BY **ALASTAIR POOLEY**

WORKING IN A SAFE SPACE

Here are steps that SMEs can take to embrace the digital economy without increasing digital risk

PHOTO: ISTOCK.COM/POPBA

THE connectedness of the digital economy, along with the explosion of cloud and SaaS (software as a service) technology, has made it easy for employees to use their own applications and devices in the workplace without information technology (IT) teams' help or knowledge. As the lines between employees' work and social lives continue to blur, their dependence on these technologies can put them on a collision course with their company's security interests.

Cyber attacks do not discriminate between organisations by size or sector, and many small to medium-sized enterprises (SMEs) may not realise that they are a target. As the driving force behind Singapore's economy, generating half of gross domestic product (GDP) and employing two-thirds of the workforce, they too are valuable to hackers, for example through a ransomware attack. However, unlike the largest enterprises, cyber security spend is still regarded as a cost centre within SMEs, often leaving them exposed to threats.

For SMEs looking to bridge this gap, it is not an overnight process, but there are steps that can be taken to mitigate risks and drive value when it comes to cyber security. While the initiative must start at the top with IT leaders who can prioritise the issue, it is ultimately about collaborating with your entire organisation to strengthen your defences without busting the budget.

- **Get a complete picture of your IT landscape**

  In today's digital economy, the IT department is no longer the gatekeeper of all technology. Employees procure the applications and devices needed to do their job – even when they do not have permission from IT. This is a common trend that is accelerating along with the rapid move to the cloud. According to Snow Software's latest research, 49 per cent of APAC employees have used work software without IT's permission, while 55 per cent of APAC employees have accessed work documents on personal computers.

  Between the rise of cyber security threats and privacy regulations, IT teams and employers need to know where company data is stored, and how that data is used. It is also essential to know that the applications employees have downloaded are up to date with the latest patches, or worse still, whether the software is improperly licensed.

  Outdated or unauthorised software is a significant challenge for any organisation, creating the potential for security vulnerabilities. Therefore, a first step for SMEs is to attain visibility into the applications in use and the data being stored, in order to help to determine if a potential threat exists.

- **Make IT policies understandable for employees**

  As more SMEs leverage government incentives such as the SMEs Go Digital programme to take their business further with advanced technological solutions, they also become increasingly vulnerable to the ever-evolving cybercrime environment. And while Singapore has some of the best security infrastructure and legislation in place, SME employees tend to have a poor understanding of cybercrimes and tactics, making human mistakes one of the most common causes of any breach.

  Your people can become one of your strongest assets in defending your business. To protect valuable company assets, SME leaders need to start involving employees in their IT policies. They can start by communicating the implications of an employee's harmful behaviour to them, whether installing unlicensed software or downloading streaming apps into their work device. This can be done through a security awareness programme, making IT policies clear yet simple enough to be understood by someone outside the IT department. The communication should begin with employee on-boarding processes and be stripped of technical jargon. The goal here is to communicate the purpose of the framework to employees, helping them understand how their participation ensures their cyber safety, protecting both their personal data along with the companies.

  This process should be an ongoing one, with staff continually educated on what potential threats look like as well as any new security policies within the business.

- **Enhance joiner, mover and leaver IT processes**

  Employees have different needs and require access to different company platforms at various stages of their career. This places great importance on a business' joiner, mover and leaver (JML) process. Leaders need to understand where employees and their IT needs fit in the organisation, to safeguard their data from unauthorised access and ensure that they have complete intelligence across their technology ecosystem. For new joiners, businesses need to consider all IT provisions required for new employees, including the devices that they will be using, and the access that they will be allowed. When an employee moves around roles, IT teams need to identify the employee's needs and grant access to any new platforms. On the flip side, when an employee departs from their role or changes teams, IT should immediately revoke or update their access to company platforms and software to prevent access to proprietary company data.

  It is also worth noting that there are tools in the market that can help improve efficiency within the JML management process, including automation platforms.

There are, of course, a range of steps an organisation can take to safeguard themselves against a potential attack, but businesses first need to acknowledge that cyberthreats are an ongoing challenge and critical to the bottom line. Following these preventative measures could minimise those risks and help strengthen your business. The goal is always to provide the best protection for your organisation while empowering employees to work effectively. You just need the visibility and intelligence around your technology to accomplish this. ■

The writer is the chief information officer of Snow Software