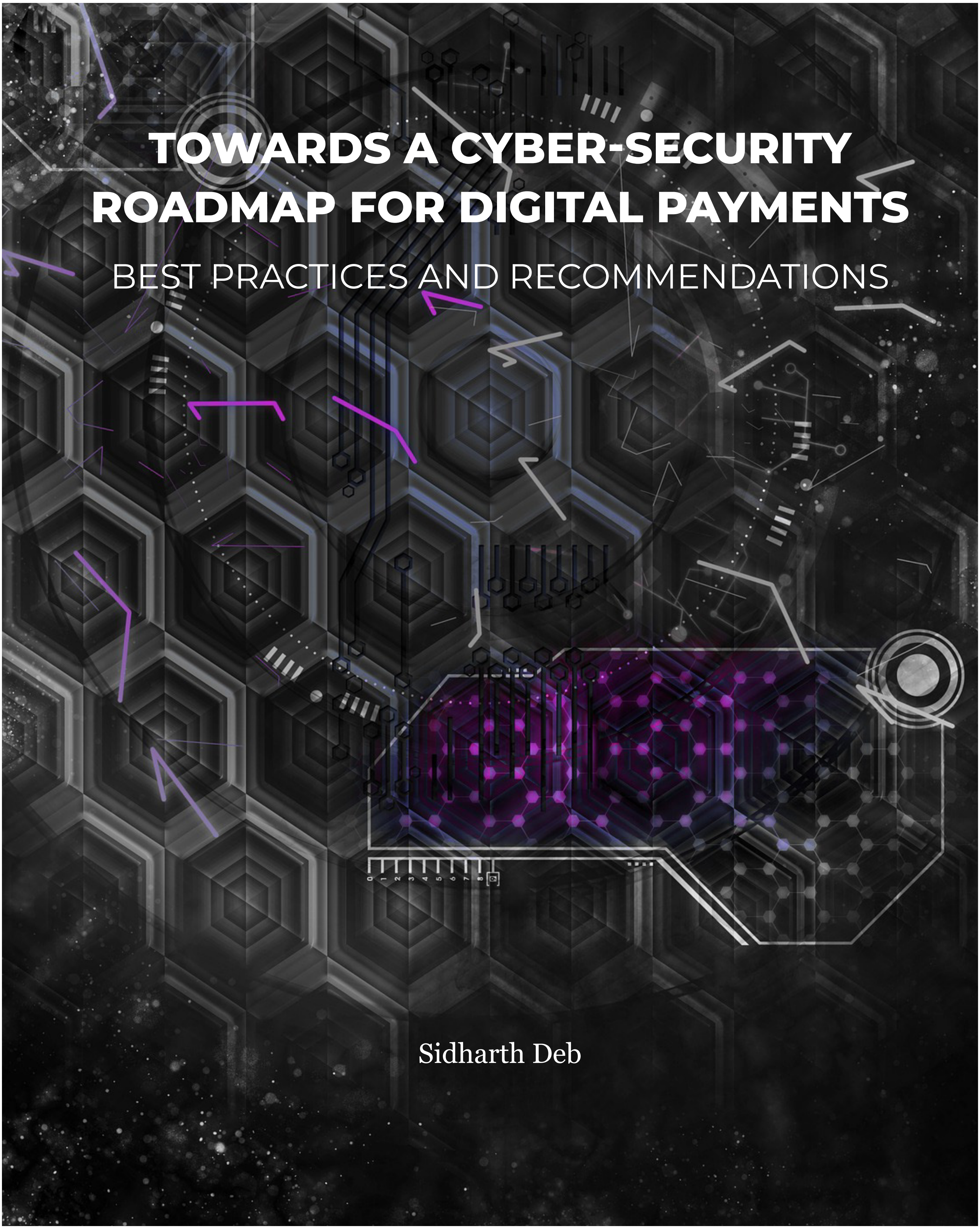


TOWARDS A CYBER-SECURITY ROADMAP FOR DIGITAL PAYMENTS

BEST PRACTICES AND RECOMMENDATIONS

Sidharth Deb

Observer Research Foundation
20, Rouse Avenue Institutional Area
New Delhi 110002
contactus@orfonline.org
www.orfonline.org

Koan Advisory
B6-1, Second Floor, DDA Commercial Complex
Safdarjung Enclave, New Delhi 110029
contactus@koanadvisory.com
www.koanadvisory.com/

Design and Layout: simijaisondesigns

Cover Image: Pete Linforth/Pixabay

ISBN: 978-93-89094-06-0

ISBN Digital: 978-93-89094-07-7

TOWARDS A CYBER-SECURITY ROADMAP FOR DIGITAL PAYMENTS

BEST PRACTICES AND RECOMMENDATIONS

Sidharth Deb

Contents

List of Abbreviations

AEPS	Aadhaar-Enabled Payment System
AML	Anti-Money Laundering
ANSI	American National Standards Institute
ANSSI	National Cyber Security Agency of France
API	Application Programming Interface
BBPS	Bharat Bill Payment System
BFSI	Banking Financial Services and Insurance
BIS	Bank for International Settlements
Bis	Bureau of Indian Standards
CDA	Card Data Authentication
C-DAC	Centre for Development of Advanced Computing
C-DOT	Centre for Development of Telematics
CERT-EU	Computer Emergency Response Team for the EU Institutions, Bodies and Agencies
CERT-Fin	Computer Emergency Response Team for the Financial Sector
CERT-In	Computer Emergency Response Team of India
CII	Critical Information Infrastructure
CISO	Chief Information Security Officer
CLOUD Act	Clarifying Lawful Use of Overseas Data Act
CNP	Card-Not-Present
CPIC	Critical Payment Infrastructure Company
CPMI	Committee on Payments and Market Infrastructures
CRS	Compulsory Registration Scheme
CSA	Cyber Security Agency (Singapore)
CSITE Cell	Cyber Security and IT Examination Cell
CVE	Common Vulnerability Exposure
DDA	Dynamic Data Authentication
D-DoS	Distributed Denial of Service
DFS	Digital Financial Services
DHS	Department of Homeland Security (US)
DoT	Department of Telecommunications
DPA	Data Protection Authority of India
DPB	Personal Data Protection Bill, 2018
EBA	European Banking Authority
EC	European Commission
ECB	European Central Bank
EMV	Europay, Mastercard and VISA
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
EU	European Union
FAR	False Acceptance Rate
FINCONET	International Financial Consumer Protection Organisation
FIRST	Forum of Incident Response and Security Teams
FMI	Financial Market Infrastructure

FSLRC	Financial Services Legislative Reform Commission
FRR	False Rejection Rate
FTE	Failure to Enrol
G7	The Group of Seven
GDPR	General Data Protection Regulation
GSC	Global Standards Collaboration
IAPP	International Association of Privacy Professionals
IB–CART	Indian Banks–Centre for Analysis of Risk and Threats
ICO	Information Commissioner’s Office (UK)
IDRBT	Institute for Development and Research in Banking Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IoT	Internet of Things
IMPS	Immediate Payment Service
ISA	Information Security Assurance
ISAC	Information Sharing and Analysis Centre
ISO	International Standards Organisation
ISP	Internet Service Provider
IT Act	Information Technology Act
ITU	International Telecommunication Union
KYC	Know Your Customer
LEA	Law Enforcement Agency
LITDC	Electronics and Information Technology Division Council
LOA	Level of Assurance
LR	Letters Rogatory
LRS	Laboratory Recognition Scheme
LVTS	Large Value Transfer System
MAS	Monetary Authority of Singapore
MeitY	Ministry of Electronics and Information Technology
MLAT	Mutual Legal Assistance Treaties
NACH	National Automated Clearing House
NATO	North Atlantic Treaty Organisation
NCCC	National Cyber Coordination Centre
NCSC	National Cyber-Security Centre (United Kingdom)
NCSP	National Cyber-Security Policy
NCIIPC	National Critical Information Infrastructure Protection Centre
NECS	National Electronic Clearing Service
NEFT	National Electronic Fund Transfer
NFC	Near Field Communication
NFS	National Financial Switch
NIST	National Institute of Standards and Technology (US)
NPCI	National Payment Corporation of India
NTRO	National Technical Research Organisation
OECD	Organisation for Economic Cooperation and Development

OTP	One-Time Password
PA–DSS	Payment Application–Data Security Standards
PCI–DSS	Payment Card Industry–Data Security Standards
PCI–SSC	Payment Card Industry–Security Standards Council
PFMI	Principles of Financial Market Infrastructures
PIPEDA	Personal Information Protection and Electronic Documents Act (Canada)
PoS	Point of Sale
PPI	Prepaid Payment Instrument
PPP	Public–Private Partnership
PRB	Payments Regulatory Board
PSD2	European Union Revised Payment Services Directive
PSP	Payment Service Provider
PSS Act	Payment and Settlement Systems Act, 2007
RBI	Reserve Bank of India
RTGS	Real Time Gross Settlement
SCA	Strong Customer Authentication
SE	Secure Element
SME	Small and Medium Enterprises
SOC	Security Operations Centre
SPDI	Sensitive Personal Data or Information
SSO	Standard Setting Organisations
STQC	Standardisation Testing and Quality Certification Directorate
TEC	Telecom Engineering Centre
TEE	Trusted Execution Environments
TRAI	Telecom Regulatory Authority of India
TSDSI	Telecommunications Standards Development Society of India
U2F	Universal Second Factor
UNGGE	United Nations Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security
UK	United Kingdom
UPI	Unified Payment Interface
US	United States of America
US–CERT	United States–Computer Emergency Response Team
US FS–ISAC	United States–Financial Services Information Sharing and Analysis Centre
USSD	Unstructured Supplementary Service Data
W3C	World Wide Web Consortium

CONTEXT, SCOPE AND STRUCTURE OF REPORT

The Indian government has outlined a target of creating a US$1-trillion digital economy by 2025.[1] Digital payments are an important constituent of this target and a national payments mission ('Digidhan Mission') has been initiated under the aegis of the Ministry of Electronics and Information Technology (MeitY). Such policy impetus has allowed the sector to continue its robust growth, clocking around 20.7 billion digital transactions in FY 2017–18, an 89.5 percent increase from the previous fiscal year.[2] Moreover, as India's wider digital ecosystem continues to grow, there will be an increase in the adoption of digital payments. Key indicators in this regard include 560.01 million internet users;[3] around 1.17 billion wireless users[4] and around 404.1 million smartphone users.[5] Extrapolating from these figures, India's digital-payments market is on pace to be a US$1-trillion proposition by 2023.[6]

The scaling up of such modernised economies necessitates a simultaneous modernisation of legal, regulatory and institutional frameworks, and Indian decision-makers are cognisant of this. For instance, in 2017, the Supreme Court of India made a landmark pronouncement that an individual's right to privacy is a fundamental right under Article 21 of the Indian Constitution. The nine-judge bench categorically included informational privacy (relevant for internet/data economies) as a key constituent of this umbrella right.[7]

Pursuant to this matter, the Indian government established an expert committee, headed by Justice B.N. Srikrishna, to give recommendations and draft a bill for a comprehensive data-protection framework for India's nascent digital economy. In July 2018, the committee released the Personal Data Protection Bill, 2018 (DPB) and its report containing sectoral data-protection recommendations.[8] While primarily designed through the lens of 'user privacy', key provisions also fall within the domain of information/cyber security.

As these processes continue, security frameworks for sectors such as digital payments must be simultaneously constructed. One clear objective of the Digidhan Mission is to secure the entire digital-payments ecosystem, which includes reviewing the efficacy of extant institutional and security frameworks. To this end, the report contextualises the various moving parts within digital payments and broader policymaking arenas to propose a forward-looking cyber-security strategy for the sector.

For this report, the term "digital payments" is used for both "online" and "mobile" payment systems.[9,10] Some common payment and settlement options in India include interbank card (both debit and credit) networks, National Electronic Funds Transfer (NEFT), Real-Time Gross

[1] https://www.meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf.

[2] http://digipay.gov.in/dashboard/default.aspx.

[3] https://main.trai.gov.in/sites/default/files/PIR08012019.pdf.

[4] https://main.trai.gov.in/sites/default/files/PIR08012019.pdf.

[5] https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/India_Device_Growth_Traffic_Profiles.pdf.

[6] Credit Suisse, "Digital Payment Statistics," 2018, https://inc42.com/buzz/digital-payments-creditsuisse-report/ http://pib.nic.in/newsite/PrintRelease.aspx?relid=181272.

[7] Justice K.S. Puttaswamy (Retd.) and Anr v. Union of India, Writ Petition (Civil) No. 494 of 2012, 24 August 2017.

[8] http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf.

[9] Section 2(1)(i), Payments and Settlement System Act, 2007.

Settlements (RTGS), Immediate Payments Service (IMPS), the Unified Payments Interface (UPI), Aadhaar-Enabled Payment System (AEPS), Bharat Bill Payment System (BBPS), National Electronic Clearing Service (NECS), the consolidated National Automated Clearing House (NACH),[11] Internet Banking, Mobile Banking, Unstructured Supplementary Service Data (USSD), and Prepaid Payment Instruments (PPIs) or “mobile wallets.”

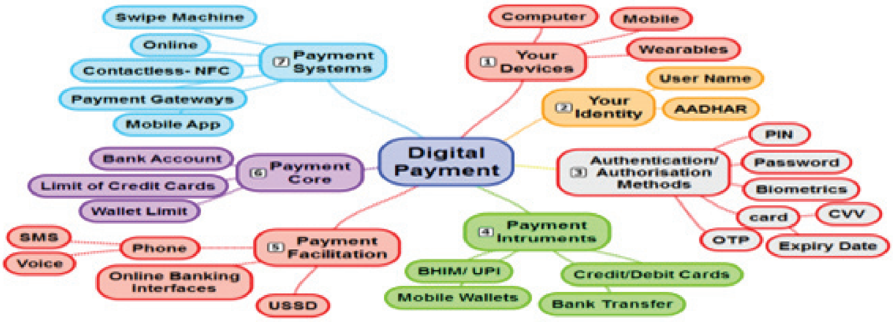
In this context, the major supply-side market participants in India’s payments ecosystem include:

- **Reserve Bank of India (RBI):** India’s sole Large Value Transfer System (LVTS) operator; facilitates both NEFT and RTGS transactions
- **National Payments Corporation of India (NPCI):** India’s sole retail payments system/ infrastructure provider, and controller of the National Financial Switch for ATMs
- **Payment Service Providers (PSPs) and Switch Providers:** These include banks, payment banks, mobile wallet companies, online payment gateway service providers, and card-network companies
- **Infrastructure Providers:** ATM network and White Label ATM Operators (WLAOs), Point-of-Sale (PoS) terminal providers, and mobile device providers
- **Other Supply-Side Participants:** Third-party vendors and network/connectivity providers

This list indicates disparate supply chain entry points for malicious actors to exploit. Multiple parties (of varying scale/size) disaggregating digital payments value chains and managing financial data increases the complexity of financial networks and adds to potential cyber risks.[12] This is further illustrated by open-card payment systems, which usually operate on the Four-Party Model, comprising the cardholder, the merchant, the merchant-acquiring bank and the card-issuing bank. Such systems must, therefore, be operated in a manner that engenders trust amongst customers.[13]

The digital-payments ecosystem also includes demand-side participants, i.e. merchants and consumers. The figure below offers a map of the digital-payments landscape from the demand-side perspective:

Digital-Payments Ecosystem in India



Source: Report of the Working Group for Setting up of CERT-Fin, 4, https://dea.gov.in/sites/default/files/Press-CERT-Fin Report.pdf.

[10] “Online And Mobile Payments: Supervisory Challenges To Mitigate Security Risks,” FinCoNet, 2016, accessed 8 January 2018, http://www.finconet.org/FinCoNet_Report_Online_Mobile_Payments.pdf.

[11] For bulk transactions.

[12] “Digital Financial Inclusion: Implications For Customers, Regulators, Supervisors, And Standard-Setting Bodies,” CGAP 2015, accessed 8 January 2018, 24, https://www.cgap.org/sites/default/files/Brief-Digital-Financial-Inclusion-Feb-2015.pdf.

[13] https://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf.

