SINGAPORE INSTITUTE OF DIRECTORS

STATEMENT OF GOOD PRACTICE

CYBER SECURITY RISK MANAGEMENT

1. Introduction

In the wake of massive and headline-grabbing data breaches and security incidents which have impacted a diverse range of industries and companies in the last few years, businesses have come to realise and accept that cyber security breaches and infringements can happen to anyone.

No industry has been spared, and despite the best-intended efforts of any organisation, determined perpetrators have been able to find loopholes. These either arise from a lapse of security controls, malicious or inadvertent actions of employees, contractors, or other business partners within the supply chain, or simply the inability of enterprises to filter the signal from the noise in the huge volume of transactions and data that is inundating the organisation.

Businesses today are under tremendous pressures to reinvent themselves as emerging technologies allow new entrants to significantly disrupt previously successful models. New entrants are entering adjacent markets as the traditional barriers of entries have been redefined through the innovative use of technology.

These are exciting times as businesses – new and old alike – reinvent themselves to address the gaps of consumer needs. Accessibility of information, speed of transaction completion and competitive pricing can now be achieved through a pure online presence without the need to visit a physical office, outlet, or branch.

Amid these exciting times, businesses with established success are finding themselves in a dilemma. There is a huge risk of becoming irrelevant if they do not look to disrupt themselves to compete with new entrants that are chipping away at their customer base. On the other hand, they may not have the necessary skills and agility to tear themselves apart and rebuild the business model securely as they continue serving the existing customer base.

The pace of change has been mind-boggling, with the introduction of a data-driven economy, combined with rapid enhancements in emerging technologies such as artificial intelligence and machine learning. New technologies and business applications are hitting the market in much shorter cycles and businesses are facing new competition from non-traditional players. With increased connectivity, businesses are expected to experience increased activity from cyber criminals.

This raises the question of whether the established governance structures that have kept us safe and secured thus far are still relevant for today's challenges. Traditional point-in-time risk snapshots either through quarterly self-assessments or annual audits

now seem to be in the magnitude of lifetimes compared with how easily a determined perpetrator can break into information and operational technology systems.

2. Principles for good cyber security management

As directors with fiduciary responsibilities to stakeholders, boards should adopt a baseline of cyber security good practices to safeguard the sustainability and viability of the company's increasing reliance on technology as a key enabler of its business strategy.

The establishment of the Cybersecurity Act in March 2018, which establishes a legal framework to ensure the right level of oversight and maintenance of national cyber security in Singapore, is a clear signal of the Singapore Government's emphasis on safeguarding the resilience of the country's digital economy.

The Cybersecurity Act defines the following sectors as Critical Information Infrastructure (CII) sectors – Energy, Water, Banking and Finance, Healthcare, Transport (which includes Land, Maritime, and Aviation), Infocomm, Media, Security and Emergency Services, and Government. Covering quite a broad spectrum with its current classification, the scope is extended further as CII operators within these defined sectors need to assess the risks arising from the use of vendors (defined as both technology suppliers and service providers within the Cybersecurity Code of Practice).

The importance of cyber security was underscored during the Circuit Breaker and Extended Circuit Breaker periods in response to the Covid-19 pandemic. Cyber security in support of other Essential Services and the digital economy has been listed as one of the Essential Services under the Information and Communications cluster.

These references clearly point to the need to elevate cyber security management beyond the conventional approach of leaving it to the sole responsibility of a technology department. It also raises the expectation for the board to provide the right level of oversight to ensure that management has introduced the commensurate level of measures to safeguard the business against ongoing and emerging cyber security threats.

This Statement of Good Practice (SGP) highlights five key areas that boards should consider in discharging the oversight of management's responsibilities over cyber security.

This SGP also references ongoing work from the National Association of Corporate Directors' *Cyber-Risk Oversight Handbook 2020 – Key Principles and Practical Guidance for Corporate Boards*. This handbook, currently in its third edition, was first published in 2014 and provides top-level guidance to boards of directors on managing emerging cyber security risks. While drawing reference from this guide, this SGP contextualises the following recommendations based on the emerging regulatory landscape around cyber security in Singapore.

2.1 Integrating cyber security risk management with ERM

Companies need to move beyond solely relying on controls and audit-based approaches to assess the company's cyber security posture. While it is an important technique to maintain, it is tactical in nature and fails to elevate the cyber security posture to a level where there is meaningful context to the implications that the controls or lack thereof pose to the business.

Without elevating cyber security as an enterprise-level imperative, there will be a large disconnect where the current operational risk metrics relevant to the cyber security aspects of the technology department are largely limited to unplanned disruption and metrics around malicious codes or activities detected in the systems. This represents a relatively small portion of all possible risk scenarios that the company might be facing.

One of the key underpinning requirements within the Cybersecurity Code of Practice as part of the Singapore Cybersecurity Act requires in-scope entities to establish a Cyber Security Risk Management Framework, which includes the following:

(a) Roles and responsibilities in managing cyber security risk, including reporting lines and accountabilities.
(b) Identification and prioritisation of CII assets.
(c) Organisation's cyber security risk appetite, and thresholds for residual risk.
(d) Cyber security risk assessment methodology.
(e) Treatment and monitoring of cyber security risk.

The risk identification, assessment, treatment and monitoring should be done at various levels of details that allow a contextual application of actual risk scenarios at the operational level. At the same time, the process should permit meaningful aggregation at the management level, culminating in the roll-up to top-level enterprise risks that are reported to the board at regular intervals along with the Enterprise Risk Management (ERM) protocols established.

Integrating the cyber risk management approach into the existing ERM methodology allows for meaningful interpretations and action plans at the various levels rather than having disjointed risk and control activities between the frontline and management reporting.

