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

SFC
證監會

Consultation Conclusions on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading

October 2017

Table of Contents

Executive Summary

1. On 8 May 2017, the Securities and Futures Commission (**SFC**) issued a Consultation Paper (**Consultation Paper**) on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading, inviting public comments on (a) proposed amendments to the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (**Code of Conduct**) and (b) proposed new Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (**Guidelines**) (collectively referred to as the **Proposals**).

2. During the consultation period, which ended on 7 July 2017, the SFC received a total of 36 written submissions from various industry associations, professional bodies, the Consumer Council, brokers, law firms, service providers and individuals.

3. The SFC has considered the responses carefully and revised the Proposals in consultation with an external cybersecurity expert[1]. This paper sets out the SFC's conclusions on the Proposals and responses to the comments received. The key proposals in the Consultation Paper received broad support. For the reasons set out in the Consultation Paper and having regard to the majority support for the Proposals, the SFC considers that only a few modifications or clarifications would be required, to address the following concerns.

   (a) A few respondents pointed out that as the proposed controls were designed as baseline entry requirements for smaller internet brokers, they might not be applicable to larger internet brokers operating highly sophisticated systems and controls. Some respondents also suggested that the Guidelines should be less prescriptive and allow internet brokers to adopt a risk-based approach in determining which controls are commensurate with their cybersecurity risk profile.

   We maintain the view that these baseline requirements are essential for all internet brokers, in particular smaller internet brokers, for reducing and mitigating hacking risks. Nevertheless, we note that there might be different means to achieve the overall objective. In this regard, in the Frequently Asked Questions (**FAQs**) on the Guidelines issued together with this conclusions paper, we specified one control which in limited circumstances does not require strict compliance (please see subparagraph (b) below for details).

   Separately, we agree that the Guidelines should be generic so that they do not easily become obsolete because of technological advances. Some of the proposed controls have therefore been fine-tuned to provide greater flexibility. We have also removed all examples (save for a few illustrative examples which should remain valid over time) from the Guidelines. However, practical examples have been provided in the FAQs to provide further guidance on the implementation of the Guidelines.

   (b) Some respondents suggested that, with the implementation of two-factor authentication (**2FA**) for clients to login to their internet trading accounts, clients should be able to opt out from receiving immediate notifications upon each system login. Whilst we maintain that notification is an effective detective control and should be included in the Guidelines, we accept that strict adherence may not be necessary if internet brokers inform clients of irregular login activities. For example, if it is

[1] Please refer to the Consultation Paper for more information on the external cybersecurity expert.

apparent that a client logs in through a device which is not customarily used by that client.

We have therefore set out in the FAQs the specific circumstances and conditions under which internet brokers may offer clients the option of opting out from system login notifications.

(c) We understand that six months may be insufficient for some internet brokers to implement all of the required controls. In this regard, whilst internet brokers are required to implement 2FA within six months, we now allow nine months for internet brokers to implement all other controls.

(d) There were other comments and suggestions of a technical nature, for example, on patch management and account lockout after multiple login attempts. Modifications have been made to the proposed Guidelines as appropriate.

4. The amendments to the Code of Conduct and the Guidelines are set out in **Appendix A** and **Appendix B**[2] respectively. Both will become effective nine months after the date of this paper, except for the requirement for implementation of 2FA which will become effective six months after the date of this paper.

5. We would like to thank all respondents for their time and effort in reviewing the Proposals and providing us with their detailed and thoughtful comments. A list of respondents (other than those who requested anonymity) is set out in **Appendix C** and the full text of the submissions can be viewed on the SFC's website at www.sfc.hk.

Comments Received and Our Responses

I. On the Consultation Questions

Question 1: The SFC is of the view that the proposed controls should be baseline requirements, which will also serve as an entry requirement for potential internet brokers. Do you agree with this approach?

Public comments

6. 22 out of the 23 respondents who answered this question were supportive of this proposal whilst one respondent preferred a risk-based approach so that internet brokers could determine the cybersecurity controls they require based on their cybersecurity risk profile.

7. In addition, a few other respondents pointed out that as the proposed controls were designed as baseline entry requirements for small internet brokers, some of the proposed controls are too prescriptive and difficult to comply with, especially for larger internet brokers operating highly sophisticated systems and with controls intertwined with their other business lines.

Our response

8. Given the majority support, we maintain the view that the proposed controls should remain as baseline requirements applicable to all internet brokers. Whilst we see the merits of a risk-based approach, we consider it more important to explain our expectations in clear

[2] The modifications made to the controls in the proposed Guidelines have been marked up in Appendix B.

and unambiguous terms for the internet broking industry at large, given that smaller internet brokers may lack the resources and capabilities to develop their own cybersecurity risk management frameworks. On the other hand, we acknowledge that parts of the Guidelines may create practical difficulties for internet brokers which operate vastly different systems, infrastructures and controls, where there was other means to achieve the desired objectives. We have therefore specified in the FAQs that it would be acceptable for internet brokers, which have met certain conditions, to provide notifications to clients when irregular system logins are identified instead of following each system login (see paragraphs 40 to 45).

9. We would like to reiterate that the Guidelines are minimum standards and are not meant to be exhaustive. Senior management of each internet broker, with the help of solution providers or technical consultants if needed, should ensure that all systems and controls are commensurate with the firm's business operations and needs, and implement additional cybersecurity controls as necessary.

Question 2: The application of Paragraph 18 of and Schedule 7 to the Code of Conduct is expanded to cover the internet trading of securities that are not listed or traded on an exchange. Do you agree that the proposed expansion of the scope of the regulation of internet trading is appropriate? If yes, is the proposed wording sufficiently clear?

Public comments

10. 18 out of the 23 respondents who answered this question agreed that the internet trading of securities which are not listed and traded on an exchange should also be covered given that such trading is exposed to the same vulnerabilities to cyber-attacks as the internet trading of exchange listed or traded securities.

11. Three respondents expressed concern about the coverage of non-exchange listed or traded securities for the following reasons:

    (a) the inherent risk for hackers to conduct market manipulative activities, such as "pump-and-dump schemes", is comparatively low for trading in non-exchange listed or traded securities; and

    (b) the hacking risk associated with accounts used for the trading of unlisted collective investment schemes (**CIS**) is very low and it may not be necessary to cover asset management companies which run internet trading systems for clients to subscribe, redeem and switch CIS investments.

    One respondent suggested that the internet trading of non-exchange listed or traded securities should at least be subject to different requirements which reflect their particular nature and associated risks.

12. Two respondents requested a list of securities which would be covered under the Proposals.

13. Separately, four respondents suggested expanding the scope of regulation to all financial products, to all information systems used by the industry or to other types of electronic trading, such as direct market access (**DMA**) and algorithmic trading.

Our response

14. As explained in the Consultation Paper, hacking of internet trading appears to be the most serious cybersecurity risk faced by licensed corporations in Hong Kong. Hence, for the purpose of developing the baseline requirements, we maintain the view that we should focus on addressing these risks.

15. We recognise that the risk or impact of hacking may be lower for internet trading of non-exchange listed or traded securities. However, they are still exposed to the same types of cyber-threats and vulnerabilities, and we do not consider it prudent to restrict the requirements to exchange listed or traded securities.

16. Separately, we do not consider it necessary to prescribe a list of securities which would be covered under the Proposals; the definition of "securities" for the purpose of the Proposals should follow the definition of "securities" under Schedule 1 to the Securities and Futures Ordinance.

Question 3: By not prescribing particular 2FA solutions, the proposed requirements should provide brokers with a measure of flexibility when providing additional safeguards against hacking risks. Do you agree that this approach is appropriate?

Public comments

17. 22 out of 27 respondents supported mandating the implementation of 2FA by internet brokers. One respondent commented that the SFC was right to focus on the importance of multi-factor authentication as a critical security control, whilst another respondent believed the implementation of 2FA will substantially increase the level of client protection because the login process is the first line of defence against cyber-attacks.

18. The same group of respondents were supportive of not prescribing particular 2FA solutions, with comments such as:

    (a) this approach would still standardise the login security level among all internet brokers, without posing an operational and financial discriminatory burden on smaller internet brokers;

    (b) this approach eliminates any unhealthy competition for clients who may seek the convenience and speedy trade execution that comes with not using any 2FA solutions. The flexibility offered by the Commission also allows internet brokers to select 2FA solutions which are the most cost-effective and appropriate for their own business models; and

    (c) from the perspective of clients, this approach provides a uniform level of security regardless of their choice of internet broker.

19. On the other hand, one respondent suggested that the SFC should prescribe the use of hardware or software tokens, and three respondents advocated the use of biometrics whilst expressing reservations about the use of a short message service (**SMS**) for transmitting one-time passwords (**OTP**). For details, please refer to paragraphs 32 and 33 below.

Our response

20. We welcome the overall support of our proposal to mandate the use of 2FA. The SFC acknowledges that there are a variety of 2FA solutions, each with its own advantages and disadvantages, and that with time some may become obsolete or ineffective. We therefore maintain our view that internet brokers should be free to select appropriate 2FA solutions based on their individual circumstances. For the avoidance of doubt, the examples included in Appendix D to the Consultation Paper were for reference only and no examples of specific 2FA solutions will be included in the Guidelines.

Question 4: Do you agree that for practical considerations, it will not be appropriate to mandate the monitoring of suspicious trading patterns?

Public comments

21. 18 out of the 22 respondents who answered this question agreed that the monitoring of suspicious trading patterns should only be included as an industry good practice, whilst four respondents suggested mandating this type of control.