Scope of Threats and Vulnerabilities

As the ecosystem expands, Indian decision-makers must evaluate the evolving threat/incident matrix permeating the wider cyberspace. According to the 2018 Thales Data Threat Report, data breaches occur more often in India than the global average.[14] As such, even at a global level, the number of cyber incidents targeting financial institutions continue to increase. According to a global map prepared by Carnegie's Cyber Policy Initiative and BAE Systems, Indian financial systems have remained a consistent target of malicious cyber actors.[15] In this regard, the analysis below offers a snapshot of some important trends and incidents:

- **Rising Cyber Frauds/Identity Theft in Digital Payments:** Countries such as Brazil, Canada and Japan have explicitly highlighted identity theft and fraud in relation to 'Card Not Present' (CNP) transactions as a primary threat to their electronic payments frameworks.[16] In India, "cyber fraud" in digital payments rose by around 25 percent (to 16,468 cases) in FY 2015–16.[17] Moreover, during March–December 2017, the number of such cases for credit card, debit card, ATM, and net-banking transactions rose to 22,740.[18] Other threats to digital payments include malware installations, phishing attacks, SIM Card Swap Attacks and unreliable devices/infrastructure.

- **Hitachi ATM Data Breach:** In October 2016, a malware injection in Hitachi's system caused a major security breach, which officially compromised 2.9 million debit cards[19] across various bank accounts. The exposure was due to a prolonged unpatched vulnerability in ATM switch servers maintained by Hitachi.[20] The breach took place over a year prior; however, it went undetected, and Hitachi (i.e. the entity controlling the concerned infrastructure) failed to inform India's designated Computer Emergency Response Team (CERT-In).[21] Poor coordination, incident response and information-sharing protocols contributed to the breach.[22]

- **Incidents with NPCI:** In March 2017, hackers took advantage of a bug in the UPI, leading to losses of around INR 250 million for Bank of Maharashtra customers.[23] The NPCI initially denied any such breach.[24]

- **Lessons from Other Sectoral Data Breaches:** The Indian e-commerce company Zomato suffered the world's sixth-largest data breach in 2017, compromising 17 million digital records. Exemplarily, Zomato disclosed the incident in a transparent manner and advised users to take specific mitigating action.[25]

[14] https://www.dailypioneer.com/business/data-breach-incidents-in-india-higher-than-global-average-thales.html.

[15] https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide.

[16] "Online And Mobile Payments: Supervisory Challenges To Mitigate Security Risks," op. cit., 40.

[17] Lok Sabha Deb, 29 February 2017, Unstarred Question no. 4521, answered by Shri P.P. Chaudhary.

[18] http://164.100.47.190/loksabhaquestions/annex/14/AU6084.pdf.

[19] "ATM/Debit Card Data Breach," Reserve Bank of India, 2016, accessed 8 January 2018, https://rbi.org.in/SCRIPTs/BS_PressReleaseDisplay.aspx?prid=38392.

[20] Lok Sabha Deb, 17 March 2017, Unstarred Question no. 2748, answered by Shri Santosh Kumar Gangwar.

[21] Saikat Datta, "India's Sluggish Response To Cyberattack That Infected 3.2 Million Cards Exposes Its Vulnerabilities," *Scroll.in*, 8 June 2017, accessed 8 January 2018, https://scroll.in/article/839892/india-has-quietly-buried-the-cyberattack-that-infected-3-2-million-debit-cards-and-remains-at-risk

[22] Saikat Datta, "India Suffered A Massive Debit Card Data Breach Because No One Connected The Dots," *Scroll.in*, 25 October 2016, accessed 8 January 2018, https://scroll.in/article/819871/india-suffered-a-massive-debit-card-data-breach-because-no-one-connected-the-dots.

[23] http://164.100.47.190/loksabhaquestions/annex/13/AU1872.pdf.

[24] Sahib Sharma, "Bank Of Maharashtra Accounts Lost Rs25 Crore Due To UPI Bug, Says NPCI," *Livemint*, 31 March 2017, accessed 8 January 2018, http://www.livemint.com/Industry/8HUcQEUGBn0CcPOD6cbfJP/Bank-of-Maharashtra-accounts-lost-Rs25-crore-due-to-UPI-bug.html.

[25] "Security Notice," Zomato, 2018, accessed 8 January 2018, https://www.zomato.com/blog/security-notice.

- **Global Ransomware Attacks:** In 2017, there was a surge in ransomware attacks targeting computer systems across multiple countries. The largest such attacks were WannaCry (May 2017) and Petya (June 2017). India was amongst the worst-hit countries by WannaCry, with over 40,000 affected computers.[26]

- **Potential Scale:** Two large-scale incidents include the 2013 Yahoo data breach, which impacted all three billion user accounts on their platform,[27] and the September 2017 data breach, involving the American credit institution Equifax.[28] In the latter, the social security numbers of over 143 million individuals and the information of over 200,000 credit cardholders were affected.[29]

- **Device-Level Threats:** In January 2018, the smartphone manufacturer OnePlus admitted that a malicious actor had compromised one of the company's servers, by injecting a script that captured user information as it was typed. This resulted in a data breach of over 40,000 credit cards.[30]

- **User-Facing Threats:** According to a report published by the security analytics firm Symantec, poor user passwords increase the likelihood of cyber crime and undermine security measures.[31]

These ecosystem developments and their accompanying scale indicate the fragility of the cyberspace. Policymakers must remain cognisant that it is impossible to completely secure technology networks and markets. Thus, digital and information security frameworks must be designed to minimise risks and to evolve strategic approaches for post cyber-attack ecosystem resilience. Additionally, policymakers must remain conscious of the limitations associated with India's technological readiness and focus on strategies engendering user trust.

Structure of Report

This report is divided into three sections. The first section analyses major institutions and proposes reforms to harmonise functions of the various actors. It also analyses the role of future institutions, such as the forthcoming Data Protection Authority of India (DPA) proposed under the DPB. The second section looks at standardisation, wherein strategies are presented for regulation as well as standard setting and testing. The discussion on regulation juxtaposes the current Information Technology Act (IT Act) framework, vis-à-vis the DPB. The final section brings together the two themes and proposes policy recommendations in relation to India's 2013 National Cyber-Security Policy. The recommendations analyse key pillars of policymaking approaches and how India can leverage the process as a tool to shed protectionist concerns such as data localisation.

[26] "India Third Worst Hit Nation By Ransomware WannaCry; Over 40,000 Computers Affected," *The Economic Times*, 17 May 2017, accessed 8 January 2018, https://economictimes.indiatimes.com/tech/internet/india-third-worst-hit-nation-by-ransomware-wannacry-over-40000-computers-affected/articleshow/58707260.cms; Ashna Kumar, "WannaCry Did Hit India And Even Central Govt Portal. So Why Did Centre Downplay the Ransomware Attack?" India Today, 19 June 2017, accessed 8 January 2018, http://indiatoday.intoday.in/story/ransomware-wannacry-cyberattack-global-ransomware-attack-india/1/981936.html.

[27] "Yahoo Provides Notice To Additional Users Affected By Previously Disclosed 2013 Data Theft," Oath: A Verizon Company, accessed 8 January 2018, https://www.oath.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/.

[28] "Notice Of Data Breach," Equifax, accessed 8 January 2018, https://www.equifaxsecurity2017.com/consumer-notice/#notice.

[29] Ron Lieber, "How To Protect Yourself After The Equifax Breach," *NY Times*, 16 October 2017, accessed 8 January 2018, https://www.nytimes.com/interactive/2017/your-money/equifax-data-breach-credit.html.

[30] "An Update on Credit Card Security," OnePlus Forums, accessed 20 January 2018, https://forums.oneplus.net/threads/jan-19-update-an-update-on-credit-card-security.752415/.

[31] https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf.

INSTITUTIONAL REFORM

This section examines major institutional frameworks across the central government and the payments sector. In this context, policy recommendations are made with respect to (a) Critical Information Infrastructures (CIIs) Protection; (b) Cyber Incident Response and Information Sharing; and (c) Sector-Specific Institutions. Its conclusion revisits the prevailing landscape and proposes suggestions to improve interdepartmental coordination towards digital payments security.

A. CII Protection Frameworks

This report discusses the need to prioritise CII protection and formulate discrete CII-specific cyber-security frameworks. It then suggests strategies to tailor the frameworks for digital payments.

Domestic Scenario

India's Information Technology Act (IT Act) defines CIIs as computer resources, whose incapacitation or destruction have debilitating effects on India's "security, economy, public health or safety."[32] According to the National Cyber-Security Policy (NCSP), 2013, CII protection is a national priority and a shared responsibility that requires effective Public–Private Partnerships (PPPs). The policy also outlines the importance of establishing a National Critical Information Infrastructure Protection Centre (NCIIPC). In 2014, a nodal NCIIPC was established under the National Technical Research Organisation (NTRO), an intelligence agency under the Prime Minister's Office.[33]

Scope and Purpose of the NCIIPC: Primary responsibilities for the NCIIPC include identification of all CII elements for government approval, issuing threat-related advisories, and offering requisite leadership and coordination to effectively respond to threats against "identified" CIIs. The NCIIPC also coordinates and shares strategic information with CERT-In.[34]

Critical Sector/CII Identification: The definition of "Critical Sectors" is analogous to CIIs (NCIIPC Rules 2013); however, specific criteria to identify such sectors remain unavailable. CIIs under each critical sector are identified on the basis of "Functionality, Criticality, Scale, Degree of Complementarities, Political, Economic, Social and Strategic Values, degree of dependence, sensitivity etc."[35] The NCIIPC recognises six overarching critical sectors, including the overarching "Banking, Financial Services and Insurance" (BFSI) sector.[36] Currently, there is no resource available in the public domain that maps all "protected systems" designated as CIIs.[37]

[32] Information Technology Act (as amended in 2008), s 70(1).

[33] Notification No. 9(16)/2004-EC, January 2014.

[34] The Information Technology (National Critical Information Infrastructure Protection Centre and manner of performing functions and duties) Rules, 2013, Rule 4.

[35] "Guidelines For The Protection Of National Critical Information Infrastructure," National Critical Information Infrastructure Protection Centre, 2015.

[36] Others being Transport; Telecom; Power and Energy; Government; and Strategic and Public Enterprises.

[37] "Protecting Critical Information Infrastructures In India," accessed 8 January 2018, https://ccgnludelhi.wordpress.com/2016/11/11/protecting-critical-information-infrastructures-in-india/.

Private-Sector Interface: Institutional guidelines place a positive obligation on CII owners to designate Chief Information Security Officers (CISOs) to directly communicate with the NCIIPC.[38] Further, the NCIIPC formally interfaces with private-sector entities to increase resilience across critical sectors. For instance, the NCIIPC has created partnerships with private-sector entities to sensitise CII owners on potential threats and is in the midst of developing sector-specific guidelines for the power sector.[39] However, India has yet to release formal sector-specific guidelines for any critical sector. One limitation of this institutional framework is the NCIIPC's placement under the NTRO which, as an intelligence agency, is naturally oriented towards secrecy and controlled information disclosure. Specifically, the lack of a transparent procedural framework, which informs CII operators on how shared-information will be used, has the capacity to deter stakeholders from being forthcoming with threat-related information.

In May 2018, the MeitY released the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018, with detailed guidance on the role of such parties in cooperating with the NCIIPC. These rules formalise in law the need for CII owners to collaborate with the NCIIPC and entrusts such institutions with the responsibility of establishing an internal Information Security Steering Committee for "protected systems."[40] The rules also prescribe that protected system owners must conform to the NCIIPC's standard operating procedure (SOP) in relation to "incident response."

International Best Practices

Intergovernmental organisations—such as the Organisation for Economic Cooperation and Development (OECD)[41] and the United Nations' Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UNGGE)[42]—endorse cyber-security strategies that prioritise protecting specific CII systems and critical sectors at large. An advantage in such policy approaches, which differentiate between critical and non-critical systems/markets, is that it can enable the growth of other service markets within the internet economy. For example, the US takes a light-touch cyber-security approach in non-critical sectors to allow for technological innovation.[43] Some recurring best practices in successful CII protection frameworks are analysed below:

- **Risk Assessment and Sub-Sector Identification:** India has six broad categories of "critical sectors," including the BFSI sector. Internationally, there is a growing debate about the veracity of such overbroad sectoral categorisations. A highly cited 2013 Chatham House Report delves into this matter and offers strategies to reduce vagueness, highlighting the need for clarity and precise metrics in categorising CIIs and critical sectors.[44] This is particularly important from a governance point-of-view, since all institutions have finite resources. As a result, prioritisation-related trade-offs must be assessed by authorities. Specifically, the report makes two important recommendations. First, to limit ambiguity, broader sectors must be narrowed down to inherently critical "sub-sectors." Second, critical nodes must be identified (using objective risk assessment and analysis) within these ecosystems. [45] The OECD, citing

[38] NCIIPC, "Guidelines for Protecting Critical Information Infrastructure," January 2015, para 6.3.4

[39] Saikat Datta, "The NCIIPC & Its Evolving Framework," 27 October 2016, accessed 8 January 2018, http://www.digitalpolicy.org/nciipc-evolving-framework/#_edn2.

[40] http://meity.gov.in/writereaddata/files/NCIIPC-Rules-notification.pdf.

[41] "CYBERSECURITY POLICY MAKING AT A TURNING POINT: Analysing A New Generation Of National Cybersecurity Strategies For The Internet Economy," OECD 2012, accessed 8 January 2018, https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

[42] "Developments In The Field Of Information And Telecommunications In The Context Of International Security," UNODA, 2015, accessed 8 January 2018, https://www.un.org/disarmament/topics/informationsecurity.

[43] "CYBERSECURITY, INNOVATION AND THE INTERNET ECONOMY," THE DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE 2011, accessed 8 January 2018, https://www.nist.gov/sites/default/files/documents/itl/Cybersecurity_Green-Paper_FinalVersion.pdf.

[44] Dave Clemente, Chatham House, the Royal Institute of International Affairs 2013, accessed 8 January 2018, https://Www.Chathamhouse.Org/Sites/Files/Chathamhouse/Public/Research/International%20Security/0213Pr_Cyber.

[45] Ibid.

jurisdictions such as the UK, Canada and Australia, recommends the development of risk assessment and risk analysis tools for CII identification.[46]

- **Institutional Design:** A report published by the International Telecommunication Union (ITU) states that CII protection-framework design should focus on early-warning systems, detection, response and crisis management. It states that it is important to gain private-sector confidence through requisite incentives, since the private sector is the principal owner of most CIIs. In this regard, PPPs are considered a promising tool. The report also states the need for institutions such as the NCIIPC to coordinate closely with CERTs to streamline security efforts.[47]

- **Adapting to National Priorities:** The OECD has stated that CII identification approaches should reflect government priorities and jurisdictional specificities.[48] The North Atlantic Treaty Organisation (NATO), too, has noted that the purpose/function of infrastructure can render a specific system critical.[49] Table 1 maps key jurisdictional practices.

Table 1

Jurisdiction	Critical Infrastructure/Sector Treatment
United Kingdom[50]	■ The UK has identified 13 broad critical sectors, including "finance." Several sectors have specifically defined sub-sectors. Each identified sector has a "lead government" arm for sector-specific critical assets. It explicitly notes that every information system in a critical sector should not be treated as "critical." ■ Its nodal Centre for Protection of National Infrastructure collaborates closely with the country's National Cyber-Security Centre (NCSC). Another key priority of its framework is ecosystem cooperation and overall coordination across relevant agencies and experts.
US[51]	■ The Department of Homeland Security (DHS), the US' nodal agency, releases monthly toolkits for CII protection and identification. ■ The US has sector-specific plans to supplement its National Infrastructure Protection Plan. In this regard, the US has identified private-sector engagement, development of sector-specific plans and collaboration with sector-specific agencies as pillars for CII protection.
Japan	■ Japan has identified 13 critical sectors, including "financial services" and "credit card services" as two discrete sectors. Its framework also identifies specific sub-sectors and IT systems.[52] This is unlike the Indian approach, which restricts itself to broad critical sectors, with limited officially recognised protection systems.

