- Computer crimes

PH HIGHLY PRONE TO CYBERATTACKS

Philippine Daily Inquirer · 3 May 2018 · A1 · By Doris Dumlao-Abadilla @Philbizwatcher

Most organizations in the Philippines are still among the most vulnerable to cybersecurity attacks, making it imperative for regulators to work harder to ensure a resilient ecosystem.

In a keynote speech during the Maybank cybersecurity forum yesterday, Assistant Secretary Allan Cabanlong of the Department of Information and Communication Technology (DICT) said that on a scale of A-to-E with "A" as the highest in terms of cybersecurity maturity, the Philippines was for now mostly in class "D."

"We rely on applying tools and technologies to assist us in reacting faster. So basically we are still reacting," Cabanlong said.

Class D is a notch better than Class E, in turn defined as a situation where actions are people-based and doing their best to put out fires.

In recent history, the Philippines has seen data breaches like that of the Commission on Elections data leak of 2016 while the last mile of the 2016 $81-million Bangladesh Bank cyberheist was carried out in the Philippines using loopholes then in the moneylaundering framework.

Cabanlong said banks, for their part, should be proactive or otherwise lose the confidence of their depositors.

"What we want to achieve is "a nation-state resilient in times of cyberattacks," Cabanlong said, referring to Class A maturity. "We need to have a predictive and focused security systems that can isolate threats and, for example, if the attacks are imminent, we can isolate, we can invert, or we can transfer or adapt our virtual system and our current system security."

Class B is defined as having a "dynamic defense," where the organization is predictive, agile and swift in finding, fixing and targeting response. Class B is when the organization is "loosely integrated with focus on interoperability and standards-based data exchange for situational awareness."

This year, the Philippines is set to launch a national cybersecurity platform, which will serve as point of contact for cybersecurity initiatives. The four key strategic imperatives are protection of critical infrastructure like utilities, mass transport systems and healthcare institutions; protection of government networks (public and military); protection of businesses and supply chains, and protection of individuals.

In the same Maybank forum, Bangko Sentral ng Pilipinas Deputy Governor Chuchi Fonacier said: "Cyberattackers are continuously evolving and changing their attack meth-

ods to bypass the controls. It's a perpetual arms race—something like an infinity war so to speak, coming from the latest Avengers movie series."

"The introduction of disruptive technologies into the picture—the likes of social media, internet of things, artificial intelligence, distributed ledger technology—places additional dimensions to cyberrisk that we should all be worried about," she added.