An important concept to establish here is the risk appetite for assessing cyber security initiatives with the purpose of advancing the digital capabilities of the company. Boards should be careful not to inadvertently stifle digital innovation by setting a "zero tolerance" risk appetite for cyber security incidents, as that lofty target is not practically achievable without severely limiting the possible adoption of emerging technology.

Instead, boards should establish clear expectations of the due diligence that management should undertake to establish the appropriate risk management frameworks, roles and responsibilities, investments to uplift the cyber security capabilities, and monitoring metrics.

2.2 Understanding legal implications of cyber security risks

We are experiencing increased regulatory and legal oversight over the management of cyber security risks of an organisation. In Singapore, some of the prevalent regulations at the time of writing include the Notices on Technology Risk Management for Financial Institutions, Personal Data Protection Act 2012, and the Cybersecurity Act 2018. There are similar regulations and legal expectations across the region and globally.

The complex dependencies present a high risk to the enterprise that goes beyond the ability of the technology department to manage by themselves. In discharging the fiduciary duties, boards should also stay informed on the evolving regulatory and legal landscape of operating in the new digital normal. These briefings should be done in combination with the aid of external advisers as well as internal teams comprising the legal counsel, business units and IT. This allows the board access to independent perspectives from outside the organisation, while retaining the contextual interpretations of these expectations in their unique operating environment.

Particularly where there are strict disclosure and reporting guidelines, Boards should ensure that these are duly identified along with the right operational metrics and mechanisms to detect and respond to the relevant triggers.

For example, the Personal Data Protection Commission provides guidance and expectations to organisations to formulate data breach management plans with the corresponding details on monitoring, responding to, and reporting data breaches as appropriate. These obligations, management plans, roles and responsibilities, should be clearly defined, communicated, practised, and reported periodically to ensure that the organisation remains effective and relevant with the changing business landscape.

2.3 Facilitating board access to expertise

With the increasing complexity of the cyber security landscape and threats to the business, boards, may find themselves struggling to grasp the full potential implications and impact on other dependencies within the organisation. This can be the case when organisations use summarised reporting without access to independent expertise familiar with the field of cyber security.

Boards can consider including external independent expertise on the subject either on an ad-hoc or retainer basis to brief the board on select topics of interest, or to provide an independent view on select cyber security matters presented to the board. This arrangement can be particularly helpful as the topics involving cyber security are so diverse that it is rare to find an individual who is equally proficient in all topics, ranging from emerging technology (e.g. FinTech, RegTech), physical IT integrations (e.g. Internet-of-Things) to application of artificial intelligence and machine learning on consumer data, just to name a few.

While this approach may be used for tactical topics, it may not be practical when

discussing strategic matters such as new business strategies, mergers and acquisitions, deployment of new technology platforms, etc., where there are naturally cyber security-related topics but difficult to involve an external party.

In that light, boards can consider including directors with cyber security experience in either the full board or sub-committees, moving beyond using external independent expertise on an ad-hoc or retainer basis. One effective approach is to include such cyber security expertise at the Audit or Risk Committees as the first-level interactions with management on topics relating to cyber security or enterprise risks. Through this structure, even though the cyber security expertise may not be a member of the full board, the Audit and/or Risk Committee Chair is able to bring the relevant insights back to the full board for further deliberation.

2.4 Building cyber resilience vs impenetrability

Operating in today's digital landscape, it is impossible to fend off all attempts to compromise the confidentiality, integrity, or availability of all digital assets. Boards should direct management to make the efforts to achieve a state of enhanced cyber resilience, which can be defined as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources.

As part of building cyber resilience, boards should direct management to consider the following:

(a) Perform a robust risk assessment to identify the critical digital assets that are key to sustaining the business operations, stakeholder trust, and regulatory expectations.
(b) Identify the means by which a malicious perpetrator may compromise the confidentiality, integrity, or availability of such assets.
(c) Identify treatment plans that may include the introduction of controls that minimise the likelihood of occurrence, or less-often considered, re-engineer the business process and its supporting systems to lower the impact of a successful security incident.
(d) Establish a clear incident response plan to recover from undesirable security events and ensure that all involved parties are aware of their roles within the plan. The plans must be practised in the presence of independent observers who can provide feedback on areas to further improve the process.

While hygiene controls are still important and relevant in safeguarding the organisation, enterprises today must operate by taking an "assume-breached" posture and architect their business processes and supporting technology to be sufficiently resilient.

The board should also ensure that management is adequately investing in automated technology to increase the efficacy of security operations particularly with the increased system complexity and volume of data to monitor.

2.5 Investing in upskilling human capital

Often, we see organisations investing in technology and process changes, but missing out on spending to train the management and employees on leveraging and interacting with the new technology. This either results in a sub-optimal attempt to disrupt the business as the full potential of technological gains are not achieved, or introduces additional cyber risks to the organisation as employees and third-parties may not fully appreciate the increased surface area of attacks.

Careless or unaware employees present a point of vulnerability, and among the top cyber threats to organisations are phishing and malware attacks that target these groups of users.

To remain digitally relevant, there are certain skillsets that should extend beyond the specialised silos, and these include cyber security, automation, data science and visualisation, and design thinking. Boards should set the tone to encourage further upskilling of leaders, management and employees in relevant emerging skills, so as to be able to lead and operate in the new digital normal as well as make such talents available to the board and its committees.

3. Conclusion

To lead and remain relevant, businesses must look to disrupt themselves, reinvent and transform to compete with greater agility and purpose. Transformation and digitisation invariably bring about increased risks and boards should lead in driving the tone at the top to challenge management to rethink conventional structures and methods in dealing with cyber security risks.

The fast pace of change will only accelerate into the future and keeping up will in itself be a risk. The time to act on cyber security risk management is now.