MAYER | BROWN

24 JULY 2024

HONG KONG PROPOSES A LEGAL FRAMEWORK FOR REGULATING CRITICAL INFRASTRUCTURES

AUTHORS: GABRIELA KENNEDY, TOW LU LIM, JOSHUA T. K. WOO, KEN TSZ LOK LAM

INTRODUCTION

The acceleration of cyber-attacks on companies in Hong Kong in the last year or so (– with over 60 notifications of such attacks being received by the Office of the Privacy Commissioner of Hong Kong in 2023,[1] and potentially many more going unreported) has also led to an acceleration of discussions about the introduction of cybersecurity legislation.

The idea of cybersecurity legislation was first announced in October 2022 during the Chief Executive's policy address. Since then, the government has engaged in extensive consultation with various stakeholders – more than 15 sessions with over 110 stakeholders, including potential Critical Infrastructure Operators (CIOs). At the end of June this year, a paper (the "Paper") was issued for discussion before the Legislative Council Panel on Security on the proposed legislative framework for regulating CIOs and Critical Computer Systems (CCS) (the "Proposed Framework"). The Proposed Framework, which has been jointly prepared by the Security Bureau, Office of the Government Chief Information Officer, and the Hong Kong Police Force, was discussed during the Legislative Council Panel Meeting on 2 July 2024 (Panel Consultation).

The Proposed Framework is the first concrete step towards the introduction of cybersecurity obligations on organisations,[2] and comes amidst a slew of recent cybersecurity developments in the region, such as the National Cybersecurity Committee in Thailand issuing cybersecurity regulation earlier in January 2024, and the Singapore Parliament passing the Cybersecurity (Amendment) Bill in May 2024, and looks to align Hong Kong with other jurisdictions that currently regulate (or are contemplating regulating) critical infrastructure, such as Mainland China, Macao SAR, Australia, the United Kingdom, Singapore, the European Union, the United States, and Canada.

In this Legal Update, we explore the key elements and provide our observations on the Proposed Framework.

KEY ELEMENTS

1. SCOPE OF APPLICATION

The Proposed Framework adopts an organisation-focused approach, imposing obligations on **CIO**[3], specifically in respect of **CCS**[4]. In other words:

1. Any non-CCSs owned, controlled or used by a CIO will **not** be subject to the Proposed Framework; and
2. It is the computer system that will be regulated, not the information contained within.

CIOs and CCSs will need to be expressly designated as such by the Commissioner's Office (see elaboration on the Commissioner's Office below). CIOs and CCSs will not be individually identified to avoid making them targets of cyber-attacks, but it is proposed that companies within certain sectors (Designated Sectors) will qualify as CIOs. The initial eight Designated Sectors are:

1. Energy;
2. Information Technology;
3. Banking and Financial Services;
4. Land Transport;
5. Air Transport;
6. Maritime;
7. Healthcare Services; and
8. Communications and Broadcasting.

When designating CIOs, the Commissioner will take into account:

1. The implications on essential services and important societal and economic activities in Hong Kong if there is an impact to such infrastructure;
2. The level of dependence on information technology (IT) of the infrastructure concerned; and
3. The importance of the data controlled by the infrastructure concerned.

This designation, however, will be subject to appeal to an appeals board, which will be established separately from the Commissioner's Office and will allow designated CIOs and CCSs an opportunity to challenge the designation imposed on them.

2. OBLIGATIONS

The Proposed Framework sets out three main categories of obligations for CIOs: (a) Organisational; (b) Preventive; and (c) Incident Reporting and Response.

Specifically, CIOs must:

A. ORGANISATIONAL

1. Maintain an address and office in Hong Kong (and keep the Commissioner's Office updated on any subsequent change);
2. Update the Commissioner's Office on the ownership and operations of CIs;
3. Establish a dedicated cybersecurity team to manage cybersecurity (outsourced or inhouse);

B. PREVENTIVE

1. Update the Commissioner's Office of material changes to CCSs;
2. Formulate, implement and submit a computer system security management plan to the Commissioner's

Office;

3. Submit a computer system security risk assessment to the Commissioner's Office annually;

4. Conduct an independent computer system security audit at least once every two years and submit a report to the Commissioner's Office;

5. Additional supervisory measures to ensure that CCSs are compliant even where a third-party service provider may be engaged;

C. INCIDENT REPORTING AND RESPONSE

1. Participate in a security drill organised by the Commissioner's Office at least once every two years;

2. Submit an emergency response plan to the Commissioner's Office;

3. Notify the Commissioner's Office of security incidents within a specified time frame:

    1. Within 2 hours after becoming aware of the incident for serious computer system security incidents; and

    2. 24 hours after becoming aware of the incident for "other" computer system security incidents.

