

PANORAMIC NEXT

Privacy & Cybersecurity

HONG KONG

 LEXOLOGY



Privacy & Cybersecurity

2024

Cybersecurity continues to represent a growing risk for companies around the world, with cyberthreats posed by nation states, commercial competitors, company insiders, transnational organised crime and 'hacktivists' continuing to grow on a global basis.

Generated: July 16, 2024

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. Copyright 2006 - 2024 Law Business Research

 LEXOLOGY

Explore on Lexology 

Hong Kong

[Cecilia Tsang](#), [Michelle Ta](#), [Jingyuan Shi](#)

[Simmons & Simmons](#)

Summary

PROFILES

About the lawyers

Q&A

What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

THE INSIDE TRACK

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

How is the privacy landscape changing in your jurisdiction?

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

Profiles

ABOUT THE LAWYERS

Michelle Ta at Simmons & Simmons has a breadth of experience across technology transactions, IT outsourcing, software and IP licensing, and privacy and data protection, and she has also made achievements in the field of financial technology. She has provided a series of data-related consulting services for virtual banks and fintech clients, and is currently seconded part-time to a virtual bank in Hong Kong to provide long-term legal support. Michelle is also an experienced cybersecurity legal adviser, and has acted in-house for a global IT services giant as the company's cybersecurity subject matter expert. Clients have described Michelle as 'one of the few lawyers I would call having the full package', 'a lawyer to watch out for in the TMT sector' and having 'excellent technical skills and great commercial judgment across banking, technology and corporate practice'. Michelle is dual-qualified in Hong Kong SAR and Victoria, Australia. She graduated from the University of Melbourne with first class honours in law and holds a second bachelor's degree in science, with double majors in biochemistry and biotechnology.

Q&A

WHAT WERE THE KEY REGULATORY DEVELOPMENTS IN YOUR JURISDICTION OVER THE PAST YEAR CONCERNING CYBERSECURITY STANDARDS?

Hong Kong does not have a dedicated cybersecurity statute or mandated cybersecurity standards.

Instead, there are provisions governing cybersecurity and cybercrime in various pieces of legislation such as the Crimes Ordinance, the Telecommunications Ordinance, the Theft Ordinance, the Control of Obscene and Indecent Articles Ordinance and the Prevention of Child Pornography Ordinance.

The Hong Kong government announced plans to implement a new cybersecurity law to help ensure the security of Hong Kong's network information systems at a macro level in October 2021. In July 2022, the Cybercrime Sub-committee of the Law Reform Commission (LRC) published a consultation paper on Cyber-Dependent Crimes and Jurisdictional Issues, which sets out the preliminary proposals for law reform to address Hong Kong's challenges to cybercrime, uphold cybersecurity and safeguard national security. In considering these proposals, the LRC closely reviewed the cybersecurity standards adopted in other jurisdictions, including Australia, Canada, England and Wales, Mainland China, New Zealand, Singapore and the United States. The five cyber-dependent crimes (ie, crimes that can be committed only through the use of information and communications technology devices, where devices are both the tool and target of the crime) addressed include: (1) illegal access to program or data; (2) illegal interception of computer data; (3) illegal interference of computer data; (4) illegal interference of computer system; and (5) knowingly making available or possessing a device or data for the purpose of committing a crime. The LRC suggested that the borderless nature of cybercrime would justify the extraterritorial application of Hong Kong law and that Hong Kong courts should have jurisdiction in cases where connections with Hong Kong exist (such as where the

perpetrator's act has caused or may cause serious damage to Hong Kong). The LRC also recommended increased penalties and possible life imprisonment for aggravated offences (such as illegal interference with computer data or computer system).

As part of the consultation, the LRC sought responses mainly on the scope of exemptions and defences to the new proposed offences. The consultation period ended in October 2022, and the LRC has yet to publish the consultation conclusions as at June 2024. This is the first of three consultation papers to be published by the LRC. The second paper will focus on cyber-enabled crimes and the macro challenges in the digital age (including data sovereignty), whereas the third paper will address evidentiary and enforcement-related matters. We expect the remaining consultation papers to be published soon and further discussions to follow regarding the proposed regime.

