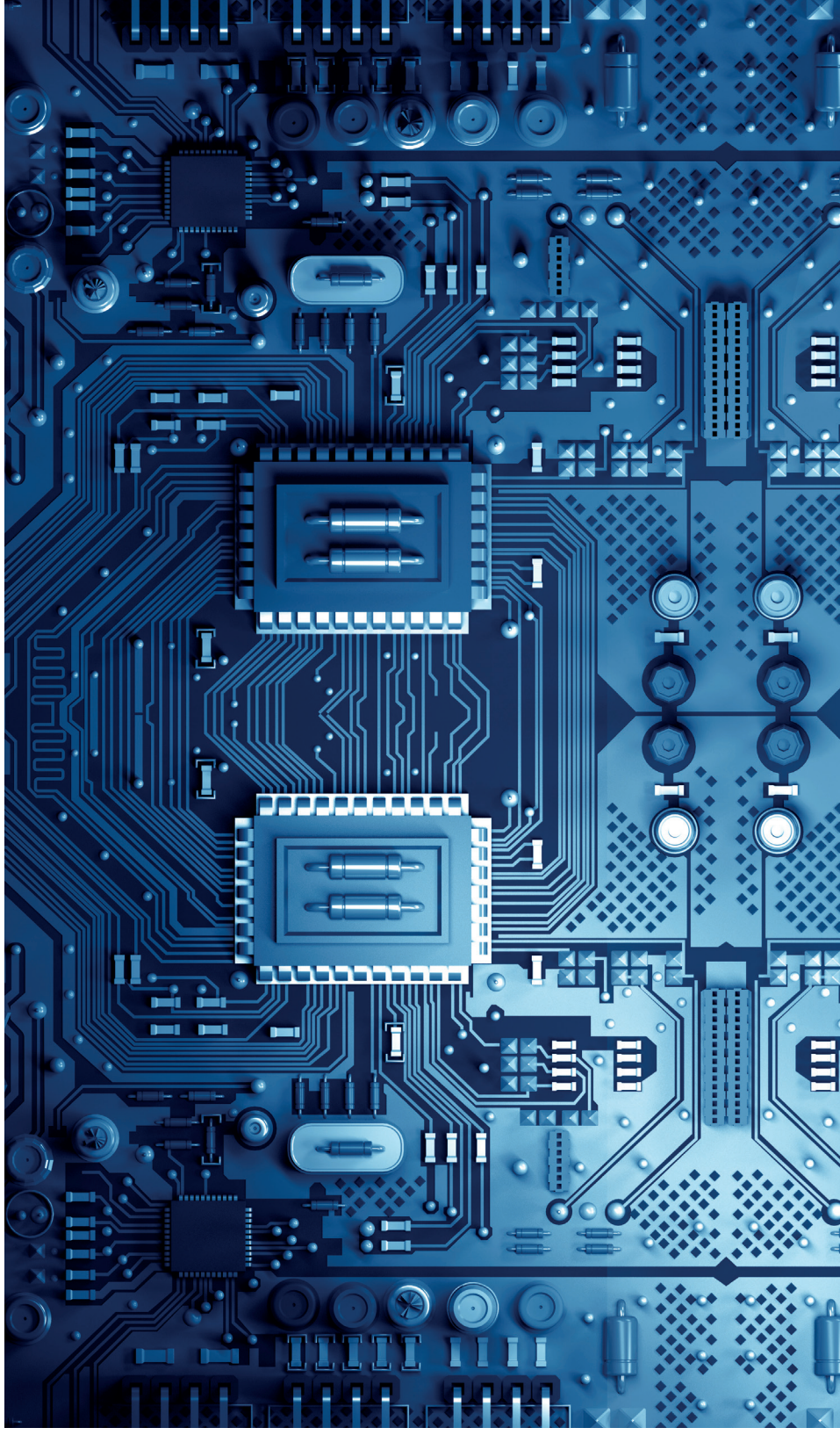

BY **LIONEL TAN**

STAY SAFE

The consequences of cyber breaches are grave, and SMEs should take measures to prevent cyber attacks from happening

SINGAPORE'S small and medium sized enterprises (SMEs) are prime targets for cyber attacks. According to a survey by the Singapore Business Federation in 2016 on the perception of cyber security, 60 per cent of SMEs polled were exposed and vulnerable to cyber attacks. Indeed, SMEs are less resilient compared with their larger counterparts. They often deploy less complex technologies and systems to guard against cyber attacks, and their staff are often not sufficiently trained to identify cyberthreats.

Despite such weaknesses, there is little impetus for SMEs to adopt stronger precautionary measures against cyber attacks. Laws such as the proposed Cybersecurity Act mandates only owners of critical information infrastructure (CII) to take certain precautionary measures. Furthermore, considering the stronger cyber security measures which CII owners will adopt in the future, hackers will inevitably target the less secured SMEs.

Indeed, a lesson may be learnt from the large US retail company, Target Corporation – which was the victim of a massive data breach in December 2013. Hackers first entered Target's network by stealing credentials from its heating, ventilation and air-conditioning supplier. Using the supplier's credentials, malware was installed on Target's point-of-sale devices to steal credit card information belonging to its customers.

SMEs should learn from this incident and be aware that hackers may actively target them to gain access into their customers' networks.

