their second factor for user authentication purposes:

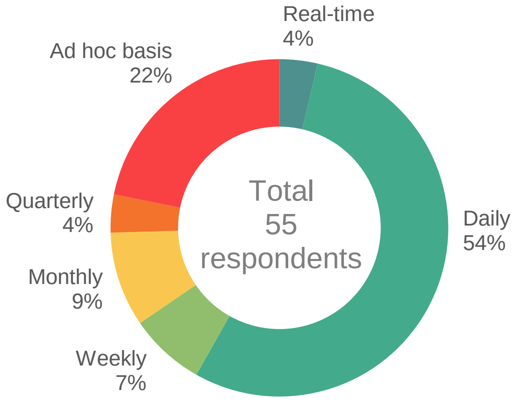


(e) Monitoring and surveillance

Mechanisms



Intervals



8. Based on the cybersecurity incidents reported to the SFC from 2016 to 2019 and the results of the survey, there were no reports of hacking of client accounts after the baseline requirements became effective. Only three internet brokers reported DDoS or ransomware attacks to the SFC. Nine of the 55 respondents reported cybersecurity issues in the year ended 31 July 2019, six of which involved system outages and three were related to fake websites.

9. The following observations can be drawn from the responses to the survey and the Business & Risk Management Questionnaire:

   (a) more than one-third of firms licensed for Type 1, 2 or 3 regulated activities provide internet trading services to their clients;

   (b) the sizes, operation models and systems controls of internet brokers vary widely;

   (c) the vast majority of internet brokers rely on external vendors to develop and support their internet trading systems; and

   (d) while the provision of desktop-based applications remains the most common, mobile applications and, to a lesser extent, designated trading websites have also become more prevalent amongst the 55 respondents.

C. Deficiencies, instances of non-compliance with baseline requirements and good practices

Protecting clients' internet trading accounts

2FA

> Baseline requirements - Paragraph 1.1
>
> *A licensed person should implement 2FA for login to clients' internet trading accounts.*
>
> *A licensed person should assess and implement a 2FA solution which is commensurate with its business model.*

10. 2FA refers to an authentication mechanism which utilises any two of the following factors: what a client knows, what a client has and who a client is.

    (a) For "what a client knows", internet brokers typically adopt user ID and password;

    (b) For "what a client has", internet brokers typically adopt one or more of the following solutions:

       (i) a one-time password (OTP) is delivered via short messaging service (SMS) to a client's designated mobile device or generated from an application installed on a client's designated device;

       (ii) an OTP is generated from a hardware token provided to a client; and

       (iii) device binding or registration where a client binds or registers a computer or other device with the firm's internet trading system which allows that computer or device to be recognised by its unique device information (eg, Media Access Control (MAC[7]) address and International Mobile Equipment Identity (IMEI[8]) number).

    (c) For "who a client is", internet brokers adopt biometric authentication—a security process which validates a client's biometric data (eg, fingerprint and facial recognition) against an encrypted version of the biometric data stored in that client's mobile device.

<u>Deficiencies and instances of non-compliance</u>

A. Email OTP

11. Two inspected firms adopted email OTP as their second authentication factor, that is, "what a client has". This is not effective as the person logging in may not be the actual client for the following reasons:

[7] A MAC address is a hardware identification number which uniquely identifies a computing device on a network for communication purposes.

[8] The IMEI number of a mobile device is its unique identification or serial number.

(a) an email OTP can be delivered to multiple devices, eg, both a mobile phone and a computer, and be accessed or read by multiple applications on each of these devices;

(b) an email OTP may not always be directed to the client as the login credentials for email accounts can be shared with multiple persons; and

(c) security protection for email accounts is insufficient, eg, the email forwarding function may result in inadvertent sharing of the OTP with other persons.

12. Separately, some internet brokers may deliver OTPs via both SMS and email. When the SMS OTP is a valid second authentication factor, it would be risky to deliver the OTP by email for reasons stated above. Internet brokers ***should not*** deliver OTPs via email.

B. Deactivation of 2FA

13. One inspected firm allowed clients to deactivate 2FA for system login. As 2FA is mandatory, internet brokers should not allow their clients to deactivate this function.