[46] Nick Mansfield and Anne Carblanc, "OECD Ministerial Meeting On The Future Of The Internet Economy," OECD, 2007, accessed 8 January 2018, https://www.oecd.org/sti/40761118.pdf.

[47] Manuel Suter, "A Generic National Framework For Critical Information Infrastructure Protection (CIIP)," Centre for Security Studies, 2007, accessed 8 January 2018, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf.

[48] Nick Mansfield and Anne Carblanc, op. cit.

[49] Lord Jopling (Special Rapporteur), 162 CDS 07 E rev 1 – The Protection of Critical Infrastructures, 2007, NATO Parliamentary Assembly, http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/270/270907/270907jopling_en.pdf.

[50] "Critical National Infrastructure," accessed 8 January 2018, https://www.cpni.gov.uk/critical-national-infra-structure-0.

[51] Homeland Security, "Critical Infrastructure Security and Resilience Month Toolkit," 2018, accessed 8 January 2018, https://www.dhs.gov/sites/default/files/publications/cisr-month-tooklit-2017-508.pdf.

[52] "The Basic Policy Of Critical Information Infrastructure Protection," Information Security Policy Council 2014, accessed 8 January 2018, https://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf.

Jurisdiction	Critical Infrastructure/Sector Treatment
China[53]	■ China's new cyber-security law added new criteria to its "CII" definition. It now seeks to develop standards to identify CII. One of these metrics is the number of users on a platform.[54]
Singapore	■ Singapore's nodal Cyber-Security Agency (CSA) is entrusted with the protection of critical sectors.[55] It has identified 11 critical sectors, including banking and finance. ■ The country consultatively developed and enacted a new Cyber Security Act, 2018.[56] The Act, *inter alia*, sought to strengthen Singapore's CII protection framework.[57] The law characterises CIIs as computer systems that are directly involved in providing "essential services." Moreover, the Act aims to provide a framework to designate CIIs and offers clarity to CII owners, vis-à-vis their obligations to proactively protect such systems against cyberattacks.[58] ■ The CSA administers a "whole-of-government" cyber-security exercise to periodically test the robustness of Singapore's cyber-incident management and emergency-response frameworks across all critical sectors.[59] (*Exercise Cyber Star*)
European Union (EU)[60]	■ The European Commission (EC) provides an indicative list of 11 critical sectors, including the financial sector. Sub-sectors under the financial sector include banking and payment ecosystems. ■ It notes that critical services should be tailored to the needs of jurisdictions and that effective collaboration with the private sector is fundamental to identifying and protecting CII assets/services.

Recommendations

- Policymakers should explore the feasibility of declaring interoperable retail and large-value payments markets as "critical sub-sectors," while not all nodes/enterprises may be deemed as CIIs. Therefore, it is prudent to deem systems operated by larger market infrastructure providers such as the NPCI as "protected systems."

- Similar to the practices in the US, China and Singapore, detailed in Table 1, India should explore revisiting its current CII protection through public consultation. Moreover, it should also consider developing sub-sector CII strategies for the digital-payments ecosystem. Specifically, the Indian government must consider developing a comprehensive CII-protection system and sector/sub-sector identification framework.

- Like Singapore's CSA (Table 1), India could start cross-sectoral penetration-test exercises for resilience and risk assessment across nodes that are deemed critical within the digital-payments ecosystem.

[53] Graham Webster, "Critical Information Infrastructure Security Protection Regulations," accessed 8 January 2018, https://chinacopyrightandmedia.wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/.

[54] Paul Triolo, "China's Ambitious Rules To Secure 'Critical Information Infrastructure'," accessed 8 January 2018, https://www.newamerica.org/cybersecurity-initiative/blog/chinas-ambitious-rules-secure-critical-information-infrastructure/.

[55] "Our Organisation," Cyber Security Agency, 2018, accessed 8 January 2018, https://www.csa.gov.sg/about-us/our-organisation.

[56] Cybersecurity Act 2018 (No. 9 of 2018), https://sso.agc.gov.sg/Acts-Supp/9-2018/.

[57] Cybersecurity Act 2018 (No. 9 of 2018), Part 3, https://sso.agc.gov.sg/Acts-Supp/9-2018/.

[58] https://www.csa.gov.sg/legislation/cybersecurity-act.

[59] Exercise Cyber Star.

[60] European Union Agency for Network and Information Security, "Methodologies For The Identification Of Critical Information Infrastructure Assets And Services," European Union Agency for Network and Information Security, 2015.

- India must improve institutional transparency. A possible solution could be a "voluntary" CII protection framework, to enhance public–private collaboration along the lines of the US' Protected CII Programme.[61]

B. Cyber Incident Response and Information-Sharing

This section suggests recommendations to augment the role of CERT-In and mirror entities within the payments ecosystem, such as the Indian Banks–Centre for Analysis of Risk and Threats (IB-CART) and the proposed Computer Emergency Response Team in the Financial Sector (CERT-Fin). Specifically, these institutional frameworks must incorporate lessons from incidents such as the Hitachi systems breach, wherein the operator only apprised sectoral institutions, i.e. the RBI and the NPCI, leaving CERT-In and the NCIIPC in the dark.[62]

Domestic Scenario

CERT-In: Section 70B of the IT Act designates CERT-In as India's nodal agency for cyber-incident response. CERT-In's functioning is governed under this provision and the concomitant 2013 CERT Rules. It is entrusted with both proactive and reactive responsibilities. The proactive responsibilities are designed to help build ecosystem resilience against oncoming threats. In this context, CERT-In has the role of forecasting and alerting the ecosystem of cyber-security incidents and related risk-mitigation strategies. It does this through a combination of dynamic advisories[63] and vulnerability notes,[64] and periodic whitepapers, guidelines, monthly bulletins and annual reports.[65]

Advisories and Vulnerability Notes are largely a reproduction of vendor disclosures or global cyber-security analysis. For instance, most outputs merely collate links from the US-Computer Emergency Response Team (US-CERT), CERT-EU, and the international Common Vulnerabilities and Exposure (CVE) database. Without India-specific outputs, exploits on indigenous software systems can go undocumented. Further, critical infrastructure systems that use software developed by institutions such as the Centre for Development of Advanced Computing (C-DAC) can be left vulnerable to bad actors. Such practices add to the insecurity of India's payment and settlement ecosystem because key institutions like the NPCI develop interoperable payments solutions based on indigenous software solutions and have worked with institutions such as the C-DAC.[66]

Experts argue that updates on the CERT-In website's 'Knowledge Base' section offer limited technical insight into these outputs, are largely outdated, and carry little value in building cyber resilience. The website's 'Annual Reports' page simply maps the types of cyber threats most prevalent across the Indian ecosystem, without any details on best-practice countermeasures to proactively secure the ecosystem.[67]

Additionally, the CERT Rules task CERT-In with the responsibility of facilitating stakeholders with Information Security Assurance (ISA) and audit services.[68] Such obligations are designed to aid stakeholders with risk management, as robust ISA protocols can improve resilience against attacks, especially from common exploits that lead to most successful cyber-attacks. To achieve this, CERT-In empanels information security auditors. As per the latest list, CERT-In has empanelled 76 such auditors. However, as per disclosures, only nine of these auditors have

[61] https://www.dhs.gov/pcii-program.

[62] Saikat Datta, op. cit.

[63] http://cert-in.org.in/s2cMainServlet?pageid=PUBADVLIST.

[64] http://cert-in.org.in/s2cMainServlet?pageid=VLNLIST.

[65] Information Technology Act, 2000, s. 70B.

[66] https://www.npci.org.in/sites/default/files/circular/Concept%20Note%20on%20NCMC%20Implementation_V1.0.pdf.

[67] https://cis-india.org/internet-governance/files/cert-ins-proactive-mandate.pdf.

[68] CERT Rules, 16 January 2014, Rule 9, http://meity.gov.in/sites/upload_files/dit/files/G_S_R%2020%20(E)2.pdf.

working expertise in digital payments and cyber-security aspects.[69] Moreover, the CERT-In's last update on the "IT Security Policy: Compliance & Assurance" webpage is from 2009 and, for critical sectors, from 2006.[70]

The CERT Rules guide CERT-In's interface with external stakeholders. Notably, the Advisory Committee to the CERT-In is structured to only include one industry association representative, a slot that is rotated sectorally on an annual basis.[71] Additionally, to effectively respond to cyber-incident/threat situations, the rules mandate the CERT-In to coordinate with other stakeholders such as the sectoral CERTs, ISPs, industry participants, vendors of security products and services, Law Enforcement Agencies (LEAs) and the NCIIPC where relevant.[72]

The rules further facilitate information-sharing by putting in place confidentiality safeguards, whereby CERT-In will publicly disclose the names of affected entities only if there is explicit consent from the particular individual or entity or an appropriate court order.[73] Further, an annexe to the rules mandates stakeholders to disclose specific types of incidents, including targeted threats against critical networks and systems and attacks on critical infrastructure.

CERT-Fin: Specific to the digital-payments and wider digital-financial ecosystem, the Indian government is in the process of establishing a sector-specific CERT-Fin.[74] According to a Working Group Report, this CERT-Fin is envisioned to have sub-sectoral CERTs under each financial regulator. Here, a sub-sectoral CERT under the RBI will deal with securing the payments ecosystem. The proposed structure requires CERT-Fin interfacing with CERT-In, the NCIIPC, and a proposed CERT that is being established for the telecom sector.[75] The report does, however, indicate reticence in working closely with the private sector. Illustratively, the overall structure and the proposed Advisory Board to CERT-Fin only comprise government officials.[76] Moreover, the report asserts that India's private sector has limited appreciation for cyber-security at board levels.[77]

IB-CART: Another key component of cyber risk-mitigation frameworks comprises Information-Sharing and Analysis Centres (ISACs). Internationally, it is agreed that the primary purpose of ISACs is to facilitate the exchange of information to bolster sectoral incident response.[78] They, however, do not perform the incident-response functions associated with CERTs. To this end, the Institute for Development and Research in Banking Technology (IDRBT)[79] has established IB-CART. Its primary functions include disseminating/sharing information regarding threats (through secure infrastructures), concomitant risk-mitigation strategies, and facilitating cross-sector information exchange.

IB-CART was established based on a recommendation by the RBI Working Group on Information Security, which stated that the Indian banking sector required an information-sharing framework similar to the US' Financial Services Information Sharing and Analysis Centre (FS-

[69] http://www.cert-in.org.in/PDF/Empanel_org.pdf.

[70] "Indian - Computer Emergency Response Team," Cert-In, accessed 8 January 2018, http://www.cert-in.org.in/.

[71] CERT Rules, op. cit., Rule 6.

[72] Ibid., Rule 10.

[73] Ibid., Rule 13(2).

[74] Budget 2017–18, Speech of Arun Jaitely Minister of Finance, Para 101.

[75] "REPORT OF THE WORKING GROUP FOR SETTING UP OF COMPUTER EMERGENCY RESPONSE TEAM IN THE FINANCIAL SECTOR (CERT-Fin)," Department of Economic Affairs, 62, Para 4.38, 2017, accessed 9 January 2018, http://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf.

[76] Ibid., 62, 68–69.

[77] Ibid., 62, Para 3.38.

[78] Isabel Skierka, et. al., "The History, Types & Culture Of Computer Security Incident Response Teams," CSIRT 2015, accessed 9 January 2018, 11–12, http://www.digitaldebates.org/fileadmin/media/cyber/CSIRT_Basics_for_Policy-Makers_May_2015_WEB_09-15.pdf.

[79] Situated under the RBI.

ISAC).[80] However, the present framework is limited to the banking sector and not the entire digital-payments ecosystem. Additionally, during the Hitachi debit card breach, IB-CART was unsuccessful in alerting banks of the systemic nature of the attack. Reportedly, this was due to IB-CART's erstwhile protocol to not categorise debit/credit card incidents as systemic cyber threats, but as 'fraud', which is attributed a lower level of significance.[81]

International Best Practices

The need for forthcoming multistakeholder knowledge-sharing in digital financial markets has been identified as a prerequisite by the G7[82] and the ITU.[83] Some key international practices that can inform Indian policymakers to improve India's present CERT structure are discussed below.

Streamlining Information-Sharing Systems and Vulnerability Discovery: The US government maintains government-monitored information-sharing platforms for anonymous disclosures to inculcate instantaneous awareness of cyber vulnerabilities and publicly share security solutions across markets.[84] Similarly, China is developing a new interoperable cyber-security/threat-sharing platform for the government, the private sector and academia. It is also developing a central cyber-security vulnerability-discovery and reporting-management system.[85] To aid with vulnerability discovery, China (like Singapore) has initiated plans on proactively conducting cross-sectoral and cross-regional emergency response drills to strengthen its cyber-security emergency response capacity.[86]

Working with Local and Provincial Authorities: The US has a comprehensive cyber-security and incident response framework, wherein central authorities such as the Department of Homeland Security (DHS) work closely with local governments. It has also formalised interstate information-sharing arrangements such as the Multi-State Information-Sharing and Analysis Centre.[87] China's cyber-security and incident response regime expands its operational scope beyond the highest levels of government, and exemplarily, its national CERT is operational at provincial and municipality/local levels.[88]

Framework Incentives: The US Cyber-Security and Information-Sharing framework (2015), *inter alia*, offers incentives such as liability protections for entities voluntarily coming forward to share threat indicators or defensive strategies. A report by Chatham House and the Centre for International Governance Innovation advocates that incident-response laws and frameworks should incentivise information-sharing and make assurances that sensitive information shared will be handled with care and used only for the purpose of risk mitigation.[89]

[80] "Indian Banks – Center For Analysis Of Risks And Threats (IB-CART)," accessed 9 January 2018, Institute for Development and Research in Banking Technology, http://www.idrbt.ac.in/ib-cart.html.

[81] Saikat Datta, op. cit.

[82] G7, "G7 FUNDAMENTAL ELEMENTS OF CYBERSECURITY FOR THE FINANCIAL SECTOR," accessed 9 January 2018, https://www.fin.gc.ca/n16/docs/g7-1014-eng.pdf.

[83] "Security Aspects Of Digital Financial Services," International Telecommunication Union, 2017, accessed 9 January 2018, https://www.itu.int/en/ITU-T/studygroups/2017-2020/09/Documents/ITU_FGDFS_SecurityReport.pdf.

[84] https://www.whitehouse.gov/wp-content/uploads/2018/02/ERP_2018_Final-FINAL.pdf, 370.

[85] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/.

[86] Graham Webster, "Critical Information Infrastructure Security Protection Regulations," articles 38 and 39, accessed 8 January 2018, https://chinacopyrightandmedia.wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations.

[87] http://mrsc.org/Home/Explore-Topics/Public-Safety/Cybersecurity/Cybersecurity-Resources-for-Local-Governments.aspx.

[88] http://www.cert.org.cn/sites/english/index.htm.

[89] Samantha Bradshaw, "Combatting Cyber Threats: CSIRTs And Fostering International Cooperation On Cybersecurity," CHATHAM House 2015, accessed 8 January 2018, https://www.cigionline.org/sites/default/files/gcig_no23web_0.pdf.

