ALLEN & OVERY

A guide to Hong Kong's cyber security laws and practices

Introduction

The past decade has seen a huge increase in the incidents of cyber crime in Hong Kong. The number of cyber crime reports rose from 2,206 in 2011 to 12,916 in 2020. This trend has been exacerbated by the global pandemic, which has forced criminals on-line, with the number of cases in 2020 representing a 55% increase on the 2019 figure alone. The value of those crimes also increased twenty-fold between 2011 and 2020, rising from HK$148 million to HK$2.96 billion.

This note provides an overview of the legal framework in Hong Kong as it relates to cyber security and cyber crime, focusing on what organisations can and must do to protect individuals' data from attempted breaches, as well as the laws that criminals break in carrying out their attacks. It also covers the powers available to the Privacy Commissioner for Personal Data, Hong Kong's personal data privacy regulator, and what organisations should do if a breach occurs.

Matt Bower
Partner – Litigation
Tel +852 2974 7131
matt.bower@allenovery.com

Fai Hung Cheung
Partner – Litigation
Tel +852 2974 7207
fai.hung.cheung@allenovery.com

Karen Chan
Of Counsel – Litigation
Tel +852 2974 7149
karen.chan@allenovery.com

Jeffrey Huang
Senior Associate – Litigation
Tel +852 2974 7244
jeffrey.huang@allenovery.com

1. CYBER SECURITY LAWS

(a) What laws govern cyber security breach incidents?

Hong Kong does not have a comprehensive cyber security law. Relevant provisions are found across various statutes.

Personal Data (Privacy) Ordinance

The Personal Data (Privacy) Ordinance (Cap 486 of the Laws of Hong Kong) (as amended by the Personal Data (Privacy) (Amendment) Ordinance 2012) (**PDPO**) consolidates the legal framework concerning privacy, data protection and cyber security in Hong Kong. Organisations that collect, hold, process or use personal data are known as 'data users' and must comply with the PDPO.

The PDPO sets out six data protection principles, including the principle that data users must use all practicable steps to ensure that personal data held are protected against unauthorised or accidental processing, erasure, loss or use (**DPP 4**). In particular, if a data user engages a data processor (such as a third-party IT provider to process personal data of employees or customers), the data user must adopt protections to ensure the security of the data. This is important because under Section 65(2) of the PDPO, the data user is liable for any act done or practice engaged in by its data processor.

The Office of the Privacy Commissioner for Personal Data (**PCPD**), an independent statutory body, was established to oversee the enforcement of the PDPO. The PCPD will issue various codes of practice and guidelines to provide organisations with practical guidance to comply with the PDPO.

Section 33 of the PDPO deals with the transfer of data outside of Hong Kong and prohibits all transfers of personal data to a place outside Hong Kong except in specified circumstances, such as where the data protection laws of the foreign country are similar to the PDPO or the data subject has consented to the transfer in writing. Section 33 of the PDPO has not been brought into force since its enactment in 1995 and according to the PCPD's media statement on 23 January 2014, the government has no timetable for its implementation in the future. In the PCPD's presentation titled "The Summit on the Greater Bay Area - Data Interconnection and Secure Development" dated 5 January 2020, the implementation of section 33 was stated to have been deferred because the business sector (1) expressed concern about its impact on operations, (2) expressed concern about difficulties in compliance, and (3) demanded more time to implement measures to comply with section 33. The PCPD is currently formulating measures to facilitate the implementation of section 33.

Unsolicited Electronic Messages Ordinance

The Unsolicited Electronic Messages Ordinance (Cap 593 of the Laws of Hong Kong) provides for the regulation of the sending of unsolicited electronic messages and any connected purposes.

Section 22 provides that a person who accesses a telecommunications device, service or network without authorisation and uses it to transmit multiple commercial electronic messages that have a Hong Kong link commits an offence and is liable on conviction upon indictment to a fine and imprisonment for 10 years. The interpretation of accessing without authorisation is broad and includes accessing the telecommunications method "by any means or in any manner" without being entitled or authorised to obtain such access.

Section 23 provides that a person who knowingly initiates the transmission of multiple commercial electronic messages that have a Hong Kong link from a telecommunications device, service or network without authorisation with intent to deceive recipients as to the source of such messages commits an offence and is liable on conviction on indictment to a fine and imprisonment for 10 years. The interpretation of initiating the transmission of a commercial electronic message without authorisation is defined broadly and includes initiating the transmission "by any means or in any manner" without being entitled to or authorised to initiate the transmission.