C. Device binding or registration

14. At one inspected firm, owing to a technical security loophole in its internet trading application, the device information for its clients' computers could be mimicked, thereby allowing a hacker to log into the clients' internet trading accounts. This security loophole made device binding or registration inoperative as the second authentication factor. Internet brokers ***should*** perform technical assessments on a regular basis to identify security loopholes for prompt rectification.

15. At another inspected firm, an unlimited number of devices could be bound or registered and concurrent logins from those devices were allowed. This is not satisfactory because an excessive number of bound or registered devices and concurrent logins would give rise to additional hacking risks where more devices could potentially be targeted and hacked. Internet brokers ***should not*** allow a client to bind or register an excessive number of devices to that client's internet trading account and ***should*** implement controls over concurrent logins. For example,

(a) where an individual client requests to bind or register more than three devices, internet brokers should understand the reasons why and assess the reasonableness of the request;

(b) where a corporate client requests to bind or register multiple devices so that they can be operated by its authorised persons, internet brokers should advise the corporate client of the creation of sub-accounts (each with its own 2FA) for those authorised persons;

(c) where a sub-account arrangement is not feasible, internet brokers should ask their corporate clients about the number of persons authorised to operate their internet trading accounts and limit concurrent logins accordingly.

Implementing monitoring and surveillance mechanisms

Baseline requirements - Paragraph 1.2

A licensed person should implement an effective monitoring and surveillance mechanism to detect unauthorised access to clients' internet trading accounts.

16. Internet brokers can adopt different methods to identify suspicious unauthorised transactions. For example, where a firm only operates internet trading on a limited scale and is familiar with its clients' trading patterns, the firm may effectively identify suspicious unauthorised transactions by manually reviewing client transactions for seeming irregularities at the end of the day. In other cases, internet brokers may, amongst other things, implement an internet protocol (IP) address monitoring tool to generate alerts automatically upon detecting abnormal changes in the IP addresses from which clients login, for example from a different country or city within a short period of time.

17. Once internet brokers detect suspicious unauthorised account access or transactions, they ***should*** immediately follow up on abnormities with the clients concerned for validation purposes. Prompt follow-up and remedial actions (eg, suspension of accounts suspected to have been hacked) are crucial for damage control.

Deficiencies and instances of non-compliance

18. Eleven of the 55 respondents only performed manual reviews of client transactions. As some of them had a large number of internet trading clients who generated substantial trading volumes on a daily basis, manual reviews alone could not effectively identify suspicious unauthorised transactions. Internet brokers ***should*** take into account the scale of their internet trading operations and implement a monitoring and surveillance mechanism which is appropriate and commensurate with their business needs.

19. Nineteen of the 55 respondents only performed monitoring and surveillance on a monthly, quarterly or ad hoc basis. This would be inadequate for ensuring timely detection and follow-up. Internet brokers ***should*** at least perform monitoring and surveillance on a daily basis.

20. Three inspected firms, when implementing automated IP address monitoring, had mistakenly assigned the same generic IP address to all login attempts from different mobile or web users due to a network gateway misconfiguration. Internet brokers ***should*** conduct sufficient technical and user testing before implementing an automated IP address monitoring tool.

Good practices

21. Four respondents developed and implemented computer-assisted monitoring tools for the detection of unusual practices or questionable client transactions. These tools would generate real-time alerts when predefined parameters or thresholds were triggered or predefined transaction patterns were detected, eg, selling all the stocks in a client's portfolio and using the proceeds to buy a small-cap stock at a price below a set level. The underlying parameters and thresholds would be reviewed and updated as appropriate on a regular basis.

22. Forty-three respondents implemented an Intrusion Detection System (IDS) to monitor the network and systems and send alerts to system administrators if a potential threat was

detected. In addition, one inspected firm had installed an Intrusion Prevention System (IPS) which can detect and prevent vulnerability exploits.

23. Internet brokers ***should*** consider a combination of the above practices in order to improve their internet trading systems as appropriate.

