Cyber resilience in Indian Financial Services is the Need of the Hour

Sohini Banerjee and K.S. Roshan Menon

Introduction

The World Economic Forum's 2021 **report** on global risks featured cyber threats as among the most significant risks to society and the economy. At the outset, it is worth noting two key factors at play. First, the financial services sector has been a prime target for threat actors; and second, the nature of cyber risk that financial entities are exposed to has changed over the last few years. The driving agents of both the abovementioned factors look alike. The financial services sector processes vast troves of personal data, and makes use of rapidly evolving technology to deliver their services better. Further, financial entities companies are becoming more decentralised in their operation – with an increasing number of linkages being developed between financial entities and external service providers. These factors complicate what constitutes robust cybersecurity risk management.

In this post, we advocate for a resilience-based approach to cybersecurity in the Indian financial services sector. We believe that adopting an approach of 'cyber-resilience' would help players to adequately guard against cyber-attacks, as well as respond to and recover from a potential cyber-attack. A cyber resilient approach would ensure that regulated entities are able to protect themselves, their customers, as well as the entire financial services sector.

A worrying picture

Recent cyber threats to the Indian financial sector paint a worrying picture. A reported data breach at Indian digital payments platform Mobikwik allegedly led to the compromise of personal data of nearly 10 crore users. The leaked information included personal data like mobile phone numbers, bank account details, and e-mail addresses. This data breach is quick on the heels of another significant data breach at Indian payments processor Juspay, where the entity confirmed that 3.5 crore records of masked card data and card fingerprint were breached. Further, metadata of 10 crore users that was not anonymised, containing e-mail addresses and phone numbers, were accessed by hackers. In both incidents, the breached data was reportedly posted for sale on the dark web.

It is evident that entities operating in India's burgeoning fintech ecosystem must sit up and take note of vulnerabilities in their technological infrastructure. This is especially crucial as even isolated cybersecurity threats can endanger systemic financial stability. Our proposal to focus on cyber resilience seeks to provide a roadmap towards a more secure paradigm.

Focussing on cyber resilience

Cyber resilience refers to the three-pronged process of building the ability of entities to proactively prepare for, respond to and recover swiftly from disruptions. Such resilience would include the **"ability to withstand and recover from deliberate attacks, accidents or naturally occurring threats or incidents"** (NIST), and can be viewed as continuous in nature. The emphasis on building cyber resilience stems from the acknowledgment that traditional cyber security measures are falling short in responding to the current terrain of cyber threats. In response, cyber resilience is a comprehensive

concept that goes a step further in building a proactive culture of cybersecurity protection by making use of a broader array of cybersecurity tools.

In other words, while cybersecurity refers to a set of risk mitigating strategies to achieve robustness of internet infrastructure, cyber resilience is an anticipatory set of strategies. Cyber resilience also encompasses within itself the aims of cybersecurity. Deploying a potent cyber resilience strategy can equip an organisation from within to withstand and tide over serious cyber threats. This has several benefits for the concerned organisation, apart from the protection of personal data, ensuring recovery from disasters, business continuity, protection of reputation, and maintenance of customer confidence.

Regulation and resilience in India

Financial regulation in India has placed emphasis on the development of resilient systems to tackle emerging cybersecurity threats. Early developments in the sector include the Reserve Bank of India's ('**RBI**') issuance of the **Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds** ('**Guidelines**') in 2011 – a specialised regulation aimed at enabling the secure use of IT by banks. Discussing cybersecurity as a concern impacting business continuity, the Guidelines urged regulated entities to devise IT strategies to be 'resilient to failure', and outlined mechanisms to assist with the same.

Over time, the RBI would move away from the narrow conception of resilience as a technical requirement and pursue it as a holistic policy objective for banks. The 2016 Circular on **Cybersecurity Framework in Banks** ('**2016 Circular**') signified this shift in regulatory outlook, with the RBI focussing on enhancing cyber-resilience while addressing cyber risk. A richly detailed instrument – the 2016 Circular led with a 'standardization' approach to building cyber resilience and outlined explicit measures to achieve the same. These measures include the institution of data protection safeguards to secure customer information, the deployment of relevant authentication frameworks by banks to weed out malicious players and the adoption of 'vendor risk management' strategies to mitigate risks arising from the purchase of faulty equipment.

Since the 2016 Circular, the RBI has sought to deepen its resilience paradigms for financial products. In light of the same, the regulator notified **the Master Direction on Digital Payment Security Controls, 2021** ('**Master Direction**'). The Master Direction requires Regulated Entities to conduct risk assessment for payments products, with due regard to the safety and digital security of such products. Such risk assessment, the Master Direction notes, "shall address the need to protect and secure payment data and evaluate the resilience of systems."

Overall, these developments seem to suggest a high-degree of penetration for cyber resilience as a policy objective in financial regulation. Despite this, cyber-attacks in India have been on the rise and have continued to overwhelm its financial institutions. This outcome offers the RBI a reason to reflect on the contents of its cybersecurity regulations.

Ideally, regulations that engage with resilience should provide clarity on strategies that minimise data breaches, preserve data integrity and stymie cyber risk. Instead, the RBI has noted an increase in the perception of cyber-risk among players and experts in its **Financial Stability Report, 2021**. This is telling – as the financial sector continues to be threatened by an increasing number of cyber-attacks, the extant regulatory framework fails to inspire confidence among players in their ability to withstand such attacks and stay resilient to their harmful effects.

Our analysis suggests that the failure of such regulation is linked to the manner in which these instruments seek to implement cyber-resilience. Discussed below are three such concerns that help understand the regulatory 'gap' that hampers the growth of effective cyber-resilience in India.

First, regulation in India does not clearly define cyber-resilience. Instead, the approach adopted by the instruments discussed above is 'illustrative' – the RBI has identified designate areas of intervention for cyber-resilience and proceeded to design targeted interventions in pursuit of the same.

The lack of a comprehensive definition for cyber-resilience has led to a myopic understanding of resilience in the Indian context. Resilience, as understood by the RBI, espouses a form of 'technological solutionism' – often involving either upscaling technology or improving general cybersecurity infrastructure. This approach is reflective of only one paradigm of resilience, known as 'technical resilience' and ignores key paradigms that drive an organisation's capability to withstand shocks to its security apparatus. For instance, a holistic definition of resilience may account for 'data minimisation' – financial firms may refrain from collecting data that is irrelevant to the purposes for processing. In not providing a comprehensive definition for resilience, the RBI choses to ignore data minimisation and other, relevant data processing principles that are critical to an organisation's data security framework.

Second, the RBI's approach does not account for *robust* self-assessment. This is to say that while the RBI, through some of its Master Directions and Circulars, does seek to incorporate elements of resilience into the delivery of financial services, it fails to do so in a manner that can help effectively realise cyber-resilience.

The term 'self-assessment' for cybersecurity refers to an entity's ability to assess the adequacy of its cybersecurity practices, and plan enhancements to its cybersecurity framework. In essence, self-assessment allows entities to simplify resilience – helping them identify a benchmark to compare themselves to, and earmark areas of improvement. A good example of this is **Cyber Security Self-Assessment Guidance** ('**Self-Assessment Guidance**'), issued by the Canadian Office of the Superintendent of Financial Institutions. Released in 2013, the Self-Assessment Guidance is a comprehensive document that allowed entities to estimate their resilience capabilities across various metrics, such as threat intelligence, organisation and resources, and situation awareness.

Initiatives such as the Self-Assessment Guidance help regulated entities better understand the measures by which regulators seek to engage with cyber-resilience in ways that are more meaningful. These strategies are invaluable – by outlining pathways for self-assessment, the regulator provides entities with a 'checklist' of resilience building measures that they may readily comply with, while simultaneously nudging entities towards estimating resilience capabilities.

Presently, the approach of the RBI does not attempt such meaningful engagement on self-assessment. A careful look at extant regulation indicates the absence of 'checklists', such as the one contained in the Self-Assessment Guidance, or a comprehensive study of resilience practices across regulated entities. Movement on both these fronts is desirable – designing such interventions serve as useful first steps towards benchmarking (entities can refer to the study for guidance on cybersecurity practices that may be adopted) and may greatly help entities in devising their own strategies for resilience.

Third, the RBI's approach does not account for the size or interconnectedness of a regulated entity. Despite the 2016 Circular and the Master Direction's insistence on entities deploying 'appropriate' governance and risk management frameworks, these instruments do not contemplate upscaling or downscaling regulation in accordance with the degree of cyber-risk posed by the entity. This has

prominent negative effects – smaller firms are burdened with enhanced compliance costs under blanket regulation, while systemically important entities may escape deserved enhanced oversight on processing activities that involve exposure to sensitive personal data or extant cyber-vulnerabilities.

In a previous **post**, we have explained the positive impact that scaling regulation in accordance with size and interconnectedness may have on cybersecurity. Scaling ensures that systemically important entities may be subject to enhanced compliance requirements, such as mandatory external audits or designated privacy and security departments. Conversely, scaling can help micro, small and medium enterprises be subject to light-touch, cost-effective regulation that permits innovation to flourish. Adopting scale sensitivity can deepen the penetration of resilience paradigms among small firms, encouraging a dynamic, bottom-up approach to cybersecurity.

Way forward

It flows from the concerns discussed above that; the first steps to build cyber resilience involve a series of regulatory interventions by the RBI. These interventions include – defining cyber resilience, designing a comprehensive guidance module for self-assessment and reviewing its cybersecurity practices for scale. These measures may result in enhancing cyber resilience and promote financial stability across markets.

Additionally, regulators must closely track resilience strategies that are developing because of the emergence of privacy law. Some tools that may be helpful in building cyber resilience include security by design, zero-trust approach to architecture and networks, and adopting privacy by design measures in accordance with data protection law.

In this vein, deploying rules that are aligned with the General Data Protection Regulation ('GDPR') in the European Union ('EU'), and the upcoming data protection law in India, are beneficial in securing cyber resilience. For instance, the GDPR, and the Personal Data Protection Bill, 2019 in India, contain rules on transparency, accountability, data security, personal data breach notifications, privacy by design, and data protection impact assessments. These are useful tools for regulated entities to ensure that they have a baseline of security safeguards in place. The baseline may be modified further to suit their unique requirements and risk profile. Further, inputs in fixing this baseline may be derived from regulations of other jurisdictions, guidance on best practices issued by entities like **ReBit**, and prior work in this space done by international organisations.

Sohini Banerjee is a Research Fellow at Shardul Amarchand Mangaldas & Co., New Delhi, India.

K.S. Roshan Menon is a Research Scholar at Shardul Amarchand Mangaldas & Co., New Delhi, India.

[*The authors are grateful to Gopalkrishna Hedge, GV Anand Bhushan and Siddharth Nair for their comments.*]