Managing cybersecurity risk in the electronic trading business

Cybersecurity risk in electronic trading

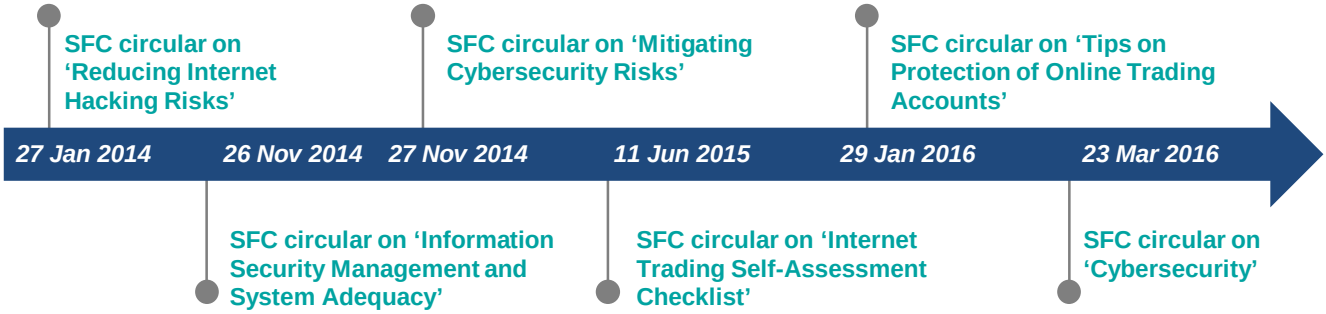
Financial institutions are common targets for cyber attacks. Securities firms constantly face cyber risks due to their tight linkages with trading infrastructure and online trading platforms, as well as the volume of transactions handled via their trading platforms.

In Hong Kong, threats of cyber attacks are on the rise, and addressing and preventing these attacks has become an ongoing challenge for securities firms. The evolving nature of cyber threats means that new types of attacks are arising daily, and companies need to play catch-up to learn and adopt new controls. In addition, cyber governance is organised and implemented differently across securities firms of different sizes in Hong Kong. For these reasons, hackers have new opportunities to target these firms and seek direct financial gain – with comparatively less effort.

In light of the rising cybersecurity risks, regulators have reiterated the importance of putting in place an effective cybersecurity management framework to prevent and detect cybersecurity incidents. The Hong Kong Securities and Futures Commission (SFC) has issued several circulars calling for immediate action to be taken by securities firms in order to ensure the security of electronic trading systems and infrastructure.

Strengthened regulatory requirements

Regulators in Hong Kong are tightening their requirements on electronic trading. In recent years, the SFC has published multiple circulars to emphasise the importance of managing cybersecurity risks in electronic trading systems with evolving requirements:



Are you managing your cybersecurity?

It is time for securities firms to put cybersecurity at the top of their agenda to ensure compliance with regulatory requirements, as well as to protect themselves and their clients from being the victims of evolving cyber attacks. Sophisticated attacks can cause massive financial and reputational loss.

Are you prepared to prevent, detect and respond to cyber attacks? Answer these questions to determine how well-prepared you are:

- **Is your board involved in making cybersecurity management decisions?**
- **Is your network infrastructure secure? When was the last assessment?**
- **Do you think you have an effective user access management process for staff and customers?**
- **Do you know how your business will continue in case of a cyber attack?**
- **Have you adopted a secure software development life cycle?**
- **Are your business partners managing cybersecurity properly?**
- **Are you able to detect and follow up on security attacks?**

Key considerations

The SFC expects a number of key cybersecurity controls to be in place and working well. Based on our experience working with securities firms in Hong Kong, the table below summarises some of the key controls that are often looked at when it comes to implementing a good cybersecurity programme.

Cybersecurity management area		Key controls
Govern	Management oversight	• Conduct regular cybersecurity risk assessments • Include cybersecurity as a standing senior management/boardroom agenda • Measure staff's security awareness, and design awareness programmes to address areas in need of improvement
	Vendor management	• Implement a formalised cybersecurity management process for service providers • Perform ongoing cybersecurity risk assessments of third-party vendors
Prevent	User access controls	• Put in place effective identity and access management to ensure effective and systematic access provisioning, update, revocation and recertification
	System implementation	• Establish a practical system development life cycle management framework • Establish secure coding practice and embed security testing across the life cycle
	Network infrastructure architecture	• Ensure robust technology controls and multi-tiered network defences • Formalise vulnerability and security patch management to proactively prioritise and remediate infrastructure weaknesses based on security intelligence
	Application controls	• Implement a secure authentication (e.g. two-factor authentication) mechanism • Establish robust application-level password and session management controls
Detect	Data management and protection	• Establish an effective information protection programme to ensure sensitive data is classified and information flows are protected • Implement a mechanism to prevent data leakage and detect potential data leakage
	Vulnerability management	• Conduct regular intelligence-driven penetration tests on internet-based systems • Monitor and actively follow up on potential fraudulent websites or mobile applications
	Monitoring	• Implement continuous, behavioural-based and intelligence-driven anomaly monitoring mechanisms • Maintain available audit trails or system logs to detect and investigate security incidents promptly
Respond	Backup and contingency	• Formulate business continuity, IT recovery and data backup plans, and include cyber incidents in drill exercises based on the latest cyber attack patterns • Make readily available an incident response team (internal/external) for any cybersecurity breaches

How can KPMG help?

Compliance assessment and remediation support	Cyber maturity assessment	Cyber in the boardroom	Data leakage prevention	Identity and access management
• Provide a list of gaps with recommended improvements and professional remediation support to address the identified gaps in an efficient and cost-effective manner • **Enable you to focus internal resources on strategically addressing any key gaps and achieve compliance**	• Measure the security maturity of the electronic trading system's cybersecurity exposure, and provide detailed findings, strategic recommendations and an actionable road map • **Enable you to take progressive steps to close key gaps**	• Provide business leaders with the confidence, knowledge and understanding to make informed cyber decisions • **Enable management to reduce the likelihood and impact of incidents, and make the most of strategic opportunities**	• Understand your risks and strengthen your defences against data loss • **Enable you to reduce the risk of data loss through various changes in your people, process and technology**	• Provide solutions that mitigate risk and meet regulatory requirements, while reducing time to market, effort and cost • **Enable you to establish a well-organised and high-quality identity and access management programme, supported by effective technologies and solutions**

Contact us

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

Kelvin Leung
Director
IT Advisory
KPMG China
T: +852 2847 5052
E: kk.leung@kpmg.com

Alvin Li
Associate Director
IT Advisory
KPMG China
T: +852 2978 8233
E: alvin.li@kpmg.com

Matrix Chau
Associate Director
IT Advisory
KPMG China
T: +852 2685 7521
E: matrix.chau@kpmg.com

kpmg.com/cn