Bird & Bird ATMD

Cybersecurity & Singapore

Disclosures for Listed Companies

July 2019

*With the spate of cybersecurity incidents on large listed companies, cybersecurity risk has increasingly become a key point that affects investor risk appetite and companies are now subject to certain disclosure requirements in respect of such. This fourth article in our **Cybersecurity & Singapore** series briefly discusses these disclosure requirements for companies which are intending to list on the Singapore Exchange Securities Trading Limited ("**SGX-ST**"), as well as those which are already listed on the SGX-ST, specifically those in relation to cybersecurity risks and incidents.*

Requirements for Companies Intending to List

A company which is intending to list on the SGX-ST will have to issue a prospectus containing the particulars listed under the Fifth Schedule ("**Fifth Schedule**") of the Securities and Futures (Offers of Investments)(Securities and Securities-Based Derivatives Contracts) Regulations 2018. In particular, Part IV Paragraph 15 of the Fifth Schedule provides that a company is to "disclose, in a specific section with the heading "Risk Factors", the risk factors that are specific to the relevant corporation and its industry as well as the shares or units of shares, as the case may be, being offered, which had materially affected or could materially affect, directly or indirectly, the relevant corporation's financial position and results and business operations, and investments by holders of shares or units of shares, as the case may be, in the relevant corporation. Where possible, state the extent to which the relevant corporation's financial position or results had been or could be affected by the risk factor." Based on this, a disclosure is required if a company is likely to be exposed to any cybersecurity risk, as well as where cybersecurity incidents had happened in the past which impacted the company.

A listing applicant would also have to disclose information regarding any significant factor, including any unusual or infrequent event or new development, which materially affected its profit or loss before tax, and indicate the extent to which such profit or loss was so affected. Additionally, a listing applicant would need to disclose any known trends, uncertainties, demands, commitments or events that are reasonably likely to have a material effect on net sales or revenues, profitability, liquidity or capital resources for at least the current financial year, or that may cause financial information disclosed to be not necessarily indicative of its future operating results or financial condition. As such, if there are material costs or a significant risk of material costs associated with cybersecurity incidents, these should be discussed in the prospectus as well. The array of costs associated with cybersecurity issues could include the immediate costs of the incident, the costs associated with implementing preventative measures, maintaining insurance, responding to

litigation and regulatory investigations and engaging in remediation efforts.

Where the listing applicant is involved in any litigation or arbitration proceedings, including those which are known or contemplated, which may have, or which have had in the 12 months immediately preceding the date of lodgment of the prospectus, a material effect on the financial position or profitability on it, this has to be disclosed in the prospectus. This requirement includes any proceedings relating to cybersecurity issues.

A company is also expected to implement internal controls and risk management systems in respect of information technology and other areas. In this regard, the listing manuals of the SGX-ST ("**Listing Manual**") further require that a prospectus or an offer document must include (i) the board's comment on the adequacy and effectiveness of the issuer's internal controls (including financial, operational, compliance and information technology controls) and risk management systems; (ii) a statement on whether the audit committee concurs with the board's comment; and (iii) where material weaknesses are identified by the board or audit committee, they must be disclosed together with the steps taken to address them. In Singapore, companies which intend to list will typically appoint an internal auditor to review its internal contorls and risk management systems for its assurance and will rectify any areas of material weaknesses prior to listing.

Requirements for Listed Companies

On an ongoing basis, a listed company has to establish and maintain an effective internal audit function that is adequately resourced and independent of the activities it audits. The audit commttee's comment on whether the internal audit function is independent, effective and adequately resourced has to be disclosed in its annual report. Additionally, a listed company will also have to include in its annual report (i) the board's comment on the adequacy and effectiveness of the company's internal controls (including financial, operational, compliance and information controls) and risk management system; (ii) the audit committee's comment on whether it concurs with the board's comment; and (iii) where material weaknesses are identified by the board or audit committee, they must be disclosed together with the steps taken to address them.

The above ties in with Principle 9 of the Code of Corporate Governance 2018, which provides that the board is responsible for the governance of risk and ensuring that the management maintains a sound system of risk management and internal controls, to safeguard the interests of the company and its shareholders. The Practice Guidance further elaborates that the board's responsibility includes determining the nature and extent of significant risks which the company is willing to take. In relation to the board's commentary required in the annual report, the Practice Guidance provides guidelines that it should include: (i) information needed by stakeholders to make an informed assessment of the company’s risk management and internal control systems; (ii) a description of the principal risks (including financial, operational, compliance and information technology risk categories) facing the company and how they are being managed or mitigated; (iii) an explanation of the company’s approach towards identifying, measuring and monitoring its key and emerging risks, and an elaboration of its approach towards the governance and management of these risks; and (iv) an explanation of how the board has assessed the prospects of the company, over what period it has done so, and why the board considers it to be appropriate to use that period.

Currently, there are no specific disclosure requirements in relation to cybersecurity incidents prescribed under the Listing Manual. Nevertheless, companies should consider whether such an incident would be one which falls under the catch-all provision under Rule 703 of the Listing Manual. Rule 703 provides that a listed company must announce any information which is necessary to avoid the establishment of a false market in its securities or would be likely to materially affect the price or value of its securities in a timely manner, unless certain conditions are fulfilled. Companies should also consider whether the knowledge of undisclosed cybersecurity risks and incidents by any insiders could violate prohibitions against insider trading.

Guidance from the SEC

In contrast to regulators from other jurisdictions such as the U.S. Securities and Exchange Commission ("**SEC**"), regulatory authorities in Singapore have not issued any guidance for listed companies that specifically address cybersecurity.

Although the recent guidance issued by the SEC on 21 February 2018 to assist public companies in the U.S. in preparing their disclosures about cybersecurity risks and incidents, which reinforces and expands the guidance previously issued on 13 October 2011 (collectively, the "**SEC Guidance**"), is not binding on companies listed on the SGX-ST, some of the principles may be applied analogously to companies listed in Singapore. We set out below some principles that Singapore listed companies may consider based on the SEC Guidance.

Determining Materiality

The SEC Guidance provide that, in determining their obligations regarding cybersecurity risks and incidents, companies generally weigh, the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact of the incident on the company's operations. The potential materiality of cybersecurity risks and incidents would depend on their nature, extent, potential magnitude and the range of harm that such incidents could cause. The SEC Guidance further clarify that a company is not required to make detailed disclosures that could compromise its cybersecurity efforts, such as specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident. The SEC Guidance also specifically provides that an ongoing internal or external investigation of a cybersecurity investigation would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident.

Risk Factor Disclosures

The SEC Guidance has listed the following issues for consideration when evaluating cybersecurity risk factor disclosures: (i) the occurrence of prior cybersecurity incidents, including their severity and frequency; (ii) the probability of the occurrence and potential magnitude of cybersecurity incidents; (iii) the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the company's ability to prevent or mitigate certain cybersecurity risks; (iv) the aspects of the company's business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks, including industry-specific risks and third party supplier and service provider risks; (v) the costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers; (vi) the potential for reputational harm; (vii) existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs to companies; and (viii) litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents. In meeting their disclosure obligations, the SEC Guidance highlighted that companies may need to disclose previous or ongoing cybersecurity incidents or other past events in order to place discussions of these risks in the appropriate context as such contextual disclosure may be necessary to effectively communicate cybersecurity risks to investors.

Risk Management Programme, Policies and Procedures

In relation to a board's role in the risk oversight of a company, the SEC Guidance suggests that disclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues would allow investors to assess how a board of directors is discharging its risk oversight responsibility in this area.

The SEC Guidance encourages companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure. Companies should also assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel such that senior management are able to make disclosure decisions and certifications and to facilitate policies and procedures. The SEC Guidance further elaborates that a company's disclosure controls and procedures should not be limited to disclosures specifically required under the laws, but should also ensure timely collection and evaluation of information potentially subject to required disclosure, or relevant to an assessment of the need to disclose developments and risks that pertain to the company's businesses. When designing and evaluating disclosure controls and procedures, companies should consider whether such controls and procedures will appropriately record, process,

summarise, and report the information related to cybersecurity risks and incidents that is required to be disclosed in filings. Controls and procedures should enable companies to identify cybersecurity risks and incidents, assess and analyse their impact on a company's business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents.

Conclusion

Although Singapore has been ranked as the country with the least exposure to cyber threats according to the findings by Cyber Intelligence House's Cyber Exposure Index, a global scoring system that calculates the exposure index of listed companies based on exposed credentials, hacker-group activity and leaked sensitive information, it is undeniable that companies are increasingly exposed to cybersecurity risks. As such, it is critical for listing applicants and listed companies to take all required actions to keep investors and potential investors about material cybersecurity risks and incidents.

Contact Us

For queries or more information, please do not hesitate to contact any member of the Capital Markets team.

Marcus Chow
Partner

Tel: +65 6428 9425
marcus.chow@twobirds.com

Jolie Giouw
Counsel

Tel: +65 6428 9415
jolie.giouw@twobirds.com

Adeline Goh
Senior Associate

Tel: +65 6428 9460
adeline.goh@twobirds.com