Institutional Transparency: The Internet Governance Forum (IGF) observes that although not necessarily inappropriate, the association of CERTs with LEAs hampers trust and dilutes their perception of being honest brokers of IT response and security. This, in turn, impedes information-sharing.[90] Here, policymakers must remain cognisant that CERTs are conduits of information response, whose success is incumbent on first-responder (primarily businesses) reactiveness.[91] Best practices, e.g. the US' information-sharing framework, call for clear and precise rules and procedural limits to the manner in which the government can use shared information.[92]

Sectoral Information-Sharing Protocols: Specific to payments, the EU's Revised Payment Service Directive (PSD2), states that PSPs are mandated to report "major" operational or security incidents to concerned payments authorities.[93] To this end, the European Banking Authority (EBA) has developed guidelines to assess the severity of incidents based on the transactions affected, the number of users affected, service downtime and economic impact, amongst others.[94]

Informal sharing of risk-mitigation strategies: Countries such as the US have designed incident response frameworks to *promote informal sharing of response and risk-mitigation strategies*. Benefits accrued include the organic development of trust amongst ecosystem participants as well as creating agile channels of communication to complement formalised mechanisms.[95] International CERT practitioners consider such channels as some of the most important and trusted forms of cooperation.[96]

Early-Warning System: China's Cyber-Security Law aims to develop an "early-warning system" to enhance situational awareness, through enhanced threat anticipation and quicker response time to incidents. Complex cyber-attacks occur over distributed phases, and effective response mechanisms to thwart such operations at initial "reconnaissance" stages can offer a fillip to the resilience of networked ecosystems. Such systems are stakeholder-oriented collaborative frameworks that leverage data analytics (using Intrusion Forecasting Systems[97]) to help pre-empt cyber threats and attacks by identifying trends related to the distribution of malicious code, which is otherwise difficult to discern. Other countries to embrace such early-warning systems include Austria[98] and Belgium.[99] Specific to payments-fraud-mitigation strategies, the ITU Focus Group on Digital Financial Services (DFS) has encouraged policymakers to explore mechanisms to share relevant data, whilst being able to maintain confidentiality, to pre-emptively detect anomalous activities. Larger pools of such data make risk detection easier. Such collaborative fraud-management practices have worked successfully within US card markets.[100]

[90] "Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security," Internet Governance Forum, 2014, 15.

[91] Robert Morgus, et. al., "National CSIRTs and Their Role in Computer Security Incident Response", November 2015, 6, http://www.digitaldebates.org/fileadmin/media/cyber/National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response__November_2015_--_Morgus__Skierka__Hohmann__Maurer.pdf.

[92] "To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes," US congress S.754, https://www.congress.gov/bill/114th-congress/senate-bill/754.

[93] Payment Services Directive 2, Article 96.

[94] "Guidelines On Major Incident Reporting Under Directive (EU) 2015/2366 (PSD2)," European Bank Authority 2017, accessed 8 January 2018, https://www.eba.europa.eu/documents/10180/1914076/Guidelines+on+incident+reporting+under+PSD2+%28EBA-GL-2017-10%29.pdf.

[95] Robert Morgus, et. al., op. cit., 5.

[96] http://www.digitaldebates.org/fileadmin/media/cyber/CSIRT_Basics_for_Policy-Makers_May_2015_WEB_09-15.pdf.

[97] Sehun Kim, "Intrusion Forecasting Framework For Early Intrusion Forecasting Framework For Early Warning System Against Cyber Attack," 2018, accessed 8 January 2018 , http://www.ieice.org/~icss/jwis2007/pdf/Invited-2.pdf.

[98] AusCERT, "Early Warning Service," 2018, accessed 8 January 2018, https://www.auscert.org.au/services/early-warning-service/.

[99] Charles Michel Prime Minister of Belgium, "'Early Warning System': Prevention Is Better Than Cure," 2018, accessed 8 January 2018, http://premier.be/en/early-warning-system-prevention-better-cure.

[100] UN, "ITU-T Focus Group Digital Financial Services: Main Recommendations," International Telecommunication Union, 2017, accessed 8 January 2018, https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/201703/ITU_FGDFS_Main-Recommendations.pdf.

Emphasis on International Cooperation: The US and regional Asian economies have thus far spearheaded international cooperation in the financial cyber-security sector. Notably, Japan's FS-ISAC has entered into a cooperation agreement with the US FS-ISAC, to expedite information-sharing processes and enhance domestic cyber-security capacities.[101] Additionally, in December 2016, the Monetary Authority of Singapore (MAS) set up a partnership with the US FS-ISAC to establish a Regional Intelligence and Analysis Centre,[102] which aims to bolster regional-sharing and analysis of cyber-security information across the financial-services sector.

Recommendations

- To improve CERT-In's performance under its proactive mandate, given that its operations are restricted by resource constraints,[103] policymakers can explore a collaboration between CERT-In, industry and independent research organisations to develop literature on appropriate cyber-security best practices and countermeasures, vis-à-vis emerging threats for the Indian payments landscape.

- India must explore appropriate incentives (e.g. liability reduction) for stakeholders to proactively share cyber-incident and threat-related information, and concomitant defensive strategies. It should also examine the feasibility of establishing a vulnerability-discovery/information-sharing system as done by the US and China. Further, CERT-In can explore working with card-network companies/research experts to develop an "early-warning system" for India's payments ecosystem.

- India must expedite the process to set up CERT-Fin and sub-sectoral CERTs for the digital-payments ecosystem, even as it promotes greater institutional transparency in the relationship between such agencies and LEAs and intelligence agencies.

- Similar to Chinese efforts, India should develop government capacity (with the help of payments industry and security experts) for cyber-incidence response efforts all the way from the central government, down to state and local levels of governance. In this regard, reports dated December 2017 suggest that Telangana was set to operationalise a state-level Security Operations Centre.[104] Similarly, strategies to augment coordination between CERT-In, State CERTs and the cyber cells of local police authorities must also be conceptualised.

- Learning from FS-ISAC-related efforts in Japan and Singapore, India should explore cross-jurisdictional information-sharing arrangements to secure digital payments and related financial sectors. India's current FS-ISAC framework (IB-CART) should be expanded beyond banking to include the rest of the payments ecosystem. CERT-In should also leverage its membership at the Forum of Incident Response and Security Teams (FIRST) to improve domestic cyber-incident and information-sharing capacities.[105]

[101] General Incorporated Association Financials ISAC Japan, "Joint Affiliate Agreement Entered Into With US FS-ISAC," 2018, accessed 8 January 2018, http://www.f-isac.jp/press_release/20150220_e.html.

[102] Monetary Authority of Singapore, "FS-ISAC And MAS Establish Asia Pacific (APAC) Intelligence Centre For Sharing And Analysing Cyber Threat Information," 2016, accessed 8 January 2018, http://www.mas.gov.sg/News-and-Publications/Media-Releases/2016/FS-ISAC-and-MAS-Establish-APAC-Intelligence-Centre.aspx.

[103] As stated in CERT Rules.

[104] "TS To Get Security Operations Centre," 2017, The Hindu accessed 8 January 2018, http://www.thehindu.com/todays-paper/tp-national/tp-telangana/ts-to-get-security-operations-centre/article21667751.ece#.

[105] "FIRST – Improving Security Together," FIRST — Forum of Incident Response and Security Teams, 2018, accessed 8 January 2018, https://www.first.org/.

C. Rationalising the Role of Payments Institutions

There are several regulatory and rule-making authorities in India's digital-payments landscape, including the RBI, the forthcoming payments regulatory board (PRB) and the NPCI. This section assesses their respective mandates and explores ways to rationalise and augment their roles.

Domestic Scenario

RBI and CSITE Cell

The Payment and Settlement Systems (PSS) Act, 2007 designates the RBI as the authority that regulates and supervises payment systems in India.[106] This includes system participants, i.e. a bank or any other person including "system providers." The Act defines "system providers" as the authorised "payments systems" operators.

Moreover, if the RBI determines that a payments system or system participant is engaging in activities deemed to carry "systemic risk," it can issue directions placing certain requirements on the concerned entity to remedy the situation.[107] In pursuance of its overarching supervisory mandate, the RBI established a Cyber-Security and IT Examination Cell (CSITE Cell) in 2015. Through this cell, the RBI leads the review and reform of extant cyber-security policies for India's banking and payments ecosystem. This cell has also previously conducted a cyber-drill exercise (in conjunction with the CERT-In) to evaluate cyber preparedness of some banks using hypothetical-scenario-based tests.

Payments Regulatory Board (PRB)

After demonetisation,[108] the Watal Committee on digital payments recommended establishing a PRB independent of the RBI to limit/reduce institutional biases (as the RBI also has a regulatory responsibility to protect the interests of the banking sector).[109] In March 2017, the government amended the PSS Act to legislate for a revised PRB to ostensibly fulfil this mandate for independence.[110] However, this amendment did not reflect the desired levels of multistakeholder inclusivity or independence from RBI as advocated by the Watal Committee. In this connection, it is worth noting that the Financial Services Legislative Reforms Commission (FSLRC) Working Group on Payment report[111] and the RBI's Vision 2018[112] document have also previously recommended establishing multistakeholder councils comprising technologists and experts across telecom, fintech and security to support the payments regulator in standard-setting and policy matters. The PRB is yet to be established.

Notably, the government is also pursuing further institutional reforms. To this end, the it appointed an inter-ministerial panel headed by the Secretary of the Department of Economic Affairs (DEA) and comprising the RBI, the UIDAI, the MeitY, the Department of Legal Affairs (DoLA) and the Department of Financial Services (DFS). In August 2018, after multiple consultations, the Committee placed a new bill to be considered for enactment before the Union Cabinet.[113] While

[106] PSS Act, Section 3(1), as amended by Section 152 of Finance Act 2017, http://164.100.47.193/BillsPDFFiles/Notification/2017-12-gaz.pdf.

[107] Payment and Settlement System Act, 2007, Section 17(b)(ii).

[108] https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=38520.

[109] http://finance.du.ac.in/du-finance/uploads/pdf/Reports/watal_report271216.pdf.

[110] Finance Act, 2017, s. 152.

[111] Financial Sector Legislative Reforms Commission, "REPORT OF THE WORKING GROUP ON PAYMENTS," Recommendation 9, accessed 9 January 2018, https://macrofinance.nipfp.org.in/fslrc/documents/wg_payments_report.pdf.

[112] RBI, "PAYMENT AND SETTLEMENT SYSTEMS IN INDIA: VISION-2018," accessed 9 January 2018, https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/VISION20181A8972F5582F4B2B8B46C5B669CE396A.PDF.

[113] https://dea.gov.in/sites/default/files/Payment%20and%20settlement.pdf.

the Bill does look to create a PRB that has a greater degree of independence from the RBI, it does not appear to reflect the principles of multistakeholderism as articulated by the FSLRC Working Group on the RBI's Vision Document.

National Payments Corporation of India (NPCI): The NPCI is India's sole retail-payments system operator and infrastructure provider. Its bouquet of offerings includes the IMPS, the UPI (an application layer built over India Stack[114]), the Bharat Bill Payments System (BBPS) and the Aadhaar-Enabled Payments Systems (AEPS). It also owns and operates the National Financial Switch (NFS) for ATMs. In addition to being the sole operator of services such as the AEPS, the NPCI offers services such as the BHIM mobile application, the recently launched National Common Mobility Card[115] and the RUPAY card scheme.[116] The primary purpose of the NPCI is to foster an umbrella retail-payments marketplace.

Prevailing Security and Privacy Challenges: Policymakers must be mindful of security challenges surrounding NPCI offerings, such as the Bank of Maharashtra UPI bug and the State Bank of India's flagging of the UPI as a vulnerable system.[117] Additionally, a November 2017 report by Privacy International expressed concern regarding the UPI's architecture as it centralises data concentration and opens up user-financial data to invasive data-harvesting/mishandling.[118] Specifically, literature suggests that the current UPI framework lacks adequate consent or data-collection safeguards and can lead to excessive collection and processing of user data.[119]

Structural Challenges: Such incidents and privacy concerns represent the inherent risks of single-player retail payments infrastructure/system-operator markets, especially those with such large-scale roll-out responsibilities (see AEPS). A constraint on resources, leading to suboptimal conditions, can erode trust, casting doubts on the integrity of India's digital-payments ecosystem. This further deters users from adopting digital-payment solutions. Consequently, the Watal Committee recommended frameworks to allow for multiple critical payments infrastructure companies (CPICs), like the NPCI, to reduce susceptibility to single points of failure.[120] For similar reasons, in January 2019, the RBI also released a white paper for creating a framework to authorise retail payment systems outside the NPCI.[121]

International Best Practices

The analysis presented here is based on approaches espoused by international financial authorities and other advanced markets. Additional details are available in **Annexure 1.**

Identifying Financial Market Infrastructures (FMIs): The Bank for International Settlements' (BIS) Committee on Payments and Market Infrastructures (CPMI) has released the overarching principles of financial market infrastructure (PFMI). The report defines FMIs as systemically important payments systems that facilitate clearing, settlement and recording of monetary and financial transactions. These principles note the importance of protecting FMIs as they concentrate risk and can lead to significant market shocks if improperly managed. They are

[114] Developed by iSPIRT, India Stack is an Aadhaar-linked set of Application Programming Interfaces (APIs) operating in "layers" that afford developers a set of tools and access to Aadhaar user data to produce curated applications and services.

[115] https://www.npci.org.in/sites/default/files/circular/Concept%20Note%20on%20NCMC%20Implementation_V1.0.pdf.

[116] "NPCI," 2018, accessed 9 January 2018, https://www.npci.org.in/.

[117] Saloni Shukla, "Public Sector Banks Including SBI Cast Doubt on Safety Of UPI," Economic Times, 2017, accessed 9 January 2018, https://economictimes.indiatimes.com/markets/stocks/news/public-sector-banks-including-sbi-cast-doubt-on-safety-of-upi/articleshow/58177183.cms.

[118] https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf.

[119] https://www.orfonline.org/research/privacy-security-risks-digital-payments/.

[120] Medium Term Recommendations to Strengthen Digital Payments Ecosystem, Watal Committee on Digital Payments, Ministry of Finance, December 2016.

[121] https://m.rbi.org.in/scripts/PublicationReportDetails.aspx?UrlPage=&ID=918.

conduits of efficient and cost-effective interoperable payments and include both large-value and retail payments infrastructure providers.[122] The seminal Watal Committee Report, too, has referenced these principles, suggesting that the NPCI be classified as a CPIC.

Regulating Interoperable FMIs: The CPMI's 2016 Guidance on Cyber Resilience for FMIs[123] states that FMI participants (e.g. PSPs using the NPCI infrastructure/systems) should adopt congruent resilience measures to access interoperable payment systems. Moreover, the BIS has previously remarked that security frameworks should note that in interoperable payments networks, hackers will probably target nodes with laxer security and, to this end, could target non-banking participants on systems, e.g. the UPI.[124]

Institutional Single Point of Failure Risks: Financial authorities such as the BIS and the European Central Bank (ECB)[125] hold that it is incumbent on sectoral regulators to identify single points of failure in the retail-payments market, whose disruption can have wider ramifications across digital-payments ecosystems.[126] The ECB notes that disruptions in non-substitutable systems increase trading frictions[127] and may drive users to use other channels, e.g. cash.

Integrating Telecom Authorities: The ITU Focus Group on DFS recommends[128] payments institutions to consider working with telecom regulators to establish infrastructure (e.g. IMSI catchers), to identify fake base stations that target capturing (via "man-in-the-middle" attacks) SMS and USSD session data for customer-payment credentials. The ITU also recommends payments and telecom regulators to collectively facilitate joint penetration tests to check the resilience of entire networks (against specific security benchmarks).

Multistakeholder Payments Advisory Councils: The ITU Focus Group cites Jordan's "DFS Council" as a best practice.[129] This council comprises various ecosystem market participants (include third-party vendors) and various regulators (across the financial sector) that help shape policy, filling in all ecosystem gaps. Similarly, Singapore has established a multistakeholder policy feedback/developing entity in the form of its Payments Council, which comprises both demand and supply-side stakeholders.[130] Security standards and policies for payments in countries such as Canada, Spain and Japan are developed in conjunction with other sectoral authorities and private-sector inputs.[131]

Recommendations

In addition to incorporating the various best practices highlighted above, the following recommendations should be considered low-hanging fruits to improve the role of sector-specific institutions in securing India's digital-payments landscape:

[122] "Principles for Financial Market Infrastructures," Committee on Payment and Settlement Systems, 2012, accessed 9 January 2018, https://www.bis.org/cpmi/publ/d101a.pdf.

[123] Ibid.

[124] Bank for International Settlements, "Non-Banks In Retail Payments," Committee on Payments and Market Infrastructures 2014, accessed 9 January 2018, https://www.bis.org/cpmi/publ/d118.pdf.

[125] "PAYMENTS AND MONETARY AND FINANCIAL STABILITY," ECB-BANK OF ENGLAND, 2007, accessed 9 January 2018, https://www.ecb.europa.eu/pub/pdf/other/paymentsmonetaryfinancialstability200801en.pdf?d3b516314e4c8178fe0a962d27eb7f61.

