37

Are Your IT Controls Truly Adequate?

GERARD TAN

Hardly a week passes without a media report on a data security breach somewhere in the world. Singapore is not spared.

In June 2014, the Infocomm Development Authority (IDA) made public the fact that 1,560 SingPass accounts (used for online government transactions) may have been compromised. Subsequently, it reported that three of those accounts were used to make six fraudulent work pass applications.

Not too long before that, there were media reports of the theft of bank statements of 647 wealthy clients of Standard Chartered Bank, the defacement of the Istana website, and the hacking of the Prime Minister's Office website.

PwC's *2014 Global Economic Crime Survey* revealed that, globally, 22 per cent of economic crimes committed (15 per cent for Singapore) relate to cybercrime. These incidents and statistics should raise concern in boardrooms.

BOARD'S ROLE

Indeed, it is the role of boards to worry about the state of the information technology (IT) risks in their companies.

The Code of Corporate Governance requires the board to comment on "the adequacy and effectiveness of the internal controls, including financial, operational, compliance and information technology controls, and risk management systems, in the company's annual report". (Guideline 11.3)

Recently, as part of the judging process for the 2014 Best Annual Report Award, I reviewed 50 of the annual reports of Singapore-listed companies. I found 14 of them (28 per cent) did not express a specific opinion on their IT risks and mitigation; they only opined on the adequacy of financial, operational and compliance risks in general. While it can be argued that IT risks are a subset of operational risks, nevertheless the great exposure and impact of IT risks in most companies today mean that it merits a separate focus and disclosure.

Boards should fulfil their role in respect of IT risks by bolstering their own capability in this area and proactively ensuring that appropriate IT controls and practices are installed.

DIGITAL DIRECTORS

A review of most listed boards would show that they have a good mix of finance, legal and business backgrounds. However, it is rare to find board members with IT security expertise.

There has recently been a call for including "digital directors" on boards. These are directors mostly with working experience in high-tech companies. The focus of these digital directors are often and, importantly, focused on the strategic application of technology to the business of the company.

However, from a risk management standpoint, there is a need for directors who understand and have a focus on cyber security and other technology risks. Such individuals could come from the IT audit or compliance units of large commercial companies and professional firms.

Regardless of the presence of directors with a strong background in IT risks and security, all board members should be equipped to understand and deal with IT risks. They should attend regular training on the latest IT developments and related security challenges in a fast-moving world. Such training would help them to better understand company IT policies and practices, and place them in a more comfortable position to opine on the adequacy and effectiveness of IT controls.

KEY AGENDA POINT

The state and review of IT controls and security should be a key and regular component of the agendas for the Risk Management Committee, Audit Committee and, indeed, the whole board.

Directors should ensure that there is a well-documented set of Corporate IT Security Policies, Standards and Processes in place. Some security experts argue that infiltration and security breaches are inevitable, and therefore the best practice is to provide for all contingencies.

Good IT controls can be found at five key levels:

- Deterrent controls to discourage would-be intruders from attempting to break into the system.
- Preventive controls to stop or make it very difficult for unauthorised users to access systems.
- Detective controls to track and report exceptions and security breaches when the preventive controls fail.
- Response controls for planned reactions to breaches.
- Recovery controls such as crisis management plans, IT disaster recovery and business continuity plans, to ensure the organisation's survival when all the other controls fail.

The key is in effective execution. Therefore, ensuring that there are technically qualified IT security personnel to implement and maintain the policies and standards is critical. The nature and costs of IT have resulted in some companies outsourcing this important capability. The risks and management of outsourcing and the selection and qualifications of the specific outsourced vendor should be key considerations for the board when it oversees the execution and monitoring of IT controls.

The above approaches should go some way in providing board members greater comfort in opining on the adequacy of IT controls in their annual reports. ■