Our response

22. In line with the majority view, the monitoring of suspicious trading patterns will be a good practice measure.

Question 5: Due to cost considerations, the proposals do not require internet brokers to assess and enhance their backup facilities (ie, disaster recovery sites) for providing internet trading services or alternative arrangements for receiving clients' orders in an emergency so as to avoid disrupting services in an unacceptable manner. Do you agree with this approach?

Public comments

23. 16 out of the 21 respondents who answered this question agreed with this approach, with one respondent citing the effort and expense which a comprehensive assessment or test of backup facilities would require. Another respondent was of the view that it is not cost-effective to maintain fully functional backup facilities. Other comments and suggestions were as follows:

    (a) given the current cyber risk environment, having a robust backup and recovery plan is essential. As seen in other regions, failing to ensure that contingency plans are tested and effective, or not having the right cyber response plan in place, can be a material risk for organisations and clients. The SFC should provide a set of guidelines based on industry good practices; and

    (b) baseline backup facilities and the provision of an alternative arrangement for processing client orders should be mandatary, especially for clients wanting to unwind existing equity positions in emergency conditions.

Our response

24. Existing requirements under the Code of Conduct[3] govern the adequacy of systems (including contingency measures). In particular, internet brokers are required to ensure that their contingency plans are periodically tested, viable and adequate. In order to ensure that contingency measures properly address potential cybersecurity scenarios, the proposed Guidelines introduce a new requirement that internet brokers cover cyber-attack scenarios in their contingency plans and crisis management procedures. However, this does not mean that all internet brokers must set up a disaster recovery site as an alternative arrangement for processing clients' requests, perform a formal assessment of their backup facilities or conduct a drill. For smaller internet brokers, some alternative arrangements such as operating a telephone hotline for handling client orders and enquiries and maintaining sufficient records for tracking the status of each client order may already be sufficient.

Question 6: In your opinion, does the current level of service offered by your service providers enable you to comply with the proposed baseline requirements? Do you envisage any difficulty in negotiating higher service levels with your service providers?

Public comments

25. 13 out of the 18 respondents who answered this question confirmed that the current level of service provided by their service providers can comply with the proposed baseline requirements. One respondent agreed that quantifiable requirements for maintenance and technical assistance should be codified in baseline requirements to create a level playing field among internet brokers. On the other hand, a few respondents envisaged difficulty in negotiating higher service levels or paying extra fees.

Our response

26. Based on the feedback received, we do not anticipate that internet brokers will be unable to negotiate higher service levels. However, industry associations might wish to consider leveraging on their substantial bargaining power and negotiate terms and fee levels with vendors on a collective basis.

II. On Specific Baseline Requirements

27. Overall, there were diverse views on the proposed baseline requirements. Some respondents considered the proposed controls to be insufficient, whereas others suggested that the SFC elaborate on certain controls. For example:

    (a) A few respondents commented that some proposed controls were not sufficiently robust and suggested various enhancements to better protect against hacking risks. In particular, some considered it important for internet brokers to assess and enhance their backup facilities (which is not one of the proposed controls), given that a suitably robust backup and recovery plan is essential in an emergency; and

    (b) On the subject of 2FA solutions, some respondents advocated the use of biometrics whilst warning against the use of SMS for transmitting OTPs.

[3] Please see paragraph 18.5 of the Code of Conduct and paragraph 1.2.7 of Schedule 7 to the Code of Conduct.

Given that our immediate objective is to set baseline requirements, we intend to reflect these useful suggestions for enhancing the proposed controls in circulars on good practices to be issued over time.

28. 11 of the 20 proposed baseline requirements received minimal or no feedback from respondents. These include:

- Protection of client login passwords (paragraph 1.5 of the Guidelines);
- Develop a secure network infrastructure (paragraph 2.1 of the Guidelines);
- User access management (paragraph 2.2 of the Guidelines);
- Security controls over remote connection (paragraph 2.3 of the Guidelines);
- End-point protection (paragraph 2.5 of the Guidelines);
- Unauthorised installation of hardware and software (paragraph 2.6 of the Guidelines);
- Physical security (paragraph 2.7 of the Guidelines);
- Roles and responsibilities of cybersecurity management (paragraph 3.1 of the Guidelines);
- Cybersecurity incident reporting (paragraph 3.2 of the Guidelines);
- Cybersecurity awareness training for internal system users (paragraph 3.3 of the Guidelines); and
- Cybersecurity alert and reminder to clients (paragraph 3.4 of the Guidelines).

29. As a result, the wording of the above requirements will remain unchanged save for a minor amendment to paragraph 3.3 of the Guidelines where greater flexibility has been provided in the areas to be covered in training programmes, whilst making clear that internet brokers should take into account the type and level of cybersecurity risks they face when designing the content of such programmes.

30. Comments received on other proposed baseline requirements and the corresponding responses from the SFC are discussed below.

1. Two-Factor Authentication (paragraph 1.1 of the Guidelines)

Public comments

31. As stated in paragraph 17 above, most respondents were supportive of the proposal to mandate the use of 2FA. However, one respondent took the view that 2FA may cause inconvenience to clients, such as those who do not have a smartphone or cannot receive an SMS (which are necessary for using certain 2FA solutions), and suggested giving clients the option to opt out from 2FA provided they understand and acknowledge the consequential risks.

32. Some were of the view that internet brokers require clear and quantitative guidelines from the SFC along with technical options and intelligence from the cybersecurity industry.

Three respondents indicated security concerns over the use of SMS for transmitting OTP. One of these respondents also cited an incident where SMS OTP was circumvented by overseas hackers who impersonated victims in order to change their SMS settings, for example, by setting up SMS forwarding with the telecommunication service provider.

33. Separately, a respondent highlighted potential solutions based on "who a client is", ie biometrics. Another respondent pointed out that the need for specific hardware should be less of a hindrance, as reliable authentication with facial recognition is now achievable through the front-facing cameras which are ubiquitous on today's mobile devices, or via webcams on laptops. Fingerprint readers are increasingly common on mobile devices.

Our response

34. We acknowledge that 2FA solutions are not fool-proof and are also mindful of the danger of hackers luring clients to disclose their login credentials. Furthermore, we recognise the importance of the user experience and take this into account in policy deliberations. As 2FA is widely recognised as an effective authentication mechanism to prevent hacking, we do not agree that clients should be able to opt out. The SFC has been working closely with the Investor Education Centre to launch a series of cybersecurity awareness programmes, including promotions on the use of 2FA. For example, in September 2017, an article titled "Keeping your personal details and passwords safe"[4] was published in both traditional and online media.

35. Given (i) the diverse sizes, operating models and financial capabilities of internet brokers; (ii) the various types of 2FA solutions available which vary in sophistication and price (such as hardware tokens, software tokens, SMS OTPs, biometric devices or their equivalents which may have been developed in-house by internet brokers); and (iii) rapidly advancing technology, the SFC remains of the view that it would be most appropriate for internet brokers to select those solutions which align with their security infrastructures and are suitable for achieving their risk mitigation objectives.

36. However, in light of public comments, in the FAQs we have:

    (a) reminded internet brokers, when selecting a 2FA solution, to assess and evaluate, with the assistance of solution providers or technical consultants where needed, the features, limitations and vulnerabilities of each 2FA solution being considered, and to put in place compensating controls as appropriate; and

    (b) suggested that internet brokers deploying SMS OTP advise their clients against forwarding OTPs to other devices.

2. Implement Monitoring and Surveillance Mechanisms (paragraph 1.2 of the Guidelines)

Public comments

37. No respondents opposed the proposed requirement to implement an effective monitoring and surveillance mechanism to detect unauthorised access to clients' internet trading accounts. However, four respondents commented on the operational challenges and effectiveness of monitoring internet protocol (**IP**) addresses, which was cited as an example in the proposed Guidelines, and suggested not to mandate this particular control. These respondents explained that there could be legitimate reasons why multiple clients

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

log in from the same IP address, for example, when they work for the same company and share an external IP address for accessing the internet.

Our response

38. The SFC appreciates that, similar to post-trade surveillance controls, monitoring IP addresses can generate both genuine alerts and false alarms. However, it may still be a useful tool to help internet brokers identify apparent irregularities for follow-up.

39. We should clarify that this example was included in the proposed Guidelines for illustration only and has been removed from the Guidelines.

3. Prompt Notification to Clients (paragraph 1.3 of the Guidelines)

Public comments

40. Two respondents commented that when 2FA is mandatory for system login, it may be unnecessary to provide an additional notification of each system login. There was a concern that clients may become less alert or even ignore notifications when they receive too many; some may even treat them as spam messages. An alternative was put forward whereby clients would only receive system login notifications when internet brokers note irregular logins, for example through a device not customarily used by the client.

41. As regards the proposed requirement to notify clients of "fund transfer to third party", a respondent was of the view that this should not be necessary if a client had already registered the third party account with the internet brokers for fund transfer purposes.

42. As regards the proposed requirement to notify clients of "change to client and account-related information", a respondent considered that this might be too broad (for example, capturing unimportant changes such as a change of preferred language) and suggested restricting this to changes in contact details used to receive security related information.

Our response

43. Whilst 2FA serves as a key preventive control, it is not fool-proof; prompt notification to clients can complement 2FA as an effective detective control. We maintain the view that the requirement to provide prompt notification to clients of certain activities should be included in the Guidelines. We also recognise that there may be problems when clients receive too many notifications and for this reason have already provided the option for clients to opt out from trade execution notifications.

44. On the subject of system login notification, based on the hacking incidents reported to the SFC, internet brokers were able to take prompt action and prevent hackers from effecting unauthorised transactions because their clients had alerted them after being notified of a system login which they had not made. This is an effective detective control that ought to be included in the Guidelines. However, we accept that clients might not need to be notified of each system login if they receive notifications of irregular logins. We have now explained in the FAQs that it would be acceptable for internet brokers who meet the following requirements to allow clients to opt out from system login notifications:

    (a) the internet broker has the capability to identify irregular logins and promptly notify clients of irregular logins;

(b) the internet broker has provided adequate risk disclosures to clients who have acknowledged that they understand the risks involved in opting-out of system login notifications; and

(c) the clients have not opted out from trade execution notifications.

45. We agree that we should only require notifications for a "fund transfer to unregistered third party". However, we do not agree that clients should only be notified of changes in contact details used to receive security related information. It is important that clients are notified of changes in client and account-related information such as bank account details and personal particulars.

4. Data Encryption (paragraph 1.4 of the Guidelines)

Public comments

46. Two respondents sought clarification of the meaning of "end-to-end encryption" and "internal networks", in particular, whether a Demilitarised Zone (**DMZ**) is considered part of an internal network.

47. Four respondents suggested some advanced encryption solutions, for example that login passwords be salted and one-way hashed, preferably with a slow hash function in order to deter brute force attacks.

Our response

48. The SFC would like to clarify that a DMZ is considered to be part of an internal network for the purpose of this requirement and this has been included in the FAQs. Also upon further deliberation, we will require internet brokers to encrypt sensitive information using a strong encryption algorithm during transmission between internal networks and client devices. We have deleted the phrase "end-to-end encryption" from the proposed Guidelines to avoid confusion.

49. The SFC welcomes suggestions about encryption solutions. Under the Guidelines, internet brokers are required to "use a strong encryption algorithm" and are free to determine which encryption technology to use based on their circumstances. Some advanced encryption solutions will be recommended as industry good practices in future circulars.

5. Stringent Password Policies and Session Timeout Controls (paragraph 1.6 of the Guidelines)

Public comments

50. All respondents acknowledged the need to establish stringent password policies and session timeout controls. They also appreciated that the proposed Guidelines do not specify a maximum timeout period and internet brokers can set the session timeout limit according to their business models and operations.

51. On the other hand, two respondents suggested removing the "maximum password age" policy from the proposed Guidelines. One respondent further argued that frequent changes of password may require customers to write down their passwords which in turn increases the risk of information leakage. This respondent also suggested, as an alternative, that a policy could be set on reminding clients to change their passwords if

they have not done so for a long time. Another respondent pointed out that such controls are no longer recommended under some international technology standards.

52. Separately, a respondent believed that an account lockout mechanism may facilitate a distributed denial-of-service (DDoS) attack[5]. As such, it would not be appropriate to mandate password policies on "account lockout after multiple invalid login attempts" and instead the respondent suggested alternatives such as increasing delays between invalid login attempts.

Our response

53. We are receptive to both suggestions and have revised the Guidelines as follows:

    (a) replacing the "maximum password age" policy with a policy about "periodic reminders for those clients who have not changed their passwords for a long period"; and

    (b) replacing the "account lockout after multiple invalid login attempts" policy with a policy about "appropriate controls on invalid login attempts" so that internet brokers can set their own policies and control measures to prevent unauthorised access to clients' internet trading accounts.

6. Patch Management (paragraph 2.4 of the Guidelines)

Public comments

54. There were some concerns over the proposed timeframe for implementing security patches and hotfixes:

    (a) two respondents felt one month is not sufficient, particularly when the testing and implementation involve third parties in some circumstances. For example, if the test requires connection with the Hong Kong Stock Exchange or an extensive global infrastructure footprint involves servers in different locations;

    (b) a respondent suggested extending the deadline to two months; and

    (c) another respondent strongly suggested more flexibility be provided where the implementation schedule for patches for different vulnerabilities should be prioritised according to the risk associated with the vulnerability and the type of asset (for example, business critical systems and less critical systems). This enables resources to be appropriately assigned to critical patch implementation, rather than to low risk vulnerabilities.

Our response

55. Time is of the essence for effective patch management. Taking WannaCry as an example, the relevant patch was released in March 2017 and the crisis followed in May, meaning that there was only a two-month window for assessing and implementing the patch. However, we also recognise the need to make allowances to perform necessary testing. As such, we have revised the Guidelines and now made clear that internet brokers should

[5] If account lockout is implemented, hackers may deliberately lock out a large number of accounts by repeatedly trying incorrect passwords, thus bringing about a service disruption.

conduct testing as soon as practicable and implement security patches and hotfixes within one month following the completion of testing.

56. Separately, as the Proposals already provide for implementation of security patches or hotfixes subject to an evaluation of their impact, internet brokers are free to set their implementation schedule based on the evaluation results.

