In-House Community **Magazine for the In-House Community** (replacing Asian-mena Counsel) Volume 1 Issue 5, 2021

iHC

In-House Community *Magazine*

COVER STORY

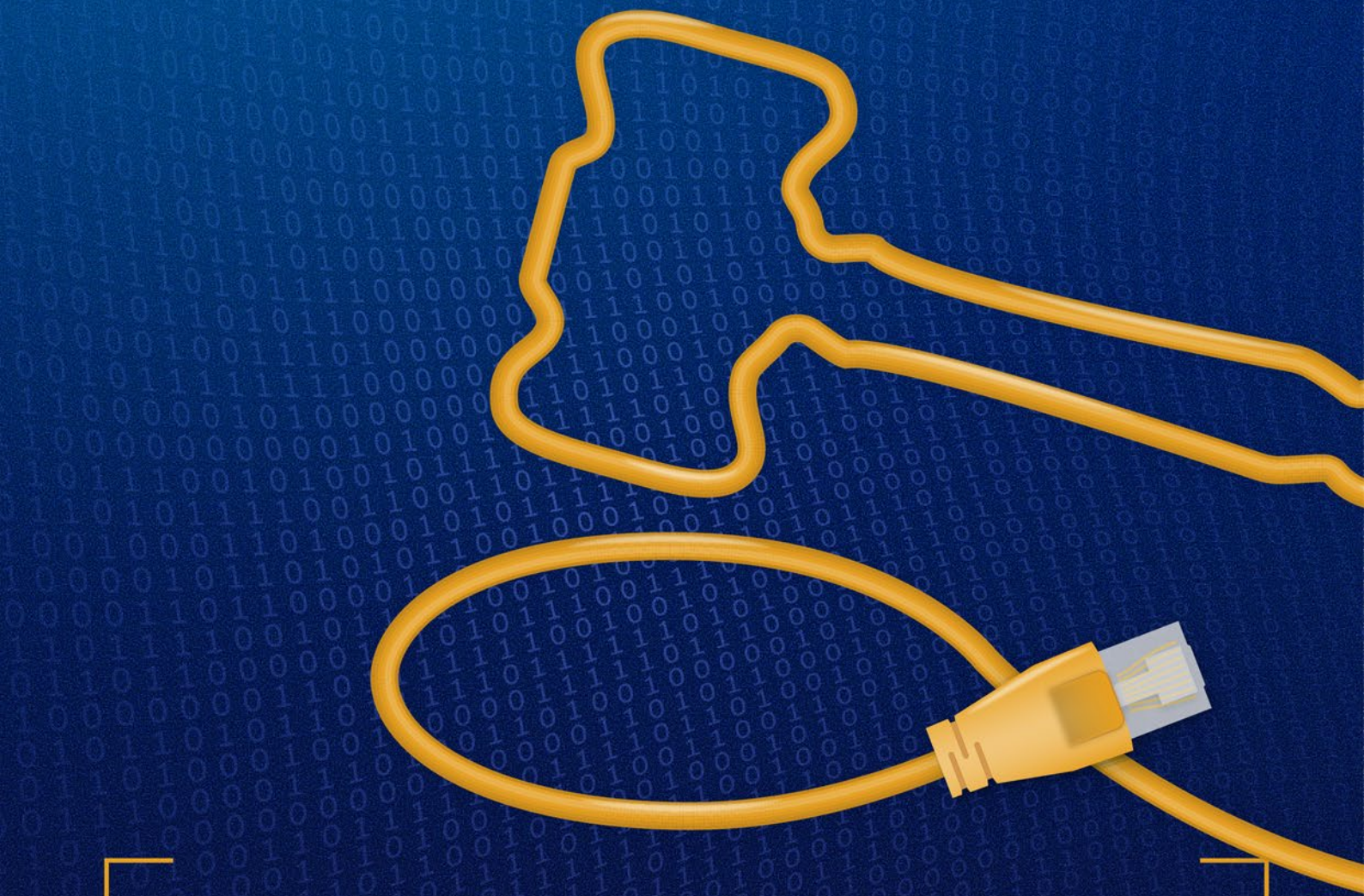
How General Counsel Can Help Prepare for Cyberattacks

IN-HOUSE INSIGHTS

In-house Insights with Maria Zarah R. Villanueva-Castro of Manila Electric Company

PHILIPPINES

Revisiting the Labor Market Test



CYBERSECURITY + DATA PROTECTION

In-House Community Magazine

PUBLISHER
Rahul Prakash
+852 8170 2951
rahul.prakash@
inhousecommunity.com

LEAD DESIGNER
Ailar Arak

EDITOR
Nathan Smith

WRITER
Butch Bacaoco

Published 10 times annually by
InHouse Community Ltd.

Publishers of
- In-House Community Magazine
- IHC Briefing

Organisers of the
- IHC Events

Hosts of
- www.inhousecommunity.com
- www.mycareerinlaw.com

Forums for the In-House Community

Opinions expressed herein do not constitute legal advice, and do not necessarily reflect the views of the publishers.

Feature contributors

Jonathan Crompton
Jonathan Crompton is a partner in RPC's Hong Kong office. He helps companies and individuals navigate complex cross-border disputes and investigations involving their Asian business, specialising in particular in financial services and technology related disputes and cyber incidents.

Keun Woo Lee
Keun Woo Lee is a partner at Yoon & Yang, specializing in intellectual property protection, privacy protection, trade secrets protection, including e-commerce and other technology, media and telecommunication areas.

Arkrapol Pichedvanichok
Arkrapol is a Senior Partner and head of the corporate and M&A practice at Chandler MHM specializing in Corporate and Mergers & Acquisitions and Capital Markets.

Chulgun Lim
Chulgun Lim is a partner at Yoon & Yang and his practice areas include disputes and litigation cases relating to personal information protection, technology, and intellectual property.

Visitsak Arunsuratpakdee
Visitsak is a Partner at Chandler MHM specializing in personal data protection, administrative law litigation and advisory, technology, media and telecommunications, mergers and acquisitions, regulatory compliance and corporate commercial matters.

Helen H. Hwang
Helen H. Hwang is a senior foreign attorney at Yoon & Yang, and her practice areas include intellectual property including patent and trademark, foreign outbound investment, and general corporate law.

Kwang-Wook Lee
Kwang-Wook Lee is a partner and a Head of firm's New Business Team at Yoon & Yang specializes in the new technology related businesses such as fintech, smart car, Internet of Things, big data, U-healthcare, and shared economy.

Le Ton Viet
Viet is a member of the Asia Data Protection & Security Practice Group of Meritas. He has a particular focus on data security, marketing and advertising practices, international data transfer and other privacy and cybersecurity matters. He counsels a broad range of clients on data privacy regulation and breach response. Additionally, he represents clients in various transactions in the field of hotel management, real estate and insurance.

In this issue

CYBERSECURITY + DATA PROTECTION

JURISDICTION UPDATES

In this issue

16

19

THE IHC BRIEFING

INDIA

IN-HOUSE INSIGHTS

IN-HOUSE DIRECTORY

Revisiting the Labor Market Test

BY NAPOLEON L. GONZALES III

It has always been Philippine policy to prioritise the welfare of Filipino workers.

Following the mandate of the Labour Code, employers may engage the services of a non-resident alien only if no Filipino is competent, able and willing to perform the service. This method of analysis, also called the *"Labour Market Test,"* is used by the Department of Labour and Employment (DOLE) whenever foreign nationals apply for an Alien Employment Permit (AEP). The AEP is a permit issued by the DOLE to foreign nationals working in the Philippines for a local company.

DOLE Department Order (DO) No. 221, series of 2021, or the *Revised Rules and Regulations for the Issuance of Employment Permits to Foreign Nationals* (the "New AEP Rules"), which took effect on 6 May, 2021, promotes the preferential use of Filipino labour, affords heightened protection to Filipino nationals and safeguards their interests by regulating the employment of foreign nationals.

Prior to the effectivity of DO No. 221-21, the Labour Market Test was satisfied once the DOLE publishes/posts the AEP application in a newspaper of general circulation, the DOLE website and the Philippine Employment Services Office job boards. The notice shall indicate that any qualified Filipino national may file an objection at the DOLE Regional Office to contest the foreign national's AEP application.

However, under the New AEP Rules, employers are required to publish the job vacancy that is intended for the foreign national at least 15 calendar days prior to filing the AEP application. The employer's publication of the job vacancy is in addition to the Labour Market Test conducted by the DOLE once the AEP application is filed. This was imposed to guarantee the priority given to Filipino nationals in terms of seeking opportunities for work.

This is similar to the practice of companies advertising their job vacancies to inform jobseekers of the need for manpower for specific positions. While the DOLE may use other forms of quad media (print, broadcast, support communications and social media) in conducting the Labour Market Test, employers should publish the job vacancy only in a newspaper of general circulation. Thereafter, a notarised affidavit stating that no applications were received, or that no Filipino applicant was considered for the position, is required to be attached to the AEP application, along with other documents.

Employers intending to apply for the renewal of their foreign employees' AEPs are not covered by the new publication requirement. However, the New AEP Rules provide that foreign nationals assigned an additional position during the validity of their current AEPs should file a new AEP application within 15 working days from their respective dates of appointment. The additional position shall require a new AEP application and should be published in a newspaper of general circulation. The rationale behind this is that the foreign national's current AEP is only valid for the position for which it was previously issued.

Another significant change of the New AEP Rules is the period to file the AEP application. Previously, AEP applications may be filed, without penalty, within 15 working days from the signing of the employment contract or appointment. Under the New AEP Rules, all applications for the issuance of AEPs shall now be filed within 10 working days after the foreign national signs his contract or after the start date. The DOLE shall impose a fine of ₱10,000 against the employer and another ₱10,000 against the foreign national for every year or a fraction thereof, for filing the AEP application beyond the prescribed period.

The New AEP Rules also sanction foreign nationals found to be working without a valid AEP, together with their employers, by barring them from applying for an AEP for five years. Those found to possess fraudulent AEPs, including their employers, shall be indefinitely barred from filing an AEP application and made to settle the applicable penalties.

Notably, the DOLE also removes foreign consultants without Philippine employers from the list of foreign nationals excluded from securing an AEP. Under the New AEP Rules, foreign consultants who work for a local employer for more than six months are now required to apply for an AEP. This is inconsistent with the fact that AEPs are only issued to foreign nationals working under an *employment arrangement* with a Philippine-based company and may be an additional variable employers should consider.

Further, to ensure that those who have been issued with AEPs are still in the Philippines working for their respective employers, the DOLE now requires employers to submit a quarterly report or an updated list of foreign nationals it has employed within 30 days of the report's reference period, along with any changes in the employer's information such as its name, address or contact details.

The objective of the New AEP Rules is to strengthen the Labour Market Test and ultimately provide the public with comprehensive guidelines on regulating the employment of foreign nationals. Towards this end, we hope the DOLE systematically implements the New AEP Rules to balance the protection of labour with the ease of doing business.

The views and opinions expressed in this article are those of the author. This article is for general information and educational purposes, and not offered as, and does not constitute, legal advice or legal opinion.

ACCRALAW®

Napoleon L. Gonzales III
nlgonzales@accralaw.com
(632) 8830-8000

Napoleon L. Gonzales III is a senior associate of the Immigration Department of the Angara Abello Concepcion Regala & Cruz Law Offices (ACCRALAW).

High Hurdles – Appointing Provisional Liquidators in the Cayman Islands

BY JEREMY LIGHTFOOT
XIA LI
YI YANG

Appointing provisional liquidators is a powerful tool, but one which often has a serious impact on the commercial operations and business reputation of a company, and so is not a step to be taken lightly. This article examines recent judicial trends in the Cayman Islands regarding the appointment of provisional liquidators, and in particular, in relation to the balance of justice that needs to be weighed as between a petitioner and the company.

The appointment of provisional liquidators by the Cayman Court is a powerful and valuable tool in the right circumstances. However, in a series of recent cases, the Court has underscored the high hurdles that must be met and emphasised that an order to appoint provisional liquidators must always be viewed as a serious step that requires a heavy and onerous evidential burden on those who seek such orders. Weighing the balance of justice between a petitioner and the company, the overriding principle is that the court should take whichever course seems likely to cause the least irremediable prejudice to one party or the other.[1]

Section 104(2) of the Cayman Islands Companies Act (2021 Revision) provides that at any time after the presentation of a winding up petition but before the making of a winding up order a creditor or contributory of a company may apply to appoint provisional liquidators where there is a *prima facie* case for making a winding up order and where such appointment is necessary to prevent the dissipation or misuse of the company's assets, or the oppression of minority shareholders, or to prevent mismanagement or misconduct on the part of the company's directors.

Doyle J in *Re ICG I*[2] summarised the statutory requirements concisely as four main hurdles for the applicants to jump over before an order can be made, being the "presentation of the winding up petition hurdle", the "standing hurdle", the "*prima-facie* case hurdle" and the "necessity hurdle". Of the four hurdles, the *prima-facie* case hurdle and the necessity hurdle are most often contested and hence considered by the Court.

In order to jump over the *prima-facie* case hurdle, previous case law suggests that whilst it is not necessary to demonstrate that a winding-up order will be granted, in the case of a creditor's petition, the threshold that the petitioner must cross ought to be nothing less than a demonstration that he is likely to obtain a winding-up order on the hearing of the petition.[3] This hurdle was most recently considered by Parker J in *Re Al Najah*. The petitioner in that case argued that there had been a justifiable loss of trust and confidence in the board due to its connection with the previous management of the company who were involved in fraud that was being investigated by the local authorities. The Court found that the fraudulent conduct of the previous directors was not attributable to the company and could not be said to be fraud in the conduct of the affairs of the company.[4] Furthermore, as there was no evidence of any on-going mismanagement at the company, the Court was not likely to conclude that it was just and equitable to wind up the company.