[126] Bank for International Settlements, "Innovations In Retail Payments," Committee on Payment and Settlement Systems, 2012, accessed 9 January 2018, https://www.bis.org/cpmi/publ/d102.pdf.

[127] "PAYMENTS AND MONETARY AND FINANCIAL STABILITY," op. cit.

[128] UN, "ITU-T Focus Group Digital Financial Services: Main Recommendations," op. cit.

[129] UN, "ITU-T Focus Group Digital Financial Services: Main Recommendations," op. cit.

[130] http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-Establishes-Payments-Council.aspx.

[131] See Annexure 1.

- India can consultatively amend the PSS Act to create a multistakeholder body to advise the future PRB on future policymaking and regulatory issues with respect to digital payments (see Singapore's Payments Council and Jordan's Digital Financial Services Council).

- The retail payments marketplace with the NPCI as the sole system operator/infrastructure provider should be redesigned to limit single points of failure. To this end, a regulated CPIC marketplace, as recommended by the Watal Committee, should be considered.

- The RBI (CSITE Cell) and the PRB should establish official arrangements with other sectoral authorities, e.g. the Telecom Regulatory Authority of India (TRAI) or the Department of Telecommunications (DoT), to coordinate cyber-security efforts for digital payments. Additionally, the CITSE cell should expand its focus to work more closely with non-banking players/non-NPCI affiliated stakeholders within the market.

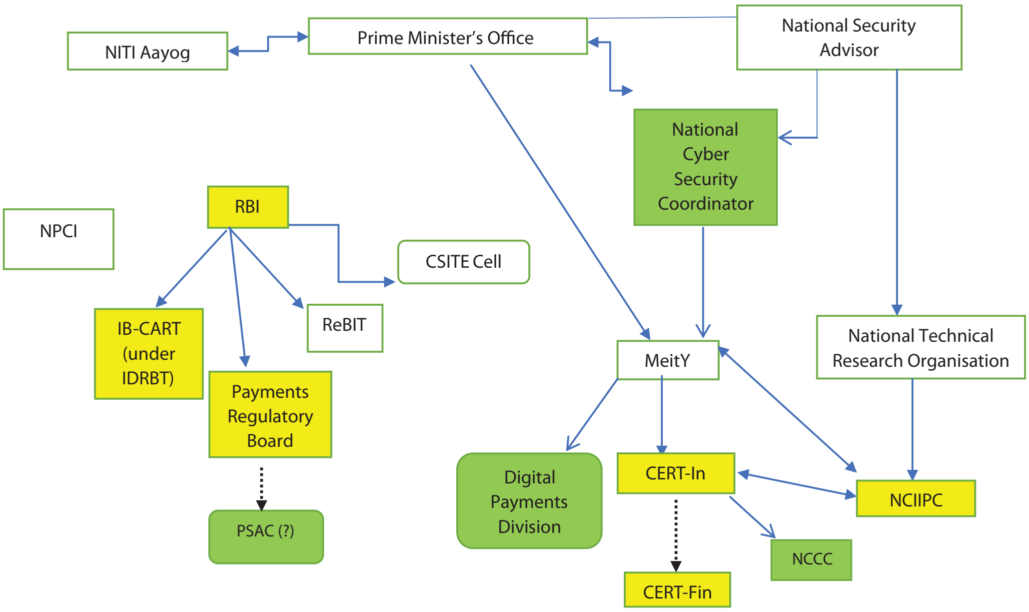
- The government's efforts under the Digidhan Mission, to promote feature-phone payments through channels such as SMS and USSD, should be complemented with appropriate security efforts. In this context, the TRAI or the DoT should consider working with telecom service providers to establish the requisite infrastructure to thwart "man-in-the-middle" cyber-attacks.

D. Coordinating the Role of Cyber-Security Institutions

It is essential for India to develop a centralised coordination framework for requisite whole-of-government institutional coordination. The OECD asserts that this helps "digital-security frameworks" promote coherence and complement collective efforts.[132] Figure 1 outlines the main institutions and organisations central to the security of India's digital-payments landscape. Other ancillary institutions of relevance may include the DoT and the TRAI.

Possible departments to anchor such coordination efforts include the National Cyber Security Coordinator's office and the National Cyber Coordination Centre (NCCC), recently operationalised under the MeitY.[133] The strategic benefit of the National Cyber-Security Coordinator is its affiliation

Figure 1: India's Cyber-Security Institutional Landscape


NITI Aayog
Prime Minister's Office
National Security Advisor
National Cyber Security Coordinator
RBI
NPCI
CSITE Cell
IB-CART (under IDRBT)
ReBIT
Payments Regulatory Board
PSAC (?)
MeitY
National Technical Research Organisation
Digital Payments Division
CERT-In
NCIIPC
NCCC
CERT-Fin

Source: Authors' own.

[132] "Digital Security Risk Management For Economic And Social Prosperity," OECD, 2015, accessed 9 January 2018, http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.

[133] Lok Sabha Deb, 17 March 2017, Unstarred Question no. 3697, answered by SHRI P.P. CHAUDHARY.

with the National Security Secretariat. However, national-security strategies must be balanced against cyber-security efforts in critical sectors such as payments, where stakeholders have economic considerations to sustain operations. Similarly, the European Union Agency for Network and Information Security (ENISA) notes that network- and information-security frameworks in the financial sector should promote centralised convergence to avoid heterogeneity of security requirements.[134]

Therefore, institutions such as the NCCC and the Cyber-Security Coordinator must embrace the following international practices.

Interface with Industry Leaders and Penetration Tests: Both Singapore (Cyber-Security Agency) and the UK's NCSC put special emphasis on working with industry to secure critical sectors. Singapore's CSA organises annual penetration-test exercises across all its critical sectors (including the financial sector).[135] The UK incorporates SMEs into its critical-sector security mandate.[136] Canada has a nodal department (Public Safety Canada) entrusted with leading the implementation of national cyber-security strategies, coordinating incident response and helping with capacity-building exercises.[137] France, too, has an integrated National Agency for the Security of Information Systems (ANSSI).[138]

Public–Private Cyber-Security Councils: Countries such as Germany and the Netherlands have established public–private National Cyber Security Councils, which continuously advise the governments on how to balance security needs with larger economic objectives while designing policies.[139]

Coordination Down to Local Levels: The US National Cyber-Security and Communications Integration Centre coordinates cyber-security activities across federal-, state- and local-level entities.[140] Similarly, Canada's cyber-security framework places an emphasis on coordination across local, provincial and the federal government.[141]

Recommendations

- Lawmakers should consider leveraging the NCCC or the National Cyber-Security Coordinator's office as the single point of contact for participants within critical sectors, through which relevant sectoral agencies can be informed. The government must encourage such offices to follow the Singapore model and start undertaking cyber resilience/penetration test exercises across all critical sectors. Such offices should be the implementation agency for major cyber-security strategies, coordinating with efforts at the state and local levels.

- Specific to payments, the government could consider establishing a multistakeholder/PPP-based Digital Payments Cyber-Security Advisory Council, learning from the efforts made by the Netherlands and Germany.

[134] ENISA, European Union Agency for Network and Information Security, 2014, Network and Information Security in the Finance Sector, https://www.enisa.europa.eu/publications/network-and-information-security-in-the-finance-sector.

[135] CSA Singapore, "CSA Leads Whole-Of-Government Exercise To Respond To Cyber Attacks," 2017, accessed 9 January 2018, https://www.csa.gov.sg/news/press-releases/csa-leads-wog-exercise-to-respond-to-cyber-attacks.

[136] "About The NCSC - NCSC Site," 2017, accessed 9 January 2018, https://www.ncsc.gov.uk/information/about-ncsc.

[137] "Canada's Cyber Security Strategy," Government of Canada, 2010, accessed 9 January 2018, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx.

[138] "The National Cybersecurity Agency Of France," ANSSI, 2018, accessed 9 January 2018, https://www.ssi.gouv.fr/en/cybersecurity-in-france/the-national-cybersecurity-agency-of-france/.

[139] "CYBERSECURITY POLICY MAKING AT A TURNING POINT," op. cit.

[140] "National Cybersecurity And Communications Integration Center | US-CERT," 2018, accessed 9 January 2018, https://www.us-cert.gov/nccic.

[141] "CYBERSECURITY POLICY MAKING AT A TURNING POINT," op. cit.

E. Integrating Future Institutions: Proposed Data Protection Authority of India (DPA)

The above coordination strategies must effectively integrate future institutions coming into the fold with minimal disruption. For instance, Chapter X of the Personal Data Protection Bill (DPB), 2018 proposes establishing a DPA. This overarching institution is assigned the general duties of protecting the interests of users ("data principals"), preventing the misuse of a data principal's "personal data," ensuring requisite compliance and promoting data-protection awareness.[142] More specifically, it is envisioned as a lead institution entrusted with powers analogous to civil courts towards, *inter alia*, promptly responding to "data security breach(es)." The DPA has a proactive mandate to promote awareness and understanding of the risks, rules, safeguards and rights with respect to data protection. Such a framework could translate into palpable functional overlaps between the DPA and institutions such as CERT-In.

Additionally, the DPB allows the DPA to issue "codes of practice" for good data-protection practices.[143] Alternatively, it can approve industry/government/civil society/regulator submitted codes of practice. Such codes can only be crystallised after the DPA undertakes requisite consultations with the public and stakeholders. The codes will not be mandatory in nature but will represent guidance, based on which fiduciaries are expected to develop their operational procedures. These codes can (amongst a comprehensive list of other privacy and data-protection requirements) cover:

- How data controllers ("data fiduciaries") process both "personal" and "sensitive personal" data (discussed in Section II); and

- Standards for security safeguards

Data fiduciaries (including those operating in the payments sector) under the DPB framework are mandated to inform the DPA of personal-data breaches that are likely to cause harm to data principals (i.e. users). These notifications to the DPA must be executed "as soon as possible," and the DPA decides if the data fiduciary must report this to the concerned data principals.[144] Additionally, Chapter X of the Bill designs the DPA as an enforcement authority with the power to make civil and criminal determinations based on the nature of non-compliance with provisions under the DPB. The DPA's decisions can be appealed before an appellate tribunal.[145] Section 108 of the DPB also grants the DPA the power to make regulations for India's data-protection/security ecosystem.

Given the overarching mandate of such a DPA, section 67 of the DPB remains cognisant of regulatory, policymaking and executive overlaps with other regulators and authorities. The same would be the case within the digital-payments cyber-security institutional landscape. This provision allows the DPA to establish memorandums of understanding (MoUs) to coordinate activities with such entities.

Recommendations

- Adding another institution such as the DPA comes with the risk of further confusion in India's cyber-security institutional landscape. Therefore, it is important for policymakers to formalise the DPA's relationship with central institutions such as CERT-In, the NCIIPC, the NCCC and the National Cyber-Security Coordinator. MoUs under section 67 of the DPB could be an effective mechanism for this.

[142] Personal Data Protection Bill 2018, Section 60(1).

[143] Personal Data Protection Bill 2018, Section 61.

[144] Personal Data Protection Bill 2018, Section 32.

[145] Personal Data Protection Bill 2018, Chapter XII.

- Any such DPA must quickly establish working arrangements with key institutions and stakeholders for critical sectors such as digital payments. These institutions can include the NPCI; the IB-CART; the RBI's CSITE-Cell; the RBI; the Digital-Payments Division; and industry-stakeholder groups, e.g. a possible payments advisory council to develop technical capacity within these complex markets.

- Policymakers should also appreciate that India's DPA could play a role in helping coordinate efforts between different sectoral authorities (e.g. the RBI and the TRAI).

- The DPA's approach to personal-data breach notification should not contradict the need for incentivising ecosystem participants to share cyber-incident and threat-related information with wider stakeholders. Policymakers should explore if any of the above institutions (including the DPA) can be pivoted as a single point of contact, through which incident and breach-related information can be communicated/notified.

STANDARDISATION APPROACHES

This section presents how future legal frameworks should be designed for the payments sector and proposes principles required to develop robust risk-based security frameworks. It concludes by analysing India's domestic and international standard-setting processes.

A. Risk-Based Approaches in Technical Regulation

This section analyses India's legal landscape and proposes appropriate risk-weighted approaches[146] to ensure *confidentiality, integrity and availability* for major payment systems. These principles form the bedrock of information security and draw inspiration from the EU's Article 29 Working Group on Data Protection.[147] The principles are listed below:

- Confidentiality refers to unauthorised access or accidental disclosure of information;
- Integrity refers to the alteration of systems to create system vulnerabilities; and
- Availability refers to the accidental loss or unavailability of access to information systems and the information within;

The Indian digital-payments security framework is governed by both general and sector-specific regulations. In this context, the analysis looks at statutes such as the IT Act and the PSS Act, sectoral institutions such as the RBI and the NPCI, advisories announced by CERT-In, and forthcoming laws such as the Personal Data Protection Bill.

Domestic Scenario

IT Act Framework: The IT (reasonable security practices and procedures, and sensitive personal data or information) Rules, 2011 (SPDI Rules) section 43A of the IT Act outlines information-security and data-protection requirements for all businesses handling SPDI, including "credit card, debit card, and other payment instrument details."[148] To effectively respond to "cyber incidents," businesses are mandated to implement privacy-respecting protocols to collect, process, transfer and disclose SPDI. The framework also mandates that information-security policies must be accompanied by appropriate risk-proportionate security controls, risk-management protocols (informed by ISO/IEC 27001 standards) and annual cyber audits.[149] The SPDI framework faces two major criticisms: a) the lack of a discernible redressal mechanism and b) negligible enforcement, with only 17 judgements and none since 2011.[150] Moreover, when the framework was first drafted, the focus was to cater to the needs of the then-thriving BPO sector.[151] In addition to the above, the IT Act contains criminal liability provisions under Section 72 and 72A for unlawful access and disclosure of personal information obtained either under law or through a contractual agreement.

[146] "Online And Mobile Payments: Supervisory Challenges To Mitigate Security Risks," op. cit.

[147] See Opinion 03/2014 on Personal Data Breach Notification, http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.

[148] The Information Technology, Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011, Rule 3(ii).

[149] The Information Technology Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, op. cit., Rule 8.

[150] http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf, 1 85.

[151] https://factordaily.com/what-works-and-hurts-business-india-new-data-protection-bill/.

Risks of Framework Inconsistency:

The definition of "cyber incidents" as under the SPDI framework has been expanded by the 2013 CERT Rules. Specifically, the CERT Rules define "cyber-security incidents" as analogous to SPDI Rules' definition for "cyber incidents." Rule 2(d) of the SPDI Rules defines the same as:

> "*Any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation*."

Conversely, the 2013 CERT Rules revise definitions for "cyber incidents" and "cyber-security breaches."

The 2013 CERT Rules[152] define them as:

- **Cyber Incident (Rule 2g):** "... any real or suspected adverse event that is likely to cause or causes an offence or contravention, harm to critical functions and services across the public and private sectors by impairing the **confidentiality, integrity or availability** of electronic information, systems, services or networks resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource, changes to data or information without authorisation; or threatens public safety, undermines public confidence, have a negative effect on the national economy, or diminishes the security posture of the nation."

- **Cyber-Security Breaches (Rule 2i):** "... unauthorised acquisition or unauthorised use by a person as well as an entity of data or information that compromises the **confidentiality, integrity or availability** of information maintained in a computer resource."

RBI-led Regulation: In accordance with its powers under the PSS Act, 2007, the RBI has proactively released regulation to secure India's digital-payments landscape. Some major legal pronouncements in this context include:

- **Organisational Control Requirements:** The RBI has developed cyber-security requirements for both banks and PPIs. Its 2016 Cyber-Security Framework for Banks[153] includes three main elements, namely, agile incident response, risk management and recovery. The framework prescribes specific baseline security requirements for banks. Requirements include establishing internal cyber-security policies, a central security operations centre for threat detection, and a bank-wide cyber crisis management plan. It also mandates network-security protocols with firewalls and other perimeter defence strategies.

