Keynote Address of H.E. Dr. Reza Baqir, Governor, SBP
Cybersecurity in the Era of Digitalization: Regulatory Perspective

13th Public Lecture: Sustainability and Cyber Resilience,
Jointly Organized by IFSB and Central Bank of the UAE
December 8, 2021 | Abu Dhabi, United Arab Emirates

H.E. Khaled Mohamed Balama Al Tameemi, Governor, Central Bank of UAE, H.E. Dr. Muhammad Sulaiman Al Jasser, President, Islamic Development Bank, H.E. Rasheed M. Al-Maraj, Governor, Central Bank of Bahrain, H.E. Tahir bin Salim bin Abdullah Al Amri, Executive President, Central Bank of Oman, Dr. Bello Lawal Danbatta, Secretary General IFSB, Distinguished speakers, Ladies & Gentlemen, Assalam o Alaikum!

It is indeed a great pleasure for me to be part of this 13th Public Lecture Series, jointly organized by IFSB and Central Bank of the UAE. At the outset, I would like to extend my appreciation to the organizers for arranging the event on one of the most momentous themes of today's world and providing me an opportunity of addressing this august forum. I believe, the overarching theme of this programme in recent time is perhaps more relevant than ever before.

In my address, I would like to touch briefly on the subject from three standpoints. First, I would like to share some facts and figures associated with the significance of cybersecurity and to quantify how big is this risk that we feel based on the available data, and try to quantify the perception of the risk of cybersecurity. Next, I will share the experience of SBP both in terms of our approach to addressing issues of cyber security and also some lessons we have learned from our experience so far. Lastly, I will suggest some key policy considerations for the global Islamic financial industry in order to take vigorous security measures, whilst embracing digitalization.

Ladies and Gentlemen,

Let me begin with significant issues and challenges concerning cybersecurity. We are seeing the immense drift of digitalization globally and have already witnessed radical shifts in the way we live and work. Without any doubt, digitalization is one of the biggest disruptors of this millennium that is remodeling the real economy and the financial sector on a global scale. Digitalization has been generating massive opportunities for economic growth and development in a number of countries across different sectors, etc.

Alongside the several benefits of digitalization; there are some potential risks/challenges associated with the increased use of technology like cybersecurity risk, data

confidentiality issues, and cloud-concentration risk, etc. These risks and issues not only have systemic implications and serious financial stability concerns, but could jeopardize the benefits of technology like efficiency and financial inclusion.

As you all are aware that cyber threats to the financial sector are continuously evolving and becoming ever more sophisticated. The attackers – be it rogue professionals, or hacktivist groups are dynamic and agile. They have different reasons for targeting the financial sector, but they each have the potential to cause disruption. Besides stealing money and data, they can undermine confidence in the entire financial system.

Before moving ahead, I want to share some key findings of various surveys and reports regarding cybersecurity threat/risk;

1) The World Economic Forum Global Risk Perception Survey 2020 states the risk of cyber-attacks as one of the top 5 risks as a critical threat to the world in short term (0– 2 years).[1]
2) According to PWC's 24th Global Annual CEO Forum, the fear of cybercrime as a risk has risen significantly from 24% in 2017 to 47% in 2021.[2]
3) Islamic Global Bankers Survey 2021 (conducted by CIBAFI) indicates cyber-security risk and technology risk among the top two concerns of Islamic banks.
4) In Pakistan, State Bank of Pakistan (SBP) conducted Systemic Risk Survey during 7th Wave of COVID-19 Pandemic in January 2021. The survey shows that cyber security risk stands among the top 5 risks facing Pakistan's financial system.[3]

In light of the statistics that I have shared with you, we can say that cyberattacks are the new frontier of war. Cyberattacks on critical infrastructure can be as damaging as a natural disaster. According to the IBM Security 'Cost of a Data Breach Report 2021', the average cost per breach within financial services was $5.72 million. In the same study, when the security risk of a bank being hit by ransomware was quantified, it was estimated that it might face $18.9 million average financial loss that is composed of response costs, lost business and regulatory fines, with a maximum loss up to $58.8 million.[4]

