

Media and Research - Speeches

Keynote Speech for Metaverse: I Am Secure Forum

Date: May 18, 2022

Occasion: Metaverse: I Am Secure Forum

Speaker: BSP Governor Benjamin E. Diokno

Members and officers of the Information Security Officers Group or ISOG, friends in the financial services sector, ladies and gentlemen, good day.

At the outset, allow us—the Bangko Sentral ng Pilipinas or BSP—to commend the ISOG for upholding its basic tenets on security awareness, inter-institutional incident response, and intelligence sharing.

Today's forum by ISOG will help strengthen information security through a discussion of something which the world is slowly being introduced to—a cutting-edge concept that is called the metaverse.

The pandemic has forced us to take the digital leap. I have to say that we Filipinos, resilient as we are, have embraced technology, innovation, and digitalization.

The numbers bear this out. In the financial sector, over four million digital accounts were opened at the onset of the community quarantine to facilitate digital payments and e-commerce transactions.

More than two years since the onset of the pandemic, remote work and school arrangements, contactless payments, online marketplace, and blockchain, have become commonplace.

Further into the future, we can expect a drastic change in our digital ecosystem with the recent developments on an old concept—the metaverse.

In a report by PricewaterhouseCoopers, the metaverse was described as a three-dimensional digital world where one can purchase and sell goods and services, sign and enforce contracts, recruit and train talent, and interact with customers and communities.

To support these capabilities, the metaverse makes use of a combination of innovative technologies which include augmented reality or AR, head-mounted displays, an AR cloud, artificial intelligence, spatial technologies, and many others.

Due to the promise of this virtual space, companies such as Facebook and Microsoft, among others, are allocating resources to their respective metaverse infrastructures.

As organizations rush to build the metaverse, cyber threat actors are also devising new tactics for these platforms and exploiting digital currency vulnerabilities to launch attacks on organizations and customers in the metaverse.

Since the potential of the metaverse is yet to be fully explored and realized, everyone is cautious of the potential threats, particularly on privacy and security.

As companies migrate to the metaverse, the BSP will remain vigilant of these developments in this uncharted area of cyberspace.

Consistent with our mandate of ensuring the stability, safety, and efficiency of the country's financial system, the Bangko Sentral will continue to adopt a comprehensive, agile, risk-based, and engaging approach toward cybersecurity.

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

Since 2013, the BSP has issued several regulations to address cyber-related risks for our supervised financial institutions. These regulations deal on various facets of technology such as social media risk management, business continuity management, multi-factor authentication, cybersecurity, electronic payments and financial services, virtual assets, and open finance.

We recently released advisories on control measures against cyber fraud and attacks on retail electronic payments and financial services, and security controls for application programming interface.

Likewise, we amended our regulations to enhance provisions on fraud management and technology outsourcing.

At this point, allow me to share some major industry-wide initiatives to strengthen the industry's cyber defenses and overall resilience.

- First, 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. This is part of BSP's role as the lead in the Banking Sector Computer Emergency Response Team under the Department of Information and Communications Technology.
- Second, we are implementing the Advanced SupTech Engine for Risk-Based Compliance, or what we call ASTERisC*, which is a unified regtech and suptech solution that will streamline and automate regulatory supervision, reporting, and compliance assessment of cybersecurity risk management for our supervised institutions.
- Third, we engage with the banking industry through the Bankers Association of the Philippines Cyber Incident Database or BAPCID. BAPCID is a web-based portal and an industry cyber threat and best practices sharing platform where participants can report incidents and threats

anonymously, and receive threat intelligence feeds and threat advisories from the BSP.

- Lastly, we are currently coordinating with relevant government agencies and industry associations for a joint consumer protection campaign to amplify our messages and raise overall cyber awareness in the country.

In closing, as we explore the opportunities offered by the metaverse, we must remain vigilant and ensure compliance with the standards of cybersecurity and data privacy consistent with established regulations and best practices.

With the rapid evolution of digital technologies, it is a must for us to continuously collaborate and share information as a community. This way, we can be proactive and take intelligent countermeasures to prevent, detect, and respond to these threats. Thank you for your attention.