RPC

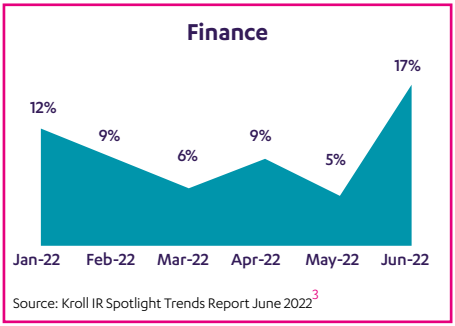
Cyber Incident Reporting Obligations for Hong Kong Licensed Financial Services Companies

August 2022

Cybersecurity and Licensed Institutions – Reporting obligations in the event of an attack

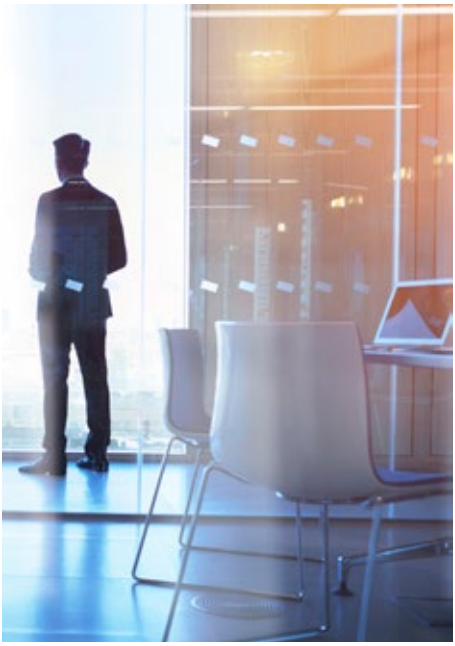
The number of cyber-attacks is on the rise. In particular, financial services companies have been identified as key targets for threat actors in the Q2 of 2022.

A recent report by leading cybersecurity services provider, Kroll, identified the Finance sector as jointly the second most attacked industry sector in June 2022 (behind Healthcare, and alongside Professional Services), with email compromise passing ransomware and other malware as the leading threat incident type.[1] Q1 2022 had seen a 54% increase in phishing attacks used for initial access compared to Q4 2021.[2]



Source: Kroll IR Spotlight Trends Report June 2022[3]

This article summarises the Hong Kong reporting obligations in the event of a cybersecurity incident under the latest guidelines for corporations licensed by the Securities and Futures Commission or authorised by the Hong Kong Monetary Authority. It also addresses the current position on under Hong Kong law on data breach notifications to the Privacy Commissioner for Personal Data and data subjects.



SFC licensed corporations

The Securities and Futures Ordinance and the *Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission* (the "Code of Conduct")[4] contain no specific references to cybersecurity incidents or data breach reporting obligations.

Rather, the Code of Conduct requires that SFC-licensed corporations ("LCs") report to the SFC immediately upon "*any material breach, infringement of or non-compliance with... the requirements of any regulatory authority*"[5] or "*any material failure, error or defect in the operation or functioning of [their] trading, accounting, clearing or settlement systems or equipment*",[6] and comply with various additional requirements when conducting electronic trading.[7]

The SFC issued a circular in 2017 reminding LCs to report to the SFC immediately "*upon the happening of any material cybersecurity incident including ransomware attacks*".[8] For the 18 months ended 31 March 2017, according to the SFC 12 LCs reported 27 cybersecurity incidents, most of which involved hackers gaining access to customers' internet-based trading accounts with securities brokers resulting in unauthorised trades totalling more than HK$110 million, and some others involved distributed denial-of-service ("DDoS") attacks targeting their websites accompanied by threats of extortion.[9]

However, neither of these Code of Conduct obligations, nor subsequent SFC circulars, provide further guidance on what the SFC considers to be a material cybersecurity incident. For example, whether all DDoS attacks or ransomware attacks must be reported. The emphasis is instead on materiality and the impact on the "*operation or functioning*" of specific systems.

LCs therefore have to make a judgment call on whether a cybersecurity incident is material and therefore notifiable to the SFC. An attack that causes an extended outage to a financial institution's trading system or client internet trading accounts is likely to be considered material. Similarly, a ransomware attack that encrypts all of an asset manager's systems preventing the collection of any client instructions or the giving of any trading orders, is likely to be material and reportable to the SFC.

The SFC has issued no specific rules or guidance on customer data leaks. An email compromise that leads to an extraction of personal data but allows normal operations to continue may not be considered material to the SFC under current regulations.

Where an LC is engaged in internet trading (i.e. where order instructions are sent through "*an internet-based trading facility*"), the SFC recommends "*minimum standards*" expected of the LC, including to establish written policies and procedures specifying the manner in which a suspected or actual cybersecurity incident should be escalated and reported internally (e.g. to the responsible officers in charge of internet trading) and externally (e.g. to clients, the SFC and other enforcement bodies, where appropriate).[10] The SFC therefore requires the LC to set the policies and procedures it must follow, rather than setting out the instances in which the LC is required to report to the SFC.