Prompt notification to clients

> Baseline requirements - Paragraph 1.3
>
> *A licensed person should notify clients promptly after certain specified client activities have taken place in their internet trading accounts. Clients may choose to opt out from either "trade execution" or "system login" notifications, subject to exceptions[9], but not password reset.*

Deficiencies and instances of non-compliance

24. Forty-eight respondents did not provide client notifications after certain actions, such as a password reset, had been taken in the client's internet trading account. Internet brokers are reminded to review the activities covered by client notifications to ensure compliance with paragraph 1.3 of the Cybersecurity Guidelines.

25. Separately, two of these 48 respondents allowed clients to opt out from receiving notifications after a password reset, and one of them allowed clients to opt out from notifications for both system login and trade execution. Internet brokers are reminded:

    (a) not to allow clients to opt out from notifications for password reset; and

    (b) only to allow clients to opt out from notifications for system login or trade execution in exceptional cases as provided for by the SFC.

Data encryption

> Baseline requirements - Paragraph 1.4
>
> *A licensed person should use a strong encryption algorithm to:*
>
> *(a) encrypt sensitive information such as client login credentials (ie, user ID and password) and trade data during transmission between internal networks and client devices; and*
>
> *(b) protect client login passwords stored in its internet trading system.*

[9] Clients may opt out from "trade execution" notifications under circumstances stipulated in Paragraph 1.3 of the Cybersecurity Guidelines. Clients may opt out from "system login" notifications after meeting the conditions set out in Q4 of the SFC Cybersecurity FAQs: https://www.sfc.hk/web/EN/faqs/intermediaries/supervision/cybersecurity/cybersecurity.html.

Deficiencies and instances of non-compliance

26. Seven inspected firms implemented data encryption algorithms which did not meet international security standards[10]. The use of weak encryption algorithms increased the risk of data breaches and system compromises. Internet brokers ***should*** review international security standards (eg, the cryptographic standards provided by NIST[11]) on an ongoing basis, check the status of their data encryption algorithms and upgrade them as appropriate.

Good practice

27. Nineteen respondents used salting[12] in the hashing algorithm to provide additional safeguards for password storage. Internet brokers ***should*** consider this practice in order to improve their internet trading systems as appropriate.

Protecting client login passwords

> Baseline requirements - Paragraph 1.5
>
> *A licensed person should establish and implement effective policies and procedures to ensure that a client login password is generated and delivered to a client in a secure manner during the account activation and password reset processes. A client login password should be randomly generated by the system and sent to a client through a channel of communication which is free from human intervention and from tampering by staff of the licensed person.*
>
> *In a situation where a client login password is not randomly generated by the system, the licensed person should implement adequate compensating security controls such as compulsory change of password upon the first login after client account activation.*

Deficiencies and instances of non-compliance

28. Two respondents did not randomly generate client login passwords or require compulsory change of password upon a client's first login to the internet trading system. Internet brokers are reminded to ensure that client login passwords are either randomly generated or that adequate compensating security controls are implemented.

[10] Examples of weak encryption algorithms identified during the cybersecurity review include:
(i) For data transmission: SSL 3.0, TLS 1.0, TLS 1.1, TLS_RSA_WITH_RC4_128_MD5
(ii) For data storage: DES, 3DES, RC4, RC5, RSA 1024-bit, Blowfish, Twofish, MD5, SHA-1

[11] National Institute of Standards and Technology.

[12] When a salt is added to the hashing process, it increases the uniqueness and complexity of the hash value, which can further mitigate the risk of password attacks.

Stringent password policies and session timeout controls

> Baseline requirements - Paragraph 1.6
>
> *A licensed person should set up stringent password policies and session timeout controls in its internet trading system, which include:*
>
> *(a) minimum password length;*
>
> *(b) periodic reminders for those clients who have not changed their passwords for a long period;*
>
> *(c) minimum password complexity (ie, alphanumeric) and history;*
>
> *(d) appropriate controls on invalid login attempts; and*
>
> *(e) session timeout after a period of inactivity.*

Deficiencies and instances of non-compliance

29. The password policies of six inspected firms did not:

    (a) require periodic reminders to be issued to clients who had not changed their passwords for a long period;

    (b) stipulate sufficient password complexity (ie, alphanumeric) or restrictions on reuse of previous passwords; or

    (c) set appropriate controls on invalid login attempts. Internet brokers are reminded to review password policies to ensure compliance with paragraph 1.6 of the Cybersecurity Guidelines.

30. Separately, for nine inspected firms, session timeout could either be disabled by clients or the idle timeout period could be as long as 24 hours. This is not satisfactory because there is an increased risk of unauthorised access when an attacker has unlimited time or an unduly long period of time for hacking attempts. Internet brokers ***should***:

    (a) disallow clients from disabling session timeout; and

    (b) limit the idle timeout period (eg, within 30 minutes) subject to prior assessment and ongoing monitoring. For example, a client conducting programme trading may need to be on standby to effect transactions at any time. In this case, internet brokers could allow a longer idle timeout period, but they would then have to more closely monitor that client’s login and logout records and trading activities.

31. At one inspected firm, a technical error led to the deactivation of its session timeout control. Clients’ internet trading accounts were not disconnected when the defined timeout period was exceeded. Internet brokers ***should*** perform sufficient testing to ensure session timeout controls are configured and functioning properly.

Infrastructure security management

Deploying a secure network infrastructure

Baseline requirements - Paragraph 2.1

A licensed person should deploy a secure network infrastructure through proper network segmentation, ie, a Demilitarised Zone (DMZ) with multi-tiered firewalls, to protect critical systems (eg, internet trading system and settlement system) and client data against cyber-attacks.

Deficiencies and instances of non-compliance

32. Two inspected firms' system servers and databases hosting internet trading applications and other critical systems resided within a DMZ, which is less secure than an internal network behind a DMZ. In addition, two other firms placed their web servers, typically used to host the company webpage or other less sensitive data, within the internal network. Internet brokers ***should***:

    (a) place internet trading applications and other critical systems within an internal network behind a DMZ; and

    (b) host servers with less sensitive data, eg, the web server hosting the company webpage, within a DMZ.

Good practices

33. All inspected firms had deployed multi-tiered firewalls of different brands and models in their network infrastructure.

34. Seven of the inspected firms had implemented anti-DDoS mechanisms such as clean-pipe services and anti-DDoS mitigation solutions. One also deployed Network Based Anomaly Detection solutions to track critical network characteristics and detect abnormal events or trends from the baseline of normal network behaviour.

35. Forty respondents adopted an anti-Advanced Persistent Threat solution and a web application firewall.

36. Internet brokers ***should*** consider a combination of the above practices in order to improve their internet trading systems as appropriate.

User access management

Baseline requirements - Paragraph 2.2

A licensed person should have policies and procedures in place to ensure that system access or the use of the systems are granted to users on a need-to-have basis. In addition, a licensed person should review, at least on a yearly basis, the *user access list of critical systems (eg, internet trading systems and settlement systems) and databases (eg, client data) to ensure that access to or use of the systems remains restricted to persons approved to use them on a need-to-have basis.*

Deficiencies and instances of non-compliance

37. Two inspected firms granted excessive rights to access critical systems and databases. One did not implement adequate procedures for granting user access rights (eg, risk management staff were granted access rights to an order input function). The other continued to grant access rights to staff after their departure. Internet brokers are reminded to conduct user access reviews at least annually to ensure that access rights are only granted and retained on a need-to-have basis.

Good practices

38. Seventeen respondents implemented a Privileged Identity Management (PIM) or Privileged Access Management (PAM) solution to manage and monitor highly privileged access (eg, superuser or administrator) within the IT environment.

39. One inspected firm deployed automated processes for user access recertification whereby all user access rights would be recertified on an annual basis by business department line managers and IT administrators.

40. Internet brokers ***should*** consider a combination of the above practices to improve their internet trading systems as appropriate.

Security controls for remote connections[13]

Baseline requirements - Paragraph 2.3

A licensed person should grant remote access to its internal network on a need-to-have basis and implement security controls over such access.

Deficiencies and instances of non-compliance

41. Seven respondents granted permanent remote access to vendors at all times. Internet brokers ***should*** avoid granting permanent remote access to external parties.

