31

Cyber Security: Not Just for the Tech-Hearted

LYN BOXALL

In today's Age of Information where data is transmitted and consumed with the help of technology at break-neck speed, IT security threats are expanding and evolving at an unprecedented rate.

We have seen high-profile attacks on multinational companies like Target and Sony Pictures where computer systems were disabled, business and personal data stolen and exposed to the public. In August 2015, data from millions of users of Ashley Madison – an adult dating site that facilitates discreet extra-marital affairs – was published as a result of a cyber-attack on the site.

Closer to home, in September 2014, hackers breached the membership database of local karaoke company, K Box, threatening to expose personal information such as identification card and mobile

phone numbers of more than 317,000 K Box members. Earlier, in 2013, James Raj Arokiasamy performed a series of seven high-profile cyber-attacks, hacking into the web servers of Fuji Xerox, The Straits Times blogs, the PAP Community Foundation, and the Ang Mo Kio Town Council. The Fuji Xerox attack compromised confidential data of 650 Standard Chartered clients. The affected organisations spent S$1.36 million dollars to repair their computer systems. James Raj was sentenced to five years in jail in January 2015.

It is evident that cyber threats represent a real risk to Singapore companies, and the country as a whole.

The government recognises this and is ramping up cyber security measures, most notably with the establishment of a Cyber Security Agency to oversee the nation's cyber security functions. The Personal Data Protection Commission followed with the issuance of a Guide to Managing Data Breaches in May 2015.

Companies need to follow suit. The International Chamber of Commerce in its *Cyber Security Guide for Business* (released in June 2015) warns that "If something of value is online, it is at risk, and is likely compromised".

CYBER RISK IS A BUSINESS RISK

Unfortunately, many boards here are not adequately handling this pressing situation. Two barriers often stand in their way. The first is fear (of being overwhelmed) and intimidation (because it is a technical area that only a few are familiar with). The second is a lack of awareness and the "head in the sand" approach to cyber risk management.

Both barriers can be torn down if directors handle cyber risk in the same way as any other business risk.

That said, directors must realise and accept that cyber risk

management is an ongoing process and that, while there is no assurance of ever attaining absolute security, they need to continually commit to manage cyber risk even when there is no stable end-state.

BOARD ATTENTION IS NEEDED

Just like any other business risk, cyber security is not an ephemeral item on the boardroom agenda and will require three broad actions.

The first step in managing any kind of organisational risk is to undertake a risk analysis exercise. This includes prioritising the risks that justify the time and expense required to manage them. It may be trite to say that scarce financial and manpower resources mean that hard choices must be made. It is neither possible nor sensible to devote scarce resources to trying to protect everything.

So an organisation must identify assets that most require protection. Management's risk analysis must enable the organisation to understand and prioritise what is important – important or critical physical and information assets are essential and therefore must be protected.

The second is leadership of the issue – starting with the board— that needs to be exhibited down the value chain. Everyone in the organisation needs to "own" cyber risk and cyber security.

Take, for example, safety in the building industry as a parallel. Once, worker safety was the responsibility of a few people – perhaps a site safety officer or a foreman. But this changed after extensive work safety campaigns raised awareness; the point is that everyone now "owns" worker safety. Interestingly, the Workplace Safety and Health Act expressly puts the burden of ensuring a safe workplace firmly on the shoulders of the board of directors. In time, that may be the case for a cyber secure workplace.

The third step in managing cyber risk is for the board to mandate management to have systems and processes in place to detect any security breach and to respond to it – internally and externally – through institutionalised processes. The response must be documented, rehearsed and updated to respond to changes in the threat environment.

BEING PREPARED

It is too late to address how to respond to a breach if it is done only after a breach has occurred. A badly executed response may do more damage to an organisation. A response showing that the organisation is in control of the situation and is reacting calmly and confidently builds trust with stakeholders.

The Cyber Security Agency of Singapore is charged with reviewing the existing cyber security laws to see if they are sufficient for the evolving landscape and whether there may be a need to introduce new ones, especially when cyber-crime is moving at a rapid rate. According to its chief executive officer, David Koh, for the agency to be able to do so, it requires organisations to report system breaches in a timely fashion – something that most are reluctant to do as it may affect their reputation and possibly divulge sensitive information to their competitors. Quite pointedly, he stressed that it is a question of when, not if, a major cyber-attack hits Singapore. ■