CIOs are also required to co-operate with the Commissioner's Office in the course of any investigation into breaches of the above obligations, including providing information "*available to them*", even if it is located outside Hong Kong.

3. OFFENCES AND PENALTIES

The offences under the Proposed Framework include non-compliance with:

1. Statutory obligations;

2. Written directions from the Commissioner's Officer;

3. Requests from the Commissioner's Officer in their conduct of an investigation; and

4. Requests from the Commissioner's Office to provide information relating to a CI.

Notably, the proposed penalties for these offences will only be applicable to the organisation and not to individuals within the organisation, save for any violations of existing legislation. The maximum penalty proposed is a fine of HK$5 million (~US$640,000), but daily fines are also envisaged for continued non-compliance. These will be determined by the court.

4. COMMISSIONER'S OFFICE

It is proposed that the Commissioner's Office will be set up under the Security Bureau, and will be empowered to investigate and respond to cybersecurity incidents, and also have power of entry, inspection and access to computer systems.

The Commissioner's Office will also be empowered to issue a Code of Practice to guide the compliance of CIOs with the Proposed Framework.

Sector regulators will be nominated to monitor the compliance with the organisational and preventative obligations under the legislation while the Commissioner's Office will monitor compliance with the incident

reporting and response obligations. The Monetary Authority and the Communications Authority have been designated as the responsible authorities for the banking and financial services sector and communications and broadcasting sector respectively.

Notwithstanding the above, the Commissioner's Office will still retain the authority to issue directions to all CIOs.

COMPARISON WITH OTHER JURISDICTIONS

Companies with similar compliance obligations in nearby jurisdictions like Singapore and China may find some of the processes and procedures familiar and may be able to draw from work already done elsewhere to set up their compliance mechanism for the proposed legislation in Hong Kong. For this purpose, we have set out a high-level comparison of some key features across these jurisdictions.

Country **Feature**	**Hong Kong**	**Singapore**	**China**
Security risk assessment	At least once a year		
Security audit	Independent computer system security audit at least once every two years.	Compliance audit with the Cybersecurity Act, codes of practice and standards of performance at least once every two years.	Depending on the Multi-Level Protection System (MLPS) grading – either every one or two years.
Security drill	Take part in a security drill organised by the Commissioner's Office at least once every **two years**.	Participation in cybersecurity exercises organised by the Commissioner is required **upon the Commissioner's direction in writing**; CIOs are required to conduct their own cybersecurity exercises at least **once every 12 months**, with reports to be submitted to the Commissioner upon	Participate in the security drill "**periodically**" organised by regulators.

		request.	
Incident reporting	Serious incidents within **2 hours** and other incidents within **24 hours**.[5]	Cybersecurity Incidents in respect of critical information infrastructure, any computer or computer system under the owner's control that is interconnected with or that communicates with the critical information infrastructure, or any other type of cybersecurity incident in respect of the critical information infrastructure that the Commissioner has specified by written direction to the owner within 2 hours after becoming aware.[6]	Immediately (**one hour** under the Draft Cybersecurity Incident Reporting Measures)[7]
Incident response plan	Emergency response plan to be submitted to the Commissioner's Office within three months of designation.	Incident response plan to be reviewed at least once **every 12 months**.	Response plan to be formulated, which will be reviewed as part of the MLPS review.

UNRESOLVED QUESTIONS

1. COMPLIANCE TIMELINE

The fact that CIOs and CCSs are being designated privately by the Commissioner's Office means that organisations in the Designated Sectors may be faced with substantial uncertainty until the Commissioner's Office makes their designation. The Proposed Framework provides the Commissioner's Office with the power to request (i) any organisation controlling a potential critical infrastructure or (ii) a CIO, to submit relevant information for the purpose of ascertaining whether an organisation should be designated as a CIO or a computer system should be designated as a CCS.

The Paper states that the government intends to crystallise the Proposed Framework into a bill by the end of 2024, and following the passage of the bill, it will establish the Commissioner's Office within one year. The proposed legislation is estimated to come into force within six months from the establishment of the Commissioner's Office, which in essence means sometime in late 2025 at the earliest or mid-2026 at the

latest.

Since the designation of CIOs and CCSs are the responsibility of the Commissioner's Office, following the proposed timeline means that CIOs and CCSs will only have six months to put in place measures to comply with the proposed legislation. This may prove operationally challenging, particularly given the concerns of stakeholders as recognised in the Paper (compliance costs, difficulties in hiring competent computer security personnel to supervise), and the fact that these organisations are likely to be large organisations, which may require a longer lead time to implement organisational changes.