Good practices

42. Twenty-eight respondents implemented multi-factor authentication (with at least two factors) for remote access by employees, vendors and users accessing privileged accounts or sensitive data repositories.

[13] For further guidance, please refer to the circular titled “Management of cybersecurity risks associated with remote office arrangements” which can be found at https://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=20EC37

43. Forty-two respondents only allowed remote access via a virtual private network which provides additional security.

44. Internet brokers ***should*** consider a combination of the above practices in order to improve their internet trading systems as appropriate.

Patch management

Baseline requirements - Paragraph 2.4

A licensed person should monitor and evaluate security patches or hotfixes released by software provider(s) on a timely basis and, subject to an evaluation of the impact, conduct testing as soon as practicable and implement the security patches or hotfixes within one month following the completion of testing.

Deficiencies and instances of non-compliance

45. Six inspected firms took a prolonged period of time, ie, more than six months, to evaluate, test and implement security patches and hotfixes, including those ranked as critical or of high severity. Only in May 2019 did one firm implement critical security patches released between 2016 and 2018. Internet brokers ***should*** identify and implement urgently needed security patches or hotfixes as soon as possible.

46. Two other inspected firms evaluated, tested and implemented all security patches and hotfixes by batches every six months. This approach could cause delay the implementation of critical security patches and hotfixes. Internet brokers ***should*** only adopt a batch implementation approach for non-critical security patches and hotfixes and implement batches at least on a quarterly basis unless, after evaluation, it determines that they may be incompatible with system applications and cannot be implemented.

47. Separately, two inspected firms used end-of-life (EOL) software[14]. Given that vendors no longer provide security fixes for EOL software, network and system vulnerabilities may be exploited by hackers. Internet brokers ***should*** ensure that vendors support the software they use, by monitoring the validity of existing software on an ongoing basis and in a timely manner and replacing or upgrading software that is EOL or close to EOL.

48. A licensed person ***should*** evaluate security patches or hotfixes released by software providers in a timely manner to identify and promptly implement those which are urgently needed to fix loopholes and vulnerabilities ranked as critical or high severity[15]. A licensed person ***should*** also implement security patches or hotfixes which are not urgently needed within a reasonable timeframe.

[14] This refers to software which has reached the end of its useful life and its vendor has stopped supporting it (eg, Windows Server 2008).

[15] Reference may be made to the National Vulnerability Database where the NIST provides severity rankings for common vulnerabilities. Please refer to https://nvd.nist.gov/vuln-metrics/cvss for details.

End-point protection

> Baseline requirements - Paragraph 2.5
>
> *A licensed person should implement and update anti-virus and anti-malware solutions on a timely basis to detect malicious applications and malware on critical system servers and workstations.*

Deficiencies and instances of non-compliance

49. Four respondents did not install anti-virus or anti-malware solution in all critical servers and one did not install anti-malware in all of its critical workstations. Internet brokers are reminded to install these solutions in all critical system servers and workstations.

System and data backup

> Baseline requirements - Paragraph 2.8
>
> *A licensed person should back up business records, client and transaction databases, servers and supporting documentation in an off-line medium on at least a daily basis.*
>
> *A licensed person should also adopt an appropriate recovery method to enable successful roll-back of major system changes.*

Deficiencies and instances of non-compliance

50. Based on the cybersecurity survey:

    (a) one respondent only backed up on a monthly basis; and

    (b) six respondents did not back up to an offline medium.

51. Internet brokers are reminded to back up their business records, amongst other things, to an off-line medium at least on a daily basis.

Good practice

52. Seven inspected firms performed restoration tests of backup records at least annually to ensure the effectiveness of data recovery. Internet brokers ***should*** consider this practice to improve their internet trading systems as appropriate.

Contingency planning for cybersecurity scenarios

> Baseline requirements - Paragraph 2.9
>
> *A licensed person should make all reasonable efforts to cover possible cyber-attack scenarios such as DDoS attacks and total loss of business records and client data resulting from cyber-attacks (eg, ransomware) in the contingency plan and crisis management procedures.*

Deficiencies and instances of non-compliance

53. Two respondents did not include cybersecurity scenarios such as data leakage and ransomware in their contingency plans. Internet brokers are reminded to cover possible cyber-attack scenarios in their contingency plans and crisis management procedures.