  For PPIs, the RBI released comprehensive master directions, including cyber-security-related provisions.[154] It requires PPIs to adopt Board-Approved Information Security Policies and accompanying risk-mitigating measures (reviewed periodically, and after breaches/system updates). PPIs must also undertake annual system audits to evaluate security controls, hardware structures and disaster recovery plans. Commendably, the RBI provides guidelines for vendor-risk management.

- **Mobile-Banking Transaction Security**:[155] This is based on confidentiality, integrity, authenticity and non-repudiability. The RBI states that end-to-end encryption is not required for transactions of less than INR 5,000 and provides an illustrative framework for technology and security standards. Mobile-banking transactions must be initiated via debit cards to be

[152] http://meity.gov.in/writereaddata/files/G_S_R%2020%20%28E%292_0.pdf.

[153] Reserve Bank of India, "Cyber Security Framework In Banks," 2016, accessed 9 January 2018, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF.

[154] Reserve Bank of India, "Master Direction On Issuance And Operation Of Prepaid Payment Instruments," 2017, accessed 9 January 2018, https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11142.

[155] https://rbi.org.in/SCRIPTS/BS_ViewMasCirculardetails.aspx?id=9869.

validated via two-factor authentication, with one of the factors being of an mPIN standard or higher. Additionally, banks (upon their own risk perception) are required to undertake appropriate risk-mitigation measures, such as transaction limits, transaction velocity checks, fraud checks and AML checks. Other requirements include risk management and vulnerability assessments.

- **Securing Card-led Digital Transactions:**[156] Most digital transactions in India are serviced over interbank card networks. To secure such channels, the RBI has adopted an ecosystem approach. It has set security standards across three layers: (1) infrastructure level (PoS and ATM); (2) instrument level (card-level); and (3) transaction level (both card present and card-not-present transactions). Such a comprehensive framework has been designed in line with standards developed by the international standard-setting organisations for payments, i.e. EMVCo and the Payments Card Industry-Security Standards Council (PCI-SSC) such as PCI-DSS and PA-DSS standards.[157] Card-not-present, or "online" transactions, have been subject to PIN-based two-factor authentication requirements through RBI notifications since 2009–10.

- **Securing Transactions over Wallets:** Critical risk mitigation requirement for PPIs include additional factor-authentication mechanisms for transactions, adequate transaction-velocity checks, suitable escalation protocols, and the maximum number of invalid access attempts and suitable timeout features.

- **Reducing Second-Factor for Low-Value Transactions:** The RBI is trying to balance transaction security standards with efforts to grow digital-payments uptake. For example, it released a notification to allow user-consent based relaxation of additional factor authentication requirements for CNP transactions of less than INR 2,000.[158]

- **KYC/Identity Verification:** All banks, PSPs, payments-system participants, and PPI-issuing companies comply with the RBI's 2016 Know-You-Customer (KYC) Master Directions, which is periodically updated.[159] These directions are prescribed under India's "prevention of money-laundering" framework and are perceived as key in securing payment and settlement ecosystems. However, identity-verification schemes with excessive verification requirements can lead to customer friction. Illustratively, studies indicate that the RBI's PPI Master Directions, which mandate full KYC requirements (even for low-value transaction accounts),[160] have stifled the adoption/usage of such mediums.[161] Nevertheless, in 2018, the Indian government was ratcheting up efforts to mandate the linkage of all banks with the Aadhaar.[162] In pursuance of this, in April 2018, the RBI amended its KYC Master Directions and mandated banks to obtain Aadhaar-related documents. However, in September 2018, the Supreme Court of India delivered its verdict on the Aadhaar case, where the constitutional validity of India's national identity framework was challenged on the grounds of the right to privacy.[163] In it, the Court struck down parts of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act"). Specifically, the Court narrowed the scope of section 57 of the Aadhaar Act provision, which enabled private

[156] https://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf, 24–26.

[157] Ministry of Finance Department of Economic Affairs, "Press Release Om The Report Of The Working Group For Setting Up Computer Emergency Response Team In The Financial Sector," 2017, accessed 8 January 2018, 24–26, http://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf.

[158] Reserve Bank of India, "Card Not Present Transactions – Relaxation In Additional Factor Of Authentication For Payments Up to INR 2000/- For Card Network Provided Authentication Solutions," 2016, accessed 9 January 2018, http://cashlessindia.gov.in/RBI_notification_relaxation_in_additional_factor_of_authentication_for_payments_upto_Rs2K.pdf.

[159] https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10292&Mode=0, Rule 3(b)(xii).

[160] Earlier low-value accounts transacting less than INR 10 thousand per month could be onboarded as per minimum self-declared standards.

[161] Medianama's Digital Payments in India Report, Medianama & Akamai, February 2018.

[162] https://barandbench.com/wp-content/uploads/2017/06/aadhaar-notification.pdf.

[163] Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors., available at (https://www.supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf).

enterprises to use an individual's Aadhaar number to verify their identity for *any purpose* **(emphasis added)**. In essence, the judgement prohibited companies from using Aadhaar's authentication/e-KYC facilities. Moreover, the Supreme Court also struck down amendments to India's Prevent of Money Laundering framework, which required mandatory linkage of bank accounts with the country's national identity number. As such, the judgement brought to light an important challenge in India's digital financial inclusion journey. **It essentially conveyed that there is an inherent tension between robust identity verification, individual's right to privacy, and the need for paperless and frictionless solutions to smoothen user adoption of digital financial solutions.**

- **NPCI Efforts:** The NPCI sets security standards for payments-system participants. For example, the UPI's procedural guidelines lay down broad security requirements for participating PSPs,[164] which are periodically updated via the NPCI's UPI Circulars.[165] The Procedural Guidelines address application security, transaction-level security requirements amongst banks and PSPs, and the delineation of liability between the NPCI and network participants. It has released a set of cyber risk-management governance guidelines with requisite security features,[166] which gives system participants access to real-time fraud risk-management services with predictive capabilities.[167]

  To enhance defences, the NPCI, in 2016, released a request for proposals to empanel a service provider as a Security Operations Centre (SOC) partner to help with (1) 24/7 real-time security-monitoring services and (2) centralised security-product management services, which include two-factor authentication tools, incident response, and forensic and vulnerability-assessment tools.[168] However, a formal partnership is yet to be announced.

- **CERT-In Advisories:** The Digital Payments Division under the MeitY,[169] through the CERT-In issued advisories, recommends multifactor authentication; robust authorisation and access controls on the basis of "permissions, privileges and user rights;" appropriate encryption standards;[170] containerised applications; and appropriate data classification for adequate risk treatment.[171]

- **Proposed Data-Protection Bill:** Given the legacy basis and criticisms directed at the information-security and data-protection framework under India's IT Act framework, as well as the Supreme Court's observations in the *Puttaswamy* case that crystalised informational privacy as a fundamental right, both the judiciary and the Indian government agreed on the need to construct a new data-protection framework. To this end, the B.N. Srikrishna Committee published its final report[172] and the accompanying "Personal Data Protection Bill (DPB)" in 2018. Curiously this bill repeals the framework under Section 43A and SPDI Rules under the IT Act, without any mention of how such an enactment affects provisions under sections 72 and 72A of the IT Act.[173] Although not its primary purpose, the proposed framework will have a direct effect on India's information/cyber-security landscape.

[164] https://www.npci.org.in/sites/default/files/UPI-PG-RBI_Final.pdf.

[165] https://www.npci.org.in/upi-circular.

[166] https://www.npci.org.in/sites/default/files/White-Paper-on-Cyber-Security-in-banking-Essential-tools-rev10.pdf.

[167] https://www.npci.org.in/fraud-risk-management.

[168] https://www.npci.org.in/sites/default/files/SecurityOperationsCentersecuritypartner.pdf.

[169] "Digital Payment Division | Ministry Of Electronics And Information Technology, Government Of India," Ministry of Electronics and Information Technology, accessed 9 January 2018, http://meity.gov.in/digidhan.

[170] For both data at rest and data transiting through networks, wherein they have advocated web-based traffic utilising Transport Layer Security (TLS) a newer iteration of SSL protocols.

[171] "Mobile And Cloud Data Security," India Computer Emergency Response Team, Ministry of Electronics and Information Technology, 2016, accessed 9 January 2018, http://cashlessindia.gov.in/CERT-In%20Advisory%20Notes-Mobile%20and%20Cloud%20Data%20Security.pdf.

[172] https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

[173] Personal Data Protection Bill 2018, Annexure A.

In this context, the DPB is designed to regulate all "processing of personal data."[174] It reimagines the relationship between users ("data principals") and the entities that determine how personal data[175] is processed ("data fiduciaries"), in an attempt to engender trust between such parties.

The Bill defines "sensitive personal data" (SPD)[176] as a subset of "personal data." It outlines specific categories/types of personal data, which are necessarily under the ambit of SPD. SPD, *inter* alia, is characterised to include "financial data" and "biometric data,"[177] where "financial data" includes account details, card or payment instrument details, or any data that reveals the nature of the relationship between a data principal and a financial institution, e.g. financial status or credit history.[178]

This is important because "personal data" and "sensitive personal data" have separate grounds based on which they can be processed. Broadly, data fiduciary activities under this Bill must satisfy the grounds of:[179]

- Fair and reasonable processing;
- Purpose, collection and storage limitation;
- Lawful processing;
- Reasonable steps taken to ensure data quality (complete, accurate, not-misleading and updated); and
- Appropriate notice to data principal.[180]

Critically, the processing of sensitive personal data (including card and payment-instrument data) requires explicit consent—which must be informed, clear and specific—from the data principal.[181] Section 21 of the DPB allows for a narrow exception for these explicit consent requirements, in the case of certain categories of SPD, including financial data.

Such processing is only allowed when it is strictly necessary: and the conditions under which such exceptions are allowed include medical situations, epidemics, and other situations (e.g. disaster), which threaten life or public order.[182] Such standards for processing can directly affect transaction velocity and monitoring systems, often deployed by payment-service providers. Alternatively, private-sector data fiduciaries are allowed to process other personal data on grounds of consent (not exclusive or explicit)[183] or for "reasonable purposes."[184] Such exceptions for consent for

[174] Personal Data Protection Bill 2018, Section 2.

[175] Defined as data that directly or indirectly identifies the data principal (Broad standard of identifiability adopted).

[176] Non-exhaustive list (which DPA can expand); additionally comprising passwords, health data, "official identifiers" including Aadhaar number, sex life, sexual orientation, genetic data, transgender status, intersex status, caste or tribe, and religious or political affiliation or belief.

[177] Personal Data Protection Bill 2018, Section 3(35).

[178] Personal Data Protection Bill 2018, Section 3(19).

[179] Personal Data Protection Bill 2018, Chapter II, Sections 4–11.

[180] Delineating the (1) purpose for which data is processed, (2) categories of personal data being collected, (3) the right and procedure to withdraw consent for processing (where available), (4) the basis of processing and consequences if such data is not available, (5) other entities which may gain access or process such data, (6) period of data retention, (7) information regarding cross-border transfers of personal data, and (8) process for grievance redressal.

[181] Personal Data Protection Bill 2018, Section 18.

[182] Personal Data Protection Bill 2018, Section 21.

[183] Which is free, informed, specific, clear, and capable of being withdrawn.

[184] Personal Data Protection Bill 2018, Section 17.

reasonable purposes allow for data fiduciaries to process data to, *inter alia*, prevent and detect fraudulent activities and for network and information security.[185]

The DPB also mandates data fiduciaries to implement security standards in relation to (1) de-identification and encryption; (2) ensuring the integrity of personal data; and (3) necessary steps to prevent unauthorised access, use and destruction of personal data.[186] Moreover, the Bill requires businesses to notify the DPA about personal-data breaches for all such incidents where harm is likely to be caused to a data principal.[187] In this context, "personal data breach" has been defined as "… any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction, loss of access to, of personal data that compromises the confidentiality, integrity or availability of personal data to a data principal."[188]

The Bill recommends that should there be any conflict under this law and other sectoral laws, the provisions under the central data-protection law should prevail. The committee identifies the PSS Act, 2007 (as one of 50 laws), which may require amendments to conform to future data-protection standards. Such reform, when commenced, is likely to affect future information/ cyber-security policy for digital payments.

International Best Practices

This analysis focuses on the standards advocated internationally to inform future policies on risk-based organisational security, technological standard adoption (e.g. encryption), KYC and transaction authentication, and data privacy (also see Annexure 2).

a) Organisational Security and Risk-Based Approaches

Expert organisations, such as the OECD, advocate cyber-security frameworks[189] to adopt risk-based frameworks.[190] Here, risks include threats and vulnerabilities capable of disrupting *confidentiality, integrity and availability* of the concerned activity. As such, international organisations emphasise the need for policies to avoid prescriptive compliance requirements. The European Network and Information Security Authorities (ENISA) states that regulations should not articulate "how" businesses comply with security requirements.[191] Instead, good IT governance can be informed by internationally endorsed standards such as the ISO 27001 and 22301, which offer international-consistent first principles on organisational security.

Indeed, ENISA has also generally posited that abstraction in security laws is beneficial as it affords businesses flexibility. Moreover, domestic policy reports by groups such as the FSLRC[192] and the Watal Committee[193] note that payment systems and adjunct services should be subject to regulatory standards commensurate to the potential risk. The Watal Report also recommends that consumer-protection regulations should account for factors such as the degree of risk associated with a particular payment service, and the degree of competence

[185] Personal Data Protection Bill 2018, Section 17(2).

[186] Personal Data Protection Bill 2018, Section 31.

[187] Personal Data Protection Bill 2018, Section 32.

[188] Personal Data Protection Bill 2018, Section 3(29).

[189] "Digital Security Risk Management For Economic And Social Prosperity," OECD, 2015, accessed 9 January 2018, http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.

[190] See ISO/IEC 31000:2009; ISCO/IEC 27000 series; ISO Guide 73.

[191] Security requirements may include handling violations; assets management; incident detection capabilities; exercise contingency plans; network and information systems testing; and compliance monitoring.", ENISA, Network and Information Security in the Financial Sector, https://www.enisa.europa.eu/publications/network-and-information-security-in-the-finance-sector

[192] "REPORT OF THE WORKING GROUP ON PAYMENTS," Financial Sector Legislative Reforms Commission, accessed 9 January 2018, https://macrofinance.nipfp.org.in/fslrc/documents/wg_payments_report.pdf.

[193] Medium Term Recommendations to Strengthen Digital Payments Ecosystem, op. cit., 66.

and experience of users.[194] According to ENISA, the degree of risk can be estimated based on the nature of the network infrastructure (public being riskier than private) being used for communication. [195]

Financial Ecosystem Principles (G7): In 2016, the G7 released “Fundamental Elements for Cyber-Security for the Financial Sector,” which espouses risk-based perspectives. According to these elements, cyber-security frameworks should be dynamic and keep pace with evolving threats and contain appropriate mechanisms to identify, manage and reduce cyber risks, on the basis of an entity’s nature, size, complexity, risk-profile and culture.[196]

Responsibilities for FMIs (BIS): In 2016, the BIS released its “Guidance on Cyber Resilience for FMIs,”[197] detailing the principles of comprehensive cyber-risk and operational-risk management practices, including governance, identification, protection, detection, change management and response/recovery (as well as transaction-replay capabilities and the resumption of critical operation within two hours of a cyber incident). Other overarching components of the FMI cyber-resilience frameworks include regular vulnerability assessments, penetration testing and situational awareness. The BIS recommends FMIs that concentrate risks and the installation of SOCs for real-time monitoring of payments infrastructure.

Risk Management: Common elements of effective risk management in advanced jurisdictions comprise (a) risk assessment, including identification, analysis, evaluation and regular stress-tests; (b) risk treatment, including adequate security measures (periodically updated through activity lifecycle); and (c) preparedness/continuity plans, including prevention, detection, response and recovery with effective escalation protocols.

Effective internal corporate-governance structures must define roles and responsibilities for personnel implementing as well as the managing and overseeing of cyber-security framework-related activities. Structures should start at the level of the board of directors, which establish cyber-risk tolerance standards.[198] Additionally, European internet-payments security frameworks require regular risk assessments and gap analysis, incident monitoring and reporting, risk control and mitigation, transaction traceability, customer identification and strong authentication, transaction monitoring, protection of sensitive transaction data, and end-user education. ENISA and the ITU[199] also emphasise the importance of supply-chain security (see ISO 28000 standards), as IT operations are being increasingly outsourced to third-party vendors.[200]

The ITU’s DFS Focus Group, in conjunction with experts, has developed a model standard for digital financial networks (See Figure 2).[201] It draws ideas from the ITU-T standard X.805.