CONSEQUENCES OF CYBER ATTACKS

Cyber breaches often lead to companies losing their customers' personal data. SMEs are required to make reasonable security arrangements to protect personal data in their possession under section 24 of the Personal Data Protection Act (PDPA). Hence, if an SME omits to adopt reasonable security arrangements, the SME may be subject to regulatory penalties if a cyber breach occurs.

In 2016, K Box Entertainment Group was rapped when it and its information technology (IT) vendor failed to remove unused user accounts and failed to enforce a password policy which led to a cyber breach and the leakage of a significant amount of personal data. The Personal Data Protection Commission (PDPC) held that this constituted a breach of Section 24 of the PDPA and imposed financial penalties.

If a Section 24 breach is established, an affected individual also has the right to sue for failing to protect his/her personal data. Section 32 of the PDPA provides an individual the right of private action if the individual can show that he/she suffered loss or damage because of the data breach. Hence, SMEs may face concurrent civil liability for failing to set up reasonable cyber security measures to safeguard personal data.

A survey by Osterman Research in 2017 revealed that 21 per cent of SMEs that faced ransomware attacks had to cease business operations after the attacks, and 11 per cent reported that they lost revenue because of the attacks.

SMEs may also face a risk of litigation for breaching contractual obligations that they owe to their clients. The same survey also revealed that 53 per cent of SMEs affected by ransomware faced downtime for a period lasting more than 24 hours. Should such downtime occur, an SME that promised to maintain continued services to its clients may breach its contractual obligations, and face possible legal actions from them.

More importantly, an SME will suffer reputational damage if the breaches are sufficiently serious. Serious data breaches of the company would very likely result in highly publicised investigations. Other companies and members of the public may lose confidence, and may be wary of doing business with them. Given their size, the loss of business often hits SMEs harder than their larger counterparts.

Indeed, the US National Cyber Security Alliance found

PHOTO: ITSOCKPHOTO

"SMES SHOULD VALUE THE IMPORTANCE OF IMPLEMENTING CYBER SECURITY MEASURES. THESE MEASURES MAY SEEM BURDENSOME IN THE SHORT TERM. HOWEVER, THE MEASURES WILL ASSIST TO MITIGATE AGAINST THE EFFECTS OF A SIGNIFICANT CYBER BREACH AND ENSURE THE CONTINUATION OF A BUSINESS."

that 60 per cent of small companies could not sustain their business within six months of a cyberbreach, due in part to reputational issues.

MEASURES TO ADOPT

Given the grave consequences flowing from cyber breaches, SMEs should take the following measures to prevent cyber attacks from happening, and to minimise their liabilities arising from cyber breaches (should they happen).

SMEs should first classify the types of personal data in their possession and identify the risks involved. They should identify the staff who have access to the personal data, and ensure that they are held accountable for their protection.

Following the classification of such personal data and identification of risks, the company should then implement appropriate cyber security solutions to combat such risks. These solutions must be kept up to date – there is no point paying for outdated protection against increasingly sophisticated forms of cyber attacks.

Companies should also establish and enforce appropriate IT security policies that are commensurate with the aforementioned risks. They should require their staff to use strong passwords which have a minimum length of eight characters, containing at least one alphabetical character and one numeric character. Passwords should be changed regularly, and account lock-outs should be implemented when a user reaches the maximum number of attempts in authenticating his or her identity.

SMEs should also inculcate a practice of encrypting sensitive information (which includes personal data) to prevent the unauthorised reading and editing of files containing such information.

Finally, SMEs need to ensure that the policies apply to all portable computing devices which staff are working on. Such portable computing devices are often connected to less secure WiFi access points at external or public places which may be vulnerable to the potential interception of personal data.

A strong technical system is still less effective if the staff operating the system are careless and do not have strong cyber security awareness. Employees are the first line of defence against such cyber attacks, and it is important to raise their awareness to prevent hackers from obtaining log-in credentials to the company's IT systems.

Accordingly, SMEs should develop ongoing awareness programmes to help educate its employees to identify possible cyber threats. For example, a company could conduct phishing simulations that test its employees' ability to identify phishing e-mails. Phishing e-mails are those which masquerade as legitimate e-mails, but contain links that when clicked on, infect the users' computer with malware. Any staff who inadvertently clicked on such e-mails would be identified and given further cyber security training.

SMEs should also put in place a detailed data breach plan in response to any possible cyber breach. The plan should identify the key company staff who will direct the investigations into the data breach. The plan should also set out the appropriate steps to secure the company's processes following the investigations.

The data breach response plan should also provide the SME with a list of external professionals to contact following the cyber breach. The list would include cyber security specialist, legal advisers and crisis communication experts. These external parties should be readily contactable and be at the scene at short notice to provide necessary assistance to remediate the breach and to minimise the damage.

Finally, SMEs should also purchase an appropriate cyber insurance plan. The insurance would indemnify the SMEs for damages arising from serious data breaches. This ensures that the SMEs can survive the financial strain arising from significant data breaches.

CONCLUSION

SMEs should value the importance of implementing cyber security measures. These measures may seem burdensome in the short term. However, the measures will assist to mitigate against the effects of a significant cyberbreach and ensure the continuation of a business.

Therefore, in light of the persistent and unrelenting threats of cyber attacks, SMEs have to give serious thought about implementing appropriate cyber security measures. ■

The writer is partner, technology, media & telecommunications, Rajah & Tann Singapore