# Tackling cyber threats head-on

https://opinion.inquirer.net/180938/tackling-cyber-threats-head-on

The World Economic Forum highlighted in its Global Cybersecurity Outlook 2025 that leaders around the world “must adopt a security-first mindset” amid an increasingly complex cyberspace where threats are becoming more sophisticated and criminals more adept at infiltrating systems and perpetrating scams and fraud that can cripple countries, institutions, and individuals.

It is thus reassuring that President Marcos seems to have taken this stance with the approval last week of the more detailed National Cybersecurity Plan (NCSP) 2023-2028, described as “a comprehensive roadmap to protect Philippine institutions, resources and citizens from the growing threat of cyberattacks.”

Mr. Marcos had earlier issued Executive Order No. 58, which adopted the NCSP 2023-2028 of the Department of Information and Communications Technology (DICT) as part of his administration’s efforts to bolster the security and resilience of the country’s cyberspace.

“This plan is not just a defense mechanism; it is a proactive framework. It outlines effective policies, secures critical infrastructure, and establishes clear response protocols to combat cyber threats head-on,” said Information and Communications Technology Secretary Ivan John Uy.

With the plan being translated into concrete actions on the ground, the Philippines should go further up the ranking of the UN Global Cybersecurity Index. As of the September 2024 report, the Philippines climbed to 53rd place from 61st, with its score improving from 77 to 93.49 points, putting the Philippines among the Tier 2 or “Advancing” nations dedicated to securing their digital future.

## Threat assessments

Further advancement is in the cards as the NSCP calls for identifying the country’s cyber assets or critical infrastructure that needs to be zealously guarded against internal and external threats.

The NSCP also provides government agencies and institutions with guidelines on how best to respond to attempted or actual cyberattacks as previously experienced by the Philippine Navy and the Department of Migrant Workers.

The newly minted plan also outlines advanced threat assessments so that potential cyberattacks can be warded off. Close coordination with international partners is also part of the cybersecurity program. The DICT said these international partnerships would enhance its ability to “identify, mitigate, and respond to threats before they cause significant harm.”

Another central feature of the NSCP is the pouring of government resources into the upskilling of Filipinos in detecting and defeating cyber threats and adopting emerging technologies such as artificial intelligence, which can be deployed by hostile nations seeking to gain access to or take control of sensitive information regarding the country’s military or strategic assets.

## Greater vigilance

However, Uy said fortifying the country’s cyber defenses involves not just systems, hardware and processes but also greater vigilance against online scams. As Uy said, cybercriminals exploit not only the system itself but the “weakness” of individuals who are spending more time online as they carry out everyday activities in the digital world, whether it be for shopping, paying bills, catching up with friends, or working from home.

This is why a nationwide information campaign against sharing personal or sensitive information online to avoid falling victim to scams is part of the NCSP.

According to an Oct 2024 report by the Global Anti-Scam Alliance, Filipinos have lost nearly P460 billion over the past 12 months to scams launched mainly through ubiquitous text messages.

Separate data from the Bangko Sentral ng Pilipinas (BSP) showed that 59.48 percent of cyber fraud losses in 2023 were due to account takeover, identity theft, and phishing attacks, with users tricked into revealing personal or confidential information used to take over deposit or credit card accounts. The losses were more than double than those recorded in 2022, which means that cybercriminals are becoming more proficient as more Filipinos are embracing the digital lifestyle.

## Aggressive security posture

The BSP, fortunately, is doing its part in bolstering cybersecurity by directing banks and non-banks to adopt an “aggressive security posture”, which means investing in a robust fraud management system that can rapidly detect and prevent potentially fraudulent transactions such as unusually rapid account activity, changes in mobile numbers, and transactions done from unexpected geographical locations.

Such a posture must indeed be adopted across the board as bolstering cybersecurity is not just the job of the government and needs a whole-of-nation approach.

This is a concept that has been bandied about far too frequently for comfort but is applicable in this case as protecting the country against bad actors is a shared and sacred responsibility that must be borne by all Filipinos.

The consequences of failure to do so are just too high a price to pay.