---

1 *Re Al Najah Education Limited* (unreported, 9 August 2021) at [34].
2 *In the Matter of ICG I* FSD 192 of 2021 (unreported, 4 August 2021) at [17].
3 *Revenue and Customs Commissioners v Rochdale Drinks* [2013] BCC 419; [2012] 1 BCLC 748 per Rimer LJ; *Re Asia Strategic Capital Fund* LP 2015 (1) CILR N-4.
4 *Re Al Najah Education* at [46].

As for the necessity hurdle, this includes showing the Court the necessity of appointing provisional liquidators to prevent dissipation of the company's assets, oppression of minority shareholders, or mismanagement or misconduct on the part of the company's directors. The threshold for establishing such a necessity has been described as a "heavy burden" that required clear or strong evidence.[5]

The test for establishing a risk of dissipation of assets was described by Segal J in *Re Asia Strategic Capital* as *"...sufficient if it is shown that the assets of the Company (or partnership) are being, or are likely to be, dissipated to the detriment of the petitioners"*.[6] It is important to note that the risk here is not dissipation in the asset freezing sense of deliberately making away with the assets but rather, any serious risk that the assets may not continue to be available to the company.[7]

As for demonstrating mismanagement or misconduct of directors, the applicant must show that there is culpable behaviour involving a breach of duty or improper behaviour involving a breach of the governing documents and governance regime.[8] In *Re ICG I*, although the judge did not doubt the evidence that the petitioner had genuine and serious concerns about the activities of the directors, he nevertheless rejected the application to appoint provisional liquidators because he found that the petitioners failed to discharge the heavy and onerous burden for satisfying the necessity hurdle.

Going forwards, creditors and contributories of a company should take heed of the Court's emphasis on the high hurdles to be met. Mere assertion or suspicion of any potential risk of dissipation, oppression, or mismanagement is unlikely to be sufficient in appointing provisional liquidators; rather applicants should prepare rigorously to discharge the substantial burden on them. Petitioners should also watch out for potential liabilities in costs in the case of a failed application. In a recent case, the Court commented:

"...I do however see the need in the case presently before me to discourage applications for the appointment of provisional liquidators which are not based on strong grounds and which are still persisted with in the face of reasonable opposition. Adverse costs orders are one way to deliver such discouragement." [9]

CAREY OLSEN

Jeremy Lightfoot
jeremy.lightfoot@careyolsen.com
+852 3628 9016

Jeremy Lightfoot is the head of Carey Olsen's litigation team in Hong Kong. He focuses on commercial and corporate litigation, insolvency and restructuring under the laws of Bermuda, the BVI and the Cayman Islands.

Xia Li
xia.li@careyolsen.com
+852 3628 9009

Xia Li is a counsel in Carey Olsen's Dispute Resolution and Litigation practice, based in Hong Kong. She has worked in multiple major legal and financial centres, including the Cayman Islands, the BVI, London, New York, Beijing, Singapore and Hong Kong.

Yi Yang
yi.yang@careyolsen.com
+852 3628 9026

Yi has a wide range of experience assisting in cross-border commercial litigation, including shareholder disputes, derivative actions, contentious insolvency and appraisal actions involving offshore companies.

[5] *Re CW Group Holdings Limited* (unreported, 3 August 2018) at [62].
[6] *Re Asia Strategic Capital Fund LP* at [45].
[7] *Re Grand State Investments* (unreported 8 April 2021) at [88]-[89].
[8] *Re Asia Strategic Capital Fund LP* at [60].
[9] *Doyle J commented in Re ICG I* FSD 192 of 2021 (unreported, 10 August 2021) at [14].

NEWS

Baker McKenzie beefs up the management of its Reinvent AI initiative


International law firm Baker McKenzie has appointed two legaltech leaders to head its artificial intelligence (AI) "Reinvent" initiative.

Brian Kuhn, former Co-Founder and Global Leader of IBM Watson Legal Consulting, and Danielle Benecke, a senior attorney at Baker McKenzie will head the 11-strong team charged with combining the firm's legal domain expertise with data science and machine learning.

Benecke is a US and global IP and technology lawyer in Baker McKenzie's IP and Technology team.

Admitted in California and Australia, she has been recognised by Fortune 500 clients in Lawyers Weekly's 30 Under 30 and in Australasian Lawyer's 50 Rising Stars. As well as being a Reinvent Ambassador, Benecke is one of Baker McKenzie's regional Reinvent Champions heling to guide other companies on their innovation journeys.

Kuhn has spent most of his career creating AI-based software offerings and AI-augmented services for lawyers.

He was vice president of Digital Strategy and Solutions at Los Angelese-based alternative legal service provider Elevate, which provides consulting, legaltech and services like ediscovery and document review to law firms and legal departments.

Kuhn also co-founded and ran the IBM Watson Legal consultancy, one of the first efforts to apply a platform strategy and rapid customisation to the design of AI-based product and consulting offerings for the legal industry.

The Baker McKenzie team will work closely with New York-based AI technology company, SparkBeyond to leverage its AI-powered advanced analytics and augmented research platforms. The two firms are aiming to use machine learning to transform the legal industry.

SparkBeyond Chief Innovation Officer Ben Allgrove said he received more than 750 applications for the roles and was "truly impressed" with the calibre of lawyers, technologists and others who applied.

"I could not have asked for a better response. We have found two people with a strong track record of successfully leading teams, collaborating across multiple jurisdictions and driving legal innovation.

"The experience they will bring will help us explore the future of machine learning enabled judgement," he said.

Baker McKenzie Global Chair Milton Cheng said the specialist, multi-disciplinary team will help the firm accelerate its Reinvent strategy.

"I look forward to seeing them take the next step in embedding machine learning in our business to create new value for our clients and our communities," he said.

The Machine Learning Venture will have a three-year runway to deliver a series of projects for clients to identify and solve problems that would most benefit from combining human judgment and machine learning.

One of the team's first projects will be the launch of "Project Liberty," an AI-driven study on the unintended negative consequences of child detention that was generated by SparkBeyond's AI engine. SparkBeyond's AI platform has mined internet data about global child detention and revealed a troubling view of cause and consequence.

Baker McKenzie plans to present these findings at the World Congress on Justice with Children in November, alongside SparkBeyond and pro bono partner Terre des Hommes.

SparkBeyond chief executive Sagie Davidovich said the company is excited to work with the two new co-founders to build the AI initiatives.

"Our work on Project Liberty is a first and major step in this direction, and we look forward to the next giant leap in leveraging AI for the greater good."

MOVES

Hadef & Partners has added **Catriona McDevitt** as partner and head of banking and finance to develop the firm's banking and finance practice in Abu Dhabi and Dubai. McDevitt has over 17 years' experience in banking and finance, gained from working at leading international law firms in the UAE and London. She is also a former Head of Legal for Wholesale Banking for one of the largest banks in the Middle East and has advised one of the region's largest oil companies. Prior to coming to the UAE, McDevitt worked in the UK and Europe at a magic circle law firm. She is an associate member of The Chartered Governance Institute (ICSA) and of the GCC Board of Directors Institute. McDevitt holds a Bachelor of Arts degree in psychology and a Bachelor of Laws degree from the University of Cape Town. She was admitted as a solicitor in England & Wales in 2005.

Goodwin has expanded its Hong Kong private investment funds team with the addition of **Phil Culhane** as a partner. Culhane previously worked at an international law firm, and is among the senior statesmen in the Asia fund formation space. He has over 30 years of experience in advising on the formation of private investment funds. He has particular expertise with representing Asia-based alternative asset managers, from start-up first time funds to established multi-strategy firms.

K&L Gates Straits Law has added **Ed Bennett** as a partner to the asset management and investment funds practice. He joins from Morgan Lewis Stamford, where he was a partner and co-leader of its Singapore investment management practice group. Bennett has extensive experience advising on direct and co-investments by funds, private equity, M&A, capital markets, secondary buyout, refinancing and fund formations. He regularly works with fund managers and institutional investors on the structuring, establishment and commitments to these funds. After relocating to Singapore from London in 2011, Bennett has focused on Southeast Asia cross-border corporate transactions and fund formations, involving investment teams in the wider Asia-Pacific region, including involvement with offshore private equity investment in Indonesia.

Phoenix Legal has added **Jatin Arora** as a partner to lead the firm's indirect tax practice out of the Mumbai office. Arora has over 22 years of experience in GST, customs, excise, service tax and VAT laws. He started his career as an independent counsel in the High Courts and various tribunals, and later worked with the Big 4 consulting firms. Arora has worked with Indian and foreign multinational companies across different sectors. He has also extensively worked on the GST regime and advised various companies on their transition to the GST regime; structured global supply chains, considering local and global trade aspects. Moreover, Arora has worked with industry associations on industry specific ramifications and advised on representations to the Government and the GST Council.

MOVES

Saraf and Partners has added **Manmeet Singh** as a partner in its Dispute Resolution – Arbitration & Litigation and Insolvency & Restructuring practices. Previously a partner in L&L Partners, Singh has 17 years of experience representing financial institutions, private equity investors and Indian conglomerates in complex and high value commercial matters across varied sectors, with a specific focus on energy and infrastructure sectors. Singh will also be part of the Management Committee, the highest decision-making body in the firm.

Stephenson Harwood has strengthened its international private wealth capabilities with the arrival of partner **Suzanne Johnston** in the firm's Singapore office. Johnston specializes in international tax and wealth planning, with a focus on advising high net worth individuals, professional trustees, family offices and private banks based in the UK and Asia. She has in-depth experience across different practice areas within private wealth, and in multiple jurisdictions across the Asia Pacific region, bolstered by having lived and worked in the region for nearly a decade. She joins from UBS.

Squire Patton Boggs has added **Ivan Chia** as a partner in its corporate practice and commodities and shipping industry group. He was previously a partner at HFW and Watson, Farley & Williams. Dual-qualified in Singapore and England, Chia is a transactional specialist with particular focus on international energy, renewables and infrastructure projects. He has advised on the development, procurement, joint venture and M&A transactions for significant projects, involving onshore and offshore wind farms, utility scale and commercial and industrial solar PV projects, ports, LNG and petrochemical plants, offshore and floating energy assets, and other infrastructure projects across Asia.

Tilleke & Gibbins has added of **Derrick Khoo** as a partner in its regional corporate/M&A team. Khoo's practice focuses on M&A, growth equity investments, pre-IPO investments, corporate real estate, FDIs, JVs and other transactions. He has represented sovereign wealth funds, private equity funds, investment banks, state-owned enterprises and other top corporations in M&A, private equity and capital markets transactions. Prior to joining the firm, he was general counsel for an international group with investments in real estate, telecommunications, F&B and other sectors, where he oversaw all legal and regulatory matters in Hong Kong, Singapore and Myanmar. Khoo is qualified as a solicitor

MOVES

of the High Court of Hong Kong SAR, an advocate and solicitor of the Supreme Court of Singapore, and a solicitor of the Senior Courts of England and Wales. Fluent in Mandarin, he will co-head the firm's China desk and serve as a key liaison with the firm's China-based clients.

Weil, Gotshal & Manges has added **Kathleen Aka** as a partner in its restructuring practice, based in the Hong Kong office. Aka joins from the Hong Kong office of another major global law firm, where she was a partner. She has extensive experience advising debtors and creditors on contentious and non-contentious restructuring and insolvency matters in the Asia-Pacific region. Aka is skilled in guiding clients through the most challenging and complex processes of financial restructuring, creditor enforcement, formal insolvency, insolvency litigation, distressed M&A, and distressed secondary debt trading. Her clients include bondholders, trustees, credit and distressed investment funds, banks, insolvency practitioners, shareholders and distressed corporations. Her industry experience covers banking and financial services, insurance and reinsurance, health, infrastructure, energy, mining and agriculture, shipping and transportation, retail and property.

Withers has continued building its litigation and international arbitration practice in Asia by adding new partner and commercial litigator **Michael Chik**. Focusing on financial and commercial disputes and regulatory matters, Chik has represented a institutional and individual clients in complex and high-value commercial transactions, trusts, shareholder's disputes, financial institution disputes and estate or probate disputes. He is also a trusted advisor to corporate clients on regulatory matters, including compliance issues in relation to the Securities and Futures Ordinance and the Listing Rules in Hong Kong. Chik also advises on highly contentious regulatory work and investigations by regulatory authorities, such as the Securities and Futures Commission and the Competition Commission, ranging from market misconduct, breach of directors' duties and precious metal price riggings. He brings experience in international arbitration under various institutional rules, including proceedings conducted under the ICC, SIAC and HKIAC rules.

ZICO Insights Law, the Singapore member firm of the ZICO Law network, has added **Hern Kuan Liu** to head its new tax practice. The new practice will provide clients with a complete service offering for Singapore law. Liu is an experienced tax lawyer in Singapore and has argued several landmark tax cases in Singapore. Liu was a tax manager in two of the Big 4 accounting firms before joining the Inland Revenue Authority of Singapore (IRAS), where he served as chief legal officer for over a decade and then headed a tax practice at a major Singapore law firm. His work primarily involves tax disputes with IRAS, though he also advises clients on domestic and international tax planning and structuring, including stamp duty relief.

Allen & Gledhill advise SPI and BCG for rooftop solar JV in Vietnam

The Vietnam office of Allen & Gledhill has acted as transaction counsel to SPI Energy Investments on a joint venture with BCG Energy to invest in rooftop solar and other renewable energy projects in Vietnam.

Allen & Gledhill managing partner Oh Hsiu-Hau and partners Tran Thi Phuong Thao and Jonathan Lin led the firm's team in the transaction.