There is some uncertainty regarding the initial eight Designated Sectors. It appears telecommunication service providers will come under the "communications and broadcasting" sector but it is not immediately clear which organisations will come within the "information technology" sector. Presumably the organisations falling within this designation will include data processors, data centres and cloud providers. Such organisations provide a host of services to a variety of customers, and some are even third-party service providers to CIOs. At this stage, it appears that some of these organisations would themselves be designated as CIOs if their services are necessary for the maintenance of the normal functioning of Hong Kong society and the normal lives of the people. In light of the proposed timeline, organisations falling within this sector would need to consider whether they will be caught by the proposed legislation and consider relevant preparatory measures.

2. SCOPE OF "COMPUTER SYSTEM"

The CIO obligations (such as the risk assessment, audit and reporting requirements) are currently envisaged to apply to "computer systems", not just CCSs. It is unclear whether this is meant to apply more expansively beyond CCSs, e.g., like in Singapore, where the amended Cybersecurity Act[8] will also require Critical Information Infrastructure Operators (CIIOs) to report incidents that affect other computer systems under the control of the CIIO even if the computer systems are not interconnected with and do not communicate with the Critical Information Infrastructure (CII).

The Proposed Framework seeks to designate as CCSs only computer systems that are relevant to the provision of essential services or the core functions of computer systems, and those systems, which if interrupted or damage, will seriously impact the normal functioning of the CIs. The focus is more on IT computer systems but the provision of essential services go beyond such systems, for example, the infrastructure of utility and mass transit companies invariably involves operational technology (OT) (which is different to IT). The provision of, say, electricity is undoubtedly an essential service, and the legislation will certainly apply to computer systems that manage, control and monitor physical industrial operations, however delineating which systems within the OT environment is not so straight forward. That said, the separation between IT and OT systems is changing due to the progression of the technological landscape. There is increasing IT and OT convergence especially with the proliferation of the Internet of Things and data analytics.

3. SUBMISSIONS SUBJECT TO REVIEW AND APPROVAL?

It is unclear whether the obligation of CIOs to submit their emergency response plans will be subject to a review and approval process from the Commissioner's Office, or if it is just a log of the relevant emergency response plans. Whether these plans are subject to the Commissioner's review will no doubt impact compliance and administrative costs, and the time to be taken by CIOs to achieve compliance.

Likewise, given that the Proposed Framework will apply to all CCSs, including those located outside Hong Kong,[9] it is unclear whether the use of such CCSs will be subject to any potential approval or review processes by the Commissioner's Office.

FURTHER OBSERVATIONS

Other than the unresolved questions raised by the Paper, organisations in the Designated Sectors should also bear in mind the following:

1. The application of the Proposed Framework to all CCSs, including those outside Hong Kong, as well as their obligation to provide relevant information to the Commissioner's Office, even if the information is located outside Hong Kong, means that organisations will need to cater for such obligations in their agreements with third-party service providers.

2. Even though the Proposed Framework adopts an organisation-focused approach, and the Paper places emphasis on the regulation of the computer systems rather than the information contained within, the importance of the data held is still a material consideration since this is one of the factors that the Commissioner's Office will take into account when designating CIOs and CCSs.

3. The emphasis placed on organisational and preventive obligations under the Proposed Framework will elevate the importance of robust information security within CIOs. The magnitude of this undertaking should not be underestimated or confined to CCSs, since sophisticated threat actors often leverage weak links in an organisation's security measures to infiltrate their environment before moving laterally to compromise the organisation's systems. In light of these requirements, the role of the chief information officer and chief information security officer will likely be mission critical in ensuring compliance with the proposed legislation.

4. All of this, coupled with the annual assessments imposed on CIOs, means an increase in business costs – a necessary "evil" that organisations should not try to economise on. Any company that has been through a cyberattack knows that "prevention is better than cure" and that the business and financial costs of "cleaning up" tend to far outweigh the costs of ensuring compliance from the outset.

5. The incident reporting timeline under the Proposed Framework for serious computer system security incidents that have a "*major impact on the continuity of essential services and normal operating of CIs or lead to a large-scale leakage of personal information and other data*" is extremely short – a mere 2 hours. Even the reporting timeline for "other" computer system security incidents – 24 hours – is relatively short compared to data breach reporting obligations around the world, such as 72 hours after becoming aware of the breach under the European Union's General Data Protection Regulation, or three calendar days under Singapore's Personal Data Protection Act. Accordingly, the ability of organisations to comply with the reporting timelines will hinge greatly on the sensitivity of the reporting threshold, e.g., when would an incident be deemed to have led to a large-scale leakage of personal information, and when would a CIO be deemed to have become aware of this incident? The Paper recognises that "becoming aware" requires a reasonable degree of certainty that a computer security event has caused harm to the confidentiality, integrity, or availability of a CCS, or has compromised operations. It also recognises that a short period of investigation may fall short of establishing this "awareness". Given the manner in which cybersecurity investigations tend to unfold, an organisation may become aware of an intrusion into their system, but may not necessarily be able to establish the magnitude of the event for a significant period of time. We expect that further clarification on the triggers for this reporting requirement will be developed under the Code of Practice to ensure that companies are given the tools to filter unnecessary notifications.

6. Moreover, the incident reporting obligation under the Proposed Framework will apply independently of any other parallel reporting obligation(s) that the CIOs may have, which includes requirements under existing regulatory regimes[10] *and* mandatory breach notification obligation that may be introduced in the Personal Data (Privacy) Ordinance in the future. Practically speaking, this means that certain

organisations may need to perform multiple assessments and make two or even three notifications to different regulators arising from a single event, which makes it even more important that they ensure they have processes in place to address each regulator's assessments and the concurrent reporting obligations.

7. The Proposed Framework aims to protect the security of CCS, and this also includes physical security. CIOs, especially in sectors where the CCSs may be exposed to risks of physical damage, are reminded that the computer system security management plan should also cover measures to ensure the physical security of CCSs and that the relevant data centres or computer rooms are located in a comprehensively protected environment.

Notably, the government has opted not to propose criminal or personal liability under the Proposed Framework after considering the impact of the proposed legislation on CIOs and the need to ensure sufficient deterrent effect, opting instead for financial penalties of up to HK$5 million.

The penalties are stated to be "*in line with the relevant legislation of the UK and EU*". Given that the penalty for non-compliance with the Network and Information Systems Regulations in the UK is up to £17.5 million (~HKD 170 million) and that the penalties under the amended Cybersecurity Act in Singapore have been revised upwards to the **higher of** SGD 500,000 (~HKD 2.9 million) or 10% of a company's annual turnover in Singapore, it is possible that the proposed fines will be revised upwards when the actual bill is put before the Legislative Council.

CONCLUSION

The government has indicated its intention to consult further with stakeholders in the relevant sectors on the Proposed Framework. Given the uncertainty introduced by some of the proposals, organisations in the Designated Sectors should ensure that they take the opportunity to share their views and seek clarification during this further consultation period.

---

[1] See the Privacy Commissioner's Office Report on its Work in 2023: https://www.pcpd.org.hk/english/news_events/media_statements/press_20240129.html

[2] There are currently no statutory requirements on the protection of the computer systems of CIs in Hong Kong.

[3] A CIO is defined in the Paper as an operator of a Critical Infrastructure (CI). A CI is a facility that is "*necessary for the maintenance of normal functioning of Hong Kong society and the normal life of people*". CIs may fall within either of two categories: (1) Infrastructure in eight specified sectors that are needed for the delivery essential services in Hong Kong; or (2) Other Infrastructure for maintaining important societal and economic activities.

[4] A CCS is defined in the Paper as a computer system that is "*relevant to the provision of essential service or core functions of computer systems, and those systems which, if interrupted or damaged, will seriously impact the normal functioning of the CIs.*"

[5] The proposed COP also contemplates the submission of a subsequent written report within 14 days.

[6] This preliminary submission only contemplates the submission of the name of the CII affected, name and contact number of the CIIO, the nature of the cybersecurity incident, when and how it occurred, the resulting effect observed, and details of the individual submitting the notification. The Cybersecurity (CII) Regulations also specifically contemplate the submission of a supplementary report within 14 days and set out the types

of prescribed incidents to be reported, which include unauthorised hacking to gain unauthorised access, installation of execution of unauthorised software, man-in the-middle attack session hijacks, or denial of service attacks.

[7] Under the *Draft* Cybersecurity Incident Reporting Measures, in addition to the initial report, CIO operators are required to submit a supplementary report within 24 hours; and provide a summary report to authorities within five working days.

[8] Singapore's Cybersecurity (Amendment) Bill was passed in Parliament on 7 May 2024.

[9] This parallels the extension of Singapore's Cybersecurity Act to computers or computer systems wholly outside Singapore and highlights an expanded recognition of critical infrastructure not just comprising hardware and physical systems but also virtualised computers and systems.

[10] For example, reporting requirements for Securities and Futures Commission-licensed corporations under the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission.

AUTHORS

PARTNER

GABRIELA KENNEDY

HONG KONG +852 2843 2380

GABRIELA.KENNEDY@MAYERBROWN.COM

ASSOCIATE

KEN TSZ LOK LAM

HONG KONG +852 2843 4458

TSZLOK.LAM@MAYERBROWN.COM

PARTNER

TOW LU LIM

HONG KONG +852 2843 4490

TL.LIM@MAYERBROWN.COM

REGISTERED FOREIGN LAWYER, (SINGAPORE)

JOSHUA T. K. WOO

HONG KONG +852 2843 4431

JOSHUA.WOO@MAYERBROWN.COM