Cybersecurity management and supervision

Roles and responsibilities of cybersecurity management

> Baseline requirements - Paragraph 3.1
>
> *The RO(s)-Internet trading should define a cybersecurity risk management framework (including but not limited to policies and procedures), and set out key roles and certain specified responsibilities.*

Deficiencies and instances of non-compliance

54. Of the 55 respondents:

    (a) two did not have any designated person or committee responsible for their cybersecurity management;

    (b) 21 did not define all of the roles and responsibilities stipulated in paragraph 3.1 of the Cybersecurity Guidelines;

    (c) one had a designated person responsible for its cybersecurity management but did not define that person’s roles or responsibilities in relation to its cybersecurity management framework;

    (d) 12 only defined a cybersecurity management framework informally, without any documentation;

    (e) 11 only conducted IT audit or cybersecurity self-assessment on an ad hoc basis; and

    (f) 26 did not sufficiently cover the baseline requirements in their IT audits or self-assessments.

55. Internet brokers are reminded to clearly define the roles and responsibilities of the designated committee, operational unit or personnel responsible for cybersecurity risk management. Internet brokers ***should*** review their compliance with the baseline requirements in their IT audit or cybersecurity assessment at least annually.

Good practices

56. In the past 18 months, 24 respondents had performed penetration testing (ie, the process of ascertaining system and data which can be accessed by a hacker through the exploitation of network and application vulnerabilities).

57. Fourteen respondents had insurance cover for cybersecurity incidents.

58. One inspected firm had set up a Security Operations Center[16] (SOC) to take charge of all security monitoring processes and technologies and coordinate incident detection and handling.

59. Another firm performed a gap analysis to compare its global cybersecurity procedures and practices against the baseline requirements and other relevant requirements in Hong Kong.

60. Internet brokers ***should*** consider a combination of the above practices to improve their internet trading systems as appropriate.

Cybersecurity incident reporting

> Baseline requirements - Paragraph 3.2
>
> *A licensed person should establish written policies and procedures specifying the manner in which a suspected or actual cybersecurity incident should be escalated and reported internally (eg, to the responsible officer(s) in charge of internet trading) and externally (eg, to clients, the SFC and other enforcement bodies, where appropriate).*

Deficiencies and instances of non-compliance

61. Three respondents did not have procedures in place for escalating and reporting suspected or actual cybersecurity incidents. In addition, one inspected firm experienced an outage of its internet trading system for one entire morning trading session. However, the clients of this firm were not informed (eg, through email or the company website) of the system outage or the alternative trading channels available during an outage.

62. Internet brokers are reminded to establish written policies and procedures to escalate and report incidents to internal and external parties as soon as practicable.

Good practice

63. Upon the identification of potential or actual unauthorised access to clients' internet trading accounts, 38 respondents would suspend the client accounts and inform the clients concerned,

[16] An SOC is a centralised unit which monitors, assesses and defends the IT systems and infrastructure of a firm and responds to cybersecurity incidents.

regulators and the Hong Kong Police. Internet brokers ***should*** consider this practice in order to improve their internet trading systems as appropriate.

Cybersecurity awareness training for internal system users

> Baseline requirements - Paragraph 3.3
>
> *A licensed person should provide adequate cybersecurity awareness training to all internal system users (ie, any permanent and contract staff having access to the internal network and systems of that licensed person) at least on a yearly basis.*

Deficiencies and instances of non-compliance

64. Two respondents did not provide any form of cybersecurity awareness training. Eighteen respondents did not provide cybersecurity awareness training to all of their internal system users. Separately, at eight inspected firms, only some internal system users attended annual cybersecurity awareness training and there was no follow-up on those who had not attended.

65. Internet brokers are reminded to provide cybersecurity awareness training to all internal system users at least annually.

Cybersecurity alert and reminder to clients

> Baseline requirements - Paragraph 3.4
>
> *A licensed person should take all reasonable steps to remind clients about and alert them to cybersecurity risks and recommended preventive and protection measures when using the internet trading system.*

Deficiencies and instances of non-compliance

66. Forty-four respondents did not provide cybersecurity tips or reminders to their clients on a regular basis. Internet brokers are reminded to take reasonable steps to provide sufficient cybersecurity alerts and reminders to clients.

