RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg

No. 161 – 6 November 2023

Data Security in ASEAN's Digital Economy: Lessons from the Philippines

By Jose Miguelito Enriquez

SYNOPSIS

Recent data breaches targeting Philippine government agencies have underscored the need to ensure a secure digital data environment. As ASEAN continues to lay the groundwork for its digital community and economy, the responsibility for data security must be shared by both domestic policymakers and relevant ASEAN mechanisms and frameworks.

COMMENTARY

When a spate of ransomware attacks and data breaches across several government agencies in the Philippines made headlines in September and October 2023, the extent of each breach sparked major concerns from both policymakers and the public.

While cyberattacks appear to be unavoidable in this digital age, these events have unmasked several domestic and regional policy problems that will need to be resolved in order to prevent more damaging data breaches in the future.

Recent Data Breaches in the Philippines

News of data breaches in the Philippines began on 25 September 2023, when the Philippine Health Insurance Corporation (PhilHealth) reported to the National Privacy Commission (NPC) that its systems had been disabled by an attack from the Medusa ransomware group three days earlier on 22 September. An investigation by the state insurer revealed that the personal information of some 13 to 20 million members – approximately 18 per cent of the Filipino population – were disclosed by hackers in the dark web.

The PhilHealth incident represented the most serious data breach of a Philippine public agency since seven years ago, when local hackers obtained the complete database of registered voters from the Commission on Elections in the middle of the 2016 presidential election. It was the beginning of a series of breaches to affect the public sector over several weeks.

On 11 October, two weeks after the PhilHealth incident, the Philippine Statistics Authority (PSA) also informed the NPC that it had suffered a data breach. The country's civil registry reported that the information illegally accessed were largely connected to recipients of the government's social welfare programmes.

Two days later, the Department of Science and Technology (DOST) also reported that the contact information of around 1,000 individuals registered in its OneExpert portal, an online registry of the country's leading scientific experts, were leaked.

These successive data breaches sparked questions over the integrity of the cybersecurity infrastructure of the respective agencies.

The Need for Proactive Data Governance

Even though inquiries by the Philippine Senate and the Department of Health (DOH) have yet to conclude, the incidents have already revealed some policy challenges that the government will need to confront. As some challenges remain unresolved, innovative policy solutions are needed.

First, there is a need to swiftly inform affected data subjects of the breach and to institute methods of data recovery. On 13 October 2023, eight days after the hackers in the PhilHealth incident had uploaded the data into the dark web, the NPC launched a first-of-its-kind portal for the public to check whether their information had been compromised.

Second, there should be improvements in how agencies tasked with cybersecurity and data protection coordinate and collaborate with each other. The NPC and the Department of Information and Communications Technology (DICT) recently launched the Digital Security and Privacy Quick Response Project (DSPQR), a system designed to swiftly respond to complaints from the public regarding potential privacy violations.

While these services are welcome developments, there is a pressing need for more proactive data governance. The proposed e-Governance Act, a bill designed to speed up digitalisation and empower the DICT to institute information security standards in the government, was certified as urgent by President Ferdinand Marcos Jr in July 2022. However, the bill's enactment has been delayed in the Philippine Senate.

It is also apparent that necessary policy reforms should not only cover cybersecurity legislation. The PhilHealth had admitted that it had not been able to renew the license for its antivirus software due to revised government procurement rules, which contributed to weakened cyber defences once the ransomware had attempted to infiltrate its system.

ASEAN’s Data Security Challenge

The data breaches in the Philippines also demonstrate the continued threat of cybercrime within Southeast Asia. In its 2021 ASEAN cyberthreat assessment, Interpol noted that while ransomware risk in the region was relatively low, it could potentially increase in the future.

Indeed, the Philippines is not the only country in the region to have suffered a major data breach. SingHealth, Singapore’s state health insurer, experienced a similar data breach in 2018. Malaysian authorities reported that more than 800 gigabytes of personal data were leaked through breaches in the telecommunications, banking, IT, and government sectors in the first half of 2023.

As ASEAN’s digital economy continues to grow and its digital community continues to thrive, the region will surely have to grapple with the increasing risk of cyberattacks. This will require dynamic policy solutions both at the domestic and regional levels that could easily respond to cyber threats and close any capacity gaps between national cybersecurity agencies.

There have already been moves at the ASEAN level to respond to this data security challenge. In 2018, ASEAN published its Digital Data Governance Framework which outlines the regional organisation’s goal to harmonise member states’ data protection laws.

More recently, ASEAN launched its Regional Computer Emergency Response Team (CERT), an initiative to enhance regional readiness to respond to cyber threats in real time and facilitate information sharing and best practice exchange that will be operational by 2024. Data protection and cybersecurity are also topics that will be negotiated during the development of the ASEAN Digital Economy Framework Agreement (DEFA).

It is important for the region to continue to take data protection concerns seriously, especially in the context of building its digital community and economy. Not doing so will come at a high economic cost. Interpol cited in its 2021 report an estimate of US$1 billion worth of global financial damage from ransomware attacks alone.

Repeated data breaches at government agencies will not invite investor confidence in the region’s digital and tech industries, which will result in ASEAN missing its digital economic potential of US$2 trillion by 2030. It may also cause ASEAN to fail in delivering on its promise to provide trustworthy e-governance and other digital services as stated in the ASEAN Digital Masterplan 2025.

Continued regional dialogue will also be necessary to prevent ASEAN member states from resorting to restrictive data localisation policies in the name of data protection, which will also negatively impact the economy and regional connectivity. Lowering localisation barriers will be required if ASEAN is serious about meeting its goals of building a regional e-payments and QR code system.

Conclusion

To become a global digital player, ASEAN’s initiatives in the digital economy and connectivity must be pursued with a steadfast commitment to ensure an effective data security architecture.

Even if data security is primarily seen as a domestic policy challenge, regional frameworks will need to move from suggested outcomes to more binding commitments from each ASEAN member state. In a tight-knit digital economy, the region’s data security will only be as strong as its weakest link.

Jose Miguelito Enriquez is Associate Research Fellow in the Centre for Multilateralism Studies at S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. His research interests include digital economy governance in ASEAN, populist foreign policy, and Philippine politics and foreign policy.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg