THE STAR ONLINE

Thursday, 31 March 2016 | MYT 6:00 AM

Spearheading cybersecurity for SMEs in Malaysia

Cyberattacks are increasing in frequency and scale, and they threaten all areas of economic activity. Industries and businesses are at risk.

Increasingly, companies of all sizes, from multinational conglomerates, mid-sized industrial sectors and small-scale sole proprietor businesses, rely extensively on Information Technology in their production and operations. As a result, they are very vulnerable to cyberattacks.

Given such a situation, the damage and losses to these companies and conglomerates are potentially immense.

According to a recent report by cybersecurity company FireEye entitled *Regional Advanced Threat Report: Asia Pacific 1H 2015*, Malaysian enterprises and institutions have a 33% chance of encountering Advanced Persistent Threats (APTs).

This level of risk is just above the Southeast Asian average of 29% and the global average of 20% cent.

In this urgent matter of cyberattack risks, attention must be paid to small and medium-sized enterprises (SMEs) in this country.

This is because SMEs are a large and important component in Malaysia’s economy. In recent years, these SMEs have incorporated IT into their production processes.

But unlike the larger corporations which have installed programs and systems to protect themselves, many SMEs are still unaware of the high risks of cyberattacks.

According to The Department of Statistics, SMEs contribute 35.9% to Malaysia’s Gross Domestics Product (GDP) in 2014.

SME Corp Malaysia projected that by the year 2020, SMEs could be on track to contribute 42% to national GDP, 62% employment and 25% of Malaysia’s exports. The figures underline the significance of the SMEs to the country’s manufacturing sector and to the future of Malaysia’s digital economy.

All efforts must therefore be made to protect this sector from cyberattacks

How really aware are SMEs of the risk of cyber-attacks and have they taken precautionary measures to protect themselves? Global insurance company Zurich polled 3,000 C-suite executives and managers of SMEs across 15 countries in EMEA, the Americas and Asia-Pacific, and its latest global survey showed that SMEs' anxiety and concern with cybercrime has doubled from 4% in 2013 to 8% in 2015.

Zurich's survey reveals that SMEs' greatest fear is loss of customer data and damage to their reputation. From a list of nine potential threats arising from cybercrime, SMEs globally rate theft of customer data as the most critical risk of cybercrime and this accounted for 28% of respondents, while damage to reputation as a result of a cyber-attack ranked second with 16%.

Surprisingly, many of those surveyed still believe they are too small in size to be at risk.

SME's dilemma in cybersecurity

SMEs in Malaysia ranked fifth among nations most worried about cyberattacks. Unfortunately, most still lack awareness on information security and this often leads to haphazard management of their information and digital assets.

Many local SMEs also outsource their data and information to third-parties to aggregate, store and process. Such sensitive data is not only about customers and their profile but also includes information about business structure, financial health, strategy, and exposure to risk.

These SMEs eventually become dependent on third-party companies to handle IT security risks.

For SMEs, managing information is often seen as costly. They do not appreciate the benefits of proper and secure information management and how this can assist to generate further revenue for their companies.

Consequently, some SMEs delay in setting aside investments to build and maintain proper and effective systems with regard to information security. This problem is compounded by a lack of in-house cyber security expertise. This attitude needs to be corrected. Small and midsize organisations simply cannot afford to disregard security.

Information Security Management System (ISMS)

In the digital economy, information such as Intellectual Properties (IP) and other digital information owned by SMEs must be protected in order to preserve the confidentiality, integrity and the availability of information.

CyberSecurity Malaysia has since 2008 retained its certification for Information Security Management System (ISMS) or better known as ISO/IEC 27001. This standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation.

Within the Critical National Information Infrastructure (CNII) agencies, the cabinet has mandated through its Nota Jemaah Menteri on the ISMS implementation on Feb 24 2010. ISMS implementation enables SMEs in Malaysia to establish systematic risk management, improved operational effectiveness, and competitive advantage.

The governing principle of ISMS is that an organisation should design, implement, and pursue a coherent set of policies, processes and systems to manage risks that could threaten its information assets. At the same time, the level of risks to information security of SMEs must be at a minimal and acceptable level.

ISMS standards require SMEs to put in place a system that ensures all information under its control remains confidential, its integrity preserved, and information readily available when needed.

Information as an asset must be protected from potential damage through malware-like viruses, Trojan horse, worms and ransomware. Apart from that, protection must be in place to prevent internal and external attackers stealing business information.

In the face of increasing cyber-attack threats that is now on an unprecedented scale, SMEs in Malaysia and other institutions must urgently address this concern. They need to change their mind-set in order to function securely in an IT landscape of escalating risks and dangers.

In this respect, Cyber Malaysia is ready to offer all SMEs its available expertise and experience to protect their assets and technology against any cyberattack.

Dr Amirudin Wahab is the chief executive officer of CyberSecurity Malaysia.