Speech by H.E The Governor of Qatar Central Bank

At the Carnegie Mellon University, Qatar

November 14, 2016

Cyber Security and Financial Stability: Some Thoughts

Thank you for inviting me to speak at the *Dean's Lecture Series* today. This is indeed a great pleasure to be here again to discuss another topical subject like **cyber security** this year, which has gained importance in policy making in the financial circle across the globe. Globally, along with rapid use of technology in the area of financial services and growing interconnections between operators in financial markets, cyber security threats have also been increasing and becoming more complex. Both attackers and their motivations are becoming more diverse – from financial gains to disrupting activity to causing political and financial instability. According to the BIS (2014), cyber-attacks against the financial system are becoming more frequent, more sophisticated and more widespread. To understand the seriousness of the issue, look at what the data says. Ministry of Interior's published data shows, cybercrime in Qatar increased by 52% in 2015 over last year. In the UK, a country, which I believe have taken a proactive approach in combatting the cybercrime, according to some published report states 65% of the large firms had a cyber breach last year and 25% of the firms experience at least one cyber-attack per month. Cyber-crime is considered as the second most reported economic crime in the case of the Middle East.

As you all know, Qatar Central Bank is the regulator of banks and also the payment and settlement system. With financial stability being a key objective, we attach significant focus on the safe and efficient

operations of the financial market infrastructure, apart from prudential regulations and supervision in Qatar. Today, I will talk on Qatar Central Bank's approach to cyber security issues in the broader context of maintaining and promoting financial stability in Qatar.

I. Introduction: Importance of Cyber-security for Financial Stability

Banking sector in most part of the globe was not complex until mid-1990s. With the advent of technology, the horizon of the banking have undergone a major shift. Competition added more fire, with banks offering customers with complex products and services in order to improve their customer base. Along with the increase in easiness to conduct banking transactions using the tip of the fingers, fraudsters also discovered alternatives to attack with the help of the same advanced technology. New channels like mobile and online banking also opened new doors for cyber attackers. Cyber criminals adopt different methods to break into the virtual world of banking to steal the information and ultimately the funds deposited with the banks. Online phishing, hacking, key stock logging malware, identity theft, remote access Trojans, etc., are some among the various tools used by the cyber criminals. Banks on the other hand have increased their attention against these attacks through communication, educating their customers, and promptly reacting to the attacks, etc. Since the cyber risk is a highly complex and rapidly developing phenomenon, identifying and managing the risk has

become challenging. Most of the cyber-attacks are continuous malicious actions and are difficult to detect and recover.

The motives behind the cyber-attack may vary, on a lower scale it may be only for “hactivism”. Hacking also sometimes targets a particular institution, or country so as to disrupt the normal functioning and to cause large damage to the reputation of the affected institution/country. In case the target is an institution, eventually it may lose customer confidence and the resulting financial loss may be significant.

Capturing confidential information is another motive. Again it can be for financial motive or otherwise. In any case, it will disturb the regular functioning of the financial sector and can affect the economic growth eventually. Any cyber-attack, whether it is small or big, causes financial loss or not, has to be examined with utmost importance since some of the not so serious attacks may be an indication for large attacks on the institution or system. Thus, the importance of protecting information and providing continuity to business and safety to national IT infrastructure have attained greater attention in the recent years. These issues are discussed not only among the IT sector, but also between the international bodies, governments, central banks and banking community as a whole.

The very complex nature and unpredictability of cyber risk warrants the urgency of having a coordinated approach to manage it. From a central bank perspective, oversight of the payment systems as

regards to its safety, security and efficiency is of great importance. Payment systems are the backbone of any financial system. Payment systems support trade, financial intermediation and overall economic activity. A weak payment system infrastructure reduces these activities and weaken the monetary policy transmission channel and the financial stability of the system. Thus, the payment system infrastructure, or in a broader sense the financial market infrastructure plays a greater role in promoting the stability of the financial system. Taking this into consideration, international standard setting bodies have taken a wide range of measures to effectively deal with cyber attacks and the worst-case scenario.

II. Global Standards: BIS/IOSCO Guidelines

Let me discuss now on the initiatives taken by the Bank of International Settlement (BIS) and the Committee on Payments and Market Infrastructure.

The guidance provided for resilience on cybersecurity is in the wider domain of Principles of Financial Market Infrastructure. The Principles of Financial Market Infrastructure are international standards for financial market infrastructure, developed by the Committee on Payments and Market Infrastructure and the Technical Committee of the International Organization of Securities Commissions (IOSCO). The Principles of Financial Market Infrastructure considers the cyber risk as an operational risk. In this

framework, cyber attacks are classified as “risks that may take the form of determined malicious action by third parties intent on creating systemic harm or disruption, with contributing financial losses”. Given this unpredictability, the guidance provided by the Committee on Payments and Market Infrastructure and IOSCO observes that cyber risk pose challenges to financial market infrastructure’s traditional operational risk management frameworks. In particular, the guidance documents notes that:

1. Unlike most other sources of risk, due to the presence of an active, persistent and sometimes sophisticated adversary, cyber-attacks are often difficult to identify, remove and determine the extent of damage.
2. Since financial market infrastructures are interconnected, cyber-attacks could come through the financial market infrastructure’s participants, linked financial market infrastructure, service providers, vendors and vendor products. Financial market infrastructures could themselves become a channel to further spread cyber attacks.
3. Cyber attacks can be silent and spread rapidly within a network of systems.

In order to systematically and proactively manage and mitigate the cyber risk, the guidance on cyber resilience for financial market infrastructure documents the importance of a strong cyber governance. First of all, a financial market infrastructure resilience framework has to

be clearly defined. The framework should articulate the financial market infrastructure's objective and risk tolerance. In particular, how the financial market infrastructure will effectively identifies, mitigates and manages the cyber risk to achieve its objective. Further, through continuous audit and compliance, the Board and senior management should assess and measure the adequacy and effectiveness of the financial market infrastructure's cyber resilience framework. Financial market infrastructure should also establish a comprehensive mechanism for detecting the cyber-attacks through continuous monitoring and step-by-step detection processes. This will facilitate its incident response process and support information collection for the further investigation including legal and forensic audit. A well designed contingency planning has to be in place to ensure a smooth flow of payment and settlement. Financial market infrastructure should analyze critical functions, transactions and interdependencies to prioritize resumption and recovery actions. Identification of potential threats through threat intelligence processes, or threat information gathering will also help in proactive mitigation. The guidance document also notes the importance of creating and developing the predictive capabilities of future cyber events based on analyzing activity that deviates from the baseline. For the purpose, financial market infrastructure should capture data from multiple internal and external sources, and define a baseline for behavioral and system activity.

III. Cyber Security Initiatives in Qatar

Qatar has taken speedy steps towards digitalization and in the near future, a significant part of its GDP is expected to come from the digital economy. Given this fact, a proactive approach in managing and mitigating the cyber risk has become a need of the situation to ensure financial stability. Now, let me touch upon some of the major initiatives taken by the national authorities to address the challenges posed by the malicious cyber risks in Qatar.

In 2013, the Prime Minister established the National Cyber Security Committee to provide a governance structure for collectively addressing cyber security issues at the highest levels. The main objective of the committee was to develop a cyber policy at the national level and to ensure that all public and private entities are adopting the right cyber agenda to protect themselves. The Committee developed Qatar's National Cyber Security Strategy, which represents a blueprint for moving forward to improve Qatar's cyber security. The National Cyber Security Strategy combines good governance with a set of cyber security initiatives, measures, and awareness programs that will result in an efficient protective strategy in long term.

Qatar's vision and approach on national cyber security is supported by five major objectives.

1. Safeguard the national critical information infrastructure;
2. Respond to, resolve, and recover from cyber incidents and attacks through timely information sharing, collaboration, and action;

3. Establish a legal and regulatory framework to enable a safe and active cyberspace;
4. Foster a culture of cyber security that promotes safe and appropriate use of cyberspace; and
5. Develop and cultivate national cyber security capabilities.

To accomplish the national vision on cyber security, a formal governance structure to implement and manage execution of the National Cyber Security Strategy is established. Towards this, a Cyber Security Coordination Office is being established. This Office will be responsible for: (i) establishing priorities to promote the highest level of cyber security in Qatar, (ii) providing strategic direction for Qatar's cyber security efforts, and (iii) working in close partnership with organizations with cyber security missions and mandates to fulfill the objectives of the Strategy.

