Bird & Bird ATMD

Cybersecurity & Singapore

A Balancing Act for Executives and the Board

June 2019

Cybersecurity risk is fast becoming one of the top concerns of many businesses. Modern business is by nature interconnected and interdependent. Rapid developments in technologies and accompanying threats require engaged management to constantly and diligently learn and monitor just to keep up. This third article in our ***Cybersecurity & Singapore*** *series discusses the legal liabilities that organisations and directors may face in respect of the organisation's failure to manage such cybersecurity risks, and ways that such liabilities may be mitigated.*

Corporate Liability

An organisation's statutory obligations and liabilities depend on its activities and the type of data it has or controls. Breaches of these statutory obligations are often accompanied by significant penalties in the form of fines, and the damage to the organisation's goodwill and reputation is often just as severe.

Under the Cybersecurity Act 2018 (No.9 of 2018) ("**Cybersecurity Act**"), organisations that own or control computers or systems designated as Critical Information Infrastructure ("**CII**") are required to comply with codes and directions issued by the Commissioner of Cybersecurity ("**Commissioner**"), conduct regular audits and risk assessments of the CII, participate in cybersecurity exercises as directed by the Commissioner, report to the Commissioner within the prescribed period if they become aware of any of the specified cybersecurity incidents, and cooperate with the Commissioner in respect of any written directions issued. Providers of specified cybersecurity services have to be licensed in order to provide the specified services.

Even if an organisation is not a cybersecurity service provider and does not own or control computers or systems designated as CII, it is still required to comply with notices and directions of the Commissioner. This includes providing access to premises, computers or computer systems, taking remedial measures or ceasing activities, and allowing the Commissioner to take possession of the organisation's computer or equipment, as part of investigations or for the prevention of cybersecurity incidents.

Where personal data is involved, organisations are required to protect personal data in their possession or under their control, including the securing of relevant computer systems, as part of their obligations under the Personal Data Protection Act (No. 26 of 2012).

Organisations may also be subject to sector-specific codes or regulations imposed by regulators such as the Monetary Authority of Singapore, Infocomm Media Development Authority, and the Energy Market Authority.

While the regulators have indicated that there are ongoing efforts to streamline incident reporting lines, organisations will nonetheless find that they are required to comply with similar and potentially overlapping ongoing obligations under the purview of different agencies or regulators. This is further complicated when organisations that are otherwise not directly regulated find themselves subject to similar obligations imposed on them by contract or otherwise when dealing with regulated organisations.

It is also not uncommon for organisations to "inherit" such liability. Recent instances of high-profile breaches in the hospitality and technology industries were reportedly

pre-existing and not discovered even during the respective merger and acquisition exercises. As a result, the acquirers have had to write-down the value of the acquisition, and are facing significant regulatory fines and litigation costs.

Obligations of Directors and Executives

When faced with guiding companies through possible overlapping obligations, it is important that Directors are familiar with not just their company's activities and operations but also developments in areas such as cybersecurity risks that may affect their industries.

Management of the company vests in the Directors who are accordingly subject to statutory obligations under the Companies Act (Cap. 50) ("**Companies Act**") to act honestly and use reasonable care, skill and diligence in the discharge of their duties (sections 156 and 157, Companies Act). Courts in Singapore tend to be slow to interfere with commercial decisions and hold directors accountable for decisions that, with the benefit of hindsight, are risky or ill-advised, but it is generally expected that in taking such decisions and discharging their duties Directors should nonetheless seek the advice of fellow Directors or obtain professional advice as necessary.

Under the Cybersecurity Act, Directors and those involved in the management of the company may also find themselves guilty of the same offence as the company if the company commits the offence as a result of their action or failure to take reasonable steps to prevent or stop the commission of the offence (section 36, Cybersecurity Act).

The Code of Corporate Governance 2018 contemplates and provides that Directors are expected to continually develop and maintain their skills and knowledge.