Interception of Communications and Surveillance Ordinance

The Interception of Communications and Surveillance Ordinance (Cap 589 of the Laws of Hong Kong) regulates the conduct of interception of communications and use of surveillance devices by or on behalf of public officers and provides for related matters.

Official Secrets Ordinance

The Official Secrets Ordinance (Cap 521 of the Laws of Hong Kong) creates offences in relation to the unauthorised obtaining or disclosure of official information.

Governance obligations applicable to certain types of companies

Governance obligations which can directly or indirectly relate to cyber security, apply to licensed persons under the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (**SFC**) and the Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the SFC.

Governance obligations can directly or indirectly relate to cyber security and can also apply to public companies under the Listing Rules.

(b) What laws apply to critical or essential infrastructure and services?

Section 24 of the Telecommunications Ordinance (Cap 106 of the Laws of Hong Kong) provides that it is an offence for a person employed with a telecommunications service to (a) wilfully destroy, secrete or alter any message that they receive for transmission or delivery; (b) forge any message; (c) utter any message that they know to be false; (d) wilfully refrain from transmitting any message, or intercept detain or delay any message; or (e) copy any message or disclose it to anyone other than the person to whom it was addressed.

In relation to personal data, section 4 and Schedule 1 paragraph 4 of the PDPO requires telecommunication service providers to take all practicable steps to ensure that personal data is protected against unauthorised or accidental access, processing, erasure, loss or use.

(c) Are organisations required to report information related to actual or potential cyber security incidents?

Reports to authorities

In relation to personal data, there is no statutory requirement for data users to inform the PCPD about a data breach incident concerning the personal data held by them. As there is no statutory requirement to notify data subjects of a data breach under the PDPO, failure to make such notification currently does not result in any penalties for the data user.

The PCPD has published a Guidance on Data Breach Handling and the Giving of Breach Notifications (the **Data Breach Guidance**). It does not have the force of law. The Data Breach Guidance states that upon a breach of data incident, data users are advised, as a recommended best practice for the proper handling of such incident, to inform the PCPD and other interested parties (e.g. the internet companies). This should be done by way of a Data Breach Notification Form (the **Data Breach Notification**). The Data Breach Notification includes details about the data breach, actions that have been or will be taken to contain the breach, the risk of harm, as well as any assistance and advice offered to individuals.

In January 2020, the PCPD identified a number of areas of reform to enhance and strengthen the Hong Kong personal data privacy regime. The proposed amendments include the introduction of a mandatory data breach notification mechanism for data users to notify the PCPD and data subjects within a prescribed timeframe. If the PDPO is amended to include such notification mechanism, failure to notify data subjects of a data breach in relation to their personal data may constitute an offence. We expect to soon see a draft bill. If enacted, these changes would create a legal notification regime.

In addition to the abovementioned general legal requirements, regulators of certain sectors (e.g. securities and finance, banking and insurance) publish guidance, circulars or good practices to their regulated entities. Such regulators issue guidance and expected standards on cyber security that may require self-reports to be made. See section 4 (Specific Sectors) below for information.

Reports to affected individuals or third parties

In relation to personal data, there is no statutory requirement for data users to inform the data subjects immediately upon the occurrence of a data breach incident. The Data Breach Guidance advises that upon occurrence of a data breach incident, data users should immediately gather essential information relating to the breach, adopt measures to contain the breach (including notifying law enforcement agencies such as the police or regulators if necessary) and assess the risk of harm. If data users consequently consider that data subjects can be identified and a real risk of harm is reasonably foreseeable, the data user should consider notifying the data subjects. There is no standard form of notification to data subjects. The Data Breach Guidance states generally that a formal notification is useful in drawing the affected persons' attention to take proactive measures to mitigate the potential harm. Depending on the circumstances of the case, a notification may include a general description of what occurred, the timing of the breach, when the breach was discovered, the source of the breach, the types of personal data involved, an assessment of the risk of harm, a description of measures already taken or to be taken and information and advice on the actions that data subjects can take to protect themselves from the adverse effects of the breach and against identity theft or fraud.

(d) Which regulators or authorities are responsible for enforcing cyber security law?

There is no one designated authority enforcing cyber security law in Hong Kong.

Hong Kong Police Force

The Hong Kong Police Force (**HKPF**) is the key enforcement authority in relation to any of the cyber-related offences mentioned above. The HKPF's powers in enforcing the laws include powers to search a reasonably suspicious person; enter and search private premises, and seize items inside; arrest and detain suspects; and take statements.

The Cyber Security and Technology Crime Bureau (**CSTCB**) of the HKPF is responsible for handling cyber security issues and for carrying out cybercrime and technology crime investigations, computer forensic examinations and prevention of technology crime.

The HKPF also maintains a close relationship with INTERPOL in tackling cybercrime in Asia. It frequently seeks assistance from INTERPOL and provides information to it with a view to combating cybercrimes involving perpetrators located outside Hong Kong.

Privacy Commissioner for Personal Data

The PCPD is the personal data privacy regulator, an independent statutory body established to oversee compliance of data users with the PDPO.

Investigation powers and enforcement notices

The PCPD has investigatory and enforcement powers under the PDPO. The PCPD may investigate complaints or notification made to him in relation to any suspected breach of the PDPO, and may issue enforcement notices to data users if he sees fit. Where an act or practice has been engaged in by a data user which relates to personal data and may be a contravention of a requirement under the PDPO, the PCPD may carry out an investigation pursuant to section 38. Under sections 42 to 44, the PCPD's powers to carry out investigations include the power to request any information, document or evidence; summon any person for examination; entering into premises; and to conduct hearings. Pursuant to section 50, the PCPD may decide to issue an enforcement notice which requires the data user to carry out certain actions to remedy and prevent recurrence of the contravention. Section 50A provides that a data user who contravenes an enforcement notice commits an offence and is liable, on first conviction, to a fine of $50,000 and imprisonment for 2 years, as well as a daily penalty of $1,000 if the offence continues after conviction. On a second or subsequent conviction, the data user is liable to a fine of $100,000 and imprisonment for 2 years, as well as a daily penalty of $2,000 if the offence continues after conviction.

In June 2019, the PCPD released its investigation report on a large-scale data breach involving Cathay Pacific, the Hong Kong airline, which led to the leakage of the personal data of 9.4 million of the airline's passengers. The report concluded that the incident happened due to perpetrators being able to exploit a vulnerability in the airline's internet-facing server which enabled hackers to bypass authentication and gain administrative access to install malware. The malware then harvested user account credentials which were used to access IT systems and the passengers' personal data stored with the airline.

The investigation report noted that Cathay Pacific should have known about the particular server vulnerability that enabled penetration of the computer systems and that the airline had already been involved in other instances of data breach. The report therefore concluded that Cathay Pacific had not undertaken all reasonable steps to reduce risks of further data breaches. The report noted that DPP 4 does not

impose an absolute duty on companies to secure personal data, but rather to take the appropriate steps to secure personal data depending on (inter alia) "the volume, kind and sensitivity of data, the harm and damage that could result from the data breach, corporate governance and organisational measures, and technical policies, operations, controls and other security measures of the reasonable quality and standard expected of an organisation".
The report found that the airline did not take all reasonably practical steps to protect personal data against unauthorised access and therefore contravened DDP 4 of the PDPO.

The report noted that the Commissioner has no power to fine a party in breach of the PDPO in its current form. Instead, the Commissioner (i) carried out investigations and published a report; and (ii) took actions to follow up on any remedial and corrective measures taken and reviewed the extent to which instructions set out in the enforcement notice were followed and implemented. The Commissioner further noted that the proposed amendments to the PDPO included a series of changes to enhance the deterrent effect of the Hong Kong legal regime.

In February 2019, the PCPD released its investigation report on a data breach involving Hong Kong Broadband Network Limited (**HKBN**), which had caused the leakage of the personal data of about 380,000 customers and service applicants. The affected database (**Database A**) had undergone a system migration in 2012 and was inactive at the time of the incident. The report concluded that Database A should have been deleted after the system migration and was not so deleted due to HKBN's failure to conduct a comprehensive and prudent review after the system migration.

The report concluded that as HKBN is a telecommunications company holding a considerable amount of customer data, it would be reasonable for customers to expect that their personal data would be properly protected. Whilst HKBN had, for example, invested in information security, developed policies and carried out independent network security audits, the report also found that the safeguards for Database A had been insufficient. Furthermore, HKBN failed to exercise control over the IT and security features for the personal data of customers and service applicants, leading to a data breach which could have been avoided.

As a result, the PCPD served an enforcement notice on HKBN to remedy and prevent any recurrence of the contravention.

The report noted that organisations should not hold on to the mindset of conducting their operations to meet the minimum regulatory requirements only. Instead, they should be held to a higher ethical standard that meets the stakeholders' expectations by doing what they "should" do, by adopting an accountability approach in handling personal data. The principles of data governance, as well as stewardship and ethics, should be incorporated as part of organisations' corporate governance.

