Amando M Tetangco, Jr: Evolving cyber threats – are we prepared?

Speech by Mr Amando M Tetangco, Jr, Governor of Bangko Sentral ng Pilipinas (BSP, the central bank of the Philippines), at the Cybersecurity Summit for the Financial Services Industry, Manila, 24 November 2015.

* * *

Good morning everyone and welcome to this first Cybersecurity Summit for the Financial Services Industry.

We at the Bangko Sentral ng Pilipinas together with our Summit co-organizers BancNet and the Information Security Officers Group are pleased that you have joined us today to tackle the matter of cybercrimes. It is a fact: cybercrimes are being committed and financial institutions and financial consumers are being targeted.

Questions are being asked: Is it widespread? Can we stop cybercrimes? How can we protect financial institutions and financial consumers from cybercrimes? Distinguished representatives from the financial services industry, technology partners, stakeholders in our financial sector, we need to address these issues together.

Digital transformation in the financial services industry

In this digital age, the transformative power of technology is evident in almost all aspects of human undertakings - from modern science, education, health care, financial markets, to personal interaction.

Technology has likewise revolutionized banking and the manner it provides services and products. Financial customers can now perform banking transactions anytime, anywhere, at their convenience.

We have also seen the adoption of technology by BSP supervised financial institutions or what we call BSFIs in offering innovative products and in the delivery of fast and efficient service at affordable prices. And through technology, financial institutions tap a new breed of costumers who expect top-of-the-line services, financial solutions and products with the flick of a finger.

Based on our records as of December 2014, around 22 million users of electronic banking services and channels were being serviced by over one hundred banks across the country. Indeed, we have seen the volume and the value of transactions using e-money and e-banking channels grow steadily over the years.

Clearly, technology innovation has become an integral part of the business that it is now considered a “must” for BSFIs to survive and thrive in the digital world.

However, as in other fields, there is a downside that comes with innovations in technology - criminal elements have likewise evolved. While it is far from widespread, cybercrimes exploit advances in technology to expand, conceal and perpetrate their criminal activities from the real world to the cyber realm.

The cyber landscape

Indeed, cybercrimes have spawned a global industry with skilled hackers-for-hire, terrorists and syndicates that target critical institutions, infrastructure or economies.

The Philippines has not been spared from cybercrimes. Considered the social media capital of the world, the Philippines is on the radar screen of cyber criminals who try cyber attacks of varying complexities. Nevertheless, industry cooperation has enabled us to stop and capture cybercriminals.

For instance, authorities have arrested foreign nationals associated with cyber syndicates who were involved in ATM skimming, credit card fraud, and phishing incidents.

Can we stop cybercrimes? Well, studies indicate that cyber attacks and similar fraudulent activities against the financial services industry are likely to continue. But we can manage the risks related to cybercrimes.

Ladies and gentlemen. Our proper response should be to broaden, deepen and escalate our own anti-cybercrime programs and activities together. The stakes are high: institutional and personal losses resulting from cybercrimes could undermine the public's trust and confidence in financial institutions and ultimately our financial system.

The right mindset

So, what can we do to ensure industry-wide cyber security? How do we benefit from technology innovations while managing attendant risks and vulnerabilities?

Well, according to a SEACEN paper , the right mindset and a holistic multi-stakeholder approach for managing cyber security must be adopted. At the Bangko Sentral, we have reduced these to three major themes that form the acronym PIN. As you know, PIN refers to the personal identification number that must be kept secure at all times by its owners, to prevent unauthorized access to their accounts.

Allow me to share what PIN means to the BSP in terms of fighting cybercrime: P is to be proactive, not reactive; I is for information sharing and collaboration; and N is a constant reminder that cybercrime is NOT a technical issue.

I will now briefly discuss each of these themes.

P is to be "proactive, not reactive"

Given a dynamic technology landscape, there is no room for complacency, one has to be proactive. While it may take years to develop a robust and effective security infrastructure, it may only take minutes or even seconds for cyber criminals to breach its defenses.

And if criminals gain access to sensitive and critical information, they could trigger financial losses, business disruptions, damaged reputation, and even threaten the viability of the institution itself.

This calls for a continuing cycle of rigorous assessments of the institution's security versus emerging threats and risks. Cyber security controls, processes and procedures must be

continuously enhanced to mitigate weak points and achieve a higher state of resilience and maturity.

This is the same rationale that underpins the Bangko Sentral's policy to continuously enhance its supervisory framework through the issuance of guidelines, public advisories and memoranda, as well as the adoption of a robust and dynamic supervisory program.

For instance BSP Circular No. 808 issued in August 2013 provides the framework for technology risk management which takes into account robust and multi-layered security controls for cyber-risk prevention, detection and response. The BSP has also introduced various initiatives and supervisory enhancements for a more proactive approach to cybersecurity supervision and oversight. These shall be discussed in detail later by BSP Deputy Governor Nestor A. Espenilla, Jr.

I is for "information sharing and collaboration"

With the increasing sophistication and coordination of attacks, cyber security is no longer confined within the boundaries of each firm or organization; it is rightfully a shared concern by legitimate users of the cyber-environment. We believe information sharing and collaboration among various stakeholders is an effective, if not the best, antidote to the threat of cybercrimes. When attacks occur, early warning can spell the difference between business continuity and business catastrophe.

While industry-wide collaboration efforts and initiatives are already in place - in coordination with industry associations, namely the Inter-Network Anti-Fraud Committee (IAFC) through the BancNet and ISOG– the ideal would be to expand it to include all stakeholders, such as technology service providers, law enforcement agencies, regulators and relevant government institutions.

Ladies and gentlemen. In the fight against cybercrimes, let us remember to be inclusive, let us involve all stakeholders. In particular, financial consumers should be informed about cyber threats and how they can evade cyber attacks to protect their accounts.

Indeed, cyber security is a shared responsibility, and each of us has a role to play in making our cyber landscape safer, more secure and resilient.

N is for "not a technical issue"

Ladies and gentlemen, cybersecurity is not achieved merely by deploying state-of-the-art security appliances and devices. In fact, a number of organizations with the most secure defenses have been subjected to cyber-attacks.

More than a technical issue, cyber security should be a top priority concern by the Board and senior management. Cyber security initiatives and investments must be supported at the highest level of management to ensure their sustainability and adoption across all processes within organizations. As a wise man once said, it is the "tone at the top" that defines an institution's cyber security culture.

Given the crucial role that the Board and senior management play in creating a safe and sound cyber security regime, I am pleased to see that we have CEOs, members of the Board and senior management at this Summit. This speaks of executives walking the talk

on ensuring cyber security; this also reflects a high degree of cyber governance in the financial services industry. You all deserve a round of applause.

Parting shots

Ladies and gentlemen. We are fortunate to have with us at this summit, distinguished experts on dealing with cybercrimes. Also with us are industry players deeply involved in ensuring cyber security who will discuss current and emerging cyber threats confronting the financial services industry. Also up for discussion are international best practices on cyber security management.

Let us therefore maximize the opportunities to be proactive, to inform and collaborate, and to remember that cybercrime is Not merely a technical issue. These are the lessons of PIN.

Indeed, there are many cyber challenges ahead of us. With this summit, I hope we can put our collective wisdom and expertise together to collaborate and develop comprehensive and united solutions for a safe, secure and healthy cyber environment. Together, let us fight cybercrimes.

Our ultimate goal is to propel our financial sector forward to an environment where robust financial institutions reach out to the unserved and the underserved to achieve financial inclusion that promotes inclusive growth.

Maraming salamat. Mabuhay ang ating mahal na bansang Pilipinas! Mabuhay po tayong lahat!