INSIGHT: SOUTHEAST ASIA

Data breaches plague Philippines as country scrambles to bolster cyber defences

THE TAKEAWAY

The Philippines has faced a rash of recent cyberattacks targeting government websites and private sector entities, with massive data breaches undermining national security and exposing the personal data of millions of citizens. To bolster the country's cyber defences, the Armed Forces of the Philippines (AFP) has introduced a 'cyber command' and is recruiting cyber experts. Manila has also prohibited its military from using AI-driven applications. Experts have long warned about the Philippines's vulnerability to cyber threats due to a lack of adequate cybersecurity infrastructure and repeated failures to hold authorities accountable for their lack of preparedness.

IN BRIEF

- Cyber attackers defaced and temporarily disabled the website of the Philippines House of Representatives, the lower house of the country's congress, on October 13. The Department of Science and Technology and the Philippine Statistics Authority (PSA) were also recently hit, resulting in data leaks.
- Hackers leaked a substantial amount of personal data from the Philippine Health Insurance Corporation (PhilHealth) servers on October 3, after the insurer reportedly refused to pay a C$410,000 ransom. Thirteen million people were affected by the data breach, including overseas Filipino workers.
- The PSA admitted to a data breach impacting its Community-Based Monitoring System — a digitized data collection and processing system for implementing poverty-alleviation programs. The PSA stated that personal information such as national ID numbers and birth certificates were not impacted by the data breach.
- In April 2023, a massive data breach exposed the personal information of millions of Filipinos, including data from critical institutions such as the Philippine National Police, the National Bureau of Investigation, and the Bureau of Internal Revenue. Stolen data logs from compromised Philippine government subdomains later appeared on the Russian black market.

IMPLICATIONS

The government has come under scrutiny for the country's cybersecurity weaknesses. A recent assessment highlighted the Philippines's high susceptibility to cyberattacks due to widespread internet usage, low cybersecurity awareness, and underdeveloped cybersecurity infrastructure. In the latest attack, hackers exposed authorities' lax cybersecurity measures,

leaving millions vulnerable to identity theft and potentially exposing military intel.

This is not the first time the country has faced a massive cyberattack. In the "Comelec leak" of February 2016, the largest cyberattack in the country's history, hackers defaced the Commission on Elections website, revealing the theft of personal data from 55 million Filipino voters. The data appeared on a Russian-hosted website with unrestricted access a month later. The authorities have yet to hold anyone accountable for the Comelec leak.

The Philippines's defence chief noted that some cyberattacks were traced to foreign sources, but he did not name any country. To strengthen its cyber defences, the AFP will ease recruitment rules to attract cybersecurity experts. Earlier this year, cyber defence training was integrated into the Philippines's joint exercises with U.S. forces.

The government has also prohibited telecommunication companies from building cell towers on military bases to prevent security vulnerabilities and unauthorized access to military facilities. The Philippine defence secretary issued an order instructing all defence personnel to avoid using digital apps utilizing artificial intelligence for creating personal portraits, stating AI applications designed for generating portraits can produce a virtual character that emulates the speech and motion of an actual person, posing privacy and security risks.

WHAT'S NEXT

1. Investigations continue

Several government agencies have launched investigations into the multiple data breaches. The National Privacy Commission (NPC) has initiated an investigation into the extent of PhilHealth's data breach, hoping to identify and possibly prosecute those responsible. The PSA has initiated a separate investigation into its own data breach.

2. PhilHealth officials face possible legal action

The NPC could hold PhilHealth accountable for negligence. PhilHealth admitted that it was using an expired antivirus software at the time of the data breach.

3. Opportunity to work with Canada

On October 16, the Philippines and Canada signed a memorandum of understanding (MoU) on data protection. The MoU focuses primarily on co-operation between Canada's Office of the Privacy Commissioner and the Philippines's NPC. This co-operation covers mutual assistance in investigations on privacy and violations of data protection laws, co-ordination of joint investigations into cross-border data breaches, and knowledge-sharing and training on privacy and data protection trends.

Produced by CAST's Southeast Asia team: Hema Nadarajah (Program Manager) hema.nadarajah@asiapacific.ca; Alberto Iskandar (Analyst); and Saima Islam (Analyst). **Edited by:** Ted Fraser. **Design by:** Chloe Fenemore.