SFC strengthens internet trading regulatory controls

November 2017

Internet trading - What needs to be done now?

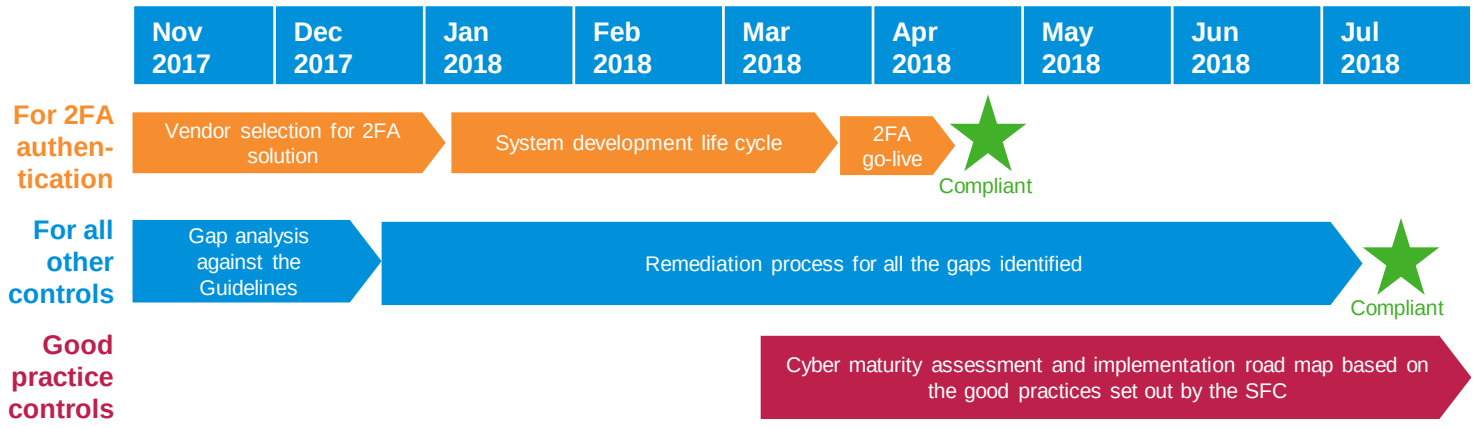
For many investors, online and mobile internet trading is now an everyday interaction with the financial market. Targeted cyber-attacks, leading to hundreds of millions in losses in the securities sector, have led to a call for more security in internet trading. In view of the evolving threat landscape that the financial services industry is facing, the Securities and Futures Commission (SFC) and Hong Kong Monetary Authority (HKMA) have tightened regulatory requirements over the years in order to enhance and safeguard the security, efficiency and resilience of the financial markets.

> ***"Robust preventive and detective controls are essential to reduce and mitigate cybersecurity risks."***
>
> *- Julia Leung, SFC Executive Director*

On 27 October 2017, the SFC released the ***Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading*** ("the Guidelines") as a result of the *Consultation Paper on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading* issued by the SFC on 8 May 2017, mandating 20 minimum control requirements over internet trading. They also released ***Good Industry Practices for IT Risk Management and Cybersecurity*** ("the Circular"), to promote additional controls that licensed corporations (LCs) engaged in internet trading could consider incorporating into their information technology and cybersecurity risk management frameworks.

As stated in the Guidelines, from **27 April 2018**, it will be a mandatory control for internet brokers to implement two-factor authentication (2FA) for clients logging into their internet trading account. Mandatory minimum control requirements are to be implemented and LCs must comply on or before **27 July 2018**.

With the tight implementation timeline for all controls required under the Guidelines, especially for the implementation of 2FA for client logins, internet brokers should act immediately to identify all gaps and implement adequate controls to ensure timely compliance.



2FA Authentication – Why and what is it?

> ***"Given that passwords have not proven effective to prevent hacking, two-factor authentication is an important part of effective cybersecurity risk management."***
>
> *- Julia Leung, SFC Executive Director*

According to the SFC, hacking incidents are minimised when 2FA has been enforced. 2FA is considered a more secure way to authenticate customers' identity than using passwords alone. It refers to an authentication mechanism which utilises any two of the following factors:

What a client knows

Password

What a client has

Hardware token/ Recognised mobile device/ SMS

Who a client is

Biometrics

There are various ways to implement 2FA. Some of the most common examples include:

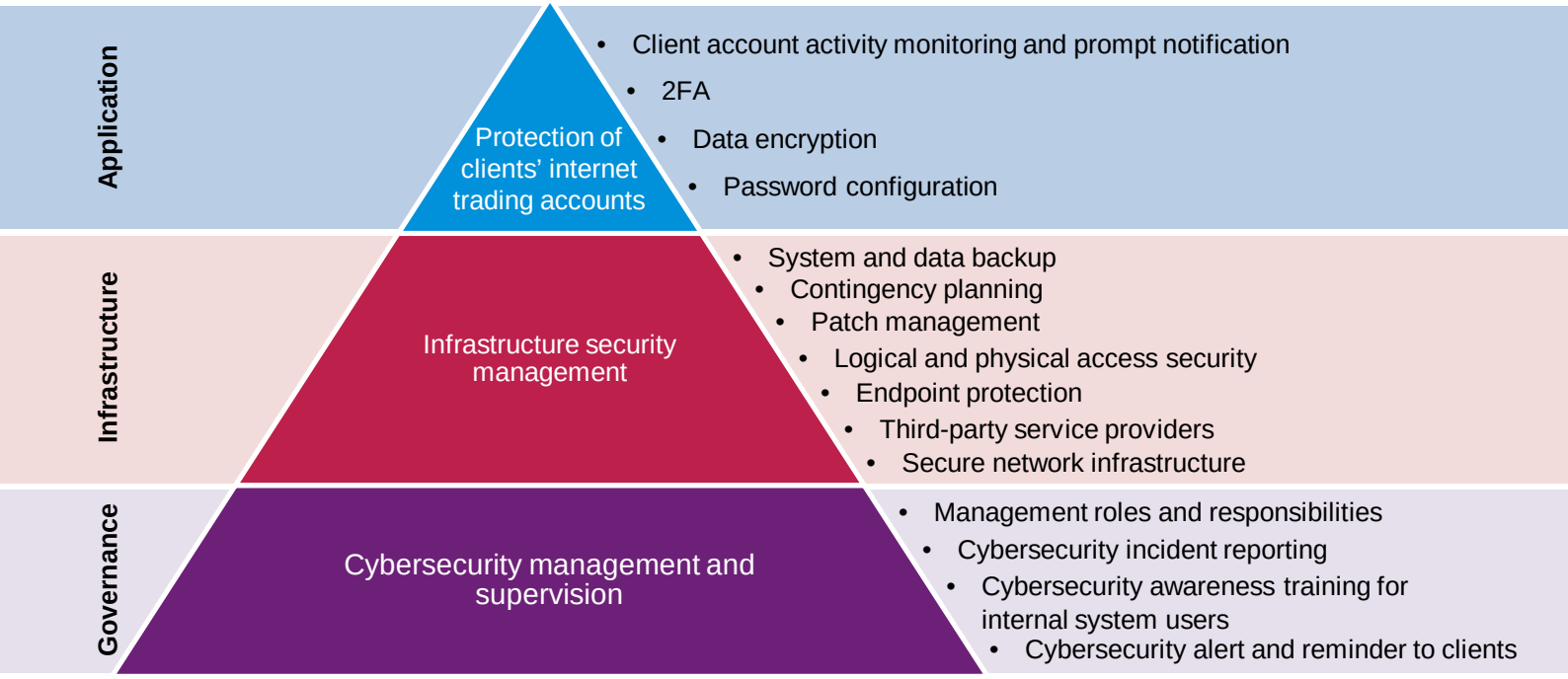
- Email token
- Hardware token
- Software token
- Phone call
- Biometric verification

When selecting 2FA solutions, LCs should perform assessment and evaluation on features, limitations and vulnerabilities; and ensure that the solution best aligns with their specific business operations and security infrastructure, and is suitable for risk mitigation purposes.

All internet brokers are required to implement 2FA on all internet trading systems for client login to their internet trading accounts on or before 27 April 2018, regardless of whether the system is deployed before or after this date. Therefore, all internet brokers must assess the impact on all relevant internet trading systems (including those existing, under development or planning to be implemented). They should also consider what the appropriate 2FA solution to be deployed is, and perform sufficient security testing to ensure that the solution is implemented securely.

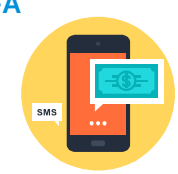
20 Mandatory control requirements in the Guidelines

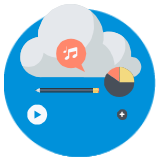
The Guidelines also set out a total of 20 baseline control requirements, including the 2FA control requirements. The following is a summary of these control areas:

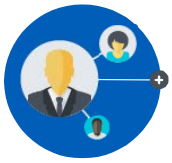
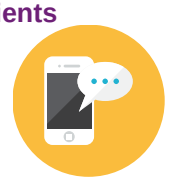


Highlights of the key control requirements in the Guidelines

The following lists out the detailed control requirements in the Guidelines compared to the requirements set out in previous SFC circulars to provide a better view of the change in regulatory requirements. It is worth mentioning that LCs should pay more attention to those control requirements marked with '⚠' as they will potentially have the most impact.