These data necessitate that financial institutions and supervisors should anticipate the risks and opportunities arising from financial technologies and innovation. Further,

[1] http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
[2] 24th CEO Survey Report (pwc.com)
[3] SBP's Systemic Risk Survey
[4] Cost of a Data Breach Report 2021 (ibm.com)

cybersecurity should be one of the top priorities for all institutions, including Islamic financial institutions not only in their larger interest but in customers as well.

Ladies and Gentlemen,

Let me share with you few of the insights from our experience on this subject. In recent years, we are seeing a number of trends in the financial sector related to cyber risk. First, the interconnection and complexity of the financial system and the massive adoption of technology has created vulnerabilities; second, threat actors are highly skilled and knowledgeable professionals; third and the most important, financial services industry is struggling to find staff with the right skills and experience; finally, true innovation is always disruptive.

Now, I would like to share policy and regulatory measures, which SBP has taken over the years to protect not only financial market infrastructure and banks but also their customers from cyber threats. State Bank's objective towards cybersecurity regulations is threefold:

- First, the regulations aim to improve overall governance arrangements in financial institutions by making cybersecurity a boardroom agenda.
- Secondly, we want to strengthen our own operational cyber resilience and that of our regulated financial institutions including Islamic banks.
- And lastly, our objective is to create and promote a culture of collaboration and coordination in the industry to respond to cyber threats in real-time.

To achieve our first objective, SBP has issued, Enterprise Technology Governance and Risk Management Framework for the financial services industry that recommends a standard framework for information/cyber security management in order to anticipate, withstand, detect, and respond to cyber-attacks in line with international standards and best practices. Our regulatory framework requires that banks' information security function is independent of technology function in order to empower the information security teams to take critical decisions without influence.

Towards our second objective of improving the operational resilience of the financial services sector, we have mandatory requirements for full-scale vulnerability assessment and penetration testing of their digital infrastructure with the objective to identify potential weaknesses in their technology platforms. SBP has also advised financial institutions to take full coverage of cybersecurity threat intelligence and advisory services including update of the indicators of compromise (IOCs) and ensure immediate compliance with preventive actions. In addition, SBP itself has a dedicated Office of

information security responsible to ensure cyber resilience of SBP's information assets. The Office is responsible to take strategic actions in order to ensure protection of network, infrastructure and related IT systems.

We have also been mandating financial institutions to adopt international standards of security including those issued by international payment schemes such as Europay, MasterCard and Visa's EMVCO and Payment Card Industry Data Security Standards (PCI DSS) for payment card security. I am pleased to share that implementation of these standards has helped banks to tackle online payment card frauds to a great extent.

And lastly, to create and promote a culture of collaboration, we have been urging the industry to use a platform within the industry for the purpose of collecting and exchanging timely information that may facilitate in detection, response, resumption and recovery of systems following a cyber-attack, breach or incident. Given the systemic nature of cyber risks and the potential for widespread disruption, collaboration and timely sharing of cyber threat intelligence between the regulators, government, financial institutions, and other private-sector firms is a crucial ingredient for improving our cybersecurity. For this purpose, we regularly share information and cyber security insights with our regulated institutions on ransomware, phishing attacks, account hijacking, and other methods of cyber-attacks targeted at banking organizations.

Ladies and Gentlemen,

Despite our best efforts over the years to improve overall cybersecurity posture of the industry, we have witnessed two major cybersecurity attacks in the past few years with one on an Islamic bank in Pakistan. Based on our assessments of these cyber-attacks, there are quite a few lessons to be learnt:

First, our incident response capabilities need a massive joint effort to not only rapidly recover and restore critical business operations but also to manage customer expectations media, especially social media management. Timely and effective media messaging is critical to keep customer trust and confidence in our capabilities to protect their funds. As you know the nature of bank runs draws a lot on communication and the first lesson we have is that institutions need to devote more of resources to developing a communication play book they need to have ready in the case of a cyberattack. Because while they are doing everything they need to restore businesses they have to manage and reassure the public otherwise they are going to magnify their problem. You cannot do that communication playbook when you have already been hit by an attack.