The PCPD is also empowered under the PDPO to issue codes of practice, which have the force of law, to advise data users on compliance with the PDPO.

Commissioner on Interception of Communications and Surveillance

The Commissioner on Interception of Communications and Surveillance oversees the compliance of government departments with the requirements of the Interception of Communications and Surveillance Ordinance.

2. CYBERCRIME

2.1 What are some common examples of cybercrime-related activities which constitute a criminal or administrative offence in Hong Kong?

There is no specific legislation in Hong Kong that deals with cyber offences. The legal framework for cyber offences is set out in existing legislation.

Extra-territory

None of the statutes mentioned below have explicit provisions conferring extraterritorial reach; they are applicable to foreign individuals or companies to the extent that they have a presence in Hong Kong or have committed the acts under complaint within Hong Kong.

Denial-of-service attacks

In Hong Kong, denial-of-service attacks refer to both denial of service attacks (**DoS**) as well as distributed denial of service attacks (**DDoS**). Both DoS and DDoS are attempts to send massive data to a host within a short period of time in order to temporarily or indefinitely interrupt and suspend the services of the host and prevent access by legitimate visitors. DoS attacks are sent by one person or system, whereas DDoS attacks are carried out by a multitude of systems.

Section 60 of the Crimes Ordinance makes it a criminal offence for a person without lawful excuse to destroy or damage any property belonging to another, intending to destroy or damage any such property or being reckless as to whether any such property would be destroyed or damaged. To "destroy or damage" any property includes the misuse of a computer, which means (a) causing a computer to function other than as it has been established to function (even if such misuse does not damage the computer, program or data); (b) to alter or erase any program; or (c) to add any program or data to the contents of a computer or computer medium (section 59(1A) of the Crimes Ordinance). A person found guilty of section 60 is liable on conviction upon indictment to imprisonment for 10 years.

In *Chu Tsun Wai v HKSAR* [2019] 1 HKC 589, the defendant was convicted of destroying or damaging property and in particular, the misuse of a computer, contrary to section 59(1A) and section 60 of the Crimes Ordinance. The defendant directed his computer to carry out DDoS attacks on a server set up by the Shanghai Commercial Bank. Lord Hoffmann NPJ construed section 59(1A)(a) liberally, holding that "the statute is concerned with what the [property] owner has set [up the property] to do" and not with the way in which the property works. Hence, a DDoS attack on a server was a misuse of the server as the owner did not intend it to handle DDoS attacks. It was irrelevant that in handling the malicious DDoS requests from the defendant's computer, the server was precisely performing the function it was supposed to do.

Also see the answer in respect of section 161 and the Crimes Ordinance below.

Hacking and phishing

Under section 27A of the Telecommunications Ordinance, it is a criminal offence for a person to, by telecommunications, knowingly cause a computer to perform any function to obtain unauthorised access to any program or data held in a computer. "Telecommunications" is defined as any transmission, emission or reception of communication by means of guided or unguided electromagnetic energy or both, other than any transmission or emission intended to be received or perceived directly by the human eye (section 2). The access of the kind in question to any program or data held in a computer (**Access**) will be unauthorised if the person is not entitled to control Access and (i) he has not been authorised to obtain Access; (ii) he does not believe that he has been so authorised; and (iii) he does not believe that he would have been so authorised if he had applied for the appropriate authority (section 27A(2)(b)). A person found guilty of section 27A of Cap 106 is liable on conviction to a fine at level 4 i.e. $25,000.

The offence of unauthorised access to a computer by telecommunications under section 27A of the Telecommunications Ordinance has effect without prejudice to any law relating to powers of inspection, search or seizure.

Section 161 of the Crimes Ordinance (Cap 200 of the Laws of Hong Kong) has been used by law enforcement agencies as a 'catch-all' computer-related offence. For example, in addition to hacking, section 161 would also apply in respect of phishing. Section 161 provides that any person who obtains access to a computer with either a view to dishonest gain for himself or another (section 161(1)(c)) or with a dishonest intent to cause loss to another (section161(1)(d)) commits an offence. A person found guilty of section 161 is liable on conviction upon indictment to imprisonment for 5 years. Section 16(1)(c) does not apply to the use by a person of his own computer, not involving access to another's computer (*SJ v Cheng Ka Yee and others* [2019] HKCFA 9).

In the recent case of *HKSAR v Chan King Hei* DCCC 164/2020, the District Court held that unauthorised access of information available by virtue of employment may constitute an offence under section 161 of the Crimes Ordinance, as well as under section 64 of the PDPO (see below). In this case, the defendant was taken in for questioning by the police after he was found taking photos of a police station using his mobile phone. Investigation of the defendant's phone showed that he had sent a message in a chat room for doxxing (the practice of researching and publicly broadcasting private or identifying information often with a malicious intent) which contained personal information of a family member of a police officer (the Victim). The defendant had downloaded the information from the database of the telecommunications company (HKT) by which he was employed at the material time.
In relation to the charge under section 161, the court held that the intended gain does not have to involve a monetary gain and includes information which the person obtaining access to the computer did not have before the access. In relation to dishonest intent, the court held that the person would be dishonest if he knew that he was not authorised to access the database to acquire private personal data of third parties for his own purposes and without their consent.

Infection of IT systems with malware

See the answer in respect of section 60 and section 161 of the Crimes Ordinance above.

In respect of ransomware, section 23 of the Theft Ordinance (Cap 210 of the Laws of Hong Kong) is also relevant. Section 23 provides that a person commits blackmail if, with a view to gain for himself or another or with intent to cause loss to another, he makes any unwarranted demand with menaces. Any person found guilty of section 23 shall be liable on conviction upon indictment to imprisonment for 14 years. Interestingly, section 23(4) also provides that any person who has in his possession or under his control any letter or writing making any unwarranted demand of any person with menaces shall be guilty of an offence and shall be liable on conviction upon indictment to imprisonment for 10 years. Whilst this sub-section has yet to be tested in the courts, theoretically the possession of ransomware code as a piece of writing, making an unwarranted demand of any person with menaces, could constitute an offence under section 23.

In relation to the offence of blackmail, no offence is committed if the person provides that he possessed or controlled the letter or writing otherwise than with intent to utter it.

Unsolicited penetration testing

Whether penetration testing constitutes an offence in Hong Kong will depend on whether such testing involves causing a computer to perform any function to obtain unauthorised access to any program or data held in a computer, which constitutes an offence under section 27A of the Telecommunications Ordinance – see above.
If it does not, then such testing will not constitute an offence in Hong Kong.

Identity theft or identity fraud

Section 2 of the Theft Ordinance provides that a person commits theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it. "Property" includes intangible property such as digital data or electronic files. A person who is found guilty of section 2 will be liable on conviction upon indictment to imprisonment for 10 years.

The Theft Ordinance section 2 would also apply in respect of electronic theft.

There are also various qualifications on the definition of theft under the Theft Ordinance which may mean that no offence has been constituted by the person. However, these qualifications depend on either (a) the person's belief that he was entitled to the property or (b) the person's belief that if the owner of the property knew of the appropriation, the owner would give consent to such appropriation. As such, these qualifications are unlikely to be applicable to the cyber security issues.

Furthermore, section 16A of the Theft Ordinance provides that a person commits fraud if any person (the **first person**) by any deceit and with intent to defraud induces another person (the **second person**) to commit an act or make an omission which results in either a benefit for anyone other than the second person or in prejudice or a substantial risk of prejudice to any person other than the first person. Theoretically, someone who uses internet services or software to defraud victims or take advantage of them may be charged with this offence. A person found guilty of section 16A will be liable on conviction upon indictment to imprisonment for 14 years.

Section 64 of the PDPO is also relevant. The PDPO applies where data relating to an individual (a **data subject**) is collected, held, processed or used by another (a **data user**). Section 64 provides that a person commits an offence if the person discloses any data subject's personal data which was obtained from a data user without the data user's consent, with an intent to gain or to cause loss to the data subject or if such disclosure causes psychological harm to the data subject. A person found guilty of section 64 is liable on conviction to a fine of $1,000,000 and to imprisonment for 5 years.

A defence is available if (a) the alleged offender believed that disclosure was necessary for the purpose of preventing or detecting crime; (b) the disclosure was required or authorised by or under any enactment, by any rule of law or by an order of a court; (c) the alleged offender believed that the data user had consented to the disclosure; or (d) the person disclosed personal data for the purpose of a news activity or had reason to believe publishing of the personal data was in the public interest.

In the case of *HKSAR v Chan King Hei* mentioned above, the defendant was found guilty of section 64 of the PDPO due to the disclosure of personal information (obtained from HKT's database) which caused psychological harm to the Victim.

Possession or use of tools used to commit cybercrime

See the answers above in respect of section 27A of the Telecommunications Ordinance, section 161 of the Crimes Ordinance, section 60 of the Crimes Ordinance and section 23 of the Theft Ordinance.

