Recent corporate governance and data protection developments in the APAC region

Diligent

Corporate governance is a framework of rules, standards and operating procedures applicable to the management of organisations that also seeks to balance the interests of an organisation's many stakeholders. And it is an issue of increasing urgency and significance across Asia-Pacific – a region impacted by a number of multilateral economic initiatives.

These include the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, a 2018 free-trade agreement between Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, Peru, New Zealand, Singapore and Vietnam and the Asia Region Funds Passport, a multilaterally agreed framework to facilitate the cross-border marketing of managed funds across participating Asian-region economies led by Australia, New Zealand, the Republic of Korea and Singapore, with Japan, Thailand and Australia already able to receive registration applications from foreign and local passport funds.

With the region made up of a diverse range of economies of varying sizes and levels of development, and each subject to non-uniform laws, policy, regulations and governments, increasing corporate governance standards across the board remains a critical challenge for the region. Data, end-user and supply chain security, data and documentation management, and regulatory compliance and disclosure continue to represent key challenges for APAC-based companies.

This white paper provides an overview of recent developments in the corporate governance landscape in Asia, with a focus on five specific jurisdictions: Hong Kong, Singapore, Thailand, Malaysia and India.

HONG KONG

A key financial centre in the region and globally, Hong Kong's corporate governance issues stem from matters such as:

- Unclear delineation of regulatory responsibilities between the Hong Kong Securities and Futures Commission (**SFC**) and the Stock Exchange of Hong Kong Limited (**SEHK**), known as the 'dual responsibilities model'
- The role of the board and the quality of disclosures.
- The ability of shareholders and regulators to seek redress from issuers and their directors where corporate governance standards have been breached.

Regulations

Recent regulatory developments from the SEHK over the past six to 12 months include:

- Amendments to the Corporate Governance Code and related Listing Rules to take effect on 1 January 2019, including strengthening the transparency and accountability of the board and/or nomination committee regarding director elections; including Independent Non-Executive Directors (**INED**) on the board; imposing minimum annual meeting requirements for the chairman and INED; enhancing the independence criteria for assessing potential INED and upgrading board diversity requirements to make them mandatory.
- Updated Environmental, Social and Governance (**ESG**) guidance materials to address the increasing demand for ESG information disclosure from listed companies.
- Changes to the Growth Enterprise Market (**GEM**) and Main Board Listing Rules (effective 15 February 2018), repositioning GEM as the market for small to medium-sized companies. The listing thresholds for both the Main Board and GEM were increased, with higher market capitalisation requirements of HK$500 million (Main Board) and HK$150 million (**GEM**).

Governance

- A 2018 Hong Kong Corporate Governance review found that less than half of the companies comprising the Hang Seng Composite Index (**HSCI**) (44%) were in full compliance with the Corporate Governance Code, a decreased compliance rate from 2017 (46%). Hong Kong's performance, in comparison to other major financial centres such as London, is considered poor, and increasing corporate governance effectiveness in the areas of information technology controls, cybersecurity and data privacy are key current concerns for regulators.

HONG KONG continued

Security

This increased focus on IT controls, cybersecurity and data privacy has arisen, in part, from increased reliance on digitisation and cloud and mobile computing, the recent enactment of the European Union General Data Protection Regulation (**GDPR**) and several recent data security breaches involving Hong Kong companies including:

- The cyberattack on Cathay Pacific that resulted in the personal information (including names, nationalities, dates of birth, telephone numbers, email and physical addresses, passport and identity card numbers) of roughly 9.4 million customers of the airline being compromised in March 2018 but not being reported to the HK Privacy Commissioner until October 2018;
- the loss by Hong Kong's Registration and Electoral Office of two laptops holding the personal information of 3.7 million voters during the election of Hong Kong's chief executive in March 2017; and
- a series of cyberattack incidents affecting more than half a million people related to an inactive database owned by Hong Kong Broadband Network.