As Figure 1 shows, to secure all layers across networks, risk-management approaches must adopt eight principles, which require risk assessments, security audits, string incident response strategies, internal penetration tests, and leveraging network scanning tools.

[194] Ibid., 110, Box 26.

[195] ENISA (European Union Agency for Network and Information Security) (2014), Network and Information Security in the Finance Sector, https://www.enisa.europa.eu/publications/network-and-information-security-in-the-finance-sector.

[196] G7, op. cit.

[197] https://www.bis.org/cpmi/publ/d146.pdf.

[198] G7, op. cit.

[199] “Security Aspects Of Digital Financial Services,” op. cit.

[200] ENISA (European Union Agency for Network and Information Security), 2014, Network and Information Security in the Finance Sector, https://www.enisa.europa.eu/publications/network-and-information-security-in-the-finance-sector.

[201] “Security Aspects Of Digital Financial Services,” op. cit.

Figure 2

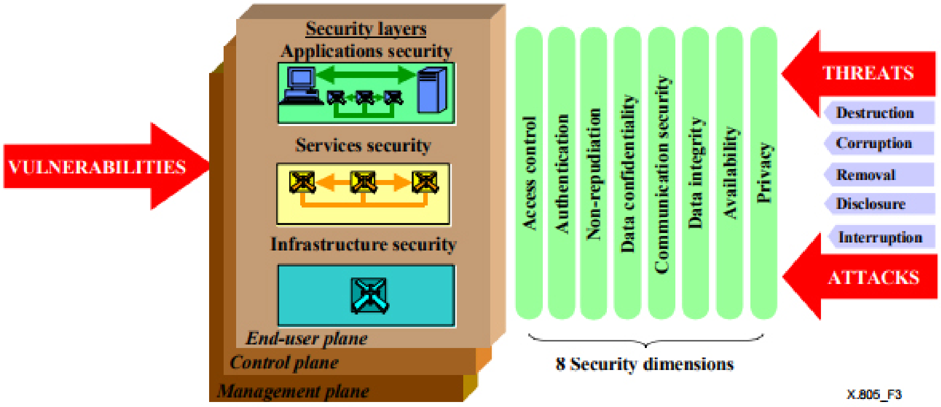


Figure 1 – Security architecture for end-to-end network security

Source: ITU-T Digital Financial Services Focus Group, Technical Report, Security Aspect of Digital Financial Services, 7, https://www.itu.int/en/ITU-T/studygroups/2017-2020/09/Documents/ITU_FGDFS_SecurityReport.pdf.

The eight principles are listed below:

- Access control (principle of least privilege)
- Robust authentication
- Non-repudiation (to ensure that particular actions have taken place)
- Confidentiality (encryption via robust cryptographic protocols)
- Security of communications
- Data integrity (integrity-monitoring tools)
- Availability (firewalls and intrusion-detection systems)
- Privacy (preventing unauthorised access)

b) Strong Technological Standards

According to ENISA, securing digital financial markets comprises two technological considerations: securely storing financial assets and transferring such assets at a comparable level of security. Technologies such as cryptography and tunnels are used for this. The BIS emphasises the importance of end-to-end encryption for high-risk concentrating FMIs.[202]

In this context, the ENISA cites the PCI-DSS and the ISO/IEC (27001:2006) as reference points for non-regulatory NIS best practices for online payments. Additionally, an ITU report on security aspects in digital financial markets identifies some core technological elements for ecosystem security, including:[203]

[202] https://www.bis.org/cpmi/publ/d146.pdf.

[203] “Security Aspects Of Digital Financial Services,” op. cit.

- Strong authentication mechanisms to demonstrate device ownership
- Promoting hardware and software mechanisms, such as Secure Elements (SE) and Trusted Execution Environments (TEEs) for mobile-device readiness for DFS
- Ensuring secure payments application design (aligned with PA-DSS best practices), subject to external security review and penetration apps, that will deploy robust authentication mechanisms to access confidential app information[204]
- Secure handset OS, with a minimal trusted computing base and latest security updates
- Appropriate cryptography, to ensure the confidentiality of data at rest and transit, and the adoption of trustworthy supply-chain practices to safeguard system integrity[205]
- The discontinuation of outdated GSM encryption ciphers such as A5/0, A5/1, and A5/2

c) Transaction Authentication and KYC/Identity Verification

India relies on an OTP-centric, two-factor authentication framework for digital payments. However, in remote areas, PIN-based authentication is often unreliable. Further, global experts such as the US National Institute of Standards and Technology (NIST) have acknowledged that SMS-led authentication requirements (e.g. OTP) are vulnerable to social-engineering (most commonly, phishing) and technical security threats.[206] Considering the Supreme Court's determination in the Aadhaar case and the challenges with respect to friction, privacy and overall framework security, India's future regulation for KYC and transaction authentication standards should be informed by the following best practices:

1. Authentication

Risk-Based Transaction Authentication (See Annexure 2): Indian policymakers must consider the viability of adopting risk-based technology-neutral frameworks (as in Austria, Brazil, US and Singapore). For instance, under the EU's Revised Payment Services Directive (PSD2), EC recently released guidelines on its Strong Customer Authentication (SCA) regime, based on factors such as knowledge, possession and inherence. The EC has adopted a risk-based and technology-neutral approach to securing internet-based payments, allowing lenient authentication standards and exemptions for lower-risk transactions, based on factors such as value of transaction, and security tools adopted by the Payment Service Provider.

Additionally, automated transaction-monitoring mechanisms have proven effective in securing digital payments in countries such as the Netherlands. International standard setters such as the EMVCo are developing risk-based SCA standards to balance security principles with user convenience. The group launched a 3D Secure 2.0 specification in October 2016, which analyses device-offered data and combines it with biometric technological innovations to offer a layered risk-based authentication standard.[207] The ITU has endorsed EMV standards as a global best practice for transaction authentication.[208]

Biometrics and Other Authentication Solutions: To promote secure and frictionless payments, countries such as South Africa are partnering with card-network companies to promote biometric authentication. The ITU has identified other promising solutions as well, including smartcard authentication (using cryptography) to supplement card-based transaction ecosystems, for

[204] Apps should be secured through encryption and coding best practices.

[205] "Security Aspects Of Digital Financial Services," op. cit.

[206] NIST, "Digital Identity Guidelines— Authentication and Lifecycle Management", NIST Special Publication 800-63B, https://pages.nist.gov/800-63-3/sp800-63b.html.

[207] "3-D Secure - Emvco" (EMVCo, 2018), https://www.emvco.com/emv-technologies/3d-secure/> accessed 9 January 2018.

[208] "Security Aspects Of Digital Financial Services," op. cit.

jurisdictions where infrastructure penetration (e.g. PoS) remains low.[209] However, policymakers must also manage the risks accompanying biometric information.

For instance, fingerprint-based authentication, while largely successful for young people, is less reliable for old manual workers or people living in arid climates. Additionally, the accuracy of face and iris biometrics is contingent on the quality of cameras, as well as environmental conditions such as lighting, backgrounds and contrast. To combat such challenges, the ITU recommends that biometric deployments should be based on three principles, namely, failure to enrol (FTE) rate, false-rejection rate (FRR) and false-acceptance rate (FAR).[210]

The ITU Focus Group on DFS states that risk concentrations with biometric authentication remains high. One such risk identified is that while password credentials are alterable in the event of a compromise, biometric details are consistent and, thus, more vulnerable. Therefore, the storage of such information in centralised databases constitutes a security challenge. In terms of scalability of biometric-based payments solutions, countries such as Bulgaria, Estonia, UK and Ireland have already experienced digital-payments disruptions due to existing IT infrastructure lacking the capacity to keep pace with the increased traffic and larger transaction volumes.[211]

2. KYC Identity Verification

Identity Verification: Target 16.9 of the UN's Sustainable Development Goals calls for "legal identity for all,"[212] especially for access to financial services.[213] The ITU recommends that KYC-verification/identity-verification mechanisms must adhere to principles of *Identity Proofing*, *Authentication*, and *Authorisation*. It observes that to fulfil financial inclusion targets, national identity schemes such as the Aadhaar should be prioritised for government scheme benefits, and transaction account identification processes should be more relaxed to promote financial inclusion. Regulators are advised to adopt risk-based identity frameworks, such that Levels of Assurance (LOA) are proportionate to the potential risks (see ISO/IEC 29115). The benefits of a dynamic, risk-based KYC approach is that it reduces friction to financial onboarding, and as new (financially riskier) services are requested, KYC requirements are escalated proportionately.[214]

Federated Identity Management: In the context of identity-verification best practices, the ITU highlights the benefits of Federated Digital Identity Management marketplaces, which, if regulated to maintain consumer choice, can create a secure and interoperable KYC-verification model.[215] A key benefit associated with such frameworks is the limitation of privacy concerns. Such management systems limit the number of times, and entities with which, data is shared by users.

Moreover, once verified, other service providers can onboard/verify the identity of customers on using corresponding tokenised information, limiting access to sensitive personal information. The US' NIST has recognised Federated Identity Management as a privacy-respecting and interoperable security best practice and has established a Trusted Identities Group to promote its adoption within identity-verification ecosystems.[216] Further, NIST released a set of "Digital Identity Guidelines" (June 2017) that, *inter alia*, strives to standardise Federated Identity Architectures.

[209] "Identity and Authentication," International Telecommunication Union, 2017, accessed 9 January 2018, https://www.itu.int/en/ITU-T/studygroups/2017-2020/09/Documents/ITU_FGDFS_Report_IdentityandAuthentication.pdf.

[210] "Identity and Authentication," op. cit.

[211] http://www.finconet.org/FinCoNet_Report_Online_Mobile_Payments.pdf, 43.

[212] https://unstats.un.org/sdgs/metadata/?Text=&Goal=16&Target=16.9.

[213] http://www.undp.org/content/undp/en/home/blog/2017/6/1/Moving-towards-digital-technology-for-legal-identity.html.

[214] "Identity and Authentication," op. cit.

[215] https://www.itu.int/en/ITU-T/studygroups/2017-2020/09/Documents/ITU_FGDFS_Report_IdentityandAuthentication.pdf.

[216] https://www.nist.gov/itl/tig/about/overview.

These standards provide industry guidance on privacy-enhancing techniques to share tokenised KYC-related information.[217] One such identity-management group is the Kantara Initiative.[218]

Privacy-Respecting Account Linkage: Austria's Citizen Card[219] framework has been cited as a privacy-respecting best practice when it comes to the linking of different accounts (e.g. bank accounts) to a national identity. This Austrian card comprises multiple sector-specific accounts, derived from the nodal national-identity number. Each identity account is individually protected through requisite cryptography, which helps avoid tracking individuals across multiple devices and enables revocation and replacement of encrypted identifiers in the event of breaches.[220]

d) Reconciling with Data Protection Laws

Processing Requirements of Financial Data: India's proposed Data Protection Bill does not allow financial data (and other sensitive personal data) to be processed without the explicit consent of users. This means that data fiduciaries are not allowed to process financial data without consent, even for purposes that fall under the "reasonable purposes" exception articulated under the Bill. The framework allows for a narrow exception to this requirement in instances where it is "strictly necessary" in the event of medical emergency, loss of life or public-order situations. As such, this approach implies that financial data cannot be processed without consent even in order to prevent unlawful activity and fraud detection, or in order to ensure network and information security.

Such strict processing conditions conflict with automated transaction-monitoring systems, which are typically leveraged for strong, risk-based transaction authentication (see EU PSD2 Regime for SCA). Moreover, it can impede common real-time fraud monitoring systems that leverage big data analytics, AI-based network intelligence and dynamic data sharing, which are deployed to monitor transaction flows and track anomalous activities. Such challenges have also been observed globally. For example, the EU has attracted some criticism for its GDPR not conforming to standards under its PSD2.[221] In this regard, Australia is an example where countries have sought to reconcile privacy frameworks to their digital payments ecosystems. Specifically, Australia's ePayments Code contains a section on adapting its National Privacy Principles to digital transactions, and also contains provisions that allow for privacy-respecting transaction-monitoring/surveillance practices.[222]

Categorisation of Financial Data as SPD: Additionally, even the Indian Personal Data Protection Bill's decision to place financial data (including payments details) under the ambit of SPD requires careful evaluation as it is not aligned with international experiences. For example, Australia's "Privacy Act" leaves financial information outside the framework's scope of "sensitive information." According to the Australian Law Reform Commission, financial information—unlike other categories—does not reveal physical attributes or personal beliefs, and moreover, financial institutions have a legitimate interest in processing such information.[223] Similarly, the UK's Information Commissioner's Office keeps financial data outside the scope of its "special-category data," which is accorded a higher level of sensitivity.[224] Even when considering the general international experiences, as was submitted by one dissenting member of the B.N.

[217] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[218] https://kantarainitiative.org/groups/user-managed-access-work-group/.

[219] http://www.buergerkarte.at/.

[220] "Identity and Authentication," op. cit.

[221] https://www.insideprivacy.com/financial-institutions/overlap-between-the-gdpr-and-psd2/.

[222] Australian Securities and Investment Commission, ePayments Code, 29 March 2016, See Section 22.

[223] https://www.alrc.gov.au/publications/6.%20The%20Privacy%20Act%3A%20Some%20Important%20Definitions/sensitive-information, Para 6.107 and 6.180.

[224] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/.

Srikrishna Committee, only one out of 68 jurisdictions (Israel) studied categorise financial data under the ambit of sensitive personal data.[225]

Questions for Indian Policymakers: Based on the above research, there is a need for India's data protection frameworks to consider the following issues in their treatment of financial data:

- Does India have a special socio-economic or cultural reason (such as stark financial inclusion challenges) to deviate from international best practices, where financial data as a general rule of thumb tends to not fall under the ambit of sensitive personal data or "special category data" equivalents?

- If yes, should strict requirements for explicit consent be retained for all financial data? Considering the tendency of cyber-attacks to target large financial institutions, is there a need for certain consent requirements to be relaxed, especially for fraud detection and network and information-security purposes?

- Is there a need for frameworks to create differentiated categories of financial data, which are placed separately in "sensitive" and not sensitive categories? Could the nature of financial data ('sensitive' or not) be determined based on the type of specific data (e.g. card details, transaction history)? Alternatively, could the sensitive or not sensitive nature of financial data be determined on a case-by-case basis based on the purpose of the particular processing (i.e. transaction security versus determining credit history)?

Personal-Data Breaches: India's DPB has provisions that inform organisational security frameworks of what constitutes personal-data breaches. Since India has disparate laws, which inconsistently define cyber incidents, cyber-security incidents and cyber-security breaches, there is a need to harmonise and contextualise these disparate definitions. The EU's Article 29 Working Group on Data Protection clearly states that personal-data breaches form a subset of wider cyber-security incidents that lead to the actual loss of personal data. The Working Group also distinguishes the two by highlighting that data breaches are typically executed through external sources of threats, whereas security incidents can result from issues in both internal and external processing.[226] Additionally, expert groups, such as the International Association of Privacy Professionals, delineate four categories (in order of priority) of such occurrences, namely, (1) events; (2) security incidents; (3) privacy incidents; and (4) data breaches.[227]

Recommendations

For the ecosystem to achieve robustly secure standards in product, device and service quality, India must focus on augmenting its domestic testing and validation processes (discussed in the next section). In this context, it is recommended that:

- India must develop network- and information-security guidelines for the digital-payments ecosystem, espousing a risk-based and technology-neutral framework. It is important to ensure that this is developed in a whole-of-government approach, to enable the convergence of security requirements.

- To secure major interoperable payment systems, the NPCI should expedite its efforts to set up an SOC for India's retail-payments ecosystem.