Second, we have learnt that cybersecurity is not only an Information Technology issue. It is not a risk that can be addressed by simply having a strong IT team in place. It is not a risk that just affects a bank's technology—it affects the business itself, in every aspect—the bottom line, reputation, processes, and so much more. Therefore, financial institution's cybersecurity program should capture all risks including those arising from their partnerships with 3rd parties such as payment schemes, cloud service providers and outsourcing vendors.

Finally, in the quest to acquire state-of-the-art and latest cybersecurity tools and technologies, we have time and again seen that financial institutions often overlook basic cyber hygiene essentials such as adequate technology inventories, data security, access management, and timely software patching. I cannot overemphasize the importance of doing the basics right.

Ladies & Gentlemen,

Lastly, I would like to share some recommendations for regulators and Islamic financial institutions in order to improve cyber resilience in this fast growing world of digitalization based on lessons learnt from various global events and our experience in Pakistan.

- Cyber Governance & Risk Management Framework

  The need of robust cyber governance and risk management framework has never been more persuasive as it is in present scenario due to acceleration of digitalization. It is essential that regulatory and supervisory authorities should not only be cognizant of the potential new risks that digitalization poses, especially cybersecurity, but should also issue regulations and standards that guide the delivery of financial services so that potential risks, especially cyber risks may be properly managed.

  Here, I would like to draw attention towards Bank for International Settlements' Basel Committee on Banking Supervision (BCBS) who have upgraded their principles for operational risk and operational resilience in March 2021, namely: 1) the revised Principles for the Sound Management of Operational Risk (PSMOR) and, 2) the Principles for Operational Resilience (POR).[5] The revised principles are aimed at global banking industry to properly identify and manage the operational risks associated with information and communication technology, including vulnerability to cyber threats and improve banks' operational resilience.

[5] BIS, Newsletter on cyber security (bis.org)

With growing digitalization of Islamic finance industry, Islamic financial institutions should develop resilient cybersecurity framework/strategies, capable of identifying and managing cyber threats and proficiently respond to breach events. The adoption of an effective cybersecurity framework may help Islamic financial institutions to minimize financial losses that are due to business disruption. IFSB technical note on Financial Inclusion provides detailed technical guide on the priorities and consideration that are pertinent for regulatory and supervisory oversight vis-à-vis the implication of technological innovation for financial inclusion through the Islamic financial services industry of member jurisdictions.[6]

It is encouraging to note that some IFSB's member countries like Malaysia, Indonesia, Kuwait, Bahrain have issued specific instructions and guidelines focusing on IT and cybersecurity for example: Bank Negara Malaysia (BNM) has issued a policy document on Risk Management in Technology which provides elaborate guidelines on Cyber Risk Management such as Cybersecurity Operations, Distributed Denial of Service (DDoS), Security Operations Centre (SOC), Cyber Response and Recovery, etc.[7] Likewise, the Central Bank of Kuwait (CBK) has issued the Cyber Security Framework for Kuwait Banking Sector which provides details on the core principles for governance, risk management and compliance, collaboration, and continual improvement in cyber-resilience.[8]

- Investments in Cybersecurity Infrastructure and effective monitoring of outsourcing activities

  It is also imperative that Islamic financial institutions should invest in security tools and processes, such as automation technologies; encryption techniques; zero-trust security models; stress testing for cyber resilience for effective incidence response; and also make concerted efforts to improve IT and security environments.

  Moreover, IT outsourcing is increasing, and many financial institutions outsource their IT to a single provider. A classic case of putting all their eggs in one basket; this creates a concentration risk that should not go unnoticed. There are cases where these concentration risks cannot be avoided, but this should then go hand in hand with tougher requirements for cyber resilience. Therefore, Islamic financial institutions should employ enough sufficiently skilled staff to monitor and oversee their outsourced activities.

[6] IFSB, Technical Note on Financial Inclusion
[7] Bank Negara Malaysia, Risk Management in IT
[8] Central Bank of Kuwait, Cyber Security Framework

It is pertinent to mention here that last month (in November 2021), the Central Bank of the UAE (CBUAE) announced the establishment of the CBUAE Networking and Cyber Security Operations Centre to enhance the protection and security of the financial system's critical infrastructure in the UAE against cyber-attacks.[9] Other jurisdictions may follow suit to build a robust cybersecurity infrastructure.

- Capacity Building

  The importance of acquiring, developing and retaining core security talent that is well-aware of new technology and business risks and is also well-equipped to handle them is a key of success. As per the International Information System Security Certification Consortium report, the cybersecurity workforce needs to grow by 145 percent to meet global demand and that, the current shortfall amounts to approximately 4 million individuals.[10]

  In this context, it is important that Islamic financial institutions should undertake capacity building and employee awareness efforts and have in place a strong capable team to address the different types of cyberattacks and threats. Cybersecurity teams must leverage proactive as well as reactive measures to ensure business continuity and remain competitive in the market.

- Enhanced International Cooperation

  The challenge of cybersecurity is global; hackers operate without borders to achieve their malicious designs. Given that the threat is global in nature, governments, financial institutions, regulators, and tech firms cannot protect the financial sector if they work in silos.

  We have example of European Union (EU), which has significantly improved regional cyber resilience and cooperation by setting out goals, enhancing information sharing and harmonizing practices across its member states. Further, there are different regional groups and cooperation forum.

  The global financial sector needs enhanced cooperation to downplay the risk arising from cyberattacks. Areas such as information and intelligence sharing may help in responding to a cyber-crisis. The effectiveness of such cooperation requires strategically aligned policy goals and bilateral and multilateral relations among Islamic countries.

[9] Central Bank of UAE, Networking and Cyber Security Operations Centre
[10] (ISC)2 Cybersecurity Workforce Study, 2019

There is a need for central banks to develop and promote centers for regional cooperation and collaboration on cybersecurity.

I also believe, IFSB can plan a pivotal role in order to provide a platform to its member countries for effective collaboration/cooperation to stay informed on local, regional and global cyber security threats and to facilitate each other for continuous improvement of cybersecurity controls among the regulators and the regulated entities in their jurisdictions.

Ladies & Gentlemen,

In my remarks I had wanted to share with you that in our perceptions, cyber resilience has become one of the top concerns of global CEOs; why the State Bank of Pakistan is so focused on cyber resiliency and what we at SBP are doing to advance both the industry's and the SBP's own resiliency against cyber incidents; how important it is for every institution to put a lot of resources not just on its ability to cope with cybercrime but its communication play book particularly in social media. The dynamic and complex nature of the cyber threat landscape, with rapid technological change and ever-evolving risks that are becoming more sophisticated and complex, can make it seem like we are always running to catch up. This can be discouraging. But if one looks back over the previous years, it is clear that much progress has been made in better understanding cyber threats and how, by working together, we can best handle those threats. My expectation is that perseverance and collaboration will continue to yield benefits in making our financial system ever more resilient. And this resiliency is critical, given the importance of the financial system to our economic health.

In the end, I would like to congratulate the organizers for further mainstreaming the agenda of cyber resilience in global Islamic finance landscape through its public lecture series. I am hopeful that today's lectures will provide key takeaways to all the stakeholders of global Islamic financial industry for its ongoing efforts and commitment towards cyber resilience while undergoing digital transformation of Islamic financial services.

Thank you.