SEPTEMBER 2024

MOORE NEWSLETTER

Hong Kong's New Critical Infrastructure Cybersecurity Law

INTRODUCTION

Hong Kong's government has introduced the Protection of Critical Infrastructure (Computer System) Bill, a significant legislative measure aimed at enhancing the cybersecurity of critical infrastructure. This proposed law seeks to establish a regulatory framework for critical computer systems (CCSs) operated by designated critical infrastructure operators (CIOs), addressing the urgent need for improved cybersecurity among rising global threats.

The legislation empowers a newly created Commissioner's Office to enforce compliance and impose specific obligations on CIOs, shifting from voluntary measures to mandatory regulations. While this initiative aims to strengthen the security of essential services in Hong Kong, it also raises important questions regarding the designation of CIOs, the scope of critical infrastructure, and the implications for businesses regarding compliance costs and vendor oversight.

KEY COMPONENTS/ KEY ELEMENTS OF THE PROPOSED LEGISLATION

I. SCOPE AND TARGETS

Regulatory framework

- The legislation will apply exclusively to CIOs designated by a newly established Commissioner's Office within the Security Bureau. The specific list of designated CIOs will remain confidential, though the sectors they belong to will be publicly identified.
- The focus of the law is on CCSs, which are defined as systems necessary for the provision of essential services. Only these designated CCSs will be subject to regulatory oversight. Other computer systems operated by CIOs that are not classified as CCSs will not fall under the law's purview.

Investigative powers

The Commissioner's Office will have the authority to investigate security incidents affecting CCSs. This includes powers to:

- request information from CIOs;
- mandate remedial actions; and
- enter premises with a court warrant for investigations related to security incidents and compliance with the law.

This new legislative framework is intended to bolster the cybersecurity posture of Hong Kong's critical infrastructure amidst rising global cyber threats, ensuring that essential services remain resilient against potential cyberattacks.

Definition of Critical Infrastructure

Critical Infrastructure (CI) is categorised into two main groups:

1. Essential services – This includes infrastructures vital for the continuous delivery of essential services. Disruption of these services could significantly impact daily life in Hong Kong. Key sectors include:

   - Energy
   - Information technology
   - Banking and financial services
   - Land transport
   - Air transport
   - Maritime
   - Healthcare services
   - Communications and broadcasting

2. Other important societal and economic activities – This encompasses infrastructures that, while not essential services, are crucial for maintaining significant societal and economic functions. Examples include major sports venues, performance spaces, and research and development parks.

II. OBLIGATIONS FOR CIOs

The proposed Protection of Critical Infrastructure (Computer System) Bill in Hong Kong outlines specific obligations for CIOs categorised into three main areas: organisational, preventive, and incident reporting and response.

Organisational obligations

CIOs are required to:

- **Maintain a local presence**: Provide an address and office in Hong Kong for official communications.
- **Report ownership changes**: Notify the Commissioner's Office of any changes in ownership or control of the critical infrastructure.
- **Establish a security management unit**: Set up a dedicated unit with professional expertise in cybersecurity, which can be either in-house or outsourced, supervised by a designated individual.

Preventive obligations

CIOs must implement proactive measures to safeguard their systems:

- **Notify material changes**: Inform the Commissioner's Office about significant modifications to their CCSs regarding design, configuration, or security.
- **Develop a security management plan:** Formulate and execute a comprehensive computer system security management plan, which must be submitted to the Commissioner's Office.
- **Conduct risk assessment**: Perform annual security risk assessments of their CCSs and submit the findings to the Commissioner's Office.
- **Independent audits**: Carry out independent security audits every two years and provide the audit reports to the Commissioner's Office.
- **Vendor compliance**: Ensure that any third-party service providers comply with the relevant statutory obligations, maintaining oversight over their security practices.

Incident reporting and response obligations

CIOs are mandated to report and respond to security incidents effectively:

- **Participate in drills**: Engage in cybersecurity drills organised by the Commissioner's Office at least once every two years to test their response capabilities.
- **Emergency response plan**: Develop and submit an emergency response plan to the Commissioner's Office.

- **Incident notification**: Report security incidents to the Commissioner's Office within specified timeframes:
  - Serious incidents: Within 2 hours of becoming aware of incidents that could significantly impact essential services or lead to large-scale data leaks.
  - Other incidents: Within 24 hours of awareness.
- **Follow-up reporting**: If the Initial report is made via phone or text, a written report must be submitted within 48 hours.

CIOs must also be prepared to provide any requested information to the Commissioner's Office during investigations, even if that information is located outside Hong Kong. This comprehensive framework aims to enhance the cybersecurity posture of critical infrastructure in Hong Kong, ensuring that CIOs are equipped to manage risks and respond effectively to incidents.

III. ENFORCEMENT AND PENALTIES

Enforcement mechanism

- **Commissioner's Office**: A new Commissioner's Office will be established under the Security Bureau to oversee the enforcement of the law. This office will have significant investigative powers, including:
  - Information requests: The ability to request information from CIOs regarding their compliance with the law.
  - Remedial actions: Authority to mandate remedial measures to address identified cybersecurity issues.
  - Premises access: The capability to enter premises with a court warrant to conduct investigations related to security incidents or compliance checks.
- **Collaboration with sector regulators**: The Commissioner's Office will work alongside existing sector regulators (e.g. the Hong Kong Monetary Authority and the Communications Authority) to monitor compliance and enforce obligations, particularly for sectors already under comprehensive regulation.

Penalties for non-compliance

The bill proposes several penalties for CIOs who fail to meet their statutory obligations:

1. **Financial penalties**:
   - Organisations that do not comply with the law may face fines ranging from HK$500,000 to HK$5 million, depending on the severity of the violation.
   - Daily fines may be imposed for ongoing non-compliance.

2. **Offences**: Specific offences under the proposed legislation include:
   - Non-compliance with statutory obligations set forth in the law.
   - Failure to adhere to written directions issued by the Commissioner's Office.

3. **Investigative authority**: The Commissioner's Office can investigate incidents affecting CCSs and enforce compliance, ensuring that CIOs are held accountable for their cybersecurity practices.

UNRESOLVED QUESTIONS

1. **Insufficiency in the current regime:** What specific insufficiencies in the existing cybersecurity measures necessitate the introduction of this new legislative framework? Stakeholders are questioning the rationale behind transitioning from voluntary measures to mandatory compliance.
2. **Centralised vs. Sectoral regulation**: Why is a centralised regulatory approach regarded as more effective than the existing sectoral regime? The implications of this shift on various sectors and their existing regulatory frameworks need clarification.
3. **Designation of CIOs**: How will the Commissioner's Office determine which organisations qualify as Critical Infrastructure Operators (CIOs)? The lack of transparency regarding the designation process raises concerns about potential unpredictable decisions.
4. **Scope of critical infrastructure**: Will social media and messaging platforms be classified as essential services? The ambiguity surrounding the definition of critical infrastructure could lead to confusion about which organisations fall under the law's purview.
5. **Overlap with privacy regulations**: How will the new law interact with existing privacy regulations, particularly those governed by the Privacy Commissioner for Personal Data (PCPD)? The potential for overlapping jurisdictions may create confusion regarding incident reporting and compliance responsibilities.

KEY CONSIDERATIONS

1. **Operational technology (OT) coverage**: The proposed law primarily focuses on IT systems, raising concerns about the exclusion of OT systems. Given that many critical services rely on OT, this hap could leave significant vulnerabilities unaddressed.
2. **Vendor oversight**: CIOs will be held accountable for compliance failures by third-party service providers. Organisations must evaluate their vendor management practices to ensure compliance and mitigate risks associated with outsourcing.
3. **Implementation costs**: The financial burden of compliance, including the establishment of security management units and regular audits, may strain resources for smaller organisations. Stakeholders need to consider how to balance regulatory compliance with operational viability.
4. **Incident Reporting timelines**: The short reporting timelines for incidents (within 2 hours for serious incidents and 24 hours for others) may impose significant operational pressures on CIOs. Organisations must prepare to respond swiftly to meet these obligations.
5. **Public awareness and preparedness**: There is a need for increased public awareness and preparedness regarding the implications of the new law. Organisations should proactively assess their status as CIOs and prepare for the upcoming compliance requirements.
6. **International standards and comparisons**: The proposed legislation is being developed in the context of international standards and practices. Stakeholders should consider how the law aligns with similar legislation in other jurisdictions, such as those in mainland China, Singapore, and Australia.

CONCLUSION

As Hong Kong prepares to implement this law, it is crucial for organisations to assess their potential status as CIOs and to strengthen their cybersecurity measures accordingly. The successful enactment of this legislation will not only bolster the resilience of critical infrastructure but also reinforce Hong Kong's position as a secure global financial hub in an increasingly interconnected world. Ongoing dialogue and collaboration among stakeholders will be essential to address the challenges and ensure that the law effectively meets its objectives while remaining practical for businesses to implement.

REFERENCES

Paper submitted to the Legislative Council by the Security Bureau:
https://www.legco.gov.hk/yr2024/english/panels/se/papers/se20240702cb2-930-3-e.pdf

Moore IT & Cybersecurity Services

Why work with us?

We are a global advisory network, with offices and member firms across the globe. Backed by our international network, we provide clients with comprehensive cybersecurity solutions and expertise from security vulnerability assessment to system penetration testing to protect them from modern cyber threats.

Our team is composed of professionals with practical and solid knowledge and experience. They are certified holders or members of professional bodies such as CISA, CISM, CRISC, CISSP, CIPP(A), CEH, OSCP and GPEN.

Our clients range from SMEs to listed companies from a wide variety of industry, and public sectors including government bureaus and authorities. Through our extensive sector knowledge, we provide comprehensive advice to suit each client's goals.

To find out more, please contact one of our experts below:

PATRICK ROZARIO
Managing Director
T +852 2738 7769
E patrickrozario@moore.hk

KEVIN LAU
Principal
T +852 2738 4631
E kevinlau@moore.hk