Good practice

67. Forty-three respondents subscribed to cybersecurity threat intelligence services to analyse and share with clients the latest information on cyber-attacks and vulnerabilities. Internet brokers ***should*** consider this practice as appropriate to improve their internet trading systems.

D. Mobile trading applications – compliance with Code of Conduct requirements

68. Our cybersecurity onsite inspection noted that all 10 inspected firms offered mobile trading applications to their clients but some did not employ adequate or appropriate preventive or detective controls to protect their internet trading systems.

> Code of Conduct requirements[17]
>
> *A licensed person should employ adequate and appropriate security controls to protect the electronic trading system it uses or provides to clients for use from being abused. The security controls should at least include:*
>
> *(a) reliable techniques to authenticate or validate the identity and authority of the system users to ensure that the access or the use of the system is restricted to persons approved to use the system on a need-to-have basis;*
>
> *(b) effective techniques to protect the confidentiality and integrity of information stored in the system and passed between internal and external networks;*
>
> *(c) appropriate operating controls to prevent and detect unauthorised intrusion, security breach and security attack; and*
>
> *(d) appropriate steps to raise the awareness of system users on the importance of security precautions they need to take in using the system.*

Deficiencies and instances of non-compliance

<u>Detective control</u>

69. Six inspected firms did not implement any controls in mobile trading applications to detect devices which had been compromised (ie, jailbroken[18] or rooted[19] mobile devices) and block the use of the mobile trading applications in these devices. Internet brokers ***should*** detect and block jailbroken or rooted mobile devices from logging into their internet trading systems.

<u>Preventive controls</u>

A. Source codes

70. Five inspected firms' source codes containing all the functions in their mobile trading applications could be easily found and understood. For one firm, the source codes also disclosed the internet trading server information. The ready availability of this information could allow hackers to modify and repackage the mobile trading applications to by-pass built-in security controls such as the detection of compromised mobile devices. Moreover, the modified and repackaged mobile trading applications could continue to function and remain connected

[17] Paragraph 1.2.4 of Schedule 7 to the Code of Conduct.

[18] Jailbreaking is the process by which Apple's operating systems are modified to remove software restrictions which can facilitate the installation of malware.

[19] Rooting is the process of allowing users of smartphones, tablets and other devices running the Android mobile operating system to attain privileged access controls (known as root access) over various Android subsystems.

to these firms’ internal network. Furthermore, hackers could distribute the repackaged and modified applications to internet forums or message boards for download. If clients were to download and use these applications, all the built-in security controls could be removed and the latest security patches or hotfixes could not be installed. Internet brokers ***should*** obfuscate their source codes to better protect them from potential manipulation.

71. Three inspected firms had some unused code libraries or modules in their mobile trading applications. This increased the risk of a buffer overflow attack whereby hackers would take advantage of the programme space to install malware. Internet brokers ***should*** purge any unused code libraries or modules from their source codes.

B. Sensitive information stored on user’s devices

72. Six inspected firms’ mobile trading applications allowed storage (ie, cache) of clients’ sensitive information in the mobile devices, such as the “remember password”, “auto fill” and “auto completion” features, and such information would not be removed from the system process memory after logoff. This increased the risk of such information being accessed by hackers for unauthorised login attempts. Internet brokers ***should*** purge clients’ sensitive information from their internet trading applications installed on clients’ mobile devices once clients exit those applications or log off their internet trading accounts.

C. Biometric authentication

73. One inspected firm’s biometric authentication, including fingerprint and facial recognition, would not be disabled after many failed attempts. In addition, biometric authentication login would be allowed after an additional fingerprint was added or a facial image was changed in the record for the mobile device without proper validation. Internet brokers ***should*** tighten security controls, such as:

    (a) requiring clients to deactivate and re-register their biometric authentication, subject to validation, if they wish to add or amend the biometric data stored in the records for their mobile devices; and

    (b) limiting the number of failed authentication attempts.