With an increased awareness and prominence of cybersecurity risks and concerns, it is unlikely that Directors and executives will be able to disclaim their liability by passively discharging their duties. Directors and executives will be expected to be at least sufficiently familiar with the subject matter to identify areas of concern, identify and appoint the appropriate service providers, and critically review external advice that is obtained.

It is also important that Directors and executives recognise that cybersecurity concerns are multifaceted and not limited to just technical issues. The human component and the company's administrative and operational processes pose significant vulnerabilities as well, requiring active and ongoing monitoring and review of internal practices and policies.

Training / knowledge-building

There is often a distinct gap between the knowledge and capabilities of those on the frontline and that of the Directors and executives. For Directors and executives to exercise any supervisory or critical review functions, it is essential that they develop some familiarity in this area and continuously develop and maintain their skills and knowledge.

A number of resources are available for continuing training and development from professional organisations, educational institutions as well as solutions and service providers. For Directors, the Singapore Institute of Directors regularly conducts courses for Directors to acquire foundational knowledge in this area.

Based on public disclosures, heavily regulated organisations and public institutions that meet or comply with current or existing regulations and/or standards have nonetheless been the subject of significant breaches and are often some of the most frequently targeted. It is essential that the Board and executives are able to appreciate the fluid nature and rapid developments in this area in order to guide their organisation to develop defences and policies that can respond and defend against threats beyond what is legally required.

Mitigating liabilities

Very few organisations have the capability to manage and address all their technology and cybersecurity requirements internally. Furthermore, not all organisations have the option of isolating their systems from external communications.

It is possible to limit some of this exposure contractually by specifying expected service levels, obtaining warranties and indemnities from the relevant counterparties, setting liability limits, holding funds or payment in escrow, and even insuring against such risks. The effectiveness of any of these measures is dependent on organisations being able to properly identify the risks to be addressed, and, especially if insurance is called upon, putting in place proper practices and processes to prevent and address incidents.

It would be prudent for the Board and executives to think of cybersecurity not as the responsibility of a single department but as part of the organisation's broader business strategy and can incorporate cybersecurity risk management as a Board and executive performance indicator. Given their leadership position, the Board and executives are often prime targets for exploitation, and can thus set an example by being involved with cybersecurity training exercises together with the rest of the organisation and becoming an integral part of the incident reporting lines.

Reinforcing this as part of the organisation's culture as a broader staff performance indicator and with frequent real-world training can greatly strengthen an organisation's frontline response and defences. When management and staff are armed with a keen awareness of the organisation's cybersecurity concerns there may be fewer points of weakness that can be exploited. Frontline employees who are familiar with the organisation's business requirements may be less likely to collect non-essential data that may in turn reduce the impact on the organisation in the event of a breach. With clear reporting lines and a culture that encourages good cybersecurity practices, employees on the frontline may be more likely to recognise and report threats allowing for earlier mitigation.

Conclusion

The recent legislative efforts to ensure the security of our info-communication infrastructure sends a clear signal that cybersecurity should feature prominently in an organisation's risk management framework. Failure to ensure compliance exposes the organisation and its officers to legal liability, and ultimately erodes shareholder value.

By adopting good cybersecurity practices and policies, and having a culture that encourages good cybersecurity practices in the workplace, organisations can go a long way in strengthening their cybersecurity infrastructure and correspondingly, mitigate cybersecurity risks.

Contact Us

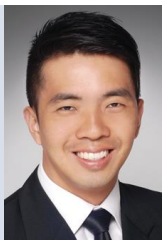
For queries or more information, please do not hesitate to contact any member of the Corporate team.

Sandra Seah
Joint Managing Partner

Tel: +6564289429
sandra.seah@twobirds.com

Jonathan Kao
Senior Associate

Tel: +6564289412
jonathan.kao@twobirds.com



Eef Gerard Van Emmerik
Associate

Tel: +6564289474
eefgerard.vanemmerik@twobirds.com

Nathanial Ng
Associate

Tel: +6564289807
nathanial.ng@twobirds.com