FEBRUARY 20, 2026

www.alpacian.com

ALPACIAN

NEWSLETTER

Image Source: Deloitte

The Critical Infrastucture Bill: Why Should We Care

Written By : Chu Wai Lam @Alpacian

Welcome to the inaugural issue of our newsletter, where we aim to enlighten our readers about the ever-changing landscape of technology, cybersecurity, and digital safety.

Today, we will briefly talk about the Protection of Critical Infrastructures (Computer Systems) Ordinance (Cap. 653) and why we should care.

Monthly Cybersecurity Tips:

- Always lock your phone, tablet, and computer when not in use.
- Consider using a password manager to store all your passwords safely.
- Adjust privacy settings on social media to limit what the public can see online.

The Latest News in Cyber Security

The prevalence of cybersecurity incidents around the world is nothing to scoff at. This month, we have selected the following news articles that we deemed worthy of your attention. Stay informed, and stay protected.

Terra Holdings Data Breach

Recently, Terra Holdings, a property management firm based in New York, reported to the Attorney General of Vermont that it had experienced a data breach in which sensitive personal identifiable information in its care may have been compromised. The breach was said to have happened in February last year, potentially compromising names, Social Security numbers, driver's licenses, and financial accounts.

Strauss Borrelli

Ransomware Attack Strikes Hotel

Washington Hotel, a well-known chain across Japan, confirmed a ransomware attack on February 13, 2026, that hit several of its servers. The breach started around 10:00 PM when the IT team spotted unauthorised access. They acted fast by cutting off external network links to stop the spread. The quick shutdown limited damage, a key lesson for others. Companies should test incident plans often and watch networks with tools like intrusion detection.

Cyber Press

Akira Strikes Again

Community Property Management, based in the US, has fallen victim to a ransomware attack conducted by Akira. The attack, discovered on February 2, 2026, resulted in the theft of 67GB of data, including tenant records and operational files. The breach disrupted services, potentially exposing personal information like addresses, payment details, and contracts.

Hook Phish

The Critical Infrastucture Bill: Why Should We Care

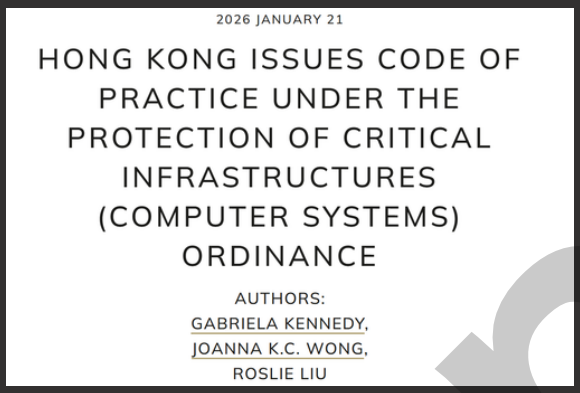
As cyberattacks continue to emerge, the essential services of cities and countries are prone to becoming targets. As such, HK has taken a proactive step and enacted the city's first dedicated cybersecurity law.

What is it about?

The Protection of Critical Infrastructures (Computer Systems) Ordinance (PCICSO) focuses on protecting the computer systems of critical infrastructures (CIs) from cyber threats, ensuring their secure operation to prevent disruptions. In essence, CIs are defined as facilities and systems essential for maintaining Hong Kong's normal societal operations falling within the eight key sectors: energy, information technology, banking and financial services, air transport, land transport, maritime transport, healthcare services, and telecommunications and broadcasting. Additionally, it also covers critical societal or economic activities, such as major sports and performance venues or research and development parks.

Under the law, designated Critical Infrastructure Operators (CIOs) must comply with statutory obligations categorised into three areas: organisational measures (establishing security management plans), preventive actions (risk assessments and regular audits), and incident response and recovery (mandatory reporting of security incidents to the authorities).

Image Source: Communication Authority



Mayer Brown

A Code of Practice, issued on the same day the ordinance took effect, provides detailed guidance to help CIOs meet these requirements, setting a baseline for compliance across sectors. Enforcement includes penalties at the organisational level for non-compliance, emphasising accountability without targeting individual employees.

Why is it established?

In our modern age, technology is so intricately woven into our everyday lives that it's safe to say it has become essential. As such, drawing inspiration from international standards and regulations in other regions, Hong Kong decided to make use of legislation to strengthen the city's overall cybersecurity resilience, reducing the risk of critical services being compromised.

Why should we care?

Although the ordinance mainly targets CIOs and their services, they serve as the backbone of society. By enforcing strong security measures, the law ensures that these essential services remain reliable and resilient, ultimately benefiting residents by lowering the chances of extensive disruptions due to cyberattacks. In a highly interconnected city like Hong Kong, this ordinance is not merely about corporate compliance; it is about safeguarding the stability and security that support daily life and long-term prosperity.