Muhammad bin Ibrahim: Demystifying cyber risks – evolving regulatory expectations

Keynote address by Mr Muhammad bin Ibrahim, Deputy Governor of the Central Bank of Malaysia (Bank Negara Malaysia), at the SEACEN Cyber Security Summit 2014 "Demystifying Cyber Risks: Evolving Regulatory Expectations", Kuala Lumpur, 25 August 2014.

* * *

It is my pleasure to welcome you to Sasana Kijang for the SEACEN Cyber Security Summit 2014. The theme "Demystifying Cyber Risks: Evolving Regulatory Expectations" is apt given that the subject is not well understood by most and developments in this area tend to change at an exponential rate. I would therefore like to commend the SEACEN Centre for taking an important step to strengthen awareness and promote collaboration among supervisors on cyber security issues.

Cyber security risk gives rise to new challenges

Cyber security risks are inherently complex. These threats are real and can have severe implications on financial institutions should the threat not properly managed. In 2013, more than 100 million customers had their credit card and personal information stolen as a result of a data breach at a major retail outlet in the US. The estimated cost of this incidence was close to $150 million. For a single cyber attack, this is a staggering amount.

Increased cyber security risk is a direct consequence of the more digital world we live in, where computing devices, online networks and technology infrastructure are becoming more integral to our daily lives. Modern financial systems also operate and depend heavily on these same networks and infrastructure. We can expect the management of cyber security risk to be even more relevant and challenging in the financial sector. Financial institutions operate critical payment and settlement systems and maintain sensitive customer information. This makes the financial system an attractive target for cyber security attacks. The adoption of more sophisticated and digital technology for key systems such as trading platforms, data warehouses and internet banking introduces new sources of cyber security issues which could be more systemic. For example, a distributed denial of service (DDoS) attack on banks in the United States in 2013 caused serious disruptions in access to online services. While causing no major losses, the increasing sophistication of the cyber attack raises concerns over critical functions of the financial system. This offers a glimpse of the potential harm confronting us in the years ahead.

No doubt, technological advancements are a force for good. They are crucial to the efficient operations of the financial system, such as through greater automation of processes, better risk management and the wider offering of products served through online platforms. This in turn benefits business and retail customers. However, the increasingly widespread adoption of advanced technology also exposes financial institutions to new cyber security risks that need to be better understood. For example, increased accessibility to a financial institution's systems by employees and customers through the use of smartphones and tablets serve as entry points for cyber crime. Cloud computing and the use of third party services also have the potential to undermine firewalls. Putting a balance to the needs of various parties would be a challenging task.

As information technology grows, so do the capabilities of cyber criminals. These criminals have a wide range of tools to execute cyber attacks, many of which are easily obtainable and relatively inexpensive to procure. For example, cyber criminals can now control networks of compromised computers through "botnets" that enable anonymity. This access can be bought or rented online. In the hands of criminal or organisations that are determined to

disrupt national stability, botnets could be used to steal sensitive data or disrupt access to critical national infrastructure. Industry players, security firms and financial supervisors may easily find themselves in a cat and mouse game, where the ability to attack constantly outpaces the ability to defend.

These challenges demand a stronger and forceful response by all parties. Recent global regulatory reforms, such as the Basel III capital adequacy and liquidity rules, have tended to focus on financial risks. There has been much less focus on technology and cyber security risks despite the real systemic threats that they pose. So far, no financial institutions in this region have encountered an attack, severe enough to disrupt its critical services or cause material losses, but we cannot leave this to chance. The regulatory community and the industry must act to ensure that supervisory practices and internal controls within the financial institution remain vigilant and install the necessary safeguards against cyber security threats. There is a need to intensify our efforts in this regard and to place cyber security issues as a priority in our effort to make the financial system safe and sound.

Driving the cyber security agenda forward in the industry

In many countries, supervisors place significant emphasis on the oversight role of the boards of financial institutions as a primary line of defence. However, in reality, the focus on technology risk remains superficial in most board discussions. In 2012, a survey by Carnegie Mellon among senior executives and directors from among the world's largest firms across various sectors indicated that, 57% of respondents viewed that boards are not reviewing the existing policies for cyber-related risks sufficiently. Faced with a multitude of issues, board members are likely to prioritise headline issues that are more pressing or more directly related to the core business of the financial institution. More often than not, the cyber security agenda gets side-lined.

