Eli M Remolona: Digital SOS - a comprehensive plan to combat cyber incidents

Speech by Mr Eli M Remolona, Jr, Governor of Bangko Sentral ng Pilipinas (BSP, the central bank of the Philippines), at the launch of the Financial Services Cyber Resilience Plan for 2025-2029, Manila, 6 August 2024.

* * *

Introduction

Senator Mark Villar, DICT (Department of Information and Communications Technology) Undersecretary Jeffrey Ian Dy, BAP (Bankers Association of the Philippines) President Jose Teodoro Limcaoco, PDIC (Philippine Deposit Insurance Corp.) President Bobby Tan, leaders in the banking and financial sector, distinguished guests and colleagues, magandang umaga po.

Digital transformation of the financial sector has brought about unprecedented opportunities. From mobile banking to digital payments, technological advancements have revolutionized the way we conduct our financial transactions.

However, with these advances come new challenges particularly in the realm of cybersecurity. Cyber threats are evolving at an alarming rate becoming ever more diabolical.

As financial institutions embrace digital innovation, they also become prime targets of cyber attacks. These attacks not only threaten the stability of individual institutions but also pose systemic risks to the entire financial system and undermine trust in the system.

Software glitch

Just three Fridays ago, we saw this in the recent global IT (information technology) outage which caused massive disruptions around the world. As the so-called blue screen of death experienced by Microsoft users worldwide unfolded, the incident reminded us of the risks associated with glitches in the digital supply chain.

Undersecretary Dy is right. It was not even a cyber attack. It was a software glitch-the kind of thing we feared would happen with Y2K (2000) more than 24 years ago.

Our own financial system and settlement system withstood the glitch. The BSP and the financial services industry have long been aware of these challenges.

Through the years, policy and supervisory reforms embodied in the BSP's (Bangko Sentral ng Pilipinas) 2015 Cybersecurity Roadmap were rolled out in coordination with industry stakeholders.

To further advance our shared cybersecurity agenda, I am pleased to now formally launch the final Financial Services Cyber Resilience Plan (FSCRP).

Our plan is not just a response with the threats we face but a proactive strategy to anticipate and mitigate future risks.

It is our commitment to creating a robust, secure, and resilient financial system that can withstand cyber incidents and recover quickly from them.

Allow me to share three crucial action points of this comprehensive plan.

Three-part plan

First is to step up capabilities. Our plan includes initiatives to sharpen the industry's capabilities in responding and recovering from major cyber incidents. This entails improvements in policies, processes, and people.

Second is to observe heightened vigilance. Our financial system is constantly under threat, and it is our responsibility to stay one step ahead. One of the key initiatives under this plan is to explore the creation of security operations centers.

This will serve as nerve centers of our cybersecurity efforts-enabling real time monitoring, swift incident response, and continuous improvements in our defensive capability.

Furthermore, the recent signing into law of the Anti-Financial Accounts Scamming Act (AFASA) is an important step in protecting our customers and ensuring trust in the system. This legislation has been described before, [it] provides mechanisms for investigating and addressing financial abuses.

Hence, I must express our heartfelt gratitude to Senator Mark Villar and Congressman Irwin Tieng for their unstinting support with the enactment of the AFASA.

Actually, AFASA is personally important to me because I myself have been a victim of a financial scam on social media a few weeks ago. There was a deep fake of me ostensibly recommending an investment scam. As long as they would do a deep fake of me, I wish they had made me better looking.

The third action item is to stay connected as we embark on the journey of implementing FSCRP. We emphasize the importance of staying connected working together.

One of the cornerstones of the FSCRP is the sharing of cyber threat intelligence across the financial community. Mechanism for information exchange can ensure that all stakeholders are equipped with the knowledge needed to anticipate, prevent, and respond to cyber threats.

Closing

I would like to extend our deepest gratitude to Secretary [Ivan] Uy and the DICT for spearheading the country's cybersecurity initiatives, their leadership and commitment for enhancing our national cybersecurity posture-which have been pivotal in our efforts.

I would also like to thank TJ Limcaoco and the Bankers Association of the Philippines for their support and active promotion of our shared goals.

May I also recognize contributions of our stakeholders, the Information Security Officers Group-ISOG, the Joint Cyber Security Working Group-JCSWG, the Joint Anti-Bank Robbery Action and Cybercrime Coordinating Committee-JABRACCC, and the National Cybersecurity Inter-Agency Committee-NCIAC, and all our other partners in the government and private sector in our fight against cybercrime.

To conclude my speech, let me draw your attention to a powerful and symbolic acronym-SOS, Step-up capabilities, Observe heightened vigilance, and Stay connected.

As you know, the acronym SOS is the universally recognized distress signal. Similarly, the FSCRP serves as our collective call to action-signaling the urgent need to fortify our defenses and safeguard our financial system against the threats of the digital age.

The 2024 to 2029 Financial Services Cyber Resilience Plan is a pillar of the industry's cybersecurity strategy. I urge all of you to embrace this plan as a commitment to building reliability, security, and trust in financial services for every Filipino.

Maraming salamat at mabuhay tayong lahat!