7. System and Data Backup (paragraph 2.8 of the Guidelines)

Public comments

57. Two respondents referred to the difficulty in backing up business records, client and transaction databases, servers and supporting documentation in an off-line medium on a daily basis because of operational and resources concerns. There were also questions about the meaning of "off-line medium," and suggestions to allow the roll-back of major system changes.

Our response

58. The SFC maintains its view that daily backup to an off-line medium is critical for data recovery and business resumption. Clarification has been made in the FAQs that an off-line medium refers to tape or any other kind of medium, including a remote backup server, which is securely segregated from the production system. However, noting the practical difficulties for large organisations when performing full back up before and after any major system changes, we agree that we should be less prescriptive and instead require internet brokers to use an appropriate recovery method to enable successful roll-back of major system changes.

8. Contingency Planning for Cybersecurity Scenarios (paragraph 2.9 of the Guidelines)

59. In respect of tackling DDoS attacks, two respondents asked why there is a baseline requirement that DDoS scenarios should be included in contingency planning when internet brokers are not required to acquire anti-DDoS solutions.

60. A respondent emphasised that internet brokers should conduct periodic disaster recovery testing.

Our response

61. As discussed under paragraph 56 of the Consultation Paper, based on feedback from the brokers and advice from the external cybersecurity expert, more affordable DDoS solutions may not always be effective in the event of a large-scale DDoS attack. On balance it seems more appropriate to focus on robust contingency planning and crisis management procedures. Although acquiring anti-DDoS solutions may not be necessary, it is nevertheless important to cover DDoS scenarios in contingency plan.

62. As discussed under paragraph 24, for smaller internet brokers, alternative arrangements for receiving client orders and providing order status information may be sufficient. For this reason, we will not include periodic disaster recovery testing as a baseline requirement.

9. Third-Party Service Providers (paragraph 2.10 of the Guidelines)

Public comments

63. Only five respondents commented on this proposed control and they all agreed that formal service-level agreements should be established between internet brokers and third-party service providers and such agreements should be regularly reviewed and revised.

64. One respondent sought clarification of whether other outsourced activities, which are not core to the internet trading business, are covered.

Our response

65. For the purposes of the Guidelines, "internet trading" has the same meaning as in paragraph 18 of the Code of Conduct. As such, paragraph 2.10 of the Guidelines only covers outsourcing arrangements associated with the internet-based trading facility used to send order instructions to the internet broker.

Implementation Timeframe

66. Some respondents were concerned that an implementation period of six months may not be sufficient for internet brokers to make necessary changes to their internal procedures and IT systems. This timeline might be particularly tight for those that operate large, highly sophisticated systems which connect internet broking with other business lines.

67. We appreciate that six months for implementing all of the required controls may be too tight for some internet brokers. However, given that 2FA is the key preventive measure to reduce and mitigate hacking risks, we consider it essential to implement this control as soon as practicable. Accordingly, the effective date of the new provision in the Guidelines as regards implementation of 2FA will come into effect six months after the date of this paper whereas all other requirements will only become effective after nine months.

68. The SFC expects all internet brokers to commence reviewing their internet trading systems and communicating with their third-party service providers and clients (if applicable) immediately to ensure compliance with the new regulatory requirements. The SFC emphasises that the lengths of the six- and nine-month implementation periods are mainly to cater for circumstances where internet brokers, despite their best efforts, encounter technical difficulties when implementing changes in their internet trading systems. It is expected that internet brokers should be able to complete other non-system-related measures well before the effective date.

Way Forward

69. The cybersecurity landscape changes rapidly as time goes by, and the SFC will continue to monitor cybersecurity developments and emerging threats. We anticipate that further policy refinements and rule changes may be necessary in order to maintain an appropriate balance between market innovation and investor protection. We also plan to supplement the Guidelines by providing additional guidance as needed from time to time.

Appendix A

Amendments to the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission

Paragraph 18 – Electronic trading

18.1 Application

This paragraph applies to a licensed or registered person which conducts electronic trading of securities and futures contracts that are listed or traded on an exchange or internet trading of securities that are not listed or traded on an exchange.

18.2 Interpretation

(f) "Internet trading" for the purposes of this paragraph means an arrangement where order instructions are sent to a licensed or registered person through its internet-based trading facility. An internet-based trading facility may be accessed through a computer, mobile device or other electronic device.

Schedule 7 – Additional requirements for licensed or registered persons conducting electronic trading

Introduction

Paragraph 18 of the Code stipulates the general principles that apply to a licensed or registered person which conducts electronic trading of securities and futures contracts that are listed or traded on an exchange or internet trading of securities that are not listed or traded on an exchange. This Schedule sets out the specific requirements in this regard.

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

SFC
證監會

Appendix B

Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading

Table of contents

Introduction

1. These Guidelines are published by the Securities and Futures Commission (SFC) under section 399 of the Securities and Futures Ordinance (SFO) and set out the baseline requirements to reduce or mitigate hacking risks associated with internet trading.