A recent study has reported that almost half (48%) of the Hong Kong organisations surveyed have either experienced a cybersecurity incident (23%) or cannot be certain if one occurred due to a failure to perform a proper data breach assessment (25%). A 2018 digital security report found that Hong Kong companies and residents lost more than HK$2 billion to cybercriminals in the first nine months of 2018, while businesses sustained more than 9,000 cyberattacks as cybercriminals increasingly targeted the jurisdiction (ranked in the top five global destinations for cybercrime).

Considering recent SFC and Hong Kong Monetary Authority circulars on cybersecurity risk, and the May 2017 SFC Consultation Paper on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading, Hong Kong boards must prioritise the issues of IT controls, cybersecurity and data privacy in defending against the current crop of expected threats in 2019, including:

- Advanced Persistent Threats (or **APTs**);
- supply chain attacks;
- botnets;
- mobile malware; and
- end-user attacks (e.g. social media, phishing, whaling).

These can give rise to material, financial, systemic, operational and reputational harm.

SINGAPORE

Regulations

Singapore was recently ranked the fourth top financial centre in the world by the Global Financial Centres Index (**GFCI**), just behind Hong Kong (3rd), London (2nd) and New York (1st).

The Monetary Authority of Singapore (**MAS**) has recently noted that with technology transforming the production, delivery and consumption of financial services, Singapore's financial sector must also transform to stay relevant and competitive.

Recent regulatory developments include:

- MAS issuing guidance for financial institutions (**FIs**) on the use of innovative technology solutions to facilitate safe, non-face-to-face customer onboarding, identification and verification (e.g. biometric identification, real-time videoconferencing and secure digital signature using Public Key Infrastructure-based credentials).
- MAS issuing a Consultation Paper on the Proposed E-payments User Protection Guidelines, which will apply to an FI that issues a payment account that is capable of being used for electronic payment transactions. Among other things, FIs should have in place procedures to notify account users of transactions on their accounts.
- MAS and the Singapore Exchange (**SGX**) issuing changes to the SGX Listing Manual (Mainboard and Catalist) and the Singapore Code of Corporate Governance (**Code**) on 6 August 2018, to take effect on and from 1 January 2019, with the aim of strengthening the Code's core tenets of good governance for listed companies.
- The enactment of the Cybersecurity Act in March 2018, which created a regulatory framework for the monitoring and reporting of cybersecurity threats to critical sectors of essential services in Singapore (including health, government, banking and finance, security, media) through a Commissioner of Cybersecurity, and a licensing regime requiring certain data security service providers in Singapore to be registered.
- The establishment in 2018 of an 'SGX Fast Track' program to recognise listed companies that have a strong corporate governance standing and compliance track record. These companies are able to access prioritised clearance for corporate action submissions to the regulator.

Governance

While the Singapore Governance and Transparency Index, a measure of corporate governance in Singapore, was at a solid rate of 56.3 in 2018, up from 52.3 in 2017 and from 33.9 (on establishment), inadequate disclosures can mask deep-seated compliance issues. The changes to the Code aim to:

- Provide clearer guidance on matters such as director independence and director remuneration;
- improve stakeholder engagement generally; and
- improve assurance systems and stakeholder engagement through ESG reporting.

SINGAPORE continued

Security

The risk vectors for threat relevant to Hong Kong (discussed above) are also relevant to Singapore. Recent data security or privacy breaches affecting Singapore include:

- In 2014, the personal information of over 300,000 customers of karaoke company K Box being made publicly available.
- In 2014, over 1,500 SingPass accounts (allowing citizens to manage, for example, their taxes and applications for state subsidies) were compromised.
- A cyberattack carried out against SingHealth's patient database from August 2017 to July 2018 which resulted in the personal data of 1.5 million SingHealth patients, and the outpatient medical data of some further 160,000 patients, being compromised.

