Mahesh Kumar Jain: Cyber security for a safer financial system

Keynote address by Mr Mahesh Kumar Jain, Deputy Governor of the Reserve Bank of India, at the "Cyber Security Exercise for Banking Sector", an international event under India's G 20 Presidency, Mumbai, 5 June 2023.

* * *

Dr. Sanjay Bahl, Director General of Computer Emergency Response Team – In (CERT-In), distinguished guests from the IMF, the BIS, delegates from other central banks and CERTs, MDs/CEOs of banks from India and their team members, global CISOs and CTOs of foreign banks, my colleagues from RBI, ladies and gentlemen. Good morning to all of you.

2. I thank all of you for joining us for this important event to deliberate upon the critical area of cyber security that has become increasingly pertinent in our rapidly evolving digital age. As financial transactions migrate to digital platforms, the reliance on information technology infrastructure grows exponentially. While this shift brings undeniable convenience and efficiency, it also exposes us to increasing risks. Cyber criminals, driven by malicious intent and motivated by financial gain, continually exploit vulnerabilities in digital systems, seeking to breach security defences and gain unauthorized access to valuable data.

3. In an interconnected world, where financial transactions traverse continents in a matter of seconds, the need for international cooperation in combating cyber threats has become paramount. Cyber-attacks targeting banks not only jeopardize the stability of individual institutions but also have the potential to disrupt financial systems, making it imperative for nations to come together and address this pressing challenge. Therefore, this event under India's G 20 Presidency is important to complement efforts of various international bodies for addressing the issues of cyber security in the banking sector.

Importance of Technology

4. Technology has been a driving force in shaping the financial sector, enabling greater efficiency, accessibility and affordability. However, the current FinTech revolution is unique in many ways being defined by increased computing power and use of new technologies. Further, there is an emergence of new entrants and innovative business models.

5. Previously, digitalisation of financial services allowed banks and financial institutions to have structured data on their consumers which was used to have an understanding of the customer's risk profile. However, with the emergence of Big Data analytics, even better insights on customer preferences and behaviour can be obtained using alternate semi-structured and unstructured data.

6. Data is often referred to as the "new oil" due to its immense value and potential for driving economic growth, innovation and the positive impact it can have when used responsibly. However, when used irresponsibly, several negative consequences follow

such as privacy violations, identity theft and frauds, manipulation using targeted advertisements, etc. In fact, irresponsible data usage not only poses risks to individuals, but undermines trust in the digital ecosystem and may even have financial stability and national security implications.

Understanding Financial Stability Vulnerabilities

7. Understanding financial stability vulnerabilities emerging from cyber perspective is critical because existing capital and liquidity prescriptions may not mitigate the effect of a cyber event the same way they mitigate financial losses. For instance, capital and liquidity can provide the financial resources to respond to a cyber incident but may not speed up the process of recovering systems or data.

8. Cyber-attacks can disrupt critical financial operations within banks, rendering them unable to process transactions, access customer accounts, or execute essential functions. This disruption can result in a loss of confidence in the banking system, as customers and businesses may face difficulties in accessing their funds or conducting normal financial activities. Such disruptions can lead to financial instability, especially if they affect multiple banks or are prolonged.

9. Enhancements in service offerings, such as longer operating hours of payment systems and shorter clearing and settlement windows, leave the financial system with fewer service breaks in which operations can be restored after a cyber incident. Uncertainty about the nature and extent of an incident may also prompt runs on counterparties, competitors, or unaffected segments of the financial entity's operations.

10. Indeed, the 2021 ransomware attack on Colonial Pipeline, though not a financial entity, highlighted the interconnectedness of critical infrastructure systems and the potential cascading effects on various sectors, including banking. It illustrated how a cyberattack could spark a run, in this case, a run-on gas stations, amplifying the effects well beyond the original shock.

11. While there is extensive ongoing supervisory attention to entity-level cyber resilience, data gaps remain. At the entity level, there is need for consistent data on cyber incidents. At the system level, relevant data measures of digital interdependencies and the speed with which backup systems can be quickly enabled, are required.

Cyber Security and Digital Financial Inclusion

12. Cyber risks can have a significant impact on financial inclusion efforts as well. Financial inclusion aims to provide access to financial services for the underserved and marginalized populations, and rapid strides have been made in this area facilitated by digital public infrastructures. However, these populations are more vulnerable to cyber risks due to their lack of awareness about cybersecurity.

13. Individuals can lose trust if they are brought online in the name of financial inclusion only to be exposed to cyber harms that they cannot recover from. For digital financial

inclusion to be successful, it is not enough to bring people into the digital economy. All the stakeholders must also ensure that people are resilient against the risks they will be likely exposed to.