2. These Guidelines should be read in conjunction with, among other provisions, 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). For the purposes of these Guidelines, "internet trading" has the same meaning as in Paragraph 18.2(f) of the Code of Conduct, being "an arrangement where order instructions are sent to a licensed or registered person through its internet-based trading facility".

3. These Guidelines apply to persons which are engaged in internet trading and are licensed by, or registered with, the SFC for:

    - Type 1 regulated activity (dealing in securities);
    - Type 2 regulated activity (dealing in futures contracts);
    - Type 3 regulated activity (leveraged foreign exchange trading). For the avoidance of doubt, these Guidelines shall only apply to leveraged foreign exchange traders licensed by the SFC; and/or
    - Type 9 regulated activity (asset management) to the extent that they distribute funds under their management through their internet-based trading facilities.

4. These Guidelines do not have the force of law and should not be interpreted in any manner which would override the provisions of any applicable law, codes or other regulatory requirements. However, a failure to follow the spirit of these Guidelines may reflect adversely on the person's fitness and properness.

5. The controls and measures specified in these Guidelines can only reduce or mitigate hacking risks associated with internet trading, but cannot eliminate them. It must be emphasised that these are the minimum standards expected of licensed or registered persons and are not meant to be exhaustive. Licensed or registered persons are expected to implement adequate and effective measures which are commensurate with their structure, business operations and needs.

1. Protection of clients' internet trading accounts

1.1. Two-factor authentication[1]

A licensed or registered person should implement two-factor authentication for login to clients' internet trading accounts.

A licensed or registered person should assess and implement a two-factor authentication solution which is commensurate with its business model.

1.2. Implement monitoring and surveillance mechanisms

A licensed or registered person should implement an effective monitoring and surveillance mechanism to detect unauthorised access to clients' internet trading accounts. ~~Examples include:~~

- ~~Logging into multiple client accounts from the same internet protocol (**IP**) address; and~~
- ~~Change of IP addresses for accessing the same client account (for example, from Hong Kong to London) in a short period of time.~~

1.3. Prompt notification to clients

A licensed or registered person should notify clients (eg, via email, short message service (SMS) or other push notifications) promptly after certain client activities have taken place in their internet trading accounts. These activities should at least include:

(a) System login;

(b) Password reset;

(c) Trade execution;

(d) Fund transfer to third party accounts unless these have been registered with the licensed or registered person for fund transfer purposes prior to the transfer; and

(e) Changes to client and account-related information.

The channel of notification to clients should be different from the one used for system login (as outlined in paragraph 1.1).

Clients may choose to opt out from "trade execution" notifications only. Under such circumstances, adequate risk disclosures should be provided by the licensed or registered person to the client and an acknowledgement should be executed by the client confirming that the client understands the risks involved in doing so.

[1] Two-factor authentication refers to an authentication mechanism which utilises any two of the following factors: what a client knows ~~(eg, password)~~, what a client has ~~(eg, hardware token, one-time-password that will expire in a short period of time)~~, and who a client is ~~(ie, biometrics)~~.

1.4. Data encryption

A licensed or registered 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~~, ie, end-to-end encryption.~~; and

(b) ~~A licensed or registered person should also~~ protect client login passwords stored in its internet trading system ~~using a strong encryption algorithm~~.

1.5. Protection of client login passwords

A licensed or registered 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 or registered person.

In a situation where a client login password is not randomly generated by the system, the licensed or registered person should implement adequate compensating security controls such as compulsory change of password upon the first login after client account activation.

1.6. Stringent password policies and session timeout controls

A licensed or registered person should set up stringent password policies and session timeout controls in its internet trading system, which include ~~among others~~:

(a) Minimum password length;

(b) ~~Maximum password age~~ Periodic reminders for those clients who have not changed their passwords for a long period;

(c) Minimum password complexity (ie, alphanumeric) and history;

(d) ~~Account lockout after multiple~~ Appropriate controls on invalid login attempts; and

(e) Session timeout after a period of inactivity.

2. Infrastructure security management

2.1. Deploy a secure network infrastructure

A licensed or registered 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.

2.2. User access management

A licensed or registered 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 or registered 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 remain restricted to persons approved to use them on a need-to-have basis.

2.3. Security controls over remote connection

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

2.4. Patch management

A licensed or registered 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 ~~of the security patches or hotfix releases~~, conduct testing as soon as practicable and implement the security patches or hotfixes within one month following the completion of testing.

2.5. End-point protection

A licensed or registered person should implement and update a~~A~~nti-virus and anti-malware solutions (including the corresponding definition and signature files) ~~should be implemented and updated~~ on a timely basis to detect malicious applications and malware on critical system servers and workstations.

2.6. Unauthorised installation of hardware and software

A licensed or registered person should implement security controls to prevent unauthorised installation of hardware and software.