In relation to the SingHealth cyberattack, a review committee found, among other things, that:
Staff lacked adequate levels of cybersecurity awareness, training and resources to understand the implications of the attack and respond effectively.

- While IT administrators were able to identify suspicious attempts to log into the database, the same administrators failed to recognise these as an advanced cyberattack.
- There was no framework around incident reporting, staff training or the need to escalate the issue to the Cyber Security Agency of Singapore.

THAILAND

Regulations

In October 2018, the Thai Office of Insurance Commission (**OIC**) published the draft *Notifications re: Corporate Governance of Life and Non-Life Insurance Companies* (**Draft CG Notifications**), legislation specifically aimed at regulating corporate governance in Thailand. To date, there has been a lack of legislation clearly describing the key requirements for good corporate governance in that jurisdiction and the Draft CG Notifications are intended to cover issues such as:

- the composition and qualifications of the board of directors of insurance companies, including maintaining a certain number of independent directors; and
- insurance companies maintaining a written good corporate governance framework that is approved by its board of directors and reviewed by the OIC. This framework must include the company's policies and strategies on appropriate checks and balances and the maintenance of supervisory systems.

Board composition provisions will take effect on 1 January 2020, with the other provisions expected to take effect at an earlier date.

In 2017, the Thai Securities and Exchange Commission (**SEC**) also published a new edition of its *Corporate Governance Code for Listed Companies* **(Thai CG Code**) together with a new *Investment Governance Code for Institutional Investors* **(IG Code**).

Among other things, the Thai CG Code requires a company's board to conduct and record an annual internal review of the implementation of the Thai CG Code. Effective from 2018, a Thai listed company is required to disclose in its annual report a board acknowledgement that it has considered and reviewed the Thai CG Code by means suitable to the company's business. Thai CG Code implementation may be taken to be an indicator of proper performance of board duties and responsibilities.

Broadly, the Thai IG Code (a principles-based code adopted by the Thai SEC) sets out measures for institutional investors who have investment management responsibilities to ensure delivery of sustainable long-term value to their investment owners and beneficiaries. Among other things, institutional investors are encouraged to invest in companies that integrate ESG factors into their business practices and to engage with investee companies to improve the company's ESG performance. The Thai IG Code is intended to promote and contribute to a good corporate governance ecosystem.

Further, on 28 February 2019 the *Personal Data Protection Act* was finally approved by the Thai National Legislative Assembly. The Act is intended to regulate both data controllers and data processors, *whether or not domiciled in Thailand*, who collect, use or disclose personal data collected from individuals in Thailand (whether Thai citizens or not). While not yet effective, organisations should note that it will have, among other things, extraterritorial applicability, notification and consent requirements

THAILAND continued

(particularly in relation to sensitive data), restrictions and exemptions for the collection, use, disclosure and cross-border transfer of personal data and cover security measures, data breaches and breach notification. While having drawn some concepts from the EU GDPR, compliance with the GDPR does not necessarily mean compliance with the Thai Act.

Governance

The Thai Institute of Directors in its *Corporate Governance Report of Thai Listed Companies 2016*, noted that one of the key governance issues for Thai listed boards is an integration of sustainability and corporate responsibility with the company's business strategies and conventional fiduciary duties. In collaboration with the Thai Stock Exchange and SEC, the Institute found that the corporate governance practices of Thai listed companies, on average, exhibited an improvement in their corporate governance practices overall and in all corporate governance categories in 2016.