SP Group said that it will own 49% of the joint venture (JV), while BCG Energy will own 51%. The JV will be rolled out in multiple phases with a target of 500 MW of rooftop projects by 2025.

As part of its first rooftop solar projects, the JV will work with Vinamilk, Vietnam's largest dairy production company, to install a combined 25 MW of rooftop solar power across nine factories and seven farms.

As part of the deal, SP Group will acquire a 49% stake in BCG Energy's subsidiary, Skylar, which has a rooftop solar portfolio across the country totalling 61.1MWp capacity.

BCG Energy chief executive Tuan Pham said there is strong growth potential in rooftop solar systems in Vietnam as it develops.

"We believe this will promote the use of clean energy in manufacturing companies and contribute to the sustainable growth of the economy," he said.

SP Group chief executive Stanley Huang added that the partnership is a key milestone for the company to grow its sustainability footprint in Vietnam.

"Our combined expertise and ambition in renewable and sustainable energy solutions will offer customers more options and encourage their transition to clean energy sources," he said.

The Vietnamese government's goal is to boost the nation's total capacity of power generation facilities from 69.3 GW in 2020 to 137.7 GW in 2030 and 233.8 GW in 2040.

Vietnam is planning to expand its LNG power plants to 4.1GW by 2025 and 59 GW by 2045, preparing for a spike in electricity demand. The Vietnamese government's goal is to secure 42.3GW of solar energy, 45.9 GW of wind power and 47.8 GW LNG power generation in 2040.

SPI Energy Investments is a subsidiary of SPI Group, a Singapore-based utilities and renewable energy company and provider of solar storage and electric vehicles (EV).

SPI Group maintains operations in North America, Australia, Asia and Europe and is expanding into fast-growing green industries such as battery storage, charging stations and other EVs.

BCG Energy is a wholly-owned subsidiary of Bamboo Capital Group, a Vietnam-based asset management, consulting and investment banking services company. The investment vehicle focuses primarily on three sectors – finance, energy and healthcare.

Launched in 2007, BCG Group has about US$290 million under management with a portfolio of 33 companies in over 20 countries.

Bamboo Capital JSC is listed on the Ho Chi Minh stock exchange.

Recent Key Reforms Proposed by India's Capital Markets Regulator

BY ROHAN KUMAR
SHINJNI KHARBANDA

A. REFORMS TO THE INDEPENDENT DIRECTORS' REGIME

Modern businesses face a perplexing issue – which stakeholder should perform governance and the appropriate way to bestow risks and rewards on various stakeholders? According to one school of thought, the corporate entity is a "legal fiction"[1] in which managers undertake various profit-making activities keeping in mind the interests of the shareholders. An opposing view considers the corporate entity as a "social being"[2] that owes obligations towards not only shareholders, but also the employees and wider society.

The Securities Exchange Board of India (**SEBI**) (*see* consultation paper dated March 1), proposed a slew of measures to address the corporate governance in India.[3] At the board meeting of June 29, SEBI retracted certain proposals aimed at overhauling the Indian corporate governance framework, while duly approving several other proposals.[4]

In the Consultation Paper, SEBI noted that an independent director (**ID**) is a critical spoke in the wheel of corporate governance, especially for safeguarding minority shareholders' rights.[5] After two recent corporate governance failures (the dismissal of Tata group director Nusli Wadia for supporting

1 Lynn S. Paine and Suraj Srinivasan, *A Guide to the Big Ideas and Debates in Corporate Governance*, Harvard Business Review (2019) https://hbr.org/2019/10/a-guide-to-the-big-ideas-and-debates-in-corporate-governance

2 Gerald F. Davis, Marina V.N. Whitman, & Mayer N. Zald, *The Responsibility Paradox*, Stanford Social Innovation Review (Winter 2008) https://ssir.org/articles/entry/the_responsibility_paradox

3 SEBI, *Consultation Paper on Review of Regulatory Provisions related to Independent Directors*, SEBI Reports and Statistics (March 2021) https://www.sebi.gov.in/reports-and-statistics/reports/mar-2021/consultation-paper-on-review-of-regulatory-provisions-related-to-independent-directors_49336.html

4 SEBI, *Minutes of the SEBI Board Meeting*, SEBI Press Releases (June 2021) https://www.sebi.gov.in/media/press-releases/jun-2021/sebi-board-meeting_50771.html

5 *Supra* footnote 3.

the minority shareholder group in the Tata vs. Mistry dispute[6] and PNB Bank – Nirav Modi scam[7]), SEBI attempted to solve the conflict of interest from the proximity of ID with the promoter and insufficient protection of minority shareholders' rights. It did this by promoting the UK and Israeli model of appointment/re-appointment of IDs.[8]

Accordingly, the Consultation Paper proposed for appointment and re-appointment of IDs through 'dual approval' route:

"(i) Approval of shareholders; (ii) Approval by 'majority of the minority' (simple majority) shareholders.... The approval at point (i) above, shall be through ordinary resolution in case of appointment and special resolution in case of re-appointment.

"If either of the approval thresholds are not met, the person would have failed to get appointed/re-appointed as ID. Further, in such case, the listed entity may either: i) Propose a new candidate for appointment/re-appointment; or ii) Propose the same person as an ID for a second vote of all shareholders (without a separate requirement of approval by 'majority of the minority'), after a cooling-off period of 90 days but within a period of 120 days. Such approval for appointment/re-appointment shall be through special resolution and the notice to shareholders will include reasons for proposing the same person despite not getting approval of the shareholders in the first vote."

The Consultation Paper also promoted a dual approval system for removal of IDs. However, in its board meeting, SEBI disregarded this approach and said any appointment, re-appointment or removal of IDs shall be carried out through a special resolution in the listed companies.[9] The amendments to the SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015, reflecting this approach will be effective from January 1, 2022.

It is noteworthy that the SEBI board of directors also agreed to reference the Ministry of Corporate Affairs for giving greater flexibility to companies while deciding the remuneration for all directors (including IDs), which may include profit-linked commissions, sitting fees, ESOPs, etc., within the overall prescribed limit under the Companies Act 2013. This would better enable companies to secure qualified and competent directors.

However, these laudatory measures may not help distance IDs from their alleged entwined relationship with the promoter group. Lingering doubts remain if IDs are truly independent.

It is worth noting that the 2000 report of Kumar Mangalam Birla Committee on Corporate Governance made a forward-looking statement that the corporate governance mechanism must dynamically cater to the needs of increased market competition and rapidly evolving technology.[10] It is not all water under the bridge yet and the regulators could give more teeth to the relevant listing regulations so listed entities can adhere to "3Cs" approach (Compliance, Conduct and Competence) while selecting, removing and setting out the roles and responsibilities of IDs.

---

6 Umakanth Varottil, *SEBI's backtrack on independent directors*, The Indian Express (July 2021) https://indianexpress.com/article/opinion/columns/tata-mistry-corporate-dispute-nusli-wadia-sebi-appointment-removal-of-independent-directors-7403380/

7 Param Pandya, *Public Sector Banks in India: Revisiting regulatory and corporate governance in the light of the PNB scam*, South Asia @ LSE' blog (May 30, 2018) https://blogs.lse.ac.uk/southasia/2018/05/30/public-sector-banks-in-india-revisiting-regulatory-and-corporate-governance-in-the-light-of-the-pnb-scam/

8 *Supra* footnote 3.

9 *Supra* footnote 3.

10 SEBI, *Report of the Kumar Mangalam Birla Committee on Corporate Governance*, SEBI Reports (2002) https://www.sebi.gov.in/media/press-releases/oct-1999/corporate-governance_18186.html

B. PROPOSED REFORMS TO THE PROMOTER REGIME

In line with SEBI's efforts to adopt international best practice, it floated a consultation paper earlier this year proposing a shift from the concept of a 'promoter' to a 'person in control.'[11] This fundamental change would impact current regulations under the Indian companies law, restructuring and insolvency law, banking and insurance law and the merger-control regime, particularly in the context of control.

The proposed reform acknowledges the current scenario relating to ownership and control of a number of Indian companies, which is a shift from the traditional family-owned, closely held structures, to widely dispersed shareholding, with institutional and private equity investments and, often, not having a clearly identifiable 'promoter' or 'promoter group', a concept which in itself is fairly unique to Indian companies.

The consultation paper even cited that *"the aggregate shareholdings of promoters in the top 500 listed entities in terms of market value, peaked at 58% in 2009 and is showing a downward trend. The promoters' shareholding was approximately 50% in 2018. At the same time, the shareholding of institutional investors in the top 500 listed companies, in terms of market value, increased from approximately 25% in 2009 to 34% in 2018."*[12] This reflects continuing control deals across sectors by private equity investors and is often tailored to unique situations in the Indian M&A and private equity regimes.

One must be mindful that the 'promoter' concept is deeply entrenched in Indian companies and the proposed reform will require a mindset change. The Consultation Paper planned for this change by proposing any reform should be carried out over a period of three years.

On August 6, the SEBI board of directors gave its in-principle approval to *"shifting from the concept of promoter to 'person in control' or 'controlling shareholders' in a smooth, progressive and holistic manner."*[13]

The authors would like to clarify that the views mentioned in this article are the authors' personal views and do not reflect the views of their respective organizations.

Rohan Kumar

Rohan Kumar is a Partner at Quillon Partners (formerly Platinum Partners, Mumbai).

Shinjni Kharbanda

Shinjni Kharbanda is a Senior Legal Manager at SpiceJet Limited, an airline company in India.

[11] SEBI, *Consultation Paper on Review of the regulatory framework of promoter, promoter group and group companies as per Securities and Exchange Board of India (Issue of Capital and Disclosure Requirements) Regulations, 2018*, SEBI Reports (May 11, 2021) https://www.sebi.gov.in/reports-and-statistics/reports/may-2021/consultation-paper-on-review-of-the-regulatory-framework-of-promoter-promoter-group-and-group-companies-as-per-securities-and-exchange-board-of-india-issue-of-capital-and-disclosure-requirements-re-_50099.html

[12] Id at page 6.

[13] SEBI, *Minutes of SEBI Board Meeting*, SEBI Press Releases (August 6, 2021) https://www.sebi.gov.in/media/press-releases/aug-2021/sebi-board-meeting_51707.html

In-house Insights with Maria Zarah R. Villanueva-Castro of Manila Electric Company

Q: TELL US A LITTLE ABOUT YOUR PROFESSIONAL BACKGROUND AND HOW YOU CAME TO BE IN YOUR CURRENT ROLE?

Sometime in 1997, I started as Court Attorney for the Philippine Court of Appeals where I assisted Justices in evaluating and drafting decisions on cases appealed before them.

I then had a short stint as department manager at a Government-owned and controlled corporation until I decided to join the Manila Electric Company or Meralco in 1999. Meralco is the largest electric distribution company in the Philippines. I started as a staff lawyer performing litigation work until I was designated to head its Corporate Legal team.

During my free time, I also teach in law schools where I impart my knowledge of commercial law.

Q: HOW BIG IS YOUR TEAM AND HOW IS IT STRUCTURED?

Our Corporate Legal office is composed of 10 lawyers and seven paralegal and administrative staff. Two teams report to me – one handles corporate legal work for Meralco and the other team renders legal services to Meralco's subsidiaries and affiliates.

Q: WHAT ARE THE BIGGEST CHALLENGES FACING IN-HOUSE LAWYERS TODAY?

One big challenge in-house lawyers inevitably face is how to balance a duty to promote the company's business and at the same time ensure it is compliant with rules, which are often perceived as obstacles in meeting goals and targets.

The bigger the organisation, the more risks are shifted to the in-house counsel and at times,

All Hands on Deck (Meralco Corporate Legal Planning)

they must make commercial decisions. So, it is for a counsel to understand the business, its goals and targets, as well as strategies. It is also imperative to communicate the risks surrounding management decisions. In-house counsel are also expected to provide commercially astute, but legally sound solutions to avoid or manage these risks.

Another challenge is balancing efficiency and effectiveness and educating the company on this balance. In this situation, an in-house counsel should proactively drive proposals that reduce costs while also identifying suitable benchmarks of efficiency.

Security of data, information and even contracts is also a common challenge, especially during this pandemic. The in-house counsel must align with the rapid changes in technology and be able to manage the associated risks posed by these developments.

Q: DID YOU HAVE A MENTOR EARLY IN YOUR CAREER? IS MENTORSHIP IMPORTANT?

I found the mentorship when I was a young lawyer to be very helpful. Because of the varied issues confronted by our company due to its highly regulated business as the largest distribution utility company in the Philippines, my mentors motivated me to always to be updated on its business and operational issues and relevant legal concerns. They exposed me to the intricacies of the power industry and how to effectively, yet politely, deal with its customers and regulators.

Mentoring is valuable to one's professional or personal growth. A mentor's feedback can help one improve their craft and instill confidence and trust in a person's capabilities. A mentor can provide impartial advice or guidance using relevant knowledge and experience. With these insights, the mentee would know what steps to take especially in crucial situations.

A mentor can also help establish a mentee's professional network and connect them to potential opportunities for free.

Q: HOW IS TECHNOLOGY CHANGING THE WAY YOU WORK?

Technology has made it possible for us to work in situations where it would be impossible to coordinate and communicate with everyone. Software tools such as Microsoft Teams, Zoom, Google Meet and other electronic conferencing applications have made it possible to connect online to discuss important issues and operational information to keep our company running efficiently and smoothly.

Despite the difficulties posed by the coronavirus, we can continue our detailed work and pass on documents, reports and other valuable information needed to coordinate with each other and keep each project on track.

Q: WHAT DO YOU MOST LOOK FOR IN A LAW FIRM WHEN OUTSOURCING WORK?

We look for reliable and trustworthy partners with sound legal minds and a competent and quality track record. We also look for timely handling of legal issues and at the punctuality in submission of their deliverables. We also look at the accuracy of their work as to our projects that need specialized handling, knowledge and experience.