2.7. Physical security

A licensed or registered person should establish physical security policies and procedures to protect critical system components (eg, system servers and network devices) in a secure environment and to prevent unauthorised physical access to the facilities hosting the internet trading system as well as the critical system components.

2.8. System and data backup

A licensed or registered 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. ~~Full back up of the above should be performed before and after any major system changes.~~

A licensed or registered person should also adopt an appropriate recovery method to enable successful roll-back of major system changes.

2.9. Contingency planning for cybersecurity scenarios

In order to ensure that appropriate contingency procedures can be effectively executed when cybersecurity situations occur, a licensed or registered person should make all reasonable efforts to cover possible cyber-attack scenarios such as distributed denial-of-service (DDoS) attacks[2] and total loss of business records and client data resulting from cyber-attacks (eg, ransomware) in the contingency plan and crisis management procedures.

2.10. Third-party service providers

If a licensed or registered person has any arrangement to outsource any activities associated with its internet trading to a third-party service provider, it should enter into a formal service-level agreement with the service provider which specifies the terms of service and the responsibilities of the provider. In particular, a licensed or registered person should ensure that the services provided by the third-party service provider enable the licensed or registered person to comply with the relevant requirements set out in, among other provisions, Paragraph 18 and Schedule 7 to the Code of Conduct and these guidelines. Service level agreements should be regularly reviewed and revised, where appropriate, to reflect any changes to the outsourcing arrangements or regulatory developments. Wherever possible, such agreements should provide sufficient levels of maintenance and technical assistance with quantitative details.

3. Cybersecurity management and supervision

3.1. Roles and responsibilities of cybersecurity management

The responsible officer(s) or executive officer(s) responsible for the overall management and supervision of the internet trading system should define a cybersecurity risk management framework (including but not limited to policies and procedures), and set out key roles and responsibilities. These responsibilities include ~~among others~~:

(a) Reviewing and approving cybersecurity risk management policies and procedures;

(b) Reviewing and approving the budget and spending on resources for cybersecurity risk management;

(c) Arranging to conduct a self-assessment of the overall cybersecurity risk management framework on a regular basis;

(d) Reviewing significant issues escalated from cybersecurity incident reporting;

(e) Reviewing major findings identified from internal and external audits and cybersecurity reviews; endorsing and monitoring the completion of remedial actions;

(f) Monitoring and assessing the latest cybersecurity threats and attacks;

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

(g) Reviewing and approving the contingency plan~~BCP~~, which covers cybersecurity scenarios and corresponding contingency strategies, developed for the internet trading system; and

(h) Where applicable, reviewing and approving the service level agreement and contract with a third-party service provider relating to internet trading.

These responsibilities can be delegated, in writing, to a designated committee or operational unit, however overall accountability remains with the responsible officer(s) or executive officer(s).

3.2. Cybersecurity incident reporting

A licensed or registered 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) or executive officer(s) in charge of internet trading) and externally (eg, to clients, the SFC and other enforcement bod~~y~~ies, where appropriate).

3.3. Cybersecurity awareness training for internal system users

A licensed or registered person should provide adequate cybersecurity awareness training to all internal system users[3] at least on a yearly basis. ~~Training programmes should be updated to include the latest cybersecurity-related rules and regulations and current and emerging cybersecurity threats and trends as well as corresponding measures.~~When designing the content of the training programme, the licensed or registered person should take into account the type and level of cybersecurity risks it faces.

3.4. Cybersecurity alert and reminder to clients

A licensed or registered person should take all reasonable steps to remind ~~and alert~~ clients about and alert them to~~of~~ cybersecurity risks and recommended preventive and protection measures when using the internet trading system, such as that login credentials should be properly safeguarded and cannot be shared.

[3] Internal system users refers to any permanent and contract staff who have access to the internal network and systems of a licensed or registered person.

Appendix C

List of respondents

(in alphabetical order)

1. A member of DTC Association
2. Capital Delight Inc. Limited
3. Cheng, Vincent
4. Chow, Chi Fai
5. Chow, Paul
6. Compliance Consulting Limited
7. CompliancePlus Consulting Limited
8. Consumer Council
9. CQG
10. Deloitte
11. Dragon Advance Tech Consulting Co. Ltd.
12. Fast Identity Online (FIDO) Alliance
13. FIL Investment Management (Hong Kong) Limited
14. Hong Kong Association of Online Brokers
15. Hong Kong Investment Funds Association
16. Hong Kong Securities Professionals Association
17. Hui, Albert
18. Kwok, Vincent
19. Leung, Frankie
20. Lok, Ka Wing
21. Moy, Eric
22. ONC Lawyers
23. Post-Quantum (HK) Limited
24. The Hong Kong Association of Banks
25. The Law Society of Hong Kong
26. 11 respondents requested that their submissions be published without disclosing their names