- Some key principles for these network-security requirements must include risk assessment, risk treatment, access-control protocols, vulnerability/penetration testing, incident detection, adequate supply-chain security protocols, and preparedness and continuity plans. In addition to independent cyber audits, regulators must explore avenues to facilitate businesses to undergo requisite penetration tests for continuous improvement of internal-security measures.

[225] http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf.

[226] https://iapp.org/media/pdf/resource_center/WP29-Breach-notification_02-2018.pdf, 7.

[227] https://iapp.org/news/a/is-it-an-incident-or-a-breach-how-to-tell-and-why-it-matters/.

- To balance transaction security with the challenges of friction/social engineering risks of PIN-based, two-factor authentication, guidance can be sought from the EC's Regulatory and Technical Standards for SCA, as under the PSD2 regime (See Annexure 2). Furthermore, policymakers can explore the adoption of the EMVCo's 3-D Secure 2.0 specification.

- It is recommended that policymakers promote business solutions by leveraging biometric-authentication solutions to facilitate "intelligent friction," wherein transactions are completed securely and seamlessly. Security procedures to localise such authentication form factors into smartcards or mobile devices should also be encouraged.

- Regarding leveraging the Aadhaar as the national instrument for KYC and transaction-based authentication, concerns regarding network traffic and authentication limitations should be considered. Regulators and policymakers can explore the adapting of these approaches to cryptographically protected smartcard instruments. Moreover, the government should strongly consider moulding these efforts to technologically reflect the Austrian Citizen Card Framework.

- To balance security and ease of KYC verification, the government must consider working with industry to promote and develop appropriate standards for Federated Identity Management frameworks. Guidance can be sought from the approach adopted by the NIST.

- With the publication of India's draft "Personal Data Protection Bill, 2018"[228] the MeitY should undertake a study with payment and settlement authorities to ascertain the effects its provisions will have on digital-payments security and the PSS Act. It must then explore how the two frameworks can be rationalised.

- It is important to re-evaluate the current catch-all placement of "financial data" as sensitive personal data, concomitant explicit consent requirements for data fiduciaries, and its implications for digital-transaction security.

- The Indian government should create a harmonised framework for cyber occurrences. This includes developing definitions for various cyber-security incidents and events to formalise the relationship between incidents and various constituents such as personal-data breaches, as well as to establish the degree of severity associated with each type of occurrence.

B. Domestic Standard-Setting and Testing Frameworks

A key component of cyber resilience is standardisation. Often seen as an obligation that drains resources, standardising information-security protocols helps (1) improve the effectiveness and efficiency of key cyber-defence processes; (2) facilitate interoperability and systems integration; (3) simplify complex cyber environments; and (4) deploy new technological and business solutions.

Common cyber-security standards support business predictability in increasingly borderless markets. In the case of digital-payments adoption, which relies on network effects, standardisation helps in boosting customer confidence in terms of the integrity of a particular product or service.[229] This section analyses the role performed by domestic standards and testing institutions, and takes stock of India's participation at relevant international Standard-Setting Organisations (SSOs).

Domestic Scenario

India's present standardisation and testing framework encompasses the nodal Bureau of Indian Standards (Bis[230]), the Standardisation Testing and Quality Certification (STQC) Directorate under the MeitY, and the Telecommunications Engineering Centre (TEC) under DoT.

[228] http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf.

[229] https://www.law.northwestern.edu/research-faculty/searlecenter/workingpapers/documents/Kyle_Salant_Participation_SSO.pdf.

[230] Not to be confused with the Bank for International Settlements (BIS).

Bureau of Indian Standards (Bis)

The Bis was established as India's national standards-setting body in 1986 and was recently brought under the ambit of a new statutory regime, i.e. the Bureau of Indian Standards Act, 2016.[231]

No Cyber-Security Testing under the Compulsory Registration Scheme: The framework allows the central government to prescribe a compulsory certification scheme for any products or services, for public interest or national-security considerations (amongst others).[232] Specific to the electronics sector, the MeitY has had three phases of updates to the Compulsory Registration Scheme (CRS).[233] As per the latest 2014 notification, the MeitY brought both PoS terminals and mobile phones under the CRS.[234] Unfortunately,[235] the CRS does not address cyber-security concerns and only inspects devices for general safety, seeking to mitigate risks of electric shocks, heat hazards, chemical hazards, radiation etc.[236]

The grant of requisite authorisation is contingent on testing at labs recognised by the Bis in India. Owing to logistical and resource constraints, the Bureau has institutionalised a Laboratory Recognition Scheme (LRS) for the purpose of creating a sufficient pool of external laboratories, both in India and abroad, to increase its capacity for product testing at a large scale. The Bis deploys certain laboratories established by the STQC[237] to test for device and electronics safety/ security requirements under the CRS.[238] The legal framework allows the government to appoint another authority/agency, in addition to the Bis, to be a similarly placed certification and enforcement authority.[239]

The prime responsibilities of the Bis include the development, recognition and promotion of Indian standards. The overarching standard formulation is performed through a technical committee structure consisting of area-specific division councils, sectional committees, subcommittees and panels.[240] Under the Electronics and Information Technology Division Council (LITDC), there are specific subcommittees that seek to develop standards for "Information Systems Security and Biometrics."[241] The committees are multistakeholder in nature, with representation from interested ministries, industry and academia.[242] This structure strives to mirror major international SSOs such as the International Standards Organisation (ISO) and the International Electrotechnical Commission (IEC). As India's national standards body, the Bis sends members of sector-specific divisional councils to represent India's interests at various international standards-developing organisations.

[231] http://pib.nic.in/newsite/PrintRelease.aspx?relid=171705.

[232] Bureau of Indian Standards Act, s16(1), 2016, accessed 31 January 2018, http://www.indiacode.nic.in/acts-in-pdf/2016/201611.pdf.

[233] http://meity.gov.in/esdm/standards.

[234] http://crsbis.in/BIS/app_srv/tdc/gl/docs/New_Gazette_Notification_2014_11_13.pdf.

[235] IS 13252 (Part I): 2010. Safety—General Requirements.

[236] https://ia801000.us.archive.org/25/items/gov.in.is.13252.1.2010/is.13252.1.2010.pdf.

[237] Specific ERTLs and ETDCs which are part of the larger STQC network, http://www.stqc.gov.in/content/ertls.

[238] http://www.bis.org.in/lab/NewLab_list1.pdf, ERTL (E), ERTL (W), ERTL (N), ETDC Bangalore, ETDC Chennai; January 2018.

[239] Bureau of Indian Standards Act, 2016, op. cit.

[240] http://www.bis.org.in/home_std.asp.

[241] LITD 17.

[242] http://www.bis.org.in/sf/compltd.pdf.

STQC

The STQC Directorate under the MeitY offers quality-assurance services for information technology and electronics sectors, through a pan-India network of laboratories and centres. It offers both qualitative testing and certification services for both public- and private-sector organisations.[243] In terms of scope, the STQC has operationalised four regional and 10 state-level testing laboratories.[244] These laboratories test for various qualitative criteria, including organisational software and IT systems' adherence to information-security standards. However, security benchmarks for organisations published on the STQC website refer to draft ISO/IEC 27001 and ISO/IEC 27002 standards from the year 2005.[245] This is problematic as the latest internationally accepted standards for these information security related processes were finalised in 2013.[246] Moreover, a palpable limitation to the STQC's capacity to test at scale is that it has only one dedicated IT Security Testing Laboratory, in Kolkata.[247]

TEC

The TEC is India's principal standards-development and certification institution for telecommunications equipment used in network infrastructure.[248] As per the Unified License Agreement for telecom service providers, all telecom equipment and products must conform to the standards set by the TEC or to the relevant standards developed by international standardisation organisations such as the ISO, the IEC, the IETF, the IEEE, the ITU or the ETSI.[249] More recently, the Indian government released the Indian Telegraph (Amendment) Rules, 2017, which mandates all telecom equipment to undergo testing and certification.[250] The DoT is developing essential requirements for the same. The current list of relevant products includes "Network Security Systems."[251] These rules are yet to be enforced. As per this framework, the testing will be carried out by accredited labs, and the role of the TEC is to certify due compliance.[252] In addition to this, another key function of the TEC is to interact with multilateral agencies such as the ITU and the ETSI, to articulate India's perspective on standardisation.[253]

The TEC has a specific cyber-security division, entrusted with the responsibility of securing overall networks by defining the ICT network security framework; participating in international SSOs, e.g. the ITU; and coordinating activities with major domestic cyber-security agencies.[254] Since 2015, the TEC has undertaken the process to develop a tender (latest draft published in December 2017) to create a Telecom Security Test Lab, with requisite testing and measurement tools to ensure resiliency and security of all types of telecom/IP equipment, ICT equipment, and various end-user devices such as mobile handsets or tablets. These tools are intended to comply with international security-testing standards as prescribed by international organisations. The proposed lab is meant to test for device and network resiliency against vulnerabilities related to cyber threats, e.g. the distributed denial of service (D-dos) attacks, botnets, phishing and identity theft.[255]

[243] http://www.stqc.gov.in/content/about-stqc.

[244] http://stqc.gov.in/content/about-testing.

[245] http://stqc.gov.in/content/information-security-testing-and-assessment.

[246] https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html.

[247] http://stqc.gov.in/content/information-security-testing-and-assessment.

[248] Not to be confused with mobile handsets.

[249] License Agreement for Unified License, Clause 23, Government of India, http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf.

[250] http://tec.gov.in/pdf/Whatsnew/eGazetteNotif.pdf.

[251] http://tec.gov.in/pdf/Whatsnew/MATCOF%20FINAL.pdf.

[252] http://www.tec.gov.in/certification-approval-procedure/.

[253] http://www.tec.gov.in/tec-functions/.

[254] http://www.tec.gov.in/cyber-security-cs/.

[255] http://www.tec.gov.in/pdf/Tenders/Technical%20requirements%20of%20Security%20lab.pdf.

Participation in International SSOs

Indian policies and institutions tend to rely on international organisations such as the ISO, the IEC, the ITU, the ETSI and the IEEE, for guidance on information- and network-security related standards. Thus, it is important for the country to participate in such fora and meaningfully shape relevant conversations. If India remains in the background, there is a risk that the global community's efforts to make payment systems interoperable will not reflect India's technological, demographic or industry-related constraints.

India's Participation (See Annexure 3)[256]

Industry specific standards are typically developed by industry-led voluntary consensus. Policymakers must keep track of sector-specific private-sector groups that drive industry standards for a particular field and the activities of countries in similarly placed product markets.[257] The major international forums that play a role in standardisation for digital payments include organisations such as the ISO, the IEC, the ETSI, the ITU, the IEEE, the W3C and the IETF, as well as sector-specific special interest groups such as the EMVCo, PCI-SSC and the FIDO Alliance. Analysing India's participation in these organisations throws light on some broad shortcomings:

- While India (represented by the Bis mirror committees) is listed as a "participating country" at the ISO, the quality of its participation in the ISO/IEC JTC 1/SC 27 on IT Security Techniques was inadequate. Anecdotal evidence reveals that Indian contingents are considerably smaller than global counterparts. Due to such capacity deficits, Indian perspectives are typically overlooked in substantive discussions. Policymakers must evaluate India's participation in another ISO technical committee on financial services for payments-system interoperability standardisation.[258]

- The NPCI is a member of the W3C, a major international SSO. However, its participation remains inadequate. For example, the W3C has a Working Group for Web Payments that aims to secure digital payments across the internet via standardisation for transaction authentication and techniques such as tokenisation.[259] Unfortunately, this Working Group has no representation from India, despite the NPCI's membership in the forum.[260]

- India's collaboration with the FIDO Alliance remains limited at best, which is leading research and development (in conjunction with W3C) on password-less and interoperable, two-factor authentication standards based on Universal Second Factor (U2F) security keys. However, in recent years, the NPCI has taken steps to improve its participation and has joined major digital-payments-specific SSOs, such as the EMVCo[261] and the PCI-SSC (as one of its eight affiliate members).

International Best Practices

The best practices suggested here offer strategies for domestic standardisation, testing and an increased presence in international discussions.

Promoting Security-By-Design and Common Criteria: Security-By-Design principles, which are updated across product lifecycles, have been established as best practices by both technologists and policymakers. For instance, advanced cyber-security jurisdictions such as Singapore[262]

[256] The analysis is based on publicly available data. The information is accurate till December 2017.

[257] https://dc.law.utah.edu/cgi/viewcontent.cgi?referer=https://www.google.co.in/&httpsredir=1&article=1010&context=scholarship.

[258] ISO/TC/68.

[259] https://www.w3.org/Payments/WG/charter-201510.html.

[260] https://www.w3.org/2004/01/pp-impl/83744/status.

[261] As both a business and technical associate.

[262] https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf?la=en.

and the UK,[263] in their respective cyber-security strategies, seek to promote security-by-design principles in digital ecosystems. The Telecom Regulatory Authority of India has also endorsed standardisation against security-by-design benchmarks.[264] To achieve a general degree of product and system robustness (while maintaining interoperability), both Singapore and the UK use the ISO/IEC-developed Common Criteria for Information Security Technology Evaluation as testing and validation benchmarks.[265]

Developing Capacity to Test at Scale: As observed earlier, India's capacity to test at scale remains inadequate, as evident in the limited number of STQC labs for information and network security. Additionally, the TEC Security Lab has been stuck in the tender-drafting phase for over two years. Other members of the global community, such as Australia, Singapore, the UK and the US have tied up with Information Security Assurance expert CREST for cyber-security accreditation and certification arrangements.[266] Another best practice in this regard is found in Germany, a country with an independent trust centre ("TÜViT") that assesses ICT security against globally recognised standards and criteria. TÜViT closely collaborates with other cyber-security testing authorities from countries such as the US, Japan, Netherlands and Switzerland. In the context of digital-payments security, it works in close coordination with security laboratories run by various payments companies and payments-standard developers.[267]

Industry-Led Standards Development and Participation: The indigenous digital-payments industries in countries such as Canada, Japan and Austria have developed effective security standards. Their efforts have benefitted from the promotion of self-regulation and industry collaboration.[268] Research indicates that the participation of Japanese and Korean firms in internet-related SSOs, e.g. the IETF, has been consistently valuable. China, which had a negligible international presence in 2003, was the second-highest participant (after the US) in 2013.[269]

National Standardisation and International-Participation Strategies: The US' national standards body (ANSI) oversees and accredits the standards-development processes of a large network of domestic standard-developing organisations. Their processes are consensus driven and follow the principles of due process. The standards processes in the US include public consultation before crystallisation of standards.[270]

Pushing National Standards Abroad: Germany's national standard-setting body[271] runs a programme that aims to help emerging economies such as Albania, Vietnam, Mongolia and Moldova with their standardisation approaches.[272] The German Standardisation Strategy identifies international participation and the adoption of German standards internationally as key priorities, and industry as a driving force in domestic standardisation. The country's concerted effort has helped German standards gain wider acceptance.[273] Standards developers in China, Japan and South Korea have aligned strategically to establish the Northeast Asia Standards Cooperation Forum for technology markets.[274] Australia has a dedicated stakeholder-engagement team to

[263] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

[264] http://trai.gov.in/sites/default/files/Recommendations_M2M_05092017.pdf.

[265] http://www.commoncriteriaportal.org/cc/.

[266] http://www.crest-approved.org/about-crest/what-we-do/index.html.

[267] https://www.tuvit.de/en/about-us/who-we-are/.

[268] http://www.finconet.org/FinCoNet_Report_Online_Mobile_Payments.pdf, 48.

[269] Jorge L. Contreas, Technical Standards, Standards-Setting Organizations and Intellectual Property: A Survey of the Literature (with an Emphasis on Empirical Approaches), UTAH LAW FACULTY SCHOLARSHIP.

[270] https://www.ansi.org/standards_activities/domestic_programs/overview?men.

[271] Deutsches Institut fur Normung (DIN).

[272] https://www.din.de/en/din-and-our-partners/international-consultation-services-ibd/projects.

[273] https://www.din.de/en/din-and-our-partners/din-e-v/german-standardization-strategy.

[274] http://en.cnis.gov.cn/zdxw/201506/t20150617_20846.shtml.

enable effective stakeholder participation in standards development internationally.[275]

Recommendations

- India must ensