Benjamin E Diokno: Fostering cybersecurity for Bangko Sentral ng Pilipinas (BSP) supervised financial institutions

Speech by Mr Benjamin E Diokno, Governor of Bangko Sentral ng Pilipinas (BSP, the central bank of the Philippines), no occasion, Manila, 15 February 2022.

* * *

To the officers and representatives from the Israel Embassy in Manila's Foreign Trade Administration, members from the Bankers Association of the Philippines, cybersecurity experts, ladies and gentlemen, good day.

Let me start by thanking the Israel's Foreign Trade Administration for organizing this event and gathering experts from the Israeli government and private sector to share best cyber-resilience practices and solutions.

We hope to engage in conversation on how Israel's cybersecurity model and best practices can be adopted here in the Philippines and how all of us can work together in combatting rapidly evolving cyberthreats.

With the growing popularity of digital channels especially during the pandemic, cyber-attackers and scammers are increasingly targeting financial consumers to defraud them of their hard-earned money.

We, at the BSP, consider cybersecurity as one of our strategic priorities. This is in line with our mandate of ensuring stability, safety, and efficiency of the financial system.

In fostering cybersecurity, the BSP adopts comprehensive, agile, risk-based, and engaging approach which we term as CARE to stay ahead of our common cyber enemies.

This approach cuts across three key areas: first our regulatory policy framework; second proactive monitoring through our surveillance capabilities and lastly, promoting resilience through supervisory and oversight activities.

The BSP is adopting policies and regulations to guide banks and other supervised institutions to take on a risk-based approach to cybersecurity management.

Since 2013, the BSP has issued several regulations aimed at mitigating the effects of technology and cyber-related risks in BSP Supervised Financial Institutions (BSFIs).

These regulations address various facets of technology, such as social media risk management, business continuity management and multi-factor authentication.

Recent issuances also include specific guidance on managing data breaches and SMS-based attacks as well as combatting ransomware.

Allow me to share with you some major industrywide initiatives to strengthen the industry's cyber defenses and overall resilience.

First, in order to operationalize the BSP's role as the lead in the Banking Sector Computer Emergency Response Team (CERT) under the Department of Information Communications Technology (DICT), the BSP is developing the Financial Services Cyber Resilience Plan that will serve as the primary framework covering strategies and plans to strengthen cyber resilience in the financial services industry.

Second, we are also in the development stage of implementing the Advanced SupTech Engine for Risk-Based Compliance, or what we call ASTERisC*.

This is unified RegTech and SupTech solution that will streamline and automate regulatory supervision, reporting and compliance assessment of BSFIs' cybersecurity risk management.

Third, the BSP continuously engages with the BSFIs through the Bankers Association of the Philippines Cyber Incident Database or BAPCID. BAPCID is currently provided by CyberIn which is a cybersecurity service provider based in Israel.

It is a web-based portal and an industry cyber threat and best practices sharing platform where participants can report incidents and threats anonymously, receive threat intelligence feeds and threat advisories from the BSP.

Lastly, the BSP is currently coordinating with relevant government agencies and industry associations for a joint consumer protection campaign and message amplification to raise overall cyber awareness in the country.

Given the supervisory expectations and industry-wide cybersecurity initiatives, there are several ways Israel companies can help BSFIs in increasing their cybersecurity capabilities and maturity and the financial sector in general.

Considering the sophistication and maturity of Israel in terms of cybersecurity controls and management, the BSP and the BSFIs would greatly appreciate hearing Israel's expertise, knowledge and technology in the following areas:

- Cybersecurity trainings, education, and capacity build-up;
- Security Operations Center (SOC);
- Incident response and forensic investigation;
- Information sharing and threat-intelligence platform; and
- Set-up and establishment of Israel's Financial Sector and National CERTs.

In closing, I hope that this session will strengthen ties and cooperation between the Philippines and Israel so that our respective financial services sectors remain safe, innovative, and resilient in the digital economy.

Thank you for your attention.