TECH

Public, financial and manufacturing sectors among top cyberattack targets in Malaysia

BY **ISABELLE FRANCIS**

Malaysia has, of late, been seeing increasingly sophisticated cyberattacks from threat groups such as organised crime groups, ransomware groups and initial access brokers (IABs).

To the uninitiated, ransomware groups are criminal organisations that specialise in carrying out ransomware attacks, which involve encrypting a victim's data to lock them out of their own files and demanding a ransom payment to decrypt it. As for IABs, they are basically cybercriminals who specialise in gaining unauthorised access to computer networks and then selling that access to other attackers, acting as middlemen in the cybercrime underworld and facilitating attacks by providing a crucial first step.

One of the threat groups was Desorden, a name that translates to disorder or chaos in Spanish, which targeted high-profile entities like Ranhill Utilities Bhd [KL:RANHILL] and Bintulu Port Holdings Bhd [KL:BIPORT] recently, intensifying the urgency for robust cybersecurity measures, says cybersecurity firm Ensign InfoSecurity.

The firm's latest report on cybersecurity, its fifth *Cyber Threat Landscape Report*, shows that the top five Malaysian industries affected by cyberattacks are manufacturing, technology, media and telecommunications, professional services, and retail.

These sectors faced ransom demands, data leaks and sale of access, which refers to unauthorised access to their computer networks or systems being sold illegally. Of the five sectors, all but retail are part of the national critical information infrastructure (NCII) regulated under the Cybersecurity Bill 2024.

Passed by the Dewan Negara in April this year, the bill, which will be gazetted into law, aims to enhance the country's cybersecurity by requiring compliance with certain measures, standards and processes in the management of cyber threats and incidents to NCII. Among its key provisions are the establishment of a National Cybersecurity Committee and the designation of NCII entities.

"Our latest global Cyber Threat Intelligence shows cyber activities linked to conflicts have significantly intensified, aligning with the World Economic Forum's *2024 Global Risk Report*, which ranks cybersecurity as the fourth most critical global risk over two years," says Clarence Chan, digital trust and cybersecurity partner at PwC Malaysia.

The growing intensity of ransomware attacks suggests a potential strategy targeting key businesses in the post-pandemic recovery.

According to Ensign Infosecurity, there is a trend of data leaks and sale of access — access that refers to a specific point of entry or foothold an attacker gets in a network or system, which becomes the "gateway" that can be exploited to launch further attacks or steal data. This reflects an ongoing interest in exploiting business vulnerabilities, which suggests that attackers' motivations extend beyond financial gain.

PWC MALAYSIA

PwC Malaysia's Chan: Digital banks, deeply embedded in the digital ecosystem, are prime targets for cyberattacks

KASPERSKY

Kaspersky's Yeo: The cost of damage to reputation is 7.5 times higher than direct recovery costs from a cyberattack

Another interesting development is hacktivism, as seen in hacker group DragonForce Malaysia's #OpsPetir campaign that targets Israeli institutions and those who directly or indirectly support Israel, says Ensign Infosecurity. It highlights how cybersecurity threats can escalate into cyberwarfare tied to geopolitical conflicts and ideological battles.

These evolving cyber threats underscore the need for Malaysian corporations and government agencies to strengthen their cyber defences.

According to Ensign InfoSecurity's cyber threat report, the manufacturing and government sectors accounted for 38.2% of organisational cyberattacks in Malaysia, with more than 58% of incidents driven by ransom, reflecting the global rise of ransomware threats.

"Malaysia has become an attractive destination for multinational companies looking to relocate high-tech manufacturing businesses. However, these companies are prime targets for cybercriminals because of their valuable data, continuous machinery operation and lower cyber hygiene," says Ensign Infosecurity general manager for Malaysia Chee Yee Cheng.

The cyber hygiene Chee talks about refers to the steps, practices and precautions that individuals and organisations take to maintain the health and security of their devices, systems and data. It is like personal hygiene, but for the digital world, focusing on preventive measures to avoid infections and vulnerabilities.

Government agencies that hold valuable data, including national security information, are also lucrative cyber threat targets. Public entities that have been attacked by ransomware groups in Malaysia include Agensi Kaunseling dan Pengurusan Kredit and Vopak Malaysia, according to Ensign Infosecurity's report.

CYBERSECURITY ASEAN

CyberSecurity Malaysia's Amirudin: Cybersecurity should be seen as an investment, not an afterthought

PATRICK GOH/THE EDGE

Universiti Pertahanan's Omar: These attacks continue due to many corporations in Malaysia taking defensive rather than offensive cybersecurity approaches

But there has been an overall advancement in detection capabilities as the average dwell time — which refers to the amount of time an attacker remains undetected within a compromised computer system — has dropped from 1,095 days to 49 days, according to the report.

Cost of cyberattacks and future trends

Quantifying the exact cost of cyberattacks is complex as they result in direct (financial damages, productivity loss, fines), indirect (reputational damage) and induced losses (loss of customers, increased spending).