The Constitutional and Mainland Affairs Bureau of the Hong Kong Government's discussion paper on the review of the Personal Data (Privacy) Ordinance (PDPO), while issued some time ago in January 2020, remains noteworthy as it remains on the public radar for upcoming development in this space. The proposed amendments included are as follows: (1) introducing a mandatory data breach notification requirement (as further discussed under the following question); (2) introducing requirements to specify a retention period of personal data collected, which must be clearly communicated to data subjects via privacy policies; (3) imposing stricter sanctions (such as pegging penalties to the data user's global annual turnover) and empowering the Privacy Commissioner for Personal Data (the Privacy Commissioner) with the ability to impose administrative fines directly in the event of a breach; (4) direct regulation of data processors (such as making data processors directly accountable for breaches); (5) expanding the definition of 'personal data'; and (6) implementing measures to combat doxxing. Among the proposed amendments, as of June 2024, only anti-doxxing measures have been implemented, while the other proposed amendments to the PDPO are still under consideration.

On a related note, if a person commits a doxxing offence under the PDPO against specified personnel (including, for example, a person who handles or is responsible for cases concerning safeguarding national security), the person may also be liable under the Safeguarding National Security Ordinance.

There continues to be in place a variety of sector-specific requirements for regulated businesses, and cybersecurity continues to be an area of intense focus for financial regulators such as the Hong Kong Securities and Futures Commission (SFC) and Hong Kong Monetary Authority (HKMA). Recent efforts include the HKMA's upgraded Cybersecurity Fortification Initiative (CFI 2.0) and the SFC's thematic cybersecurity review of internet brokerages and further guidance on managing the cybersecurity risks of remote working, among others.

Albeit not legally binding, the Privacy Commissioner has also issued a number of new guidance notes to assist companies in uplifting their cybersecurity measures.

The Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data was issued May 2022, in which two new sets of recommended model contractual clauses (RMCs) were introduced, namely data-user-to-data-user RMCs and data-user-to-data-processor RMCs. The data-user-to-data-user RMCs set out model clauses for data transfers between two data users (or data controllers) and are aimed at ensuring that a transferor takes all reasonable precautions to ensure that personal data

transferred to a transferee acting in the capacity as a data user is not processed in a manner that would violate the PDPO. The data-user-to-data-processor RMCs sets out model clauses reflecting the PDPO requirement that a data user remains accountable for the acts of its data processors and imposes contractual obligations to oblige data processor transferees to comply with the requirements of the PDPO. The RMCs are recommended by the Privacy Commissioner to be incorporated in agreements where personal data may be transferred outside Hong Kong by a local entity to an overseas entity, or between two entities outside Hong Kong where the transfer is controlled by a data user that is subject to the PDPO.

In reality, the RMCs are difficult to implement and are likely to be resisted by data processors, because they comprise certain obligations that lie beyond the control of data processors, such as requiring the transferee to ensure personal data transferred is adequate but not excessive. The actual law itself has not changed (and in particular, the relevant section of the PDPO (section 33) restricting cross-border transfer of data is still yet to come into effect). In February 2023, members of the Legislative Council expressed grave concerns about the slow progress of bringing section 33 of the PDPO into operation; however, no timetable has been announced for its implementation thus far.

Adoption of the RMCs is not mandatory. Organisations are also free to adapt and modify the RMCs or use alternative wording as long as they are consistent with PDPO requirements. As such, the RMCs are likely to be negotiated heavily by both data users and data processors, and we have not seen the same level of widespread use as that seen, for example, with the standard contractual clauses under the General Data Protection Regulation (GDPR) in Europe.

Another recent guidance from the Privacy Commissioner includes the Guidance Note on Data Security Measures for Information and Communications Technology issued in August 2022, which aims to provide data users with recommended data security measures for the ICT industry to facilitate their compliance with the relevant requirements under the PDPO and pointers towards good practices in strengthening their data security systems.