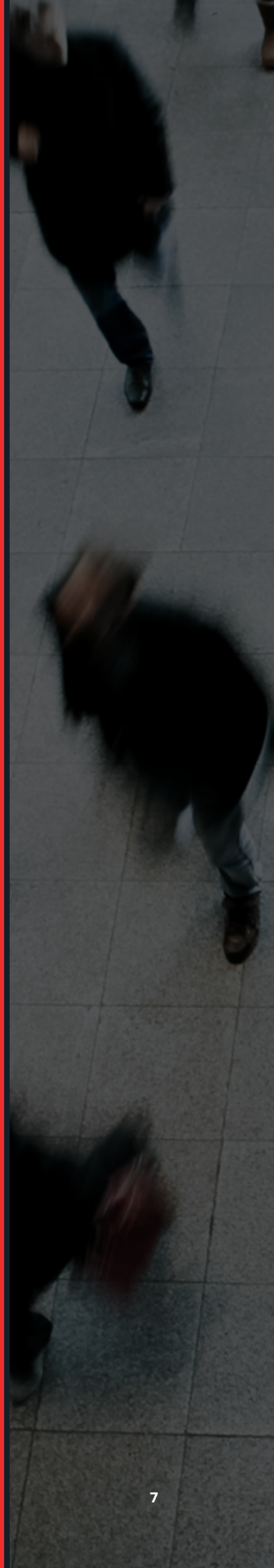
However, it remains to be seen how very recent changes to the Thai regulatory landscape will impact upon Thailand's standing in the APAC region regarding compliance with corporate governance principles and standards.

Security

The risk vectors for threats relevant to Hong Kong and Singapore (discussed above) are very relevant to Thailand, which experienced recent major data security or privacy breaches including:

- The 2018 cyberattacks on two Thai commercial banks (Kasikornbank and Krung Thai Bank) which resulted in the stolen customer data of at least 123,000 customers (including approximately 3,000 corporate customers).
- The 2018 data breach at Thai mobile operator True Corporation affecting 11,400 customers (including access to copies of their national identification cards).
- The 2018 data security threat affecting more than 10,000 Thai subscribers to TrueMove H, a Thai mobile-phone firm.
- In 2016, social media users discovering that a database with the names, addresses, job titles and passport numbers of more than 2,000 foreign nationals living in Thailand's southern province was widely available online, which also featured a digital map pinpointing the expats' location and their personal details.

Incidents such as these, going forward, will test the effectiveness of the new *Thai Personal Data Protection Act* when it comes into force.



MALAYSIA

Regulations

The Malaysian Securities Commission (**MSC**) released the new *Malaysian Code on Corporate Governance* (**MCCG**) on 26 April 2017, which took effect immediately. All public listed companies are required to disclose compliance with the MCCG in their annual reports while other types of Malaysian companies (e.g. non-listed, SME or state-owned) are encouraged to adopt the MCCG, which introduces a new set of best practices aimed at 'internationalisation' of Malaysia's corporate governance culture and enhancing greater accountability, transparency and sustainability. Part of the MCCG's aim to boost corporate governance standards include:

- two-tier voting processes for appointments of long-serving independent directors (beyond 12 years), with specific voting requirements for controlling shareholders and non-controlling shareholders; and
- a requirement of at least 30% women directors on the board, with the recommendation that non-listed companies should also work to encourage female participation in senior management.

Governance

The corporate governance culture in Malaysia has also been strengthened by the recent establishment of the Institute of Corporate Directors (launched 1 October 2018) and the MSC's stated intention to establish a Corporate Governance Council to drive corporate governance initiatives.

In terms of Malaysia's data privacy laws, the *Personal Data Protection Act 2010* currently only covers the inappropriate use of personal data for commercial purposes and has no extraterritorial application where personal data is processed outside Malaysia, although a government source has indicated that the Malaysian government is committed to a review of its data protection laws by mid-2019 to prevent data breaches (of the kind discussed in the "Security" section below) from recurring.

