BUSINESS & INVESTMENT WEEKLY
THE EDGE MALAYSIA

4 January 2023

MANAGING CYBERSECURITY CHALLENGES IN PURSUITOF DIGITAL TRANSFORMATION

KUALA LUMPUR (Jan 4): In today's online world, cybersecurity has become a pressing issue for businesses and organisations of all sizes.

It is especially pertinent for Malaysian companies, which are undergoing a digital transformation in various sectors. This is especially true due to recent cyber attacks on Bursa Malaysia-listed companies.

For instance, the Air Asia group fell victim to a ransomware attack on Nov 11 and 12 last year by the Daixin Team. The severity of the cyberthreat to Malaysia cannot be overstated.

According to the Malaysia Cyber Security Strategy 2020-2024 report,the country may face economic losses of up to RM51 billion due to cyberthreats. This has raised the need for curated detection and response tools, strategic plans and cybersecurity awareness initiatives to be implemented to protect businesses from data breaches and malicious activities.

It is thus important for Malaysian companies to stay informed, and to be aware of the cyberthreats they face. This is especially important, given their increasingly digitalised operations.

In such a vulnerable environment, the safety of businesses, organisations and individuals is paramount. Thus, a comprehensive understanding of the cyberthreat landscape, as well as the implementation of appropriate cybersecurity measures, is needed in order to mitigate potential risks.

In an interview with theedgemarkets.com, GDEX Bhd managing director and group chief executive officer Teong Teck Lean and DOC2US CEO and co-founder Dr Raymond Choy shared how educating and investing in cybersecurity initiatives can help in minimising cyber risk to their businesses.

Teong

BUSINESS & INVESTMENT WEEKLY
THE EDGE MALAYSIA

4 January 2023

MANAGING CYBERSECURITY CHALLENGES IN PURSUITOF DIGITAL TRANSFORMATION

Courier services

Lean said that apart from threats from hackers, cyberattacks, and ransomware, there are an array of challenges, as there are many requirements to get the most up-to-date technology for such systems to work.

Teong, who is also the president of the Association of Malaysian Express Carriers (AMEC), said this requires a lot of investment, as most of these technologies are licensed per user or device. Specifically, he said that for the delivery platform infrastructure, there will be thousands of computers and gadgets that need to be connected.

"Users will expect the most up-to-date technologies to have the best customer experience, system performance, user-friendliness, as well as speed.

"The vast amount of data keeps building up as businesses expand, and the amount of digital exposure simultaneously adds up too," he said.

Teong said cybersecurity makes up about 40% of GDEX's annual budget for information technology (IT), and that the company will continuously improve when it comes to keeping data on customers and partners safe.

He said GDEX, which encountered a cybersecurity incident last year, saw no loss of data during the incident. A small portion of its systems was slightly affected, according to him.

"We have since taken all necessary steps, as guided by regulators and
guidelines, besides engaging with third-party specialists.

"This was one of the main reasons why we decided to switch to machine learning and artificial intelligence-based cybersecurity solutions," he said.

Electronic prescription

Separately, DOC2US's Choy said while the penetration of electronic prescription in the pharmacy industry is less than 50% in total, it's clear that more education and awareness of cybersecurity are required in this regard.

Choy

"Having a foundational technical understanding of the importance of cybersecurity is also imperative.

"To overcome this, we need to ensure all stakeholders are fully aware of the risks and mitigation measures should there be any cyberattacks," he said.

He, however, said the digital health platform and e-prescriptions issuer had not suffered any cyberattacks so far.

Choy said DOC2US has an internal team to manage its IT systems.

BUSINESS & INVESTMENT WEEKLY
THE EDGE MALAYSIA

4 January 2023

MANAGING CYBERSECURITY CHALLENGES IN PURSUITOF DIGITAL TRANSFORMATION

"We also work with Agmo Holdings, one of the top mobile application development companies in Malaysia, which is also our strategic partner since day one of DOC2US.

"Leveraging their resources, talent and expertise in the space of cybersecurity, we constantly ensure that we are working in an effective ecosystem, from the front end to the back end, upholding upto- date practices in the cybersecurity as per industry standard," he said.

Choy said while cyberthreats are not at an alarming rate to the electronic prescription sector, due to the nature of personal health data, which is highly sensitive and private, the growing risks may potentially and inevitably lead to severe threats in terms of cybersecurity.

"Therefore, proactive, preventive and timely robust mitigating measures in cybersecurity are quintessential in order to reduce the risks.

"Constant maintenance, upgrading and improvements are also a must," he said.

What the experts say

Meanwhile, British-based security software and hardware company Sophos Group plc's managing director for Greater China, Southeast Asia and Korea Sandra Lee said as technology becomes a key component of services, cybersecurity is becoming a top priority for businesses.

She said given the current environment, it has become critical for organisations to protect sensitive intellectual property data, financial papers, and customer information.

Lee

"However, we continue to witness more data breaches and cyberattacks rising at an alarming rate, as cybercriminals become more sophisticated and complex in Malaysia," she said.

Lee said many businesses hire dedicated IT employees, but some opt to hire external IT service providers.

"The complexity of modern operating environments and the velocity of cyberthreats make it increasingly difficult for most organisations to successfully manage detection and response on their own, and the need for always-on security operations has become imperative.

BUSINESS & INVESTMENT WEEKLY
THE EDGE MALAYSIA

4 January 2023

MANAGING CYBERSECURITY CHALLENGES IN PURSUITOF DIGITAL TRANSFORMATION

"Organisations are struggling to keep pace with cyberattackers, who are continuously innovating and industrialising their ability to evade defensive technologies alone," she said.

Lee said that in Malaysia, cyberattacks have been on the rise in the past several years, making it a growing concern for organisations.

She said that according to CyberSecurity Malaysia, on average, Malaysia gets hit with 31 cybersecurity incidents a day, such as fraud, data breaches, and hacking.

"As of September this year, an estimated 6,002 cybersecurity incidents were reported. The number of cases in a year has been consistently surpassing 10,000 since 2018.

"These cyber incidents continued to be costly. It was reported that the nation lost US560 million to cybercrime last year," she said.

Separately, Japanese multinational cybersecurity software company Trend Micro Inc has warned that cyberthreat actors will ramp up attacks targeting security blind spots in the home office, software supply chain, and cloud in the coming year.

In conjunction with a report titled "Future/Tense: Trend Micro Security Predictions for 2023" released recently, Trend Micro managing director for Malaysia and nascent countries Goh Chee Hoh said since the end of last year, organisations in Malaysia have either returned to the office, permanently switching to remote arrangements, or opting for a combination of both.

Goh

"However, these arrangements take employees away from the safety of a more secure and monitored IT environment in the office.

"Renewed threat actors focus on unpatched virtual private networks (VPNs), connected home-office devices, and back-end cloud infrastructure in 2023.

"In response, organisations will need to focus on helping overworked security teams by consolidating attack surface management and detection and response to a single, more cost-effective platform," said Goh.

He said VPNs represent a particularly attractive target, as a single solution could be exploited to target multiple corporate networks.

Home routers will also be singled out, as they're often left unpatched and unmanaged by central IT, he said.