Opening Remarks

Veerathai Santiprabhob, Governor of the Bank of Thailand

ASEAN Banking Cybersecurity Conference 2019

Crystal Hall, 3rd Floor, The Athenee Hotel, Bangkok, Thailand
6 September, 2019

TBA Board of Directors,
TBA members,
Members of ASEAN banking community,
Distinguished guests,
Ladies and gentlemen,

I am delighted to be here with you this morning, and I would like to thank TB-CERT for inviting me to speak at this event.

Technology and the internet have undeniably become integrated into our daily lives. Customers' behaviors continue to evolve and adapt to the technological progresses. In response, new technologies are developed to serve and accommodate customers' ever-evolving needs. A prime example is the invention of smartphone over a decade ago, which has completely transformed our ways of lives and increased people's connectivity to unprecedented levels. The banking industry, too, is undergoing massive digitalization, from the user-facing tools like mobile banking apps to back-end infrastructure and essentially everything in between. These developments are the key drivers behind the convenience and productivity that we all enjoy today.

But, inherent to any invention, these technological revolutions come with their own form of risk: cyber risks. The more "digital" banks become, the more channels for potential points of attacks from cyber criminals, who are constantly evolving to exploit new loopholes. Even when these loopholes are identified and patches are issued, delayed updates could also pose potential risk.

We have repeatedly witnessed that the various—and many times severe—cyber-related incidents often revolve around financial institutions. Some infamous examples include the Bangladesh Bank incident, the hacking of ATMs in Taiwan and various other countries, Target's credit card data breach which resulted in data of

over 70 million credit cards stolen, Equifax's data leakage in which the company was fined 700 million USD, and more recently the case of Capital One Bank in which over 100 million customers' data were leaked. Thailand is also not immune to these cyber threats. A state bank's ATMs were hacked, customers' data from 2 large banks were leaked on the Dark Web, and the WannaCry ransomware outbreak.

In addition to attacks on financial institutions, customers' behavior and lack of cyber threat awareness also pose significant cyber risks as well. Social media scams through LINE or Facebook Messenger in which attackers pretend to be the victim's acquaintance, asking for a favor to transfer money; or users' submitting their bank account information to questionable, illegal gambling website from which their data eventually got leaked a few weeks prior are some examples of cyber-attacks that hinge on the user's inexperience or lack of awareness of online threats.

As such, I don't think it is an over exaggeration to say that cyber threats have kept many bank executives and regulators awake at night given the nature of these threats that can occur anytime and anywhere without warning, and the significant damage they could cause.

In addressing these threats, it is important to operate under the assumption that it is not a matter of "if" but rather "when" these threats will occur, and focusing solely on "protection" and "detection" is no longer sufficient. In other words, cybersecurity alone is not enough, but we also need to proactively think about cyber resilience: how do we not only prepare, but also withstand and recover from disruptions. In the short time I have today, I'd like to highlight three key drivers for effective cyber resilience.

First, cyber resilience is not only the responsibility of a company's IT department, but rather an important, organization-wide agenda. The board of directors and senior management must understand and endeavor to prioritize cyber risk management frameworks into the organization's operation. This includes making sure that cyber resilience policies put in place are applied effectively, setting a clear organizational structure that includes the roles and responsibilities of staff across all levels, establishing a risk management process according to international practices, and ensuring that employees are always vigilant on cyber security issues. The Bank of Thailand, for example, requires financial institutions to have at least one member with IT knowledge or IT-related experiences to be on the board of directors. We also organize regular capacity-building courses for board members and high-level executives from Thai financial institutions to provide them with the knowledge and

understanding of how to address cyber threats. In addition to tone from the top, staff members at the operational level must also be more vigilant of the cyber risks involved in their day-to-day tasks.

Second, while in the past much efforts had been put on reinforcing protection and detection systems, we must now shift our focus towards improving response and recovery. Readiness in addressing cyber-attacks—preparing a response plan or a playbook—remains a common gap among financial institutions. Frequent cyber exercises are also crucial, as vulnerability of response plans are often discovered during these exercises which allow organizations to continually improve their response processes. Regular practice is the best practice. Not only should these exercises be done by individual firms, but also at an industry level. The financial sector, for example, has started these exercises within the banking sector and will soon expand to other parts of the financial sector. As time goes by, our society becomes more interconnected, and eventually these cyber resilience exercises need to be done at the inter-industry level. For instance, the banking sector needs to have joint exercise with telecommunication companies for scenarios involving mobile banking attacks, or with the utilities sector for power outage scenarios.

Third, collaboration and information sharing are crucial in strengthening the overall cyber resilience. Cyber threats are becoming much more complex that an individual organization's defensive technology may not be able to catch up. Close cooperation and sharing of cyber threat information will help organizations better monitor the development of cyber threats, recognize unfamiliar threats, and develop more comprehensive plans for dealing with such issues. Cooperation is also more than just information sharing: whether it is cooperation in terms of supervision, development of standards, cyber exercises, or capability building. These kinds of cooperation that would eventually create a "Cybersecurity Ecosystem" requires efforts from all sides, including governments, regulatory agencies, the private sector, and the education sector.

It is very welcoming that today there are already a number of information sharing platforms available at the national, regional, and international levels. Thailand's finance, banking, capital markets, and insurance industries have established a Computer Emergency Response Team (CERT) for their respective industry. The teams share cybersecurity information on a daily basis. At the regional level, ASEAN has established the Cybersecurity Resilience and Information Sharing Platform (CRISP). The Central Banks, Regulators, and Supervisors (CERES) forum serves as a

platform for the international community. These collaborations on multiple levels present opportunities for countries to learn from one another. More recently, under our capacity as the 2019 ASEAN Chairman, Thailand has collaborated with the Bank for International Settlement (BIS) to organize the ASEAN Financial Regulators' Program on Cyber Resilience, a series of training programs, the last of which concluded just yesterday. We envision that these Cyber Range collaborations will continue to be held for ASEAN members going forward.

Although the financial sector has made significant progress in terms of cyber resilience, the never-ending development of cyber threats means that we too must continue to improve our defenses. In this regard, there remains many issues which the Bank of Thailand, along with other central banks in the region, intend to drive forward, such as overseeing more comprehensive cyber resilience policies and promoting the development of human resources. In response to cyber-attacks that may target vulnerable customers, it is crucial that we strive to increase consumer technology literacy to nudge them towards safer cyber behaviors and ensure a sufficient level of Cyber Hygiene.

Ladies and gentlemen, I would like to take this opportunity to thank the Thai Bankers' Association and TB-CERT for organizing "ASEAN Banking Cybersecurity Conference 2019" which has brought our ASEAN members together today. This is an opportunity not only to gain knowledge from expertise in different areas, but also to enhance connectivity and collaboration among professionals which is vital to improve our Cyber Resilience going forward. I wish all of you a fruitful conference and an enjoyable stay in Bangkok. Thank you.