Security

Malaysia has not only been hit by several critical cyberattacks, it has also been identified as one of the major global operational bases from which hackers launch malware attacks. Malaysia has experienced recent major data security or privacy breaches including:

- a 2014 data breach that resulted in the personal details of over 46 million mobile-number subscribers in Malaysia (including home addresses, identification card numbers, dates of birth and SIM card information of both citizens and foreign residents) being leaked for sale (now the subject of a civil suit against the Malaysian Communications and Multimedia Commission and Nuemera (M) Sdn Bhd, which managed the compromised Public Cellular Blocking Service);
- the leaking of 81,309 records from the Malaysian Medical Council, Malaysian Medical Association and Malaysian Dental Association; and
- the information of 220,000 Malaysians and their next of kin, regarding organ donation, becoming publicly available.

Incidents like these only serve to emphasise the necessity for an urgent review of the country's outdated data privacy laws.

INDIA

Regulations

To date, India, a highly digitised and data-based economy, has not had specific data protection laws.

In response, the Central Government of India set up the Srikrishna Committee to consider the challenges surrounding data protection, privacy and management in India. In late 2018, the committee handed down its assessment and recommendations including a draft piece of legislation entitled the *Personal Data Protection Bill 2018*. The draft data protection bill takes into account key approaches to data protection from three overseas jurisdictions: the US (a sectoral approach), the regulatory approach of the European Union's GDPR and China's approach to data protection (aimed at averting national security risks).

Among other things, the draft Indian bill introduces the concepts of *data principals* (e.g. individuals) and *data fiduciaries* (e.g. organisations). Data principals will be granted certain rights (e.g. the rights to access, correction, data portability) while data fiduciaries in India and data fiduciaries offering goods and services to data principals in India, or performing any activity that involves profiling of data principals within India, will have compliance obligations under the proposed legislation.

While not yet enacted, the proposed legislation envisions an overarching data protection framework spearheaded by a centralised Data Protection Authority. The proposed law will seek to enforce limitations on collection and data storage, increase transparency, require security safeguards and better define 'personal data', including sensitive personal data.

Governance

Commentators have noted that India's corporate governance landscape faces unique challenges due to the predominance of family-run businesses and the common practice of promoters acting as 'independent' directors in each other's companies, or appointing relatives as 'independent' directors.

In June 2017, the Securities and Exchange Board of India (**SEBI**) formed a committee under the chairmanship of Uday Kotak with the aim of improving corporate governance standards for listed Indian companies. SEBI accepted 69% of the recommendations in the resulting *Kotak Report* in March 2018, which included that the *SEBI (Listing Obligations and Disclosure Requirements) Regulations* be amended so that:

- persons who are part of the 'promoter group' of a listed company cannot be appointed as independent directors. There will also be a clamp-down on common non-independent directors on boards of listed companies;
- boards of top 500 listed companies will now be required to have at least one woman as an independent director (from 1 April 2019); and
- boards of top 1,000 listed companies will now be required to have at least one woman as an independent director (from April 1st 2020).