HKMA authorised institutions

The Banking Ordinance similarly has no specific reference to cybersecurity or cyber incidents, although the HKMA is highly concerned with cybersecurity of banking services.

The HKMA stresses in its Supervisory Policy Manual for Technology Risk Management[11] and its circular on Incident Response Management Procedures[12] that once an authorised institution authorised by the HKMA under the Banking Ordinance ("AI") becomes aware that a "*significant incident*", "*IT-related fraud or a major security breach*" has occurred, it "*should notify the HKMA immediately and provide [the HKMA] with whatever information is available at the time*". The HKMA is clear that AIs must not wait until they have rectified the problem before reporting the incident to the HKMA. This is clearer than the obligations stated by the SFC.

The HKMA's Incident Response and Management Procedures circular also provides a specific obligation to "*proactively notify the customers affected or likely to be effective... and advise them of the steps or precautionary measures that they need to take as well as whether the bank would reimburse any losses*". In the event of a "*cyberthreat*", AIs should also endeavour to issue warning messages to all or the relevant customers as appropriate as soon as practicable.[13] AIs are further required to "*consider making a public announcement where the situation so warrants*" for example where the nature of the incident is serious (e.g. disruption to any "*essential and critical banking service channel*" or where "*the disruption may last for a prolonged period of time*") or where a large number of customers have been affected.

However, the HKMA emphasises that these are only "*the broad principles*" and AIs may need to take into account other factors. The HKMA has not set out lists of what incidents it considers should be notifiable to it, and what would not. Once an AI has become aware that a "*significant incident*" has occurred, it is required to notify the HKMA immediately. The burden therefore rests on AIs, in deciding whether to report cyber incidents to customers or the HKMA, to consider the impact and severity of the cyber incident and how it might affect customers and the AIs' operations. AIs are also expected to make a separate public announcement if an incident "*has wider implications for the general public*".

The HKMA has gone further than the SFC in providing specific guidance on customer data protection and when a reporting data "*privacy incidents*". In the event of an incident involving "*stealing, loss or leakage of customer data*", the HKMA's circular

on Customer Data Protection[14] sets out procedures required by AIs to handle, respond to and report the incident. These include:

(i) having effective incident handling and reporting procedures in place (i.e. before an incident occurs);

(ii) assigning an officer of sufficiently senior ranking or a designated management committee, which is chaired by senior management, to oversee the handling and reporting of privacy incidents;

(iii) reporting the incident to the HKMA and "relevant regulatory authorities" including the PCPD "*where appropriate*"; and

(iv) notifying affected customers "*as appropriate*" or providing a justification why it did not notify affected customers.

AIs should also comply with any relevant codes of practice issued or approved by the Privacy Commissioner for Personal Data (the "PCPD") giving practical guidance on compliance with the Personal Data (Privacy) Ordinance (the "PDPO")[15].

The HKMA is clear that where the nature of a data privacy incident is serious, e.g. the incident will likely have a high impact on the AI's reputation, the number of customers affected is large or the customer data stolen is sensitive, the affected AI is expected to report the incident to the HKMA and the PCPD, and notify affected customers "*as soon as practicable after the AI... is aware of or notified of the incident*".

There remains some discretion for AIs under the HKMA's Customer Data Protection circular, but it provides fairly clearer guidance on when AIs are expected to report a customer data breach.

For AIs offering internet trading services, the HKMA has mandated that they refer to the SFC's Internet Trading Guidelines[16] for when to report a cybersecurity incident.

Personal data privacy legislation

As we have stated in previous articles, there remains no mandatory obligation under the PDPO to report a data breach to the PCPD or to data subjects.

Until a statutory breach reporting obligation is introduced, the PCPD considers data breach reporting to be "recommended practice for proper handling" of such incidents.

In terms of industry-specific guidance, the PCPD has issued the following guidance notes:

(i) Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry, which assists banks and "**other financial institutions**" (including LCs) in understanding and complying with the relevant requirements under the PDPO as well as promoting good practices in relation to the collection, accuracy, retention, use, security of and access to customers' personal data; and

(ii) Tips for Using Fintech, which includes recommended (not mandatory) good practices for FinTech providers / operators including to "*develop procedures in relation to handling of data breach incidents*".

The HKMA's guidance therefore goes further than both the PCPD and the SFC in mandating cyber incident reports to the regulators and affected data subjects. For SFC-licensed entities there remains larger discretion in whether an incident is material enough to require a report to the SFC and there is no mandatory obligation to report to the PCPD or affected data subjects. However, if a LC does not report a data breach, the SFC, in determining the appropriate response to the incident, is likely to ask why.

Commentary

In handling and responding to any cybersecurity incident, time is of the essence. A quick, pre-planned response can be critical in preventing the impact of the incident being worse than needed.

As financial services and data privacy regulators tighten their regulations and impose more onerous cyber incident reporting obligations, financial services companies would benefit from implementing a comprehensive cyber-risk prevention and control system to ensure effective and effective immediate handling of such incidents. This should include the designation of responsible staff for handling the report of cybersecurity incidents to regulatory bodies.