3. HOW CAN ORGANISATIONS PROTECT THEIR IT SYSTEMS?

Monitoring employees' internet usage

An employer is not prohibited from monitoring its employees' internet usage in order to prevent or mitigate the impact of cyber attacks. However, any monitoring that involves handling personal data must comply with the PDPO. The Privacy Commissioner has also published Privacy Guidelines on Monitoring and Personal Data Privacy at Work which offers guidance to employers on the application of the provisions of the Ordinance as they relate to the activity of employee monitoring, although the Guidelines do not have the force of law.

The Basic Law and, in particular, the right to freedom and privacy of communication in Article 30, must also be considered and balanced against the obligations of the organisation to implement security measures in respect of potential incidents.

Specific cyber prevention measures

There are no specific laws prohibiting the use of the following measures in Hong Kong:

(a) **Beacons** (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content). However, where the use of a web beacon involves processing personal data, the organisation's use of the web beacon must be in accordance with data protection laws;

(b) **Honeypots** (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data); and

(c) **Sinkholes** (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks).

There are no specific restrictions on the import or export of technology designed to prevent or mitigate the impact of cyber-attacks.

4. RECENT INCIDENTS

There has been a significant increase in cyber fraud cases since the Covid-19 outbreak. In addition, Hong Kong is one of the primary destinations for the proceeds of cyber fraud to be transferred to.

It has been reported that a large financial media corporation lost USD29 million in an email fraud involving international transfers of money from its US subsidiary to Hong Kong recipients. On the back of this fraud, the corporation obtained injunctive relief against certain defendants in the Hong Kong court.

We expect an increase in civil recovery actions before the Hong Kong courts. There have been a number of court proceedings commenced by victims of cyber fraud. In addition to declaratory relief, default judgment and injunction, the plaintiffs (victims) often apply for a vesting order (compelling the bank to transfer the money in the recipient's account to the victim) under the Trustee Ordinance (Cap 29 of the Laws of Hong Kong) against the recipients of the funds. These applications have given rise to a number of recent divergent decisions as to whether a constructive trust can arise and vesting orders be granted under the statute. While there is likely to be more court decisions on this topic, we expect there to be appellate guidance in this uncertain area of the law.

5. SPECIFIC SECTORS

In addition to the general legal requirements under section 1 (Cyber Security Laws) above, regulators of certain sectors (such as securities and finance, banking, and insurance) publish guidance, circulars or good practices to their regulated entities. The regulators issue guidance and expected standards on cyber security, and regulate and supervise the industry to protect consumers. Some examples are set out below. These requirements are not legally binding but failure to adhere may result in disciplinary action.

Securities and financial sector

The Securities and Futures Commission (**SFC**) has:

(a) provided guidance and expected standards on cyber security relating to internet brokers;

(b) reminded licensed corporations (**LCs**) to assess their operational capabilities and implement appropriate measures to manage the cyber security risks associated with the remote working arrangements in light of Covid-19;

(c) issued a Circular to Licensed Corporations – Use of external electronic data storage. It sets out requirements on licensed corporations in engaging an external data storage provider, including cloud services. It also reminds LCs to ensure the preservation and integrity of the records or documents they are required to keep under the Securities and Futures Ordinance (Cap 571 of the Laws of Hong Kong) (**SFO**) or the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap 615 of the Laws of Hong Kong);and

(d) issued the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading, which sets out cyber security requirements for SFC registered or licensed entities performing internet trading.

Banking sector

The Hong Kong Monetary Authority (**HKMA**) has:

(a) introduced the Cybersecurity Fortification Initiative (**CFI**) in 2016, which aims to raise the cyber resilience of Hong Kong's banking system. The CFI requires all authorised institutions (**AIs**) to conduct risk assessment of their cyber security measures and complete a simulated cyberattack test. It launched an upgraded CFI 2.0, which came into effect on 1 January 2021. The aim of CFI 2.0 is to raise the cyber resilience of the banking sector to an even higher level;

"Hugely experienced disputes team with a distinguished track record acting for high-profile banking and corporate clients on contentious matters… One client states: 'I have been very pleased with all the professionals at Allen & Overy as they provide commercial and practical advice to us, considering issues from different perspectives to ensure clients' interests are well protected.'"