Q: OTHER THAN LAW FIRMS, WHAT SERVICES AND TOOLS HELP YOUR LEGAL DEPARTMENT THE MOST?

Due to the need to work from home, reliable internet service is invaluable these days. We also rely on communication software and sometimes, even our smart phones have become important tools for communication, especially when needing to communicate without our laptops around.

Q: WHAT ASPECTS OF YOUR IN-HOUSE ROLE DO YOU MOST ENJOY?

Our corporate legal team is often consulted with decisions that affect the operations and business decisions of our company. I enjoy that my team has a direct connection with important aspects not only of Meralco, but also to provide legal services for its subsidiaries/affiliates. We also have exposure to varied businesses – like collection, power generation, financing, construction, e-transport, telecommunications, renewable ventures and insurance among other things.

It is challenging but intellectually fulfilling when we resolve issues with projects and contracts. We learn a lot especially when the counter party is a foreign entity. These experiences could teach us new ideas to bolster our own processes.

Lastly, our lawyers treat each other like we are a family. While we often argue on legal issues presented to us, which is a good intellectual exercise for everyone, but, at the end of the day, there is this sense of respect and support on the ultimate decision or direction to take. I personally believe that lawyers are happier with their job when they have close friendship or camaraderie at work.

Q: WHAT CHANGES DO YOU FORESEE IN HOW LEGAL SERVICES WILL BE PROVIDED IN THE COMING YEARS?

Legal services will always have legal research and writing at their core, so as far as those functions are concerned, they will probably remain constant. What will change is the interactions between lawyers and clients. These days, physical interaction is risky because of the threat of the coronavirus, and so new ways will have to be explored for lawyers to meet their deliverables efficiently.

Providing results also will depend on accurate research, which is sometimes difficult,

especially if the data can only be collected through field work. But there are always new challenges and ingenious solutions. It is just a matter of keeping abreast of technology and looking for clever ways to connect with people.

Q: WHAT ADVICE WOULD YOU GIVE YOUNG LAWYERS STARTING THEIR CAREERS TODAY?

Do not be afraid to step out of your comfort zones. In the past, I was a timid person and always cautious of accepting work I thought I would not be able to do, mainly because I never had any experience in the past.

Be honest in rendering legal advice. Flag risks but recommend measures to mitigate or manage them.

Manage your deadlines. List them and learn to prioritise. Ensure quality yet timely disposal of your deliverables.

Learn from your mistakes. Learn to recover from them. Be humble and appreciate that these mistakes will make you a better lawyer someday.

Relish your relationships with your mentors but learn to develop independence. Your mentors will not be with you forever.

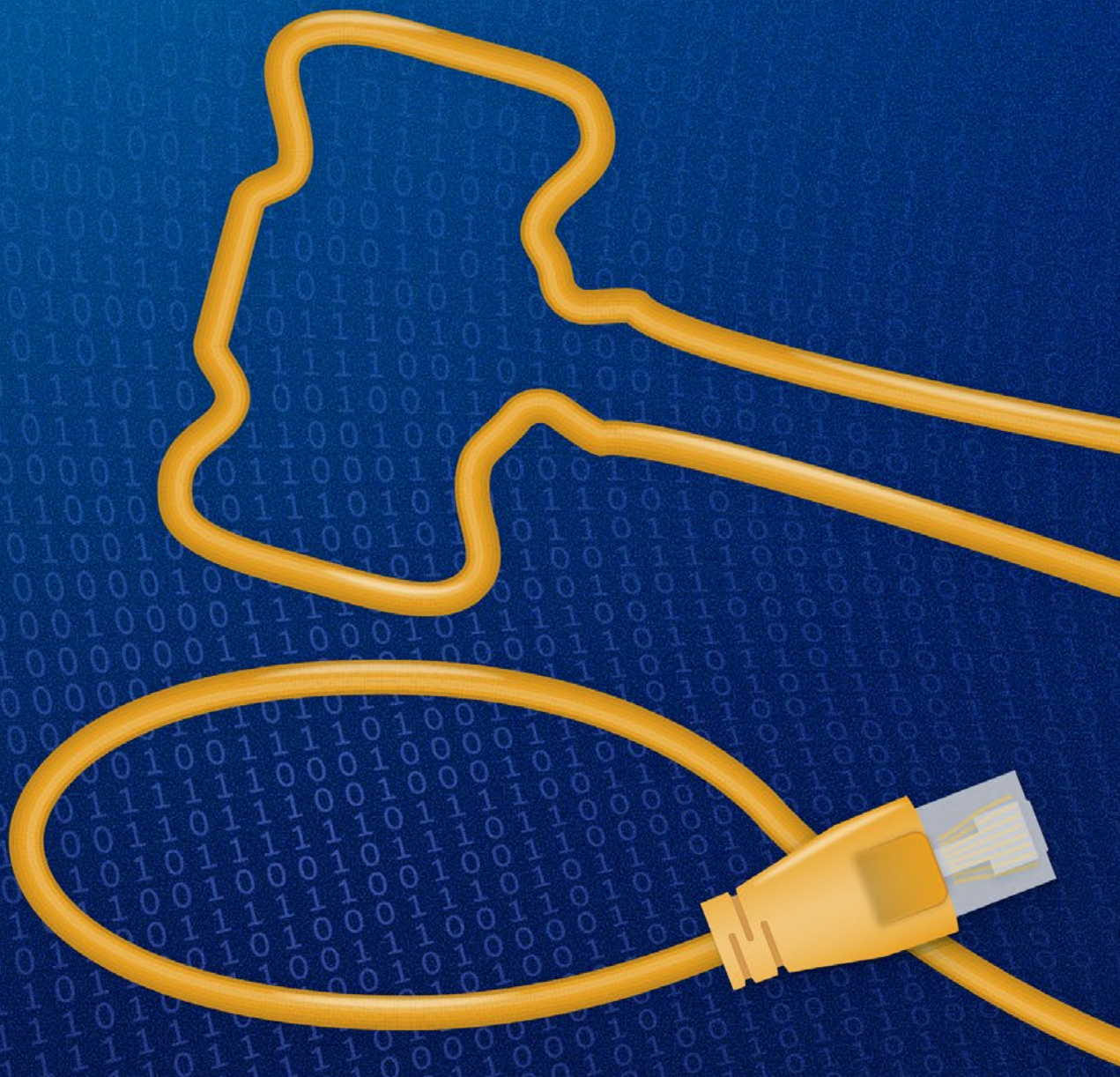
Establish good relationship with your colleagues and co-workers. Be respectful and polite but articulate your legal position with conviction. This will earn the trust of your superiors and co-workers.

Lastly, be kind to yourself. Eat healthy food, regularly exercise and unwind from time to time.

Q: WHAT IS YOUR HINTERLAND (WHAT DO YOU MOST LIKE TO DO AWAY FROM WORK)?

I choose to handle work-related stress with style. Aside from teaching in law school where I get to mentor students to become lawyers, painting is also a pensive way of dealing with stress. When I hold the brush and blend colours onto the canvas, I feel at peace with myself. I look for inspiration in a lot of things, such as a beautiful view, colours in the sky or just about anything that may be driving me at that moment.

During this pandemic, we all suddenly found ourselves within the walls of our homes, and many felt a frustration and helplessness while worrying about what may happen next. My hobby of painting helped bring tranquillity and happiness and released tension, fears and uncertainties. Likewise, it also helps me re-energise, when needed.



How General Counsel Can Help Prepare for Cyberattacks

BY NATHAN SMITH, featuring JONATHAN CROMPTON

In-house lawyers can be the fence at the top of the cyber cliff, creating procedures to prevent the worst effects of a cyberattack and responding quickly and effectively when (not if) a cyberattack occurs.

Given how quickly cybersecurity has risen from being a line-item on the IT department's annual budget to top of the list for most companies, in-house lawyers are now a critical gear in the machinery protecting a firm's digital assets, client data and balance sheet.

General counsel must lead the charge in encouraging the C-suite to create, implement and test a robust cybersecurity incident response (IR) plan. The future success of their company could depend on it.

Just how much of a problem are cyberattacks and breaches in 2021?

US-based cybersecurity provider FireEye said in its M-Trends 2021 report that the Asia Pacific (APAC) region is the "most-targeted" region in the world for ransomware.

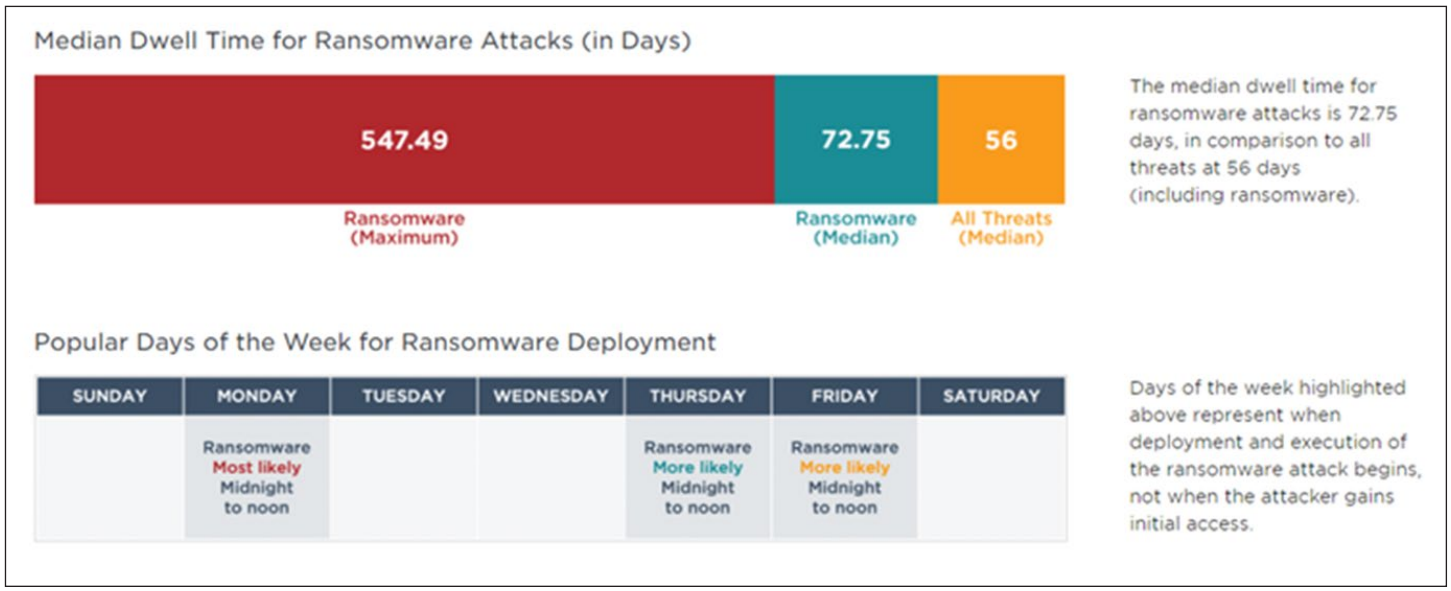
Ransomware is a form of malware that encrypts a victim's computer files. The attacker then demands a ransom to restore access to the data. Users are shown instructions for how to pay a fee to get the decryption key.

FireEye's report said on average, APAC organisations are attacked by ransomware roughly 51 times per week in 2021.

But it's not just ransomware that is rising. Between May 2020 and May 2021, recorded instances of all types of cyberattacks on APAC-based companies rose 168%. And in just one month – April-May of this year – the entire region saw a whopping 58% increase in cyberattacks, year-on-year.

Unfortunately, the preparedness of APAC companies is not keeping pace with the rising cybercrime. Indeed, it may even be slipping further behind.

A study earlier this year by British security firm Sophos called The Future of



Ransomware on the rise. 'Dwell time' indicates the time an attacker or malware variant sits on a computer system before it is activated or detected (credit: FireEye)

Cybersecurity in Asia Pacific and Japan found 54% of Asia Pacific (APAC) companies had not updated their cybersecurity strategies at all in the last 12 months – despite the Covid-19 pandemic which forced millions of employees to work remotely.

"We asked organisations if they had a cybersecurity team in place that could detect, investigate and respond to threats. In 2019, 50% of organisations answered 'no', in 2021 that increased to 52%," the study said.

RANSOMWARE AND 'DOUBLE EXTORTION'

RPC partner Jonathan Crompton said while Covid-19 popularised the term "work from home," the sheer number of these cyberattacks in 2021 will make "ransomware" and "double extortion" the cybersecurity buzzwords of 2021.

"Ransomware attacks have significantly increased as a proportion of all cyber incidents on which we are advising. We are also regularly seeing threat actors adopting the 'double extortion' technique by extracting personal data before triggering a ransomware encryption.

"It often comes with a threat that if payment isn't made, the data will be published. Threats like this are designed to increase the chances of a victim company paying a ransom even if it has restored its systems. One group has even begun publishing the fact of a successful attack while negotiating the ransom payment to increase pressure on the company," he said.

IronNet's 2021 Cybersecurity Impact Report said APAC's impressive economic growth means the region will continue to offer many juicy, high-value targets in a low-security environment for many years until companies realise the danger they are in and take action to defend themselves.

"Rapid digital transformation has expanded APAC cyberattack surface and there remains a disproportionately low level of investment in cybersecurity and risk management strategies by many organisations," IronNet's report said.

All this might seem daunting for in-house legal teams. However, a lot can be done – quickly and efficiently – by general counsel to mitigate the major vulnerabilities in their company's computer systems.

After all, the in-house legal team is often the first phone call (after the IT department) that a CEO will make during a cyber incident to figure out what happened. So, they better have a plan.

INCIDENT RESPONSE

Some of this work has already begun in many companies.

In-house legal teams are often consulted to create data policies, business continuity plans, insurance options or by inserting appropriate clauses in contracts to protect a company's interests.

The problem facing in-house legal teams is that there can be a breakdown in process when a well-thought-out response plan is dusted off and executed in the crisis situation of a cyberattack. On top of that, many legal teams are still stuck using manual, ad hoc processes and out-of-date information which hurts their ability to make critical decisions during a breach.

One example of a recent cyber incident shows the importance of including general counsel in all conversations about security – ideally long before an incident arises.

Philippines struggling to cope with cyberattacks (credit: Sophos)

The incident described below occurred at a major asset management company. A legal counsel for the company told IHC about the breach on condition of anonymity.

> *"Our firm identified a potential unauthorised access of an employees' Outlook account (which our firm locked upon identification of the unauthorised access).*
>
> *"Upon discovery, we took immediate action to remediate the situation and the unauthorised access to the employee's account by this third party was terminated. We also engaged technical experts, including a cyber incident response manager and an independent leading global provider of risk solutions to thoroughly investigate the matter.*
>
> *"The expert concluded the breach was limited to one email account and that the actions of the unauthorised actor were motivated by financial fraud and not theft or exfiltration of personal data," the legal counsel said.*

The counsel added that the incident could have been much worse if the company did not have in place appropriate policies and procedures to address cyberattacks quickly and if the key staff didn't follow those steps.

Everyone did what they were supposed to do because they had the appropriate training, drills and assistance when those were all needed – before the cyberattack took place.

IN-HOUSE COUNSEL AT THE CORE

Crompton said in-house lawyers must be at the core of building a good crisis response plan by ensuring that data governance and security are regularly on the board's agenda as a standing item.

"Preparation is key to post-breach response. It is much better to over-prepare than under-prepare," he said.

Crompton added that a full cybersecurity and data governance plan must involve all areas of the business, including IT

(infrastructure and security), finance and risk (insurance), communications (messaging) and the business.

Having access to good cyber insurance is also a great way to protect against the potentially significant costs of third-party service providers investigating and responding to a cyberattack.

Speaking on condition of anonymity, a general manager of legal and risk management at a multinational retail and supply chain group said instead of just focusing on the law, in-house counsels should know the operations side of the company as well, have a decent level of technical IT knowledge and, more importantly, be good communicators.

"Be quick, be transparent, be determined. Have specialists ready to call in an emergency. A business continuity plan (BCP) will avoid panic and we strongly advise having the BCP tested on a regular basis.

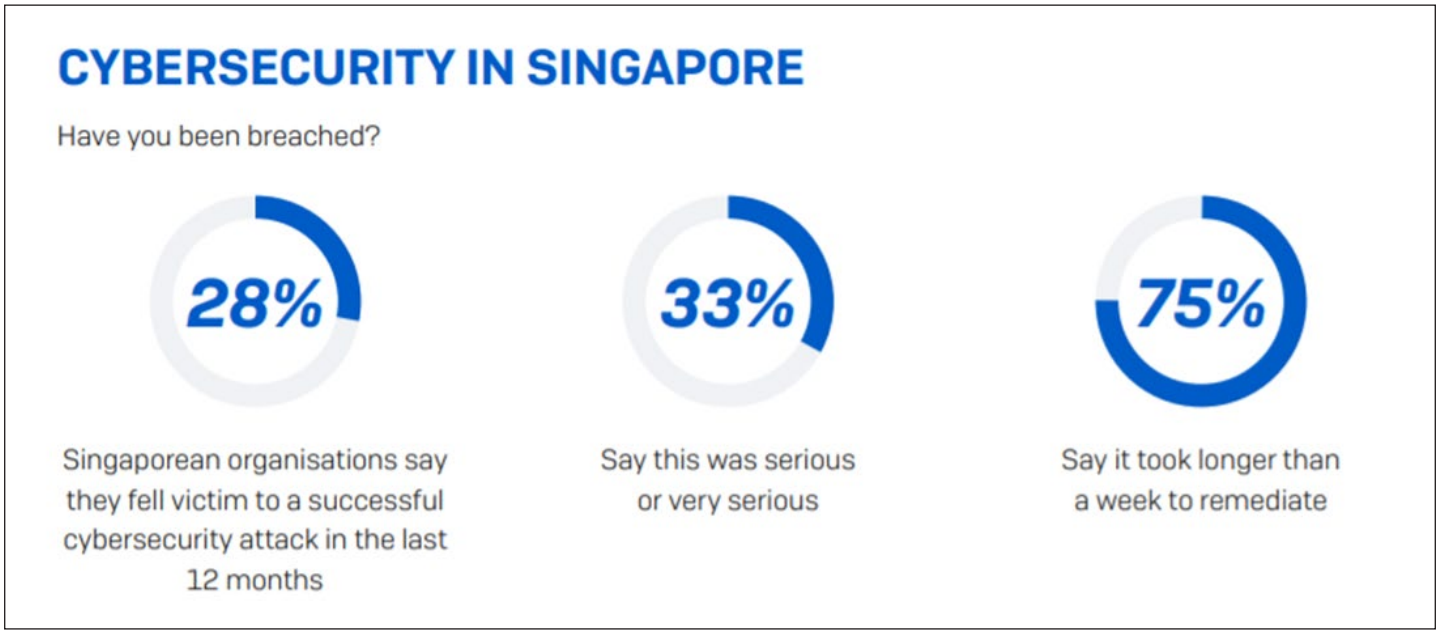
"But, the most challenging part of a plan is always the execution and the follow through," the general manager said.

It's not necessary for general counsels to have all the same technical information as an IT specialist, but they should have a basic understanding of all terms. They also need to be aware that cyberattacks can occur suddenly and can escalate rapidly.

Also, a general counsel should build a network of in-house and external lawyers to share how they handled cyber breaches and learn some tricks. This can be done through outside counsel if needed. Having these connections can relieve significant uncertainty (and therefore pressure) on an in-house team when a crisis happens, Crompton said.

DEALING WITH RANSOMWARE

It seems above all other types of cyberattacks, ransomware is likely to be the type to hit most companies, at least over the next few years.



Singapore-based companies say it can take a long time to recover from cyberattacks (credit: Sophos)

Five things in-house lawyers can do to prepare for cyberattacks

1 CONNECT

The complexity of the modern company means computer systems are likely "siloed" (stored in different locations). While this can be a great defence against cyberattacks, it also can be a vulnerability if in-house counsel can't see the whole landscape of a company's information assets.

Staying connected also means ensuring the C-suite, the board, HR and even external lawyers and cybersecurity professionals can all talk to each other should a cyber incident occur. On top of that, it is essential for general counsel to build a strong partnership with the chief information security officer (CISO).

2 PLAN

CSO's Global Intelligence Report: The State of Cybersecurity 2021 found only half of respondents said mandatory IT security training had been in place "for some time," with 20% saying such initiatives were only just introduced "recently."

This is too slow, the report said. Companies should be proactively planning for a cyber breach – since it is not a matter of 'if,' but 'when.' Regular, mandatory cybersecurity training can also be a key factor in a regulator's decision whether to impose a penalty or not.

In developing a strategy, in-house counsel must start with the low-hanging fruit. Gaps in security often are the result of oversight or the accumulation of "exceptions" to security policies that build up over time. These are often the easiest parts to fix first.

3 PRACTICE

"Practice as you want to play" is great advice for cybersecurity. An incident response (IR) plan can be tailored to a specific company, but if such a plan is immediately shoved into a filing cabinet it will be worse than useless – everyone will develop a dangerous false sense of security.

Instead, regularly conduct tabletop crisis exercises with all team members and have external experts "on call." This includes walking a CEO through a communications strategy and practicing various responses with them. If the teams are walking away from these exercises without identifying weaknesses or asking questions, it's likely there are still gaps in the plan.

4 PROTECT

The first responsibility for general counsel is to maintain attorney-client privilege before and after a breach. The aim of coordinating communications is about containing financial, market, technical, operational and reputational damage to limit the company's potential legal liability.

There is no guaranteed way to maintain privilege when working with outside counsel, but it should be a top priority and general counsel is best-placed to advise on this.

5 CONSIDER

Part of any good IR plan is to consider getting cyber insurance. A Cyber Insurance Risk Assessment is a quick, high-level analysis of a company's risk level based on its technology, processes and people.

While cyber insurance can offload some risk, it doesn't nullify all risks. For example, insurance cannot repair any damage to a company's brand or core business. Insurance is helpful, but prevention will always be key.

According to Steve Ledzian, CTO and Vice President, APAC of FireEye ransomware is "spiralling out of control" in the Asia Pacific.

Unfortunately, Ledzian says it can take an average of 76 days for organisations in the region to notice and respond to these kinds of intrusions, falling behind EMEA (Europe, Middle East, Africa) which averages 66 days and the Americas, averaging just 17 days.

"In many cases the attacker's work is done well before the victim even knows something is wrong," Ledzian said.

So, what can be done if a company's computer systems are locked by ransomware?

Firstly, it may be possible to purge the locked systems, restore backed-up versions of the data and keep going as if nothing happened. After all, many large companies have the discipline to store multiple copies of their data so they can pivot to new machines easily without needing to pay the criminals a ransom to release it. It also pays to keep a hard copy of the response plan in case none of the computers are accessible during an attack.

But for others – smaller firms or larger companies caught off-guard – the only realistic option to recover the data or prevent further leakage is to attempt to pay the criminals. There is no guarantee the data will be unlocked (some criminals lock the data but don't have the unlock codes themselves, while others will simply refuse to unlock the data even if they get a ransom).

If a company suffering a ransomware attack does choose to negotiate with the criminals, there are a few things to consider first, said RPC's Crompton.

RPC has advised several companies that chose to pay a ransom. Crompton said these experiences show the benefit of using a cyber ransom negotiator if companies get caught by a ransomware attack.

"Good specialist negotiators are very cost-effective, can provide intelligence on the ransomware group or affiliates, can advise if, by how much and over how long the negotiators might realistically negotiate down ransom demands for that specific group, and can effectively negotiate 'proofs of life' (of the stolen data) and extensions of time.

"These factors can help the victim decide if a negotiation could meaningfully reduce a ransom or provide a window to investigate and implement a response strategy, including notifying data subjects and regulators before a public leak of any stolen information," Crompton said.

He also explained that "threat actors" (groups or individuals responsible for cyberattacks) are often just looking for a "pay day," even if it is much lower than the initial demanded ransom. There is often room for a strong negotiation. Threat actors are often happy to receive a small proportion of the initial demand, but they have limits.

Bizarrely, some are even happy, after receiving payment, to explain how they breached the victim's systems in the first place, giving insights on ways to avoid compromise in the future. There seems to be a tiny bit of honour among cyber thieves.

"However, the victim should be ready for a roller-coaster ride of threats to leak the data and should be ready to move quickly on the payment, once a deal has been reached," Crompton said.

IS IT LEGAL TO PAY RANSOM?

Even with a strategy and willingness to pay a ransom, in some jurisdictions it may not even

be legal to pay cyber criminals to release a firm's data. It is important to always check the local laws, said Crompton.

While ransomware attacks are international, multi-jurisdictional and often jurisdiction agnostic, there is no overarching international legal framework for cybersecurity, data protection or ransom payments.

In Hong Kong, Singapore and other Common Law countries, companies generally need to consider if the payment itself is illegal – this is generally a 'proceeds of crime' question. Such laws will rarely (if ever) have been tested for ransomware payments, but guidance is available from normal ransom cases.

It is also worth considering if the ransom payment will be made to a prohibited person – this is generally an AML/CTF/sanctions issue. Cyberattackers are, by nature, anonymous but a victim company must do due diligence, checking the information it has about the attackers against the latest sanctions lists.

Some jurisdictions will provide victims with a defence if the paying company notifies law enforcement before or immediately after making a ransom payment.

"Getting early advice is key if the company thinks it might have to pay a ransom. Some insurers have established checklists for if a ransom payment is covered under the policy. Again, it is best to check with the insurer as soon as the company thinks it might make a claim for a ransom payment under its policy," Crompton said.

He added that data laws are getting more stringent and more localised. When the Europe-based general data protection regulation (GDPR) came into force in 2018, it was described as a "monster" and has had enormous implications across the world for how companies should store and process personal data.

The upcoming Chinese Personal Information Protection Law also poses a huge challenge for handling data. Laws are moving fast so companies need to move faster.

Compounding this problem, legal costs in the post-Covid-19 business atmosphere (just like any other costs) are being scrutinised and it can be a challenge to come up with the resources to stay on top of the game.

"The APAC cybersecurity and data privacy landscape is always evolving, and regulators understand that cyberattacks cannot always be prevented" said Crompton.

"...but they are looking for evidence that a victim company did all it could to protect the data, prepare for a breach and respond quickly. A good, well-executed incident response plan can even result in a regulatory warning instead of a financial penalty. This helps both the company's reputation and its bottom line."

Nathan Smith
Editor, IHC Magazine

With collaboration from Jonathan Crompton from RPC.

Jonathan Crompton
jonathan.crompton@rpc.com.hk

Jonathan Crompton is a partner in RPC's Hong Kong office. He helps companies and individuals navigate complex cross-border disputes and investigations, with particular experience in financial services and technology related matters. Jonathan leads RPC's Asia cyber response team.

Personal Data Protection/ Cybersecurity Law in Thailand

BY ARKRAPOL PICHEDVANICHOK
VISITSAK ARUNSURATPAKDEE

1. INTRODUCTION

Thailand did not have a specific data protection law until 2019 when the Personal Data Protection Act (PDPA) and the Cybersecurity Act (CSA) were promulgated.

The PDPA sets high standards for personal data protections and is largely based on the EU's General Data Protection Regulation (GDPR) with the intention of having equitable standards. For example, the PDPA mirrors the GDPR's legal basis for data processing, extraterritorial applicability, and a data subject's rights. However, the two are not identical.

While the PDPA specifically prescribes that a request for consent must be explicit in a written statement or via electronic means (unless such a request cannot be done), the GDPR focuses on consent being given by a clear affirmative act, such as an explicit oral statement. Also, the PDPA imposes criminal penalties for non-compliance in addition to monetary and administrative penalties.

2. THE PDPA

2.1 Overview

The PDPA has been effective since 28 May, 2019, but the enforcement of most provisions is delayed until 2022. Key provisions for personal data protection, a data subject's rights, duties of a data controller and processor, complaints, civil liabilities and penalties will not be effective until 1 June, 2022.

2.2 Scope of law

Generally, the PDPA applies to the collection, use or disclosure of personal data by a data controller or processor in Thailand. As in Article 3 of the GDPR, the PDPA also applies extraterritorially to the collection, use or disclosure of personal data of Thailand-based data subjects by a foreign data controller or processor in relation to the following activities:

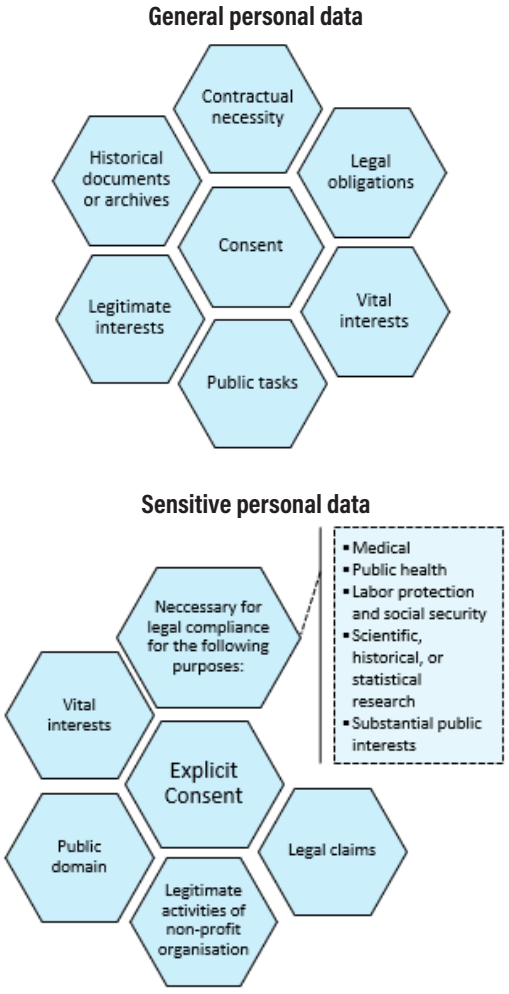
1. the offering of goods or services to data subjects in Thailand; or
2. the monitoring of the behaviour of data subjects taking place in Thailand.

2.3 Definition of personal data

Personal data - Any information relating to a natural person, enabling the identification of a person, directly or indirectly, but not including the information of deceased persons.

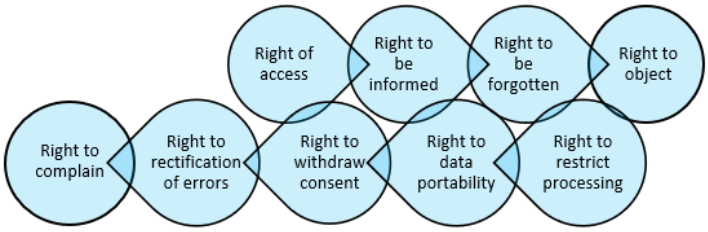
Sensitive personal data - The law does not provide a definition. However, explicit consent is necessary for collecting personal data pertaining to: racial or ethnic origin; political opinions; culture; religious or philosophical beliefs; sexual behaviour; criminal records; health data; disabilities; labour union information; genetic data; biometric data. The processing of sensitive data is subject to more stringent requirements and violations carry criminal penalties.

2.4 Legal basis for processing personal data



2.5 Rights of data subject

Under the PDPA, data subjects have the following rights regarding their personal data:



2.6 Duties of a data controller/data processor/ data protection officer (DPO)

Data controller - A person or a juristic person with the power and duties to make decisions regarding the collection, use or disclosure of personal data.

Duties:

- Adopt appropriate technical and organisational measures to assure the collection, use and disclosure of personal data accords with the PDPA. For example:
  - Inform data subjects with sufficient information such as the purpose of data processing, data subject rights, etc;
  - Maintain and record processing activities;
  - Process data in accordance with the informed purposes;
  - Provide sufficient security measures to safeguard personal data.

Data processor - A person or a juristic person operating in relation to the collection, use, or disclosure of personal data pursuant to the orders given by or on behalf of a data controller, whereby such a person is not the data controller.

Duties:

- Provide sufficient guarantees for the technical and organisational measures required by the PDPA. For example:
  - Carry out processing activities pursuant to the lawful instructions given by the data controller;
  - Provide sufficient security measures to safeguard personal data;
  - Maintain and record processing activities.

Data Protection Officer DPO - Not specifically defined. Note: The Personal Data Protection Commission (PDPC) may prescribe the qualifications of the DPO in the future.
Duties:

- Advise data controllers or data processors regarding compliance with the PDPA;
- Investigate the collection, use or disclosure of personal data by data controllers or processors;
- Liaise with the PDPC on data protection matters;
- Keep personal data known or acquired confidential.

2.7 Data breach

The data controller must notify the PDPC of any personal data breach without delay and, where feasible, within 72 hours after becoming aware of a breach, unless the data breach is unlikely to be a risk to the rights and freedoms of data subjects.

If a personal data breach is a high risk, the data controller must also notify the data subjects without delay after learning about the personal data breach and about the remedial measures being implemented.

2.8 Penalties

Civil liability

A court may impose compensation as punitive damages up to double the actual damages.

Criminal penalties

Imprisonment for a term not exceeding one year and/or a fine not exceeding ฿ million, depending on the non-compliance.

2.9 Development of PDPA since enactment

Although the PDPA is already in force, the PDPC has not officially been set up and the subordinate laws under the PDPA are being drafted. Additionally, the regulating authority is preparing PDPA guidelines for seven sectors: 1) tourism, 2) public health, 3) education, 4) retail and e-commerce, 5) transportation and logistics, 6) real estate and 7) state operations.

3. THE CYBERSECURITY ACT

3.1 Overview

The CSA came into force on 28 May, 2019. The CSA aims to govern cybersecurity activities to prevent and combat cyberthreats.

A "cyberthreat" is broadly defined as "any action or unlawful undertaking done using a computer, computer system or undesirable program with an intention to cause harm to a computer system, computer data or other relevant data, and includes imminent threats that would cause damage or affect the operation of a computer, computer system, or other relevant data."

Under the CSA, cyberthreats can be categorised into three levels of severity:

(1) non-critical cyberthreats;
(2) critical cyberthreats; or
(3) crisis cyberthreats.

Each threat level depends on the effect to a country's infrastructure, national security, economy, public health, public order or important information infrastructure. The level of threat determines the level of response the Cybersecurity Supervision Committee (CSSC), the authority tasked with monitoring and supervising compliance with the CSA, must use to combat such threat.

For example, in a serious cyberthreat specific provisions authorise the CSSC to examine computers, computer systems and data and seize computers, computer systems or any other equipment as necessary.

3.2 Critical Information Infrastructure

The CSA defines Critical Information Infrastructure (CII) as a computer or computer system used by a government agency or private organisation that relates to maintaining national security, public security, national economic security or public interest infrastructures.

The CSA also designates certain organisations as Critical Information Infrastructure Organisations (CIIO), including organisations providing: 1) national security, 2) important public services, 3) banking and finance, 4) information technology and telecommunications, 5) transportation and logistics, 6) energy and public utilities, 7) public health and 8) other services prescribed by the National Cybersecurity Committee (NCSC). Therefore, a private sector operator providing any of these services is regarded as a CIIO and is subject to the CSA.

3.3 Policies and Plans

The NCSC is developing a master plan and subordinate regulations related to cybersecurity in Thailand. Recently, the NCSC approved subordinate regulations including: 1) policies and plans in relation to cybersecurity; 2) a code of practice and a standard framework regarding cybersecurity for government agencies and the CIIO; 3) NCSC's notification relating to the establishment, duties and authorities of the national coordinating agencies for the security of computer systems; 4) the NCSC's notification in relation to the duties and responsibilities of the coordinating agencies for the security of computer systems for the CIIO; and 5) the NCSC's notification prescribing characteristics of the organisations with a mission or that provide services as a CIIO. However, these

provisions are in the early stages of development and will require further approval.

3.4 Coping with Cyberthreats

To cope with cyberthreats, the CIIO has the following duties: 1) notify the contact information of the owner, person in possession of and operator of a computer system, along with any changes thereto to the authorities; 2) comply with the code of practice and minimum cybersecurity standards; 3) conduct risk evaluations of cybersecurity at least once per year and submit the results to the authorities; 4) implement mechanisms or procedures to monitor and resolve any cyberthreats or incidents relating to the CIIO; and 5) report any cyberthreats.

While the CSA requires the CIIO to ensure that appropriate cybersecurity measures are in place to protect its organisations from cyberattacks, the PDPA also requires organisations to ensure that both technical and organisational security measures are implemented to prevent unauthorised or unlawful loss, access to, use, alteration, correction or disclosure of personal data.

4. SELF-CHECK

4.1 Is your entity ready for the full enforcement of PDPA?

Given the grace period until June 2022, it is crucial that organisations review their personal data related activities to ensure their compliance with the PDPA.

Steps	Self-check	Steps	Self-check
Data mapping	✓	Consent management	✓
DPO appointment	✓	Security measure	✓
Training/Awareness	✓	Data subject rights management	✓
Record of data processing activity	✓	Data processing agreement	✓
Privacy notice	✓	Data breach management plan	✓

4.2 How to effectively handle data breaches?

Data breaches may occur for a variety of reasons. Therefore, organisations should create measures to monitor and take pre-emptive actions when handling any data breaches. A data breach management plan should be adopted to enable organisations to manage data breaches effectively and systematically. Moreover, regular training teaching personnel about personal data protection is recommended.

5. CONCLUSION

As digital business rapidly expand, the PDPA and the CSA provide an important foundation for organisations to handle and deal with potential legal exposures and risks regarding breaches to personal data and cyberthreats.

While some organisations may choose to wait for the full implementation and subordinate regulations under the PDPA, early actions in complying with these laws should be considered to grasp the benefits (and avoid punishment) of technology advancements. Operators in Thailand should undertake internal organisational preparations to comply with the PDPA, as implementation of required measures may take several months.

CHANDLER MHM

Arkrapol Pichedvanichok
arkrapol.p@mhm-global.com

Arkrapol is a Senior Partner and head of the corporate and M&A practice at Chandler MHM specializing in Corporate and Mergers & Acquisitions and Capital Markets.

Visitsak Arunsuratpakdee
visitsak.a@mhm-global.com

Visitsak is a Partner at Chandler MHM specializing in personal data protection, administrative law litigation and advisory, technology, media and telecommunications, mergers and acquisitions, regulatory compliance and corporate commercial matters.

Artificial Intelligence & Personal Information Protection in Korea

BY KWANG-WOOK LEE
KEUN WOO LEE
CHULGUN LIM
HELEN H. HWANG

1. INTRODUCTION

The rapid development of artificial intelligence (AI) promises plenty of benefits and opportunities but also comes with risks when processing personal information.

These risks include:

(a) *Large-scale data processing:* the extensive learning data used in AI development likely involves a variety of personal and sensitive information;

(b) *Complexity and lack of transparency:* the methods used in processing personal information to develop and operate AI services are complex, which makes it difficult for data subjects to know how their personal information is processed;

(c) *Automation and uncertainty:* the difficulty in predicting the results of data processing in automated services can lead to unexpected consequences such as privacy infringement, social discrimination and bias.

A recent controversy in South Korea about AI and personal information protection involved "Lee Luda," an AI chatbot service released on December 23, 2020. Lee Luda was quickly shut down due to complaints about its inappropriate use of personal information. For example, the providers of Lee Luda were accused of directly copying user conversations from another website they serviced without consent. Although the service providers claimed they had consent to collect and use personal information, their stated purpose for collecting and using the data – "service development" – was considered to be too abstract.

To address the many issues, South Korean regulators are strengthening the safety and integrity of AI-related personal information processing. For example, the Ministry of Science and ICT released its "People-centred National Artificial Intelligence Ethical Guidelines," while the Personal Information Protection Commission released the "Guidelines for Protecting Personal Information Processed by Automated Methods" along with the "Artificial Intelligence Personal Information Protection Self-Checklist."

This article provides an overview of these recent regulatory trends in South Korea relating to personal information protection in the era of AI.

2. AI AND PERSONAL INFORMATION PROTECTION RULES

Considering the nature of AI technology and services, protecting personal information requires: a) compliance with personal information protection obligations under applicable statutes; b) self-regulating activities in accordance with "Privacy by Design," in which organisations implementing AI technology and policies must consider privacy throughout the entire life cycle of products and services; and c) compliance with personal information protection rules in designing and operating AI to prevent privacy infringement, social discrimination and bias.

AI-related personal information protection rules that are regulated by current statutes are mandatory, while those unregulated by current statutes are only recommended. The following is a list of the important rules in South Korea.

Mandatory:

- Obtain voluntary, clear and specific consent and minimise the personal information items to be collected.
- Generally, personal information can be used or provided to a third-party only if to do so is within the scope of the original purpose for collection. Thus, a separate legal basis is required to use or share personal information beyond the original purpose.

(i) Personal information may be used without the consent of the data subject if reasonably related to the initial purpose of collection, there is no disadvantage to the data subject and appropriate measures (e.g. encryption) are in place to ensure the security of the personal information. (Personal Information Protection Act Article 15(3));

(ii) Unless there are special circumstances, personal information collected to offer a service can be used or provided to third-parties without additional consent to develop AI to improve the service. This is because the use is reasonably related to the original purpose of collection, the data subject can predict the use and it is unlikely the use will unfairly infringe on the data subject's interests. (Authoritative Interpretation).

- Using and providing pseudonymous information without the data subject's consent is limited to statistical, scientific research and public archiving purposes. Accordingly, additional consent is generally required. Data controllers must also avoid risks of re-identification.

  (i) Although AI uses scientific methods such as modelling, learning and testing, it is difficult to view the operation of AI-related services as scientific research. AI service providers must clearly notify data subjects and obtain additional consent when using (disclosing or providing) pseudonymous personal information. However, additional consent is not required if scientific methods such as technical development or substantiation are employed to improve functions and enhance algorithms. (Authoritative Interpretation);

  (ii) Pseudonymous AI learning data requires caution because it is extensive and may include identifiable and attributable information along with private information. For example, in the case of SNS conversation data, it is necessary to pseudonymise not only the identifying information of the speaker, but also the identity or private information of any individuals mentioned in the conversation;

  (iii) If pseudonymised information is disclosed to unspecified individuals, someone may have information that, in combination with the disclosed information, can identify an individual. Service providers should refrain from disclosing pseudonymised information to unspecified individuals and anonymise any personal information provided to unspecified third-parties.

- Safely store and manage personal information used in the development and operation of AI with measures such as encryption and access control;
- Immediately destroy personal information that becomes unnecessary due to, for example, the termination of the AI development or operation;
- Manage, supervise and educate data controllers involved in the development and operation of AI.

Recommended:

- Analyse and remove privacy infringement risks and follow relevant AI regulations and privacy protections in accordance with the Privacy by Design principle. In particular, identify the general status of the data to be collected and used, and analyse personal information items and types (identifiers, attribute information, etc.) to determine the use and grounds for collecting each personal information item (e.g. consent);
- Actively self-regulate personal information protection activities during the development and operation of AI and obtain user trust by clearly disclosing how the AI service works;
- Incorporate countermeasures in the service system and constantly monitor the quality and risk of learning data to avoid social discrimination and bias resulting from processing personal information during the development and operation of AI.

3. EXAMPLES OF RELATED MEASURES

A. Personal Information Processing Based on Consent

In the case of a service collecting and analysing TV viewing data to suggest personalised content, service providers should inform users of the items, purpose and how long they intend to keep their personal information collected and any disadvantages of not giving consent. They should also prove that consent was obtained from users who clearly understood the terms of the consent.

B. Processing the Minimum Amount of Personal Information Needed

In the case of AI speaker devices that are on standby and activated through a "wake" word or sensor and voice recognition to perform commands such as playing music, these devices risk being activated unintentionally by other noise. This may lead to conversations being recorded without a user's knowledge. These devices should include a function to inform a user when personal information is being collected, for example, by flashing LED lights when the device is recording. Furthermore, the device should allow users to turn off voice recognition and standby mode giving them control over whether or not to use the recording function.

C. Anonyms and Pseudonyms

In the case of a service that analyses viewing data from smart TVs to provide personalised content to users, there is a risk emerges that names and phone numbers could be leaked since this information is often saved together with the viewing data. Service providers should identify if it is necessary to separate the various types of personal information collected and anonymise or pseudonymise any personal information the service does not require to function.

D. Transparent Disclosure of Personal Information Processing Methods

In the case where a service makes personalised recommendations by providing to third-parties smart TV viewing data and voice information, third-party provisions drafted in fine print could prevent users from realising their information may be provided to third-parties. To avoid this issue, service providers should prominently disclose personal information processing policies, including collection, use, storage, sharing and destruction, to the user with infographics and diagrams. Such information should also be easily available to users on a smartphone application or TV system.

E. Ability to Request Access, Correction and Deletion of Personal Information

In the above case of the AI speaker devices , it may be difficult for users to enforce their privacy rights. For example, it may be difficult for users to delete voice information collected or saved without their knowledge

because they don't know how to make such requests. Accordingly, service providers should allow users to easily learn how their information was used and request correction or deletion of their information. Also, services should prepare automated measures to quickly respond to user requests.

YOON & YANG
법무법인(유) 화우

Kwang-Wook Lee
kwlee@yoonyang.com

Kwang-Wook Lee is a partner and a Head of firm's New Business Team at Yoon & Yang specializes in the new technology related businesses such as fintech, smart car, Internet of Things, big data, U-healthcare, and shared economy.

Keun Woo Lee
klee@yoonyang.com

Keun Woo Lee is a partner at Yoon & Yang, specializing in intellectual property protection, privacy protection, trade secrets protection, including e-commerce and other technology, media and telecommunication areas.

Chulgun Lim
cglim@yoonyang.com

Chulgun Lim is a partner at Yoon & Yang and his practice areas include disputes and litigation cases relating to personal information protection, technology, and intellectual property.

Helen H. Hwang
hkhwang@yoonyang.com

Helen H. Hwang is a senior foreign attorney at Yoon & Yang, and her practice areas include intellectual property including patent and trademark, foreign outbound investment, and general corporate law.

Vietnam Focuses On Cybersecurity and Data Protection

BY LE TON VIET

Vietnam has taken large steps to improve its cybersecurity and data protection. The task is not over, and the steps are controversial.

Cybersecurity and data protection are governed by the Cybersecurity Law, the Law on Network Information Security (LNIS) and the Law on Information Technology (LIT), with the former two more relevant to cybersecurity and protection of data.

UNCLEAR AND CONFUSING ENVIRONMENT

Since the Cybersecurity Law came into effect in 2019, there has been an ongoing conversation largely opposing the requirement of data localisation, that offshore entities must have a local presence and the government's ability to censor "inappropriate" Internet content. Strict enforcement, it is feared, will disrupt the continuous flow of data, so crucial for commercial development.

However, the government has not clarified or even enforced the law yet. Business continues to operate in the shadow of the law while awaiting guidance. The circumstances are further clouded by the broad language of the law. But lack of clarity and selective enforcement are not new in Vietnam, and they often serve the government's purpose of indirect control.

For businesses, this means past practices in a lightly-regulated environment can be voluntarily and incrementally modified. But with no detail, this is unlikely. The muddled situation may soon change. The past 12 months has seen active development of new draft legislation to clarify the current law but also focus on implementation and enforcement of current requirements.

RECENT DEVELOPMENTS IN CYBERSECURITY LEGISLATION

In early 2020, the Ministry of Information and Communications (MIC) proposed to amend Government Decree No. 72/2013 on the provision, management and use of services and information on the Internet. The draft

regulations introduced a host of new and compulsory licenses and requirements for content management, social networks and application distribution platforms. Later in 2020, the MIC proposed to amend Decree No. 181/2013 to regulate cross-border advertising services.

These drafts drew much criticism from the business community. In a letter to the MIC, the Asia Internet Coalition said some of the new requirements are "impossible or unduly onerous to comply with," are "discriminatory against foreign organisations and individuals" and violate Vietnam's national treatment obligations in WTO and CPTPP commitments. These drafts represent the government's focus on gaining control, ensuring the security of Vietnam's cyberspace and enhancing the overall technical capabilities of its cyberinfrastructure. However, businesses depend on the free flow of information and their voices cannot be ignored.

SWEEPING CHANGES IN THE PROTECTION OF PERSONAL DATA

Meanwhile, the Ministry of Public Security is drafting a decree to deepen the protection of personal data (PDPD). The decree will extend the scope of what it means to "process personal data" to cover "collection, recording, analysis, storage, alteration, disclosure, grant of access, retrieval, recovery, encryption, decryption, copy, transfer, deletion and destruction of personal data or other related actions."

The PDPD would also separate personal data into "basic personal data" and "sensitive personal data." Processing sensitive personal data will be subject to additional requirements. The overall principle of PDPD is "privacy by design," which requires companies and individuals to integrate the security of personal data into their core systems. Of some relief, the regulations of the PDPD are broadly based on the principles of the EU's General Data Protection Regulation (GDPR). Companies that have already adopted or are guided by GDPR standards will be prepared to adapt to the PDPD.

CONCLUSION

Over the past few years, few cases have resulted in penalties for violating existing personal data and cybersecurity standards. However, the government has also slowly introduced an enforcement regime for the violation of rules on the protection of personal data and on cybersecurity. This includes administrative sanctions and, in extreme cases, authority to revoke the company's right to process data.

Will the government actively enforce its regulations? We do not know. But controlling conduct through a threat of enforcement is often a conscious government strategy. In theory, companies are motivated to comply and the government is motivated to ignore violations that are not flagrant.

In the end, businesses must prepare to move from the previous lightly-regulated legislative landscape of cybersecurity and privacy to a more vigorous environment.

RUSSIN & VECCHI

Le Ton Viet
LTViet@russinvecchi.com.vn

Viet is a member of the Asia Data Protection & Security Practice Group of Meritas. He has a particular focus on data security, marketing and advertising practices, international data transfer and other privacy and cybersecurity matters. He counsels a broad range of clients on data privacy regulation and breach response. Additionally, he represents clients in various transactions in the field of hotel management, real estate and insurance.

IHC Directory

Your 'at a glance' guide to some of the region's top service providers.

Practice Area key

- INV Alt' Investment Funds (inc. PE)
- COM Antitrust / Competition
- AV Aviation
- BF Banking & Finance
- CM Capital Markets
- REG Compliance / Regulatory
- CMA Corporate & M&A
- E Employment
- ENR Energy & Natural Resources
- ENV Environment
- FT FinTech
- INS Insurance
- IP Intellectual Property
- IA International Arbitration
- IF Islamic Finance
- LS Life Sciences / Healthcare
- LDR Litigation & Dispute Resolution
- MS Maritime & Shipping
- PF Projects & Project Finance (inc. Infrastructure)
- RE Real Estate / Construction
- RES Restructuring & Insolvency
- TX Taxation
- TMT Telecoms, Media & Technology

— Law Firms — ASIA

CAMBODIA

MAR & Associates
Tel: (855) 23 964 876, (855) 23 987 876
Email: borana@mar-associates.com
Contact: MAR Samborana (Mr.)
Website: www.mar-associates.com
CMA · E · IP · RE · REG

CHINA

Broad & Bright
Tel: (86) 10 8513 1818
Email: broadbright@broadbright.com
Contact: Mr Jun Ji (Jun_ji@broadbright.com)
Website: www.broadbright.com
COM · CMA · ENR · LDR · TMT

East & Concord Partners
Tel: (86) 10 6590 6639
Email: Beijing@east-concord.com
Contact: Mr. Dajin Li
Website: www.east-concord.com
BF · CM · CMA · IP · LDR

Llinks Law Offices
Tel: (86) 21 31358666
Email: master@llinkslaw.com
Website: www.llinkslaw.com
BF · CM · CMA · INV · LDR

W. K. To & Co.
Tel: (86) 10 8587 5076
Email: wktoco@wktoco.com
Contact: Cindy Chen
Website: www.wktoco.com
CMA · E · LDR · RE · REG

HONG KONG

Conyers Dill & Pearman
Tel: (852) 2524 7106
Email: hongkong@conyers.com
Contact: Christopher W.H. Bickley, Partner, Head of Hong Kong Office
Website: www.conyers.com
BF · CM · CMA · INV · LDR

Elvinger Hoss Prussen
Tel: (852) 2287 1900
Email: xavierlesourne_hk@elvingerhoss.lu
Contacts: Mr Xavier Le Sourne, Partner, Ms Charlotte Chen, Counsel
Website: www.elvingerhoss.lu
* Elvinger Hoss Prussen's Hong Kong office provides inbound and outbound legal services only under Luxembourg law
BF · CM · CMA · INV · TX

Vivien Teu & Co LLP
Tel: (852) 2969 5300
Email: Vivien.teu@vteu.co
Contact: Vivien Teu, Managing Partner
Website: www.vteu.co
BF · CM · CMA · INV · REG

W. K. To & Co.
Tel: (852) 3628 0000
Email: mail@wktoco.com
Contact: Vincent To
Website: www.wktoco.com
CMA · E · LDR · RE · REG

INDIA

Anand and Anand
Tel: (91) 120 4059300
Email: pravin@anandandanand.com
Contact: Pravin Anand - Managing Partner
Website: www.anandandanand.com
IP · LDR

Clasis Law
Tel: (91) 11 4213 0000, (91) 22 4910 0000
Email: info@clasislaw.com
Contacts: Vineet Aneja, Mustafa Motiwala
Website: www.clasislaw.com
CMA · E · LDR · REG · RES

ABNR (Ali Budiardjo, Nugroho, Reksodiputro)
Tel: (62) 21 250 5125/5136
Email: info@abnrlaw.com
infosg@abnrlaw.com
Contacts: Emir Nurmansyah, enurmansyah@abnrlaw.com)
Nafis Adwani, nadwani@abnrlaw.com
Agus Ahadi Deradjat, aderadjat@abnrlaw.com
Website: www.abnrlaw.com
BF · CM · CMA · ENR · PF

Emir Pohan & Partners
Tel: (62) 21 2965 1251
Email: emir.pohan@eplaw.id
Contact: Emir Pohan
Website: www.eplaw.id
COM · E · LDR · RES

Lubis Ganie Surowidjojo
Tel: (62) 21 831 5005, 831 5025
Email: lgs@lgslaw.co.id
Contacts: Dr. M. Idwan ('Kiki') Ganie
Website: www.lgslaw.co.id
CMA · COM · INS · LDR · PF

Makarim & Taira S.
Tel: (62) 21 5080 8300, 252 1272
Email: info@makarim.com
Contact: Lia Alizia
Website: www.makarim.com
BF · CMA · E · LDR · PF

Mochtar Karuwin Komar
Tel: (62) 21 5711130
Email: mail@mkklaw.net, ek@mkklaw.net
Contact: Emir Kusumaatmadja
Website: www.mkklaw.net
AV · CMA · ENR · LDR · PF

SSEK Legal Consultants
Tel: (62) 21 521 2038, 2953 2000
Email: ssek@ssek.com
Contact: Denny Rahmansyah - Managing Partner
Website: www.ssek.com
Twitter: @ssek_lawfirm
BF · CMA · E · ENR · RE

MALAYSIA

Adnan Sundra & Low
Tel: (603) 2070 0466
Email: enquiry@adnansundralow.com
Contacts: Deepak Sadasivan, Rodney D'Cruz
Website: www.asl.com.my
BF · CM · CMA · IF · PF

Azmi & Associates
Tel: (603) 2118 5000
Email: general@azmilaw.com
Contact: Dato' Azmi Mohd Ali - Senior Partner
Website: www.azmilaw.com
BF · CM · CMA · ENR · PF

Trowers & Hamlins LLP
Tel: (601) 2615 0186
Email: nwhite@trowers.com
Contact: Nick White – Partner
Website: www.trowers.com
BF · CMA · ENR · IF · PF

PHILIPPINES

ACCRALAW (Angara Abello Concepcion Regala and Cruz Law Offices)
Tel: (632) 830 8000
Email: accra@accralaw.com
Contacts: Emerico O. De Guzman, Ana Lourdes Teresa A. Oracion, Neptali B. Salvanera
Website: www.accralaw.com
CMA · E · IP · LDR · TX

DivinaLaw
Tel: (632) 822-0808
Email: info@divinalaw.com
Contact: Nilo T. Divina, Managing Partner
Website: www.divinalaw.com
BF · CMA · E · LDR · TMT

Morales & Justiniano
Tel: (632) 834 2551, (632) 832 7198, (632) 833 8534
Email: ramorales@primuslex.com
Contact: Mr. Rafael Morales - Managing Partner
Website: www.primuslex.com
BF · CM · CMA · IP · LDR

Ocampo & Suralvo Law Offices
Tel: (632) 625 0765,
Email: info@ocamposuralvo.com
Contact: Jude Ocampo
Website: www.ocamposuralvo.com
CMA · ENR · PF · TX · TMT

SyCip Salazar Hernandez & Gatmaitan
Tel: (632) 8982 3500, 3600, 3700
Email: sshg@syciplaw.com
Contact: Hector M. de Leon, Jr. - Managing Partner
Website: www.syciplaw.com
BF · CMA · E · ENR · PF

Villaraza & Angangco
Tel: (632) 9886088
Email: fm.acosta@thefirmva.com
Contact: Franchette M. Acosta
Website: www.thefirmva.com
CMA · IP · LDR · REG · RES

SINGAPORE

Joyce A. Tan & Partners
Tel: (65) 6333 6383
Email: joyce@joylaw.com
Contact: Joyce T. Tan - Managing Director
Website: www.joylaw.com
CMA · E · IP · LDR · TMT

SOUTH KOREA

Bae, Kim & Lee LLC
Tel: (82 2) 3404 0000
Email: bkl@bkl.co.kr
Contact: Kyong Sun Jung
Website: www.bkl.co.kr
BF · CMA · IA · LDR · RE

Kim & Chang
Tel: (82-2) 3703-1114
Email: lawkim@kimchang.com
Website: www.kimchang.com
COM · BF · CMA · IP · LDR

Yoon & Yang LLC
Tel: (82 2) 6003 7000
Email: yoonyang@yoonyang.com
Contacts: Jinsu Jeong, Junsang Lee, Myung Soo Lee
Website: www.yoonyang.com
COM · E · IP · LDR · TX

Yulchon LLC
Tel: (82-2) 528 5200
Website: www.yulchon.com
COM · CMA · IP · LDR · TX

TAIWAN

Deep & Far Attorneys-at-Law
Tel: (8862) 25856688
Email: email@deepnfar.com.tw
Contact: Mr. C. F. Tsai
Website: www.deepnfar.com.tw
COM · CM · E · IP · LDR

THAILAND

Chandler MHM Limited
Tel: (66) 2266 6485
Email: jessada.s@chandlermhm.com, satoshi.kawai@chandlermhm.com
Contacts: Jessada Sawatdipong, Satoshi Kawai
Website: www.chandlermhm.com
BF · CMA · ENR · PF · RE

Kudun & Partners Limited
Tel: (66) 2 838 1750
Email: info@kap.co.th
kudun.s@kap.co.th
chinawat.a@kap.co.th
pariyapol.k@kap.co.th
Contacts: Kudun Sukhumananda - Capital Markets, Corporate M&A, Banking & Finance
Chinawat Assavapokee - Tax, Corporate Restructuring, Insolvency
Pariyapol Kamolsilp - Litigation / Dispute Resolution
Website: www.kap.co.th
CMA · CM · LDR · RES · TX

Pisut and Partners Co., Ltd.
Tel: (66) 202 66226, 202 66227
Email: info@pisutandpartners.com
Contacts: Mr. Pisut Rakwong
Website: www.pisutandpartners.com
CM · CMA · E · LDR · RE

Warot Business Consultant Ltd.
Tel: (66) 81802 5698
Email: warot@warotbusinessconsultant.com
Contact: Mr. Warot Wanakankowit
Website: www.warotbusinessconsultant.com
CM · CMA · E · REG · TX

Weerawong, Chinnavat & Partners Ltd.
Tel: (66) 2 264 8000
Email: Veeranuch.t@weerawongcp.com
Contacts: Veeranuch Thammavaranucupt - Senior Partner
Website: www.weerawongcp.com
BF · CM · CMA · LDR · PF

VIETNAM

Bizconsult Law Firm
Tel: (84) 24 3933 2129
Email: info-hn@bizconsult.vn
Contact: Mr. Nguyen Anh Tuan - (84) 24 3933 2129
Website: www.bizconsult.vn
CM · CMA · LDR · RE · RES

Global Vietnam Lawyers LLC
Tel: (84) 28 3622 3555
Email: info@gvlawyers.com.vn
Contacts: Nguyen Gia Huy Chuong
Website: www.gvlawyers.com.vn
CMA · IP · LDR · RE · REG

Indochine Counsel
Ho Chi Minh Office:
Tel: (84) 28 3823 9640
Email: duc.dang@indochinecounsel.com
Contact: Mr Dang The Duc
Hanoi Office:
Tel: (84) 24 3795 5261
Email: hanoi@indochinecounsel.com
Website: www.indochinecounsel.com
CM · CMA · PF

Russin & Vecchi
Ho Chi Minh Office:
Tel: (84) 28 3824-3026
Email: lawyers@russinvecchi.com.vn
Contacts: Sesto E Vecchi - Managing Partner
Nguyen Huu Minh Nhut – Partner
Nguyen Huu Hoai – Partner
Hanoi Office:
Tel: (84) 24 3825-1700
Email: lawyers@russinvecchi.com.vn
Contact: Mai Minh Hang – Partner
Website: www.russinvecchi.com.vn
CMA · E · IP · INS · TMT

VILAF
Tel: (84) 28 3827 7300, (84) 24 3934 8530
Email: duyen@vilaf.com.vn, tung@vilaf.com.vn, anh@vilaf.com.vn
Contacts: Vo Ha Duyen, Ngo Thanh Tung, Dang Duong Anh
Website: www.vilaf.com.vn
BF · CMA · RE · ENR · LDR

— Law Firms — MIDDLE EAST

BAHRAIN

Trowers & Hamlins
Tel: (973) 1 751 5600
Email: bahrain@trowers.com
Contact: Louise Edwards - Office Manager
Website: www.trowers.com
BF · CMA · IF · LDR · RE

OMAN

Trowers & Hamlins
Tel: (968) 2 468 2900
Email: oman@trowers.com
Contact: Louise Edwards - Office Manager
Website: www.trowers.com
BF · CMA · LDR · PF · RE

UAE

Afridi & Angell
Email: dubai@afridi-angell.com
Contact: Bashir Ahmed - Managing Partner
Website: www.afridi-angell.com
BF · CMA · LDR · RE · REG

AMERELLER
Tel: (971) 4 432.3671
Email: gunson@amereller.com
Contact: Christopher Gunson
Website: www.amereller.com
CMA · E · IA · LDR · REG

Horizons & Co
Tel: (971) 4 354 4444
Email: info@horizlaw.ae
Contact: Adv. Ali Al Zarooni
Website: www.horizlaw.ae
CMA · E · LDR · PF · RE

Trowers & Hamlins LLP
Dubai office:
Tel: (971) 4 351 9201
Email: dubai@trowers.com
Contact: Jehan Selim - Office Manager
Abu Dhabi office:
Tel: (971) 2 410 7600
Email: abudhabi@trowers.com
Contact: Jehan Selim - Office Manager
Website: www.trowers.com
BF · CMA · LDR · PF · RES

— Law Firms — NORTH AMERICA

CANADA

Fasken Martineau
Tel: (416) 366-8381
Email: mstinson@fasken.com
Contact: Mark Stinson
Website: www.fasken.com
BF · CMA · ENR · LDR · TMT

Meyer Unkovic Scott
Tel: (412) 456 2833
Email: du@muslaw.com
Contact: Dennis Unkovic
Website: www.muslaw.com
CMA · IP · IA · LDR · RE

— Law Firms — AFRICA

JOHANNESBURG

Fasken Martineau
Tel: (27) 11 586 6000
Email: johannesburg@fasken.com
Contact: Blaize Vance - Regional Managing Partner
Website: www.fasken.com
CMA · E · ENR · LDR · PF

— Arbitration — Services

Beijing Arbitration Commission / Beijing International Arbitration Center (Concurrently use)
Tel: (86) 10 85659558
Email: xujie@bjac.org.cn
Contact: Mr. Terence Xu（許捷）
Website: www.bjac.org.cn

Hong Kong International Arbitration Centre
Tel: (852) 2525 2381
Email: adr@hkiac.org
Website: www.hkiac.org

Maxwell Chambers Pte Ltd
Tel: (65) 6595 9010
Email: info@maxwell-chambers.com
Website: maxwell-chambers.com

Shenzhen Court of International Arbitration (Shenzhen Arbitration commission)
Tel: (86) 755 83501700, (86) 755 25831662
Email: info@scia.com.cn
Website: www.scia.com.cn

Alternative Legal Service Providers

LOD - Lawyers On Demand
Tel: (65) 6326 0200
Email: singapore@lodlaw.com
Contact: Oliver Mould
Website: lodlaw.com

KorumLegal
Email: Titus.Rahiri@korumlegal.com
Contact: Titus Rahiri
Website: www.korumlegal.com

Vario from Pinsent Masons (HK) Ltd
Tel: (852) 2294 3454
Email: enquiries@pinsentmasonsvario.com
Website: https://pinsentmasonsvario.com

Risk, Investigation — and Legal — Support Services

LegalComet Pte Ltd (LEGALCOMET)
Tel: (65) 8118 1175
Contact: Michael Lew, Founder & CEO
Email: michael@legalcomet.com
Website: www.legalcomet.com

Mintz Group
Tel: (852) 3427 3717
Contacts: Jingyi Li Blank
Email: jblank@mintzgroup.com
Website: www.mintzgroup.com

— Legal — Recruitment

Hughes-Castell
Tel: Hong Kong (852) 2520 1168
Singapore (65) 6220 2722
Beijing (86) 10 6581 1781
Shanghai (86) 21 2206 1200
Email: hughes@hughes-castell.com.hk
Website: www.hughes-castell.com

ALS International
Tel: Hong Kong – (852) 2920 9100
Singapore – (65) 6557 4163
Beijing – (86) 10 6567 8729
Shanghai – (86) 10 6372 1098
Email: als@alsrecruit.com
Website: alsrecruit.com

Lewis Sanders
Tel: (852) 2537 7410
Email: recruit@lewissanders.com
Website: www.lewissanders.com

Horizon Recruitment
Tel: Singapore – (65) 6808 6635
Hong Kong – (852) 3978 1369
Email: Jessica.deery@horizon-recruit.com
Website: www.horizon-recruit.com

Jowers Vargas
Tel: (852) 5808-4137
Email: alexis@evanjowers.com
Website: https://www.evanjowers.com/

— Non-Legal — Recruitment

True Recruitment Asia
Tel: (852) 5325 9168
WhatsApp: (852) 5325 9168
Email: kannan@truerecruitmentasia.com

— Meditation —

Kadampa Meditation Centre Hong Kong

KMC HK is a registered non-profit organisation. We offer systematic meditation and study programmes through drop-in classes, day courses, lunchtime meditations, weekend retreats and other classes.

Tel: (852) 2507 2237
Email: info@meditation.hk
Website: www.meditation.hk

— Sport & Leisure —

Splash Diving (HK) Limited

Learn to Dive and Fun Dive with the Winner of the PADI Outstanding Dive Centre/Resort Business Award!

Tel: (852) 9047 9603, (852) 2792 4495
Email: info@splashhk.com
Website: www.splashhk.com

— Charitable — Organisations

Impact India Foundation

An international initiative against avoidable disablement. Promoted by the UNDP, UNICEF and the World Health Organization in association with the Government of India.

Tel: (91) 22 6633 9605-7
Email: nkshirsagar@impactindia.org
Website: www.impactindia.org

mycareerinlaw.com™

The **best** opportunities from top legal recruiters