Indian Perspective

14. I would like to take this opportunity to share the Indian perspective. While encouraging innovation and digitization of financial products and services, RBI's approach has been to ensure that innovation should be assimilated in the financial system in a non-disruptive manner and the course of digitisation should ensure customer protection at every step.

15. India is one of the few countries that protects users through the mandate of two-factor authentication for digital payment transactions. Although it is now recognised as an innovative regulation, at the time when RBI introduced it about a decade back, there was a push-back and criticism. Similarly, the recent measures such as better customer control on card usage, shorter Turn-Around-Times for transaction failures, tokenisation, etc. are all initiatives intended to protect the customer.

16. In the Payments space, Real Time Gross Settlement (RTGS) and National Electronic Fund Transfer (NEFT) have been made 24x7. Further, RBI catalysed the setting up of appropriate institutions like the Institute for Development and Research in Banking Technology (IDRBT) in 1996 and the National Payment Corporation of India in 2008, which have been instrumental in pioneering various payment system technologies and solutions.

17. Through appropriate regulatory frameworks, the RBI has encouraged innovations in Digital Lending, Open Banking and P2P lending platforms. A Regulatory Sandbox framework was created in 2019 which has run several cohorts to incentivise adoption of innovative financial products and services. The Reserve Bank Innovation Hub (RBIH) has been set up for collaborating with financial sector institutions, the technology industry and academic institutions for exchange of ideas and development of prototypes related to financial innovations. Competitive events like the Hackathons are held to provide a channel for the fintech and start-up sector to showcase innovations.

18. The supportive regulatory environment, with its focus on safety, speed and scalability has positioned India as a leader in payment system innovation. Illustratively, UPI, India's instant payment system, launched in 2016, has witnessed remarkable growth in India with daily transactions averaging over 300 million in volume and 480 billion in value during May 2023. Recently, India and Singapore tied up their UPI and Pay Now systems allowing for real time cross border money transfers between the two countries. Indeed, there is immense potential for use of UPI globally through partnership and collaboration with other countries.

19. The RBI is also continuously trying to strengthen its supervisory oversight over cyber risks. Simulated phishing, cyber reconnaissance and other cyber exercises complement supervisory processes in getting a systemic view of the prevailing cyber risks. RBI has also encouraged development of innovative tools like the Sectoral Security Operations Centre (S-SOC) which can help address the cyber risk of the banking and financial sector in a major way.

20. Though cyber risks are said to outpace regulations, the Reserve Bank of India has been proactively taking measures to strengthen IT and Cyber Risk management in its regulated entities. As early as 2011, detailed guidelines for managing IT risks were issued to the banks, followed by a principles-based Cyber Security Framework in 2016. Regulations have also been issued on Digital Payment Security Controls and on Outsourcing of IT Services. RBI has also published draft guidelines on IT Governance which shall be finalised and issued shortly.

Need for collective effort

21. Considering the global nature of cyber threats, efforts by governments, financial entities, and technological companies are insufficient to protect against them. Cyber threats transcend geographical boundaries, making it necessary for countries and financial institutions to work together to address them.

22. I would like to outline six strategies that would help improve the global cyber security environment:

i. Firstly, the global financial system's interdependencies need to be better understood by mapping key operational and technological interconnections, including that of critical infrastructure. Better incorporation of cyber risk into financial stability analysis will improve the ability to understand and mitigate system-wide risk.

ii. Secondly, a minimum common framework for cybersecurity needs to be devised that outlines best practices and standards for financial institutions to follow. This can help ensure that all institutions are taking the necessary steps to protect themselves from cyber threats.

iii. Thirdly, to the extent feasible as per domestic laws, countries can share information and intelligence about cyber threats and attacks. This can help to identify emerging threats and vulnerabilities and enable financial institutions take proactive measures to prevent attacks.

iv. Fourthly, countries can work together to develop and implement incident response plans. This can help to ensure that in the event of a cyber-attack, there is a coordinated and effective response that minimizes the impact on the financial sector.

v. Fifthly, cyber-attacks should become more expensive and riskier for the perpetrators through effective measures to confiscate proceeds of crime and prosecute criminals. Stepping up international efforts to prevent, disrupt and deter attackers would reduce the threat at its source.

vi. Finally, countries can collaborate on capacity building and training programs to ensure that financial institutions have the necessary skills and resources to manage cyber risks effectively. This can include training on cybersecurity best practices, incident response planning, and the use of advanced technologies to detect and prevent cyber-attacks.

Conclusion

23. Let me now conclude. With growing interconnections across the world, curbing cyber risk requires an international effort. It is expected that the G20 forum would complement the efforts of various international bodies towards building an approach for helping financial sector through capacity development initiatives aimed at designing and implementing international standards and best practices as a priority.

24. I request all to participate actively in the upcoming cyber security exercise that will be held today. Together, we can make the financial sector more secure and trustworthy.

Thank you