Chambers Asia Pacific 2021, Litigation - China

(b) introduced the Enhanced Competency Framework (**ECF**) on cyber security to help banks offer reliable and innovative banking services. The ECF is one of the HKMA's measures to enhance the risk management capability of banks. The HKMA encouraged banks to make use of the competency framework on cyber security to raise and maintain the professional competence of their cyber security practitioners;

(c) issued a Supervisory Policy Manual module TM-E-1 on the risk management of e-banking. It provides guidance to AIs on the risk management of e-banking; and

(d) issued a circular titled Cyber Security Risk Management.

In addition, the PCPD has issued Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry. The guidance is not legally binding. It aims to assist the banking industry in understanding and complying with the 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.

Insurance sector

The Insurance Authority (**IA**) has published a Guideline on Cybersecurity (**GL20**) to regulate and supervise the insurance industry for the protection of existing and potential policy holders. It sets the minimum standard for cyber security that authorised insurers are expected to have in place and the general guiding principles which the IA uses in assessing the effectiveness of an insurer's cyber security framework. This Guideline on Enterprise Risk Management contains supplemental cyber risk provisions.

6. CORPORATE GOVERNANCE

What kind of standard is a director or officer expected to meet when an incident takes place?

Companies (listed or private)

Directors owe fiduciary duties and statutory duties to the company for which they are a director under section 465 of the Companies Ordinance (Cap 622 of the Laws of Hong Kong). Section 465 provides that *"a director of a company must exercise reasonable care, skill and diligence*" and "*reasonable care, skill and diligence mean the care, skill and diligence that would be exercised by a reasonably diligent person with the general knowledge, skill and experience that may reasonably be expected of a person carrying out the functions carried out by the director in relation to the company; and the general knowledge, skill and experience that the director has.*" If the director fails to act in accordance with this standard, he may be liable for breach of duty.

Listed companies

The Guidance for Board and Directors issued by the Stock Exchange of Hong Kong Limited (**HKEX**) provides that the board is responsible for risk identification and control. The company is expected to analyse the source of potential internal and external risks that may arise in relation to the company's business, including the risk of cyber security. Failure to meet such expectations will not result in the imposition of sanctions by the HKEX.

SFC licensed entities

The SFC expects the responsible officer(s) or executive officer(s) responsible for the overall management and supervision of the internet trading system to define a cyber security risk management framework (including but not limited to policies and procedures) and set out their key roles and responsibilities. For example, they have to review and approve cyber security risk management policies and procedures and arrange to conduct a self-assessment of the overall cyber security risk management framework on a regular basis. 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). Failure to meet such expectations will not result in the imposition of sanctions by the SFC, but may reflect adversely on the relevant officer(s)'s fitness and properness to act as such.

HKMA authorised institutions

The board and senior management of an AI have the responsibility of protecting the AI's critical assets, including sensitive information of its customers. They are expected to play a proactive role in ensuring effective cyber security risk management in the AI, covering at least the following areas: risk ownership and management accountability, periodic evaluations and monitoring of cyber security controls, industry collaboration and contingency planning, regular independent assessment and tests, etc. Failure to meet such expectations will not result in the imposition of sanctions by the HKMA.

"Offers expertise in regulatory investigations and mis-selling claims, leveraging off the strength of the firm's fraud, white-collar crime and money-laundering practices."

Chambers Asia Pacific 2020, Litigation – China

Insurance Authority authorised insurers

The board of directors of an authorised insurer should hold the overall responsibility for cyber security controls and ensure accountability within the insurer by articulating clear responsibilities and lines of reporting and escalation for cyber security controls. Where the board establishes a designated management team, the board and the designated management team are responsible for overseeing the design, implementation and assessment of the effectiveness of the insurer's cyber security strategy and framework and for ensuring these are continuously kept up to date. Failure to meet such expectations will not result in the imposition of sanctions by the IA, but may reflect on the IA's view of the continued fitness and properness of the directors or controllers of authorised insurers.

The board of directors of an authorised insurer should establish a defined risk appetite and tolerance limit on cyber risks for the insurer and oversee the design, implementation and effectiveness of related cyber security programs. It may establish a designated management team to oversee and implement cyber security measures and controls. The designated management team should consist of members with the appropriate skills and knowledge to understand and manage cyber risks. Insurers should identify cyber risks and conduct assessment on the effectiveness of the mitigating measures to protect against and manage cyber risks within the risk appetite and tolerance limit set by the board or its designated management team. A self-assessment tool for the overall cyber risk management program should be put in place, as part of an enterprise risk management program.

What other industry specific disclosure requirements are listed companies / regulated entities subject to in relation to cyber security risks or incidents?