INDIA continued

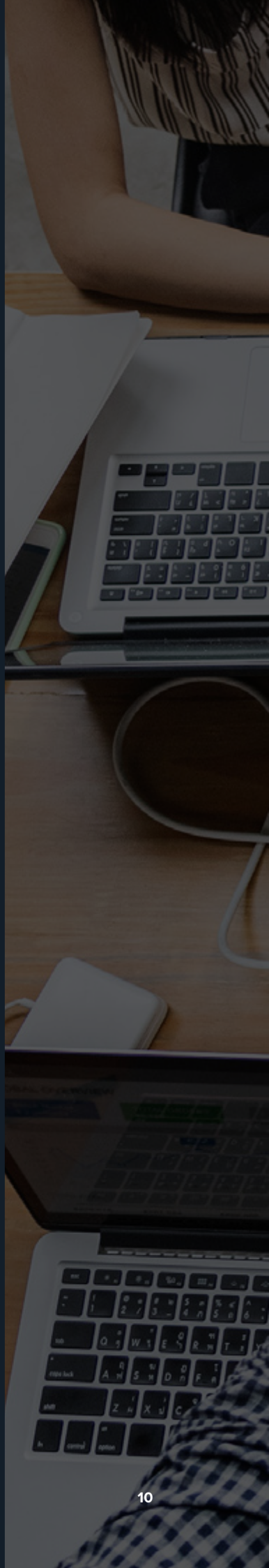
Security

According to a recent global report released in October 2018, India is only second to the United States (at 57%) as a target for cyberattacks, representing 37% of global breaches in terms of data compromised, stolen or leaked. The risk vectors for threats relevant to Hong Kong, Singapore, Thailand and Malaysia (discussed above) are extremely pertinent to India, which has experienced recent major data security or privacy breaches including:

- During the first six months of 2018, the compromising of almost 1 billion records in a breach incident affecting the national Aadhaar database, the world's largest biometric database to which more than a billion Indian citizens have uploaded their biometric details (including photos, fingerprints and iris scans) in exchange for a unique 12-digit ID. Name, address and other personally identifiable information was compromised in the breach.
- Between April 2017 and January 2018, over 22,000 Indian websites (114 of these government portals) being hacked including a May 2017 incident involving the personal data of millions of Indians registered with the Employees' Provident Fund Organisation.

On the corporate governance front, India has also recently experienced some large-scale corporate governance scandals involving issues of conflict of interest or insider trading including:

- The ICICI Bank's female former managing director and CEO, Chanda Kochhar, resigning from her post in October 2018 in the wake of allegations of loan fraud (high-value loans approved in favour of companies connected with family members).
- SEBI requiring the listed Axis Bank, India's fourth-largest private-sector lender, to strengthen its internal processes and systems after price-sensitive information regarding financial results leaked on WhatsApp before official announcement to the stock exchange. Similar leaks occurred in relation to other listed companies including Cipla Limited, HDFC Bank Limited and Tata Steel Limited.



CONCLUSION

What is clear from this overview of five key jurisdictions in the region is that the trend towards strengthening standards of corporate governance is only intensifying, providing a source of competitive advantage in dealing with more developed nations across the globe.

What's also disturbingly clear is that corporate regulators in APAC, along with the companies they oversee, are struggling to keep pace with the threat vectors affecting their increasingly digitised economies and diverse populations.

Just as the industries of each of these economies must respond to these threats with increased security technology, resources and infrastructure dedicated to data security (such as encryption of board-level communications, offsite data hosting, biometrics and dedicated incident-response teams), so too must regulators keep pace with the rate of technological change in order to minimise security and network-wide threats posed to their nations by cybercriminals.

Diligent is the pioneer in modern governance. We empower leaders to turn governance into a competitive advantage through unparalleled insight and highly secure, integrated SaaS applications, helping organisations thrive and endure in today's complex, global landscape. Our trusted, cloud-based applications streamline the day-to-day work of board management and committees, support collaboration and secure information sharing throughout the organisation, manage subsidiary and entity data, and deliver the insights and information leaders need to mitigate governance deficits and seize new opportunities.

The largest global network of corporate directors and executives, Diligent is relied on by more than 16,000 organisations and 650,000 leaders in in over 90 countries. With award-winning customer service across the globe, Diligent serves more than 50% of the Fortune 1000, 70% of the FTSE 100, and 65% of the ASX.

For more information or to request a demonstration, please contact us by:

Phone: **+65 6932 2638**
Email: **info@diligent.com**
Visit: **diligent.com/au**

REFERENCES

1. https://thediplomat.com/2018/02/what-now-for-economic-integration-in-the-asia-pacific/
2. https://dfat.gov.au/trade/agreements/in-force/cptpp/Pages/comprehensive-and-progressive-agreement-for-trans-pacific-partnership.aspx
   https://www.bbc.com/news/business-43326314
3. http://fundspassport.apec.org/
4. http://fundspassport.apec.org/2019/02/01/the-asia-region-funds-passport-is-live/
5. http://www.asiabriefing.com/news/2014/07/corporate-governance-challenges-asia-pacific/
   https://www.opengovasia.com/cybersecurity-predictions-for-2019/
6. https://www.hkicpa.org.hk/-/media/HKICPA-Website/HKICPA/section5_membership/Professional-Representation/corporate-governance/HKICPA_CG_Report_on_Improving_Corporate_Governance_in_Hong_Kong.pdf
   https://www.law.ox.ac.uk/business-law-blog/blog/2018/06/recommendations-improve-hong-kongs-corporate-governance-system
7. https://www.bakermckenzie.com/-/media/files/insight/publications/2018/08/al_china_corporategovernancecodeined_aug18.pdf?la=en
8. https://globalcompliancenews.com/sehk-releases-esg-report-disclosure-environmental-information-20181129/
9. https://www.charltonslaw.com/amendments-to-hkex-main-board-and-gem-listing-rules-take-effect-on-15-february-2018/
10. http://www.grantthornton.cn/uploadfile/2018/1224/20181224045200331.pdf
11. https://www.scmp.com/business/companies/article/2124514/more-half-hong-kong-listed-companies-do-not-meet-corporate
12. https://diligent.com/au/cathay-pacific-cybersecurity-breach/
13. https://www.scmp.com/news/hong-kong/transport/article/2170259/worried-after-cathay-pacifics-data-breach-heres-all-you
14. https://thelawreviews.co.uk/edition/1001264/the-privacy-data-protection-and-cybersecurity-law-review-edition-5
15. Ibid
16. https://news.microsoft.com/en-hk/2018/06/14/cybersecurity-threats-to-cost-organizations-in-hong-kong-us32-billion-in-economic-losses/
17. https://www.scmp.com/news/hong-kong/law-and-crime/article/2177062/financial-losses-hk22-billion-and-more-9000
18. https://www.opengovasia.com/cybersecurity-predictions-for-2019/
19. https://sbr.com.sg/financial-services/news/heres-why-singapore-cant-beat-hong-kongs-financial-centre-ratings
20. https://www.reuters.com/article/us-singapore-economy-banking/singapore-unveils-plan-to-bolster-its-status-as-an-asian-financial-hub-idUSKBN1CZ0HE
21. https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-asia-pacific-financial-services-regulatory-update-feb-18-150318.pdf
    http://www.mas.gov.sg/News-and-Publications/Media-Releases/2018/MAS-Encourages-Financial-Institutions-to-Use-Technology-to-On-Board-Customers-More-Efficiently.aspx
22. https://www.lexology.com/library/detail.aspx?g=4e018cdf-0a91-4494-b647-1a884ebe0fa9
23. https://home.kpmg/content/dam/kpmg/sg/pdf/2018/10/Singapore-Corporate-Governance-Changes-Fact-Sheet.pdf
24. https://www.dataprotectionreport.com/2018/09/singapores-new-cybersecurity-act-come-into-force-heres-what-you-need-to-know/
25. https://www.csa.gov.sg/legislation/cybersecurity-act
26. https://sbr.com.sg/markets-investing/news/sgx-regco-launches-list-firms-good-corporate-governance
27. http://thinkbusiness.nus.edu/article/governance-reforms-lack-bite-if-compliance-is-not-enforced/
28. http://thinkbusiness.nus.edu/article/governance-reforms-lack-bite-if-compliance-is-not-enforced/
29. https://www.rsm.global/singapore/insights/our-expert-insights/key-changes-singapore-code-corporate-governance-related-listing-rules-1
    https://www.twobirds.com/en/news/articles/2018/singapore/a-new-spin-to-corporate-governance-in-singapore-2018
30. https://newnaratif.com/research/singapores-flawed-data-privacy-regime/

REFERENCES

31. Ibid
32. https://www.zdnet.com/article/singhealth-breach-review-recommends-remedies-that-should-already-be-basic-security-policies/
33. https://globalcompliancenews.com/thailand-corporate-governance-for-the-board-of-directors-of-insurance-companies-20180920/
34. http://www.cgthailand.org/microsite/documents/cgcode.pdf#page=67
35. http://www.cgthailand.org/microsite/ii_en.html
36. https://www.bakermckenzie.com/en/insight/publications/2019/03/the-first-thailand-personal-data
37. https://www.dataprotectionreport.com/2018/08/overview-of-thailand-draft-personal-data-protection-act/
38. https://www.bakermckenzie.com/en/insight/publications/2019/03/the-first-thailand-personal-data
39. Ibid
40. http://www.thai-iod.com/imgUpload/CGR%202016%20Report(1).pdf
41. http://www.thai-iod.com/imgUpload/CGR%202016%20Report(1).pdf
42. http://www.khaosodenglish.com/news/business/2018/08/01/massive-data-breach-hits-two-major-thai-banks/
43. https://iapp.org/news/a/thai-mobile-operator-announces-data-breach/
44. http://www.nationmultimedia.com/detail/opinion/30343532
45. https://www.cio.com/article/3293060/the-biggest-data-breaches-in-the-asean-region.html?page=2
46. https://www.bakermckenzie.com/en/insight/publications/2017/04/malaysian-code-corporate-governance
https://www.hg.org/legal-articles/the-malaysian-code-on-corporate-governance-mccg-48962
47. https://icdm.com.my/about-us
48. https://www.sc.com.my/news/media-releases-and-announcements/sc-releases-new-malaysian-code-on-corporate-governance-to-strengthen-corporate-culture
49. https://www.nst.com.my/opinion/columnists/2019/02/459321/data-privacy-laws-malaysia-has-long-way-go
50. https://www.cio.com/article/3293060/the-biggest-data-breaches-in-the-asean-region.html
51. https://www.thestar.com.my/news/nation/2017/10/31/msia-sees-biggest-mobile-data-breach-over-46-million-subscribed-numbers-at-risk-from-scam-attacks-an/; https://asiancorrespondent.com/2018/02/malaysian-govt-sued-data-breach-affecting-millions/
52. http://www.businessworld.in/article/The-Personal-Data-Protection-Bill-2018-An-Answer-To-India-s-Data-Protection-Issues-/01-01-2019-165633/
53. https://www.forbes.com/sites/sindhujabalaji/2018/08/03/india-finally-has-a-data-privacy-framework-what-does-it-mean-for-its-billion-dollar-tech-industry/#d19854c70fe8; http://www.businessworld.in/article/The-Personal-Data-Protection-Bill-2018-An-Answer-To-India-s-Data-Protection-Issues-/01-01-2019-165633/
54. https://iapp.org/news/a/understanding-indias-draft-data-protection-bill/
55. https://iapp.org/news/a/understanding-indias-draft-data-protection-bill/
56. http://www.businessworld.in/article/The-Personal-Data-Protection-Bill-2018-An-Answer-To-India-s-Data-Protection-Issues-/01-01-2019-165633/
57. https://privateclient.cyrilamarchandblogs.com/2018/04/indias-tough-new-corporate-governance-regime-impact-promoters/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original
58. Ibid
59. https://www.financialexpress.com/industry/technology/data-breach-in-india-second-highest-after-us-in-h12018-gemalto/1350406/
60. https://www.sbs.com.au/news/what-is-aadhaar-india-s-controversial-billion-strong-biometric-database
61. https://qz.com/india/1325647/data-breaches-cost-indian-companies-millions-of-dollars-says-ibm-study/
62. https://www.businesstoday.in/top-story/chanda-kochhars-fall-from-grace-here-is-how-she-was-caught-step-by-step/story/321344.html
63. https://economictimes.indiatimes.com/markets/stocks/news/whatsapp-leak-case-sebi-likely-to-pass-order-on-axis-bank/articleshow/62270452.cms