In 2017, the Singapore government will table a Cyber Security Bill in Parliament to keep pace with the evolving cyber security landscape. The Bill will empower the Cyber Security Agency to keep oversight of cyber incidents and raise the standards of cyber security providers in Singapore.

A business issue

Beyond these technology and regulatory considerations, it cannot be stressed enough that cyber security is a business issue. An attack can cause real and untold damage to the business.

That being so, the board must ensure that management satisfactorily addresses cyber threats. These are fundamental strategic issues as they pose severe financial and reputation risks.

Improving affordability

However, the cost of information security is an important consideration. Here, boards need to ensure that management properly and sensibly weighs the cost to protect against the cost of a breach.

In finding the right balance, boards can look into a number of areas to improve the affordability of information security.

The first is to require management to implement a well thought-out information security policy to protect confidential information in both electronic and hard-copy form.

For example, in the K Box case, the PDPC identified several basic technical issues such as weak passwords, unencrypted email, and lack of security systems testing. These should be part of any basic information security policy.

Studies also show that more than half of data breaches are directly attributable to careless or disgruntled staff. Staff carelessness includes not following or having proper information security policies. Disgruntled staff can cause data breaches when safeguards are not in place

to protect against actions aimed at damaging the company. Only about 20 percent of data breaches are attributable to pure cybersecurity attacks, i.e., those that do not involve staff, whether complicit or unwitting.

Most crucially, instead of merely creating an awareness of security and controls, companies need to create a security culture based on actively changing behaviour. This can be achieved through inculcating a belief that all staff are responsible for information security, not just those in the IT department. This should be accompanied by auditing compliance and ensuring policy enforcement. K Box, for instance, had a fairly typical password policy but in the absence of enforcement, one staff member's password comprised of a single letter, and that of the website administrator's was "admin". A whistle blowing mechanism reinforces a security culture.

Another layer of defence is cyber insurance, which is evolving as rapidly as technology. What is considered core coverage today was not available several years ago. Thus, first-party insurance is now available for data destruction, denial of service attacks, theft and extortion. Other areas of coverage include crisis management, forensic investigations, data restoration, and business interruption. ■

Boardroom Matters is a weekly column by SID for The Business Times and its online financial portal, BT Invest, where this article was first and recently published.