Supervisors have an important role in encouraging boards to strengthen their oversight over cyber security risks. In fact, because of its importance, a mandatory requirement ought to be the norm. In the digital era, cyber security demands a more strategic and specific focus and should be properly understood at all levels within the financial institution. Supervisors need to ensure that cyber security becomes a permanent agenda in the board's engagements with senior management. There should be on-going dialogue about emerging trends and vulnerabilities, and the measures in place to address them. This would raise awareness of security concerns and ensure that existing cyber security risk management practices are effectively integrated with the firm's wider business strategy and risk appetite.

It is equally important to ensure that the board of directors' of the financial sector invests adequately in cyber security infrastructure systems and procedures. The amount of funds allocated should commensurate with the nature and scale of an institution's business activities, and its strategic direction. 65% of respondents in an Ernst and Young survey in 2013 cited an insufficient budget as the primary challenge for information security functions to meet the demands of the business. As supervisors of the financial system, we should require financial institutions to continuously benchmark infrastructure and systems against leading best practices in cyber security. This includes the application of security testing measures to identify key potential vulnerabilities in a financial institution's information security system. Financial institution ought to take a long term view on this matter. Supervisors can do more to encourage financial institutions to improve the response to evolving threats by ensuring continued access to external and internal expertise necessary to rapidly develop controls and defences that protect critical assets and operations.

Today, the lack of skilled resources remains a key barrier to value creation in regard to information security. Financial institutions must be convinced that there is a long term gain by hiring cyber risk specialists, including in-house specialists that can develop timely and customised solutions based on a deep understanding of the institution's operating systems, business needs and organisational culture. There is also substantial scope for the financial

industry to work more closely with telecommunications firms, internet service providers and other vendors to ensure that cyber criminals do not take advantage of external vulnerabilities to penetrate the security perimeter. In most countries, such initiatives lacked the coordination necessary to provide an effective system-wide defence against cyber crimes. Part of this change will be influenced by the attention and importance that supervisors place on the management of security risks.

The role of supervisors and the public sector

In the face of further digitisation of the financial sector, the responsibility of financial supervisors in ensuring the stability and integrity of the financial system will become increasingly challenging. Regulatory and supervisory frameworks need to be updated to acknowledge the significance of cyber security threats. It is necessary for us to establish a clear expectation on the management of such risks by financial institutions. We should outlined clearly in key areas that could cause threats such as outsourcing arrangements with third party service providers, stress testing, anti-money laundering requirements and business continuity plans. To carry out our oversight responsibilities effectively, supervisors will also need to develop the capacity to assess and identify key vulnerabilities in the increasingly sophisticated web of information networks and systems upon which the financial sector depends. For one, supervisors need to arm themselves with the skills and knowledge to make assertive and rigorous assessments of a financial institution's IT risks and be able to form judgments about the adequacy of control systems. Training and development programmes for supervisors should therefore give the same emphasis as other critical risks such as credit and market risk. The establishment of specialist supervisory teams or units dedicated to IT risks also plays an important role in building a strong knowledge base within supervisory authorities to support effective supervision of IT risks. Just like industry practitioners, it is imperative that any knowledge and skills acquired by supervisors are in tandem with the latest developments in both cyber security and cyber threats.

Beyond efforts to build technical capabilities, supervisors and other law enforcement agencies also need to be equipped with the legal powers to investigate and prosecute cyber criminals. Given the borderless nature of cyber risk, this is a significant challenge. Cyber crimes can be launched from anywhere in the world, with targets in many countries. This underscores the need for a more coordinated global response that should involve criminal law enforcement agencies and financial regulatory authorities. In this regard, cross border collaboration must be intensified to establish information sharing arrangements on cyber risks and trends. Looking further into the future, a more comprehensive legal international framework, such as a treaty, may be useful to empower authorities to bring cyber criminals to justice.

Concluding remarks

Let me now conclude. The digitisation of the economy and the financial sector is a process that cannot be stopped and we need to embrace it to our benefit. As financial institutions grow bigger and have greater international presence, the nature and extent of cyber risks will continue to expand. Events like this summit help propel the cyber security agenda forward. It is my hope that the sharing of knowledge and experiences here will generate new ideas to stem threats to cyber security. With that, I wish you all a productive and fruitful experience for the next two days. Thank you.