Prior to the establishment of National Cyber Security Strategy, policies and procedures were already implemented to safeguard the Critical Information Infrastructure.

I would like to mention some of those initiatives.

National Information Assurance Policy and the National ICS Security Standard are developed, which provide important guidance on security controls and practices to protect critical information infrastructure and improve internet security. In addition, as part of the National Information Assurance Framework, Qatar published Anti-Spam

Guidelines in 2013 to reduce the impact of unsolicited electronic messages (or spam) on entities and individuals.

To improve the security of financial transactions, the Qatar Central Bank issued Banking Supervision Rules, which identifies the cyber security controls that banks must follow, such as reporting cyber incidents and attacks to Qatar Central Bank and the Qatar Computer Emergency Response Team (Q-CERT).

Another existing initiative is the establishment of Information Risk Expert Committees in the finance, energy, and government sectors. These public-private partnerships deal with a variety of cyber security issues, including threats, vulnerabilities, and consequences; readiness activities; and mitigation strategies. The Information Risk Expert Committees facilitate the exchange of information within each sector and with other stakeholders to enhance Critical Information Infrastructure resilience.

In December 2013, Qatar held its first national-level cyber exercise for critical sectors, including banking and finance, energy facilities and networks, government, and transportation, to enhance these organizations' capabilities to identify and mitigate cyber threats.

Other initiatives in enhancing Qatar's ability to investigate cybercrime include establishment of capabilities in digital forensics, developing strong international alliances and becoming an active participant in global efforts to shape international standards and norms on cyber

security, including efforts in the International Telecommunication Union and Forum for Incident Response and Security Teams.

IV. Qatar Central Bank Guidelines on Cyber-security

We have discussed global as well as national coordinated approach in monitoring and mitigating cyber risks. Now let me touch upon some of the measures taken by Qatar Central Bank to combat the technology risks in the financial sector.

In tandem with the global technological advancements, technology driven services provided by the Qatari banking sector has grown significantly in the past few years. As a result, the use of technology in daily operation of the sector has become important, as they are responsible to keep the business activity operations healthy.

I would like to mention some of the existing instructions to the banks in safely conducting internet and mobile banking and card payments.

- A prior approval from Qatar Central Bank should be taken if a bank wishes to implement an online banking service where customers can make transactions.
- At least two-factor authentication is required.
- Public Key Interface (PKI) technologies should be used for authentication
- At least two penetration-testing sessions per year and four regular vulnerability assessment exercise per year has to be conducted.

- All payment card must be Europay Mastercard and Visa (EMV) compliant

An update on the current instructions and guidance are underway and is mainly drawn in the lines of National Information Assurance Policy, NIST Cyber Security Core Framework, etc. as well as drawing inputs from guidance on technology risk approach taken by some of the Central Banks across the globe.

Over and above, a Committee for information security between banks and Qatar Central Bank is established. The aim of this Committee is to share the knowledge, awareness and alerts regarding information security that banks may face. The Committee meets quarterly and as and when required.

Going forward, in order to benefit the resiliency efforts of the financial institutions, Qatar Central Bank is preparing a "Qatar Financial Sector Information Security Strategy". The Vision of the Strategy is to enhance and maintain information security and have a more resilient and secure cyberspace to safeguard the financial sector in Qatar. Accordingly, the strategy action plan for the period 2017 -2022 aims at:

- Protecting the financial sector in the areas of information and cyber security;
- Being alert to any cyber-attacks;
- Taking the proper action with the main focus on coordination and information sharing;

- Raising the level of information and cyber security awareness in the financial sector; and
- Having qualified human resources and continuously train them.

Finally, yet importantly, as a responsible Central Bank, awareness on information security among the stakeholders of the financial sector is being continuously improved through focused workshops and conferences.

V. Conclusion

Financial sector, to keep pace with the global competitiveness, needs to adapt to the evolution of modern technology. However, this exposes them to the downside risk of cyber security. Payment systems are also not immune to these emerging challenges. Central banks and banking community have to be proactive and ensure the cyber resiliency of the payments systems, given the importance of a safe and uninterrupted payment system to the financial and economic development of the country.

With this, I will conclude, by thanking you once again for giving me this opportunity and for your kind attention. I wish the Carnegie Mellon University and the students all success.