WHEN DO DATA BREACHES REQUIRE NOTICE TO REGULATORS OR CONSUMERS, AND WHAT ARE THE KEY FACTORS THAT ORGANISATIONS MUST ASSESS WHEN DECIDING WHETHER TO NOTIFY REGULATORS OR CONSUMERS?

There is currently no general mandatory data breach reporting regime in Hong Kong. Nonetheless, reporting of data breaches is encouraged by the Privacy Commissioner. In this regard, the Privacy Commissioner revised its Guidance on Data Breach Handling and Data Breach Notifications (despite being non-legally binding guidelines) in June 2023, which provides data users with suggested practical steps to take in handling data breaches in order to mitigate the loss and damage caused to those involved. The latest revision to the Guidance recommends companies adopt a comprehensive data breach response plan by setting out the specific procedures to be followed in the event of a data breach, including the data user's strategy for identifying, containing, assessing and managing the impact brought about by the incident from start to finish. Additionally, the guidance recommends that data users should notify the Privacy Commissioner and the affected data subjects as soon as practicable, after becoming aware of the data breach, especially if the breach is likely to result in a real risk of harm to the affected data subjects.

As a matter of practice, we see clients take a range of approaches to voluntary reporting (whether that is reporting to the regulator or affected consumers). Usually the factors that clients weigh up include whether the data breach might have to be reported on a mandatory basis in another jurisdiction (in which case, clients tend to lean to voluntary reporting in other affected jurisdictions); the size of the data breach; and the risk of harm to affected individuals. Factors such as negative public perception and financial consequences are also important considerations.

That said, since the start of 2020, the Hong Kong government has been discussing a range of changes to Hong Kong privacy laws, including introducing a mandatory data breach notification regime (as discussed above, in the first question). While we are yet to see legislative progress regarding a mandatory data breach notification regime, we expect this to stay high on the agenda in Hong Kong and that it may become law in the not-too-distant future.

Of course, for regulated businesses – and in particular, those subject to the supervision of financial regulators – there continue to be sector-specific regulatory expectations to report data incidents within certain time frames.

WHAT ARE THE BIGGEST ISSUES THAT COMPANIES MUST ADDRESS FROM A PRIVACY PERSPECTIVE WHEN THEY SUFFER A DATA SECURITY INCIDENT?

The biggest issues that companies need to consider from a privacy perspective arise even before companies suffer a data security incident.

First of all, data security (and privacy protection in particular) should be board-level issues. Too often, they are considered the sole domain of certain stakeholders (the chief information Security officer, a data protection officer or another ‘tech’ or ‘legal’ person) – so the first issue that companies need to address from a privacy perspective is an understanding that this is an enterprise-wide responsibility.

Dealing well with a data security incident starts from prevention in the first place, followed by good preparation for the worst-case scenario. The companies that do this best have a multidisciplinary team (stakeholders from senior management through to lawyers, public and government relations experts, cyber forensics professionals) that have been trained and drilled for cyber incident simulations so that they can mobilise quickly to respond to a data security incident when it (inevitably) occurs. Those companies know what steps they need to take and the order in which they need to take those steps – from initial containment of a data breach, through to ensuring key evidence is collected in a way that maintains chain-of-cus-tody (particularly important so that digital evidence is not accidentally erased or changed in an effort to fix a breach), through to taking measures to fix vulnerabilities and post-mortem reviews. All of that will be important if a company is required to report an incident to a specific regulator (for example, the HKMA) or if the company decides it wants to voluntarily report the incident to the Privacy Commissioner or affected customers.

WHAT BEST PRACTICES ARE ORGANISATIONS WITHIN YOUR JURISDICTION FOLLOWING TO IMPROVE CYBERSECURITY PREPAREDNESS?

There are a range of approaches in Hong Kong to cybersecurity preparedness. Banks are among those that have the highest level of regulatory expectations when it comes

to cybersecurity preparedness and cyber resilience. In terms of best practice, regulated banks in Hong Kong must meet a minimum baseline of cybersecurity readiness, which is set out in the HKMA's Cybersecurity Fortification Initiative. This comprises three pillars: (1) the Cyber Resilience Assessment Framework, which helps banks assess their cyber risk posture and benchmark their level of defence and resilience; (2) the Professional Development Programme, which is a certification scheme for cybersecurity practitioners in the industry to boost technical capability in areas such as attack simulation testing; and (3) the Cyber Intelligence Sharing Platform, which is aimed at sharing cyberthreat intelligence to help the industry stay informed of, and prepare for, emerging hacking tactics and patterns.

The HKMA has also undertaken thematic examinations on authorised institution's management of cyber risk associated with the use of third party services and issued a circular on the observed sound practices in December 2023. Authorised institutions should adopt the sound practices as set out in circular, which include: (1) integrating third party cyber risks into the risk governance framework; (2) identifying, assessing and mitigating cyber risks throughout the third-party management life cycle; (3) assessing supply chain risks of third parties; (4) expanding cyber threat intelligence monitoring; (5) preparing for supply chain attacks; and (6) adopting the latest standard, practices and technologies.

This is consistent with common cybersecurity wisdom that cybersecurity is a patchwork of defences in an organisation's people, processes and technology.

Other sectors take a range of approaches to cybersecurity preparedness, and there remains a broad spectrum of cybersecurity maturity levels in Hong Kong.

ARE THERE SPECIAL DATA SECURITY AND PRIVACY CONCERNS THAT BUSINESSES SHOULD CONSIDER WHEN THINKING ABOUT MOVING DATA TO A CLOUD HOSTING ENVIRONMENT?

Yes – in particular organisations that are supervised by the SFC and HKMA in Hong Kong should in particular be aware of the requirements and best practice imposed by each of these regulators.

For licensed corporations regulated by the SFC, additional requirements are imposed by the SFC on the use of external electronic data storage services (like cloud hosting services) to store their data and records. The SFC issued a Circular in late 2019, and in late 2020 a set of accompanying FAQs, setting out certain requirements for licensed corporations wishing to move their data storage to a cloud hosted environment. Some of the requirements set out in this regime impose expectations that are rather unusual both from the perspective of cloud service agreements in a broader sector-agnostic context as well as when contrasted with expectations in similar sectors of other jurisdictions. This includes, for example, a requirement to maintain a full and immutable audit trail to memorialise access logs by every unique user of a data record.

Authorised institutions regulated by the HKMA should be aware of the Guidance on Cloud Computing issued by the HKMA in August 2022, which addresses the increased cyber risks that come into play as authorised institutions begin to deploy cloud services for more important functions (and not merely for basic and non-core operations only) over recent years. Authorised institutions are recommended to put in place an effective governance framework and carry out proper due diligence of the cloud service provider. Ongoing risk

management and controls are recommended for the authorised institution to continually monitor and mitigate risks as necessary. Authorised institutions should also ensure that suitable arrangements are made to allow it to comply with HKMA's supervisory access and other supervisory expectations. Topping that off, authorised institutions should equip staff overseeing cloud operations with adequate knowledge and skills to securely use and manage the risks associated with cloud computing.

Outside of these requirements of the SFC and the HKMA, there are of course all the usual requirements that businesses (both regulated and non-regulated) should generally consider when thinking about moving data to an environment hosted by a third party. These include due diligence to ensure that the relevant cloud product is fit for the intended purpose, that the vendor is certified against prevailing industry cybersecurity standards, that the vendor can meet required data availability and uptime commitments and that there is a certain level of redundancy and disaster recovery to guard against data loss.

In addition, cross-border data transfer restrictions and increased exposure to mandatory government or regulatory access to cloud hosted data (and in some cases, conflict of law issues) remain important considerations when looking to move data to the cloud.

HOW IS THE GOVERNMENT IN YOUR JURISDICTION ADDRESSING SERIOUS CYBERSECURITY THREATS AND CRIMINAL ACTIVITY?

A specialist unit within the Hong Kong Police – the Cyber Security and Technology Crime Bureau – is responsible for investigating and handling technology crime, computer examinations and preventing technology crime.