Protection of clients' internet trading accounts		
	In previous SFC circulars	In the new Guidelines
⚠ **Client account activity monitoring and prompt notification** 	In previous SFC circulars, there was no specific requirement regarding client notification upon certain client activities.	An effective monitoring and surveillance mechanism should be implemented to detect unauthorised access to clients' internet trading accounts. Clients should be notified promptly after certain client activities have taken place in their internet trading accounts, including: (a) System login (b) Password reset (c) Trade execution (d) Fund transfer to unregistered third-party accounts (e) Changes to client and account-related information.
⚠ **2FA** 	2FA is recommended but not a mandatory requirement.	For login to clients' internet trading accounts, it is mandatory for LCs to implement 2FA which is commensurate with their business model on or before 27 April 2018.
Data encryption 	Apply data encryption to protect sensitive information transmitted outside secured internal network (e.g. over the internet) or stored in portable storage devices (e.g. USB memory key, CD/DVD-ROM or floppy disk) without strong physical/logical protection.	The requirement for data encryption has been refined, mandating a strong encryption algorithm to be applied on sensitive information such as client login credentials, trade data during transmission, as well as client login passwords within the internet trading system.
Password requirements 	Establish an effective password policy and ensure appropriate settings are applied in the password management of electronic trading systems, which should at least include requirements on password length, password age, password complexity, password history, account lockout attempts and session timeout. Implement effective controls to ensure secured delivery of passwords to clients.	Additionally, in terms of password age, LCs should send periodic reminders to clients who have not changed their passwords for a long period (generally 90 days).

Infrastructure security management		
	In previous SFC circulars	**In the new Guidelines**
System and data backup 	In previous SFC circulars, there was no specific requirement on backup medium and backup frequency. In addition, previously there was no requirement on the roll-back of major system changes.	LCs must back up business records, client and transaction databases, servers, and supporting documentation in an offline medium on at least a daily basis. LCs should also adopt an appropriate recovery method to enable the successful roll-back of major system changes.
Contingency planning 	Cyber-attack scenarios should be included in the incident response plan and crisis management procedures.	LCs should also make all reasonable efforts to cover possible cyber-attack scenarios in the contingency plan and crisis management procedures.
Patch management 	LCs should monitor the release of 'hotfixes' and system security patches on a regular basis and analyse the feasibility of implementing this into the internet trading systems.	The Guidelines puts in a specific requirement that LCs must conduct testing as soon as practicable and implement security patches or hotfixes within one month following completion of testing.
Logical and physical access security 	User access management and controls (including privileged access and remote access) should be established and effectively enforced. Formulate and implement a physical security policy to protect critical computer equipment (including the server and network devices) in a secure environment.	An additional requirement that user access recertification should be performed at least on a yearly basis has been added. The Guidelines puts in specific requirements on physical access restrictions to prevent unauthorised physical access.
End-point protection 	There were no specific requirements on the timely updating of the corresponding definition and signature of anti-virus and anti-malware solutions.	LCs should implement and update anti-virus and anti-malware solutions on a timely basis.
Third-party service providers 	Arrange service level agreements (SLAs) with major vendors (including intra-group entities) providing for sufficient levels of maintenance and technical assistance with quantitative details.	Additional specific requirements on regularly reviewing and updating the SLAs with vendors has been added.
Secure network infrastructure 	In previous circulars, the requirement of network segmentation by setting up a DMZ was already in place.	The guidelines reiterated the importance of implementing a DMZ with multi-tiered firewalls to protect critical systems (e.g. the internet trading system and settlement system) and client data.

Cybersecurity management and supervision		
	In previous SFC circulars	**In the new Guidelines**
Management roles and responsibilities 	There should be at least one responsible officer or executive officer responsible for the overall management and supervision of the internet trading system.	Management's responsibilities are specified to include oversight on: • Cybersecurity risk management policies and procedures • Budget and spending on resources for cybersecurity risk management • Regular self-assessment • Cybersecurity incidents • Major findings identified in internal and external audits • The latest cybersecurity threats and attacks • Cyber-specific contingency plan • SLA with vendors.
Cybersecurity incident reporting 	Communication protocols and procedures should be formulated in the event of a system outage and major security incidents.	Cybersecurity incident management and escalation procedures as well as communication strategies should be formulated and formally documented.
Cybersecurity awareness training for internal system users 	Cybersecurity awareness training should be regularly provided to all staff, from senior to junior levels, and service providers if applicable, followed by assessments (e.g. a simulated phishing exercise) to assess whether staff and/or service providers are equipped with a strong cybersecurity awareness culture.	Adequate cybersecurity awareness training should be provided to relevant parties annually.
Cybersecurity alert and reminder to clients 	Provide updated security tips to clients on internet trading systems including web and mobile applications.	LCs should provide regular recommendations on preventive and protection measures to clients, such as that login credentials should be properly safeguarded and cannot be shared.

Additional good industry practices recommended by the SFC

The SFC's control requirements set out in the Guidelines are only the minimum requirements. Internet brokers should implement additional controls commensurate with their business model as necessary. ***Good Industry Practices for IT Risk Management and Cybersecurity*** lists out a set of good industry practices that LCs may consider deploying and incorporating into their own cybersecurity management framework. These controls are not mandatory, but LCs should consider adopting the appropriate controls based on their risk profile and risk appetite, aligned with their cyber strategy.

Legal and compliance

- Cyber insurance policy subscription
- Independent professionals to perform post-mortem review in the event of material security incidents

Leadership and governance

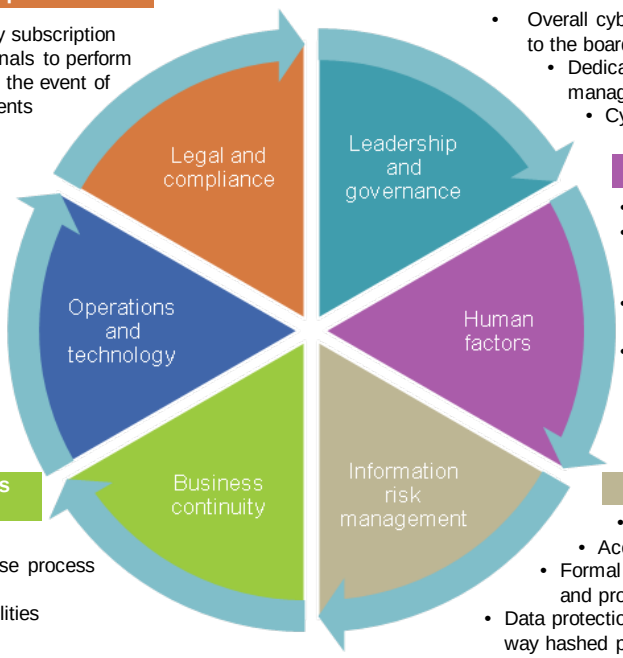
- Overall cybersecurity assessment, with reporting to the board or relevant committee
- Dedicated function for IT and cyber risk management
- Cyber intelligence subscription

Operations and technology

- Security operations centre or equivalent function to perform security monitoring
- Trade surveillance capability
- Tailored behavioural monitoring solutions
- Regular review on audit trail records/access logs
- Proper test cases for critical functions in system development and program change process
- Production codes escrow arrangement

Human factors

- Staff training and qualifications
- Evaluation of staff members' understanding and compliance with company cyber-related policies
- Qualified professionals to conduct cyber-specific assessment
- Reasonably sufficient cybersecurity alerts and reminders to clients using various channels



Business continuity and crisis management

- Performance monitoring and alerts
- Red teaming to test incident response process and capabilities
- High resiliency and recovery capabilities

Information risk management

- Application whitelisting solutions
- Access control, record and monitoring
- Formal cryptographic key management policies and procedures
- Data protection using secure login with salted and one-way hashed passwords
- Data flow of sensitive information identification and documentation

How can KPMG help?

Due to the tight implementation timeline for the 20 baseline controls set out in the Guidelines, internet brokers and banking corporations who offer internet trading should act now to ensure timely compliance. KPMG has dedicated cyber teams that can help you to:

- Quickly assess your current exposure to the requirements and determine an in-scope system authentication mechanism
- Evaluate your readiness to meet the new requirements around 2FA as well as 20 mandatory controls
- Establish a plan for your company, with clarity about how you will comply with the three requirements: 2FA, 20 mandatory controls and good practice
- Implement and/or remediate controls within your trading platform as well as cyber strategy
- Test and document the compliance level of mandatory controls, demonstrating robust security objectives.

Contact us

Henry Shek
Partner,
IT Advisory
KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

Vivian Chui
Head of Securities and Asset Management,
KPMG China
T: +852 2978 8128
E: vivian.chui@kpmg.com

Brian Cheung
Associate Director,
IT Advisory
KPMG China
T: +852 2847 5026
E: brian.cheung@kpmg.com

kpmg.com/cn