The World Bank notes that from 2019 to 2023, about US$5.2 trillion globally was at risk from cyberattacks, with 10.5 million records lost or stolen monthly and a single large-scale attack potentially causing US$53 billion in economic losses.

Yeo Siang Tiong, Southeast Asia general manager for Kaspersky, says his firm blocked 2.5 million local threats and 26.8 million online threats targeting Malaysian businesses in 2023. "The cost of damage to reputation is 7.5 times higher than direct recovery costs from a cyberattack," he notes.

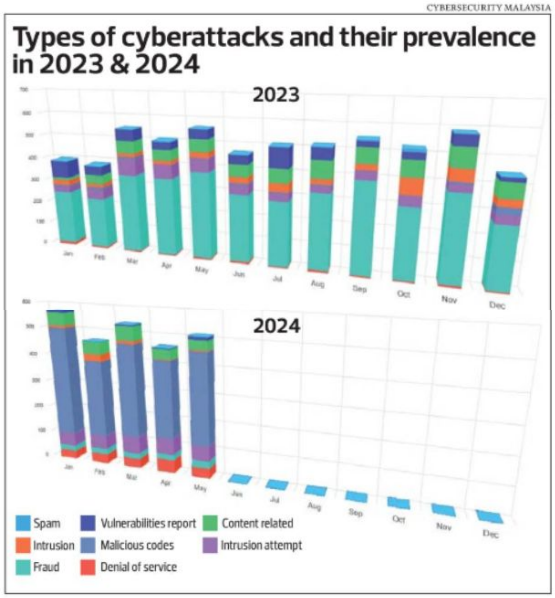
PwC's Chan says risk management capabilities need to surpass traditional risk analysis to assess the full financial impact of a cyber breach and should encompass broader repercussions such as business interruption costs, lost productivity and reputational damage. "Cyberattacks often have hidden costs beyond immediate financial losses," he adds.

Sectoral shift in cyber targeting

While financial institutions have historically been the primary targets, attacks have shifted to the manufacturing sector, which holds a vast amount of valuable data and is vital to economic stability and recovery. Disruptions can lead to severe operational and safety issues.

Telecommunications and other essential services also attract cyberattacks due to their central role in economic activities.

CYBERSECURITY MALAYSIA



Experts suggest that this shift may be influenced by geopolitical dynamics and hacktivism, with Ensight Infosecurity noting high cyber activity periods coinciding with political events in the second quarter to the fourth quarter of 2023, including when the six state elections took place in August that year.

Still, PwC's Chan affirms that financial services remain prime targets for cyberattackers due to their inherent value and, surprisingly, because of their adoption of new technologies. This is because the adoption of new technologies like cloud computing and AI, as well as expansion through third parties, inadvertently expands the "surface of attack", creating new avenues for potential attacks and leaving organisations vulnerable to exploitation.

The recent launch of digital banks in Malaysia adds another layer of complexity, he says. "Digital banks, deeply embedded in the digital ecosystem, are prime targets for cyberattacks. Cloud security, being a top risk concern among the C-suite in PwC's *Digital Trust Insights Survey 2024* (Malaysia report), makes them very susceptible to attacks."

He adds that the current regulatory framework does not yet promote threat intelligence sharing among institutions, although efforts are underway to address these challenges.

"There is a growing momentum for collaboration between regulators and FS (financial services) institutions to improve information sharing and enhance cybersecurity," says Chan, adding that while organisations often battle cyberattackers alone, lacking the unified front their adversaries possess, there is a growing momentum for collaboration between regulators and financial institutions.

He cites the example of the collaboration between Bank Negara Malaysia and CyberSecurity Malaysia to develop cybersecurity strategies to bolster Malaysia's financial sector and facilitate better information sharing, best practices and technical support to handle complex cyber risks.

Addressing humans as the weakest link

Human error remains a significant concern as attackers increasingly target this "weakest link" through fraud attempts.

While the number of fraud cases decreased in the first four months of 2024 compared with the previous corresponding period, financial losses from scams remain significant. Cybersecurity Malaysia reported 1,309 fraud cases in 1Q2024 compared with 3,705 in the previous corresponding quarter and 5,917 cyberthreat cases for the whole of last year.

"These attacks continue due to many corporations in Malaysia taking defensive rather than offensive cybersecurity approaches," says Prof Dr Omar Zakaria of Universiti Pertahanan Nasional Malaysia, or the National Defence University.

Continuously updating cybersecurity measures to adapt to new threats and technological advancements is crucial, though "having sophisticated security systems is useless without well-trained personnel", he says.

That highlights the importance of top management's commitment, says Datuk Dr Amirudin Abd Wahab, CEO of CyberSecurity Malaysia. "Lack of awareness in top management about the impact of cyberattacks contributes to the reluctance to allocate sufficient resources. Cybersecurity should be seen as an investment, not an afterthought."