Listed companies

If a listed company is subject to an incident, it is required to disclose the same to the public if the incident amounts to inside information.

SFC licensed entities

Under the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (section 12.5), a licensed or registered person, as a firm, should report to the SFC immediately upon "*any material breach, infringement of or non-compliance with … the requirements of any regulatory authority*". This includes a breach of the SFC's guidelines regarding cyber security and the provisions under the PDPO and the guidelines issued by the PCPD.

Under the Report on the 2019-20 thematic cyber security review of internet brokers, it is suggested that upon the identification of potential or actual unauthorised access to clients' internet trading accounts, internet brokers should consider suspending the client accounts and informing the clients concerned.

The Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading require a licensed or registered person to establish written policies and procedures specifying the manner in which a suspected or actual incident should be escalated and reported internally (e.g. to the responsible officer(s) or executive officer(s) in charge of internet trading) and externally (e.g. to clients, the SFC and other enforcement bodies, where appropriate).

HKMA authorised institutions

Under the HKMA's Circular on Customer Data Protection, if sensitive customer data is stolen, lost or leaked, institutions are expected to report the incident to the HKMA and notify the affected customers as soon as practicable after the AI concerned is aware of or notified of the incident. If a large number of customers are affected, the AI concerned should consider issuing a public announcement.

Under the HKMA's Supervisory Policy Manual module, if an incident involves a disruption of critical e-banking services and may last for a prolonged period of time, AIs should consider issuing a press release.

Insurance Authority authorised insurers

Under the Insurance Authority's Guidance on Cybersecurity (GL20), in case of an incident, insurers should notify the IA within 72 hours from detection, and also internal and external stakeholders.

7. CIVIL RIGHTS OF ACTION

If a data subject suffers any damage caused by a data user in an incident in contravention of the requirements under the PDPO, he can make a civil claim for compensation from the data user for the damage. In particular, a data user should note that DPP 4 (data security) requires him to take all practicable steps to protect the personal data he holds against unauthorised or accidental access, processing, erasure, loss or use.

In addition, the victim of an incident may have a basis to bring an action for breach of contract or negligence against an entity (for example, a service provider) subject to the incident, provided that the incident is related to the entity's insufficient cyber security measures. Depending on the circumstances, a victim of an incident may also have other civil causes of actions available such as unjust enrichment, constructive trust, knowing receipt, breach of confidentiality, breach of fiduciary duty, trespass to chattel, misuse of private information, deception, misrepresentation, derivative actions and other economic torts. If a director of a wrongdoer company acts as joint tortfeasor or has conspired to commit the wrongdoing, the victim may bring a tortious action against both the director and the company. These are alternatives to the action under section 66 of the PDPO.

8. INSURANCE

In Hong Kong, cyber security insurance usually covers:

(a) First party losses: the response to the cyber security event, business interruption, data and system recovery, cyber extortion, and

(b) Third party losses: privacy, network security liability, media liability.

We are not aware of any regulatory limitations specifically to cyber security insurance coverage.

"An exceptional magic circle firm with an extensive global presence in key jurisdictions worldwide, housing leading disputes teams across Europe and Asia."

Chambers Global 2021, Dispute Resolution – Global-wide

Allen & Overy's Global Cyber Security Practice

Clients turn to us to manage legal risk in relation to the threat of cyber-attacks as well as when looking for response specialists to ensure they are resilient to cyber-attacks, or other data breaches. Across our international network, our cyber security practitioners advise on all aspects of preventing and reacting to cyber breaches or data incidents.

Computers, the internet, mobile devices and electronic transactions all play an important and ever-increasing role within the corporate environment, particularly for businesses with a strong online presence. However, the continued growth of "cyber" technologies and the growing phenomenon of cyber-attacks pose significant risks to businesses. Cyber attackers are often quick to spot the potential vulnerabilities of new technologies and to exploit them to commit civil and criminal offences (and to frustrate detection of those activities).

Risks include:

– damage to reputation
– business interruption
– financial loss
– litigation
– costs
– loss of IP and confidential information
– regulatory sanctions

As well as advising clients on how to manage legal risk in relation to the threat of cyber-attacks, our cross-practice team of cyber-incident response specialists supports clients to ensure they are resilient to cyber-attacks or other data breaches which may impact them or their own clients' services. We also assist clients with their reaction where a risk has been realised. This requires an integrated approach across traditional security disciplines proactively to understand, detect and respond to advanced and evolving threats. We act as a partner to make sure you can react quickly and effectively.

UK
CS2104_CDD-64040_ADD-96180