In addition, as discussed in further detail above in question 1, an amendment was passed in 2021 to reform the PDPO to combat malicious doxing acts and protect the public's personal privacy. A raft of new enforcement powers were also conferred on the Privacy Commissioner to investigate and prosecute doxing crimes, as well as granting the Privacy Commissioner with the power to issue cessation notices with extraterritorial effect.

In relation to the proposed development of a local cybersecurity law, the LRC's consultation paper on Cyber-Dependent Crimes and Jurisdictional Issues in July 2022 (as discussed above under the first question) is the first of three consultation papers to introduce proposed legal reforms (of which the third paper is expected to cover enforcement-related issues). We expect to see further efforts in enhancing the cybersecurity of critical infrastructure in Hong Kong through legislation that will seek to require all private and public enterprises to comply with cybersecurity regulations.

WHEN COMPANIES CONTEMPLATE M&A DEALS, HOW SHOULD THEY FACTOR RISKS ARISING FROM PRIVACY AND DATA SECURITY ISSUES INTO THEIR DECISIONS?

All companies should be doing appropriate level of privacy and data security due diligence when looking at a potential acquisition or merger target. This involves due diligence from a legal perspective (eg, whether there have been any recent mandatory or voluntary data breaches notified to regulators, whether there have been any near misses and whether there have been any data handling complaints or litigation that may indicate a systemic issue), as well as from a technical perspective (eg, bringing in cybersecurity professionals to assess a potential target's cybersecurity posture). This is particularly important for

companies that engage in businesses that are data-intensive, businesses that interface directly with consumers or businesses that are subject to particularly strict privacy laws in other jurisdictions. A history of multiple or serious non-compliances with applicable data law spotted during the due diligence process may affect the value, terms or continuation of the deal. These risks should also factor into decisions about M&A deal shapes and ways in which sellers may be required to remain financially responsible or accept more onerous terms for latent privacy and data security issues.

The Inside Track

WHEN CHOOSING A LAWYER TO HELP WITH CYBERSECURITY, WHAT ARE THE KEY ATTRIBUTES CLIENTS SHOULD LOOK FOR?

Clients should look for curious lawyers with an in-depth understanding of technology, computers and cybersecurity as a discipline (ie, knowledge beyond the strictly legal) with a good team of litigator colleagues working alongside them to cover tricky dealings with customers or regulators. It is important to look for a team with a good working knowledge of data law across multiple jurisdictions.

WHAT ISSUES IN YOUR JURISDICTION MAKE ADVISING ON CYBERSECURITY AND PRIVACY COMPLEX OR INTERESTING?

The fact that Hong Kong data law has been around for so long (since 1995!) and remains relatively unchanged today is a very interesting contrast to the pace of change in data regulation in other parts of the world. This is particularly the case as many multinational companies have their Asia headquarters in Hong Kong, and the interplay in practice between different laws can become very complex and interesting as data itself often lives in more than one location in today's cloud-reliant business environment.

HOW IS THE PRIVACY LANDSCAPE CHANGING IN YOUR JURISDICTION?

Hong Kong's data and privacy laws definitely win the prize for longevity! They are due for a change (although I am constantly amazed at the resilience of the PDPO and how well a law drafted in 1995 still holds up and adapts so well to so many novel practical situations today).

WHAT TYPES OF CYBERSECURITY INCIDENTS SHOULD COMPANIES BE PARTICULARLY AWARE OF IN YOUR JURISDICTION?

In Hong Kong, phishing still remains one of the top tactics for bad actors to infiltrate systems. Threat actors are becoming more sophisticated and more patient and will wait longer to execute large-scale attacks, such as targeted emails to senior executives to trick them into transferring large sums from their business.



Cecilia Tsang
Michelle Ta
Jingyuan Shi

cecilia.tsang@simmons-simmons.com
michelle.ta@simmons-simmons.com
jingyuan.shi@simmons-simmons.com

Simmons & Simmons

[Read more from this firm on Lexology](#)