Box 6.1: Emerging challenge of Cyber Attacks- Implications for financial sector

Today, cyber-attacks are characterized by an increase in sophistication, potential for disruption and global prevalence. The World Economic Forum Global Risk Perception Survey 2018 cited the risk of cyber-attacks as one of the top 10 risks in terms of both impact and likelihood. The overall cost of cyber-attacks is predicted to be USD 8 trillion over the next five years. Noteworthy examples of cyber-attacks during CY17 are the WannaCry ransom ware attack during May 2017, which affected more than 300,000 computers across 150 countries[291] and the Petya ransom ware attack, which targeted various large organizations across the globe. The threat of cyber-attacks is a disruptive cross-border phenomenon, which merits urgent global efforts.

The global financial system is not aloof of cyber security risk. The cyber-heist on Bangladesh Bank in 2016, which resulted in a loss of USD 81 million, is one of the notable examples from the recent past. As more and more financial institutions continue to leverage information technology to offer efficient and innovative services and products, technology becomes an integral part of their business models and operations. Consequently, it entails greater investment in cyber-security architecture and a robust regulatory and supervisory regime to ensure smooth functioning of payment and settlement systems to hold the trust of the general populace.

The emergence of cyber-security risks, which now pose a challenge of systemic proportions, is driven by a host of factors. These include the widespread use of technology, both by financial institutions and consumers, growing interconnectedness among financial institutions through the use of technology-based platforms, increasing reliance on data and the evolving nature and sophistication of cyber-attacks. Moreover, as financial institutions continue to adopt the evolving technologies, their dependence on technology firms for emerging services like cloud computing firms, FinTech platforms, etc. increases. Since these firms, generally, fall outside the perimeter of the financial regulators, the oversight of cyber-risks becomes a challenge.

The key risks associated with cyber-attacks, which compromise the integrity of the financial system, include:

- Breaches of data security/privacy resulting in financial losses,
- Vulnerability of IT systems to malicious viruses such as ransom wares,
- Disruption in IT systems of financial institutions leading to a halt in operations,
- Vulnerability of IT based financial solutions such as ATMs, internet banking and mobile banking to frauds such as skimming, phishing, pharming etc.,
- Reputational loss for financial institutions which may have systemic implications, and
- Vulnerability of national and cross-border payment and settlement systems which may pose contagion risk,

International bodies are making concentrated efforts towards addressing the issue affecting the cyber-resilience in the global financial system. The Committee for Payments and Markets Infrastructure (CPMI) and International Organization for Securities Commissions (IOSCO) have issued Principles for Financial Markets Infrastructures (PFMIs) which comprehensively deal with the risk management of financial market infrastructures[292]. Building on that, CPMI-IOSCO issued guidelines on cyber-resilience for financial market infrastructures which aims at improving cyber-governance, preparedness in case of a cyber-attack, threat intelligence and awareness among end-users. Similarly, the G7 published the "fundamental elements of cyber security for the financial sector", which outlines various elements to serve as building blocks upon which an entity can design and implement its cyber-security strategy[293].

The results of the 1st wave of SBP Systemic Risk Survey depict that cyber security risk stands among the top 10

[291] The Global Risks Report, *2018 (World Economic Forum)*
[292] Principle 17 of PFMIs deals with operational risks related to functioning of financial market infrastructures.

[293] https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf?69e99441d6f2f131719a9cada3ca56a5

risks facing Pakistan's financial system (**See SRS Results in Box:1 in Executive Summary**). However, the level of cyber security risk to Pakistan's financial sector remains within tolerable bounds. The industry has not seen any significant disruption in functioning of the payment and settlement systems, which has maintained the confidence of the participants.

State Bank of Pakistan (SBP), being the supervisor and regulator of the banking sector and payment systems, has long been cognizant of the growing threat of cyber security risk and is continuously working in close coordination with the banks to ensure cyber readiness.

In this regard, SBP has issued *the Framework for Risk Management in Outsourcing Arrangements by Financial Institutions* which addresses the risk emanating from reliance of banks on third party service providers[294].The SBP has detailed set of instruction on *Prevention against cyber-attacks, in terms of which* banks are required to continuously enhance their cyber security controls, processes and procedures in order to anticipate, withstand, detect, and respond to cyber attacks. For the purpose, banks need to formulate cyber security controls as an integral part of their IT risk management policy, accompanied by appropriate Standard Operating Procedures to safeguard against potential cyber threats[295].

To ensure that the payment cards in the country are secure, SBP has issued *Regulations for Payment Cards security* to facilitate the card service providers (CSPs) to develop a card security framework according to international best practices. The regulations require all cards to be issued in compliance with the Europay, Mastercard and Visa (EMV) standard from June 30, 2018 onwards, to protect the consumers from frauds such as skimming[296].

To protect the increasing consumer base using internet banking channels, SBP has issued *Regulations for the Security of Internet Banking* requiring banks to develop a comprehensive internet banking security framework[297]. The regulations emphasize on customer awareness by the banks about identity theft and fraud techniques as part of the preventive controls.

To cater to cyber security risk, Government of Pakistan has also taken various initiatives. The legal framework against cyber crimes was strengthened through promulgation of Prevention of Electronic Crimes Act, 2016. The legislation outlines a mechanism for investigation, prosecution and trial related to electronic crimes such as cyber-attacks. On the institutional front, a National Response Center for Cyber Crime (NR3C) is working under the Federal Investigation Agency with a mandate to deal with technology based crimes.

Cyber-security challenges for the financial sector need urgent attention of the global community. As the first line of defense, awareness among the human resources of financial institutions and end-consumers of financial services must be enhanced. Moreover, regulators must work closely with financial institutions to ensure that adequate safeguards are in place to defend against the cyber-attacks. Most importantly, owing to the cross-border nature of cyber-attacks, international collaboration between states, supervisory bodies, law enforcement agencies and financial institutions is pivotal to manage and mitigate the risks associated with these attacks.

[294] BPRD Circular No. 06 of 2017; http://www.sbp.org.pk/bprd/2017/C6.htm
[295] BPRD Circular No. 07 of 2016; http://www.sbp.org.pk/bprd/2016/C7.htm
[296] PSD Circular No. 05 of 2016; http://www.sbp.org.pk/psd/2016/C5.htm
[297] PSD Circular No. 03 of 2015; http://www.sbp.org.pk/psd/2015/C3.htm