The regulatory reporting obligations in Hong Kong still provide a lot of ambiguity in relation to when a cyber incident is material enough to require reporting to the financial services regulators, although the HKMA's guidance is clearer. We have not yet seen any enforcement actions by the SFC, the HKMA or the PCPD for failing to report, or late reporting, of a material cybersecurity incident. There remains no statutory data breach reporting obligation to the PCPD under Hong Kong's personal data protection law.

In determining whether a cybersecurity incident is notifiable to the regulators, customers or the public, LCs and AIs should consider the potential impact on the company and its reputation, the seriousness of the incident, and the extent of impact to the customers. They should also seek immediate legal advice if there is any doubt.

If there is any doubt about whether an incident should be reported, LCs and AIs may wish to file a voluntary report to the SFC / the HKMA 'out of an abundance of caution' in order to demonstrate to the regulators that the company is taking a responsible approach to being the victim of an illegal attack.

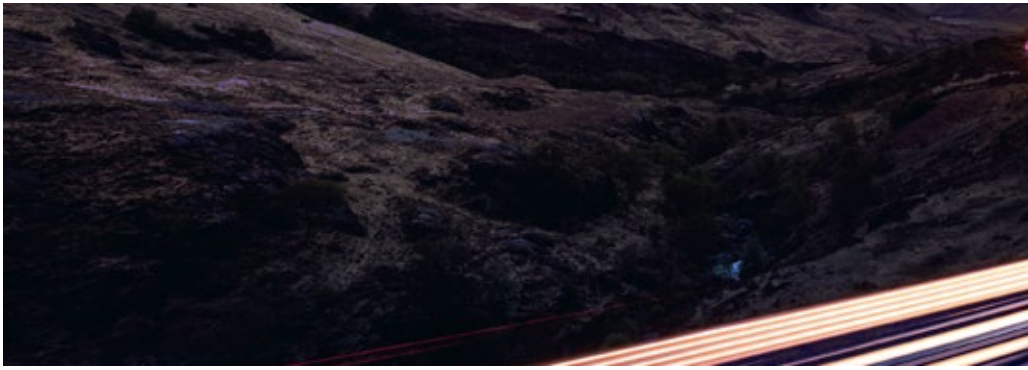
As a final note, this article looks only at the reporting obligations under Hong Kong law and regulations. Data privacy and cybersecurity laws and regulations across Asia are evolving. In addition to the increasingly extraterritorial reach of data privacy laws, the international nature of financial services means that companies may be subject to reporting obligations in more than one jurisdiction.

By contrast to the Hong Kong position, financial institutions falling within the respective Singapore reporting obligations are required to report a personal data breach to Singapore's Personal Data

Protection Commission within 3 calendar days, or a system malfunction or IT security incident to the Monetary Authority of Singapore within 1 hour. LCs and AIs operating across Asia should therefore consider the legal and regulatory reporting obligations in all relevant jurisdictions (which may include places where they have customers but no operations).

A structured data mapping exercise, pro-active and periodic cybersecurity training and simulations, and preparation of a cyber incident / data breach response plan can all save time, money and anguish, and can even result in a lighter sanction (if any) from the regulators.

RPC's Asia Cyber Incident Response team advises companies across Asia and across industries, including Financial Services, on ransomware, email compromise and other attacks. Our pre-structured cyber response service incorporates legal, forensic IT and reputation risk management / communications advisors. Having responded to over 60 cyber incident calls since we launched in Asia in 2017, we are well-placed to advise on the appropriate response to cyberattacks and other data breaches. https://www.rpc.co.uk/expertise/services/data-and-cyber/data-breach-resecure/



1. Kroll *IR Spotlight Trends Report June 2022*
2. Kroll *Q1 2022 Threat Landscape: Threat Actors Target Email for Access and Extortion*
3. Note 1, at page 5
4. https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/codes/code-of-conduct-for-persons-licensed-by-or-registered-with-the-securities-and-futures-commission/Code_of_conduct-Dec-2020_Eng.pdf
5. *Code of Conduct*, at paragraph 12.5 (a)
6. *Code of Conduct*, at paragraph 12.5 (e)
7. *Code of Conduct*, at 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
8. *Circular to All Licensed Corporations - Alert for Ransomware Threats* (https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=17EC26)
9. *Consultation Paper on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading* (https://apps.sfc.hk/edistributionWeb/api/consultation/openFile?lang=EN&refNo=17CP4)
10. *Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading, at paragraph* 3.2 (https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/guidelines/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading.pdf)
11. *Supervisory Policy Manual on General Principles for Technology Risk Management* (https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-1.pdf)
12. *Incident Response and Management Procedures circular* (https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2010/20100622e1.pdf)
13. *Code of Banking Practice, at paragraph 16* (https://www.hkma.gov.hk/media/eng/doc/code_eng.pdf)
14. *Customer Data Protection circular* (https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2014/20141014e1.pdf)
15. *Code of Banking Practice, at paragraph 8.2* (https://www.hkma.gov.hk/media/eng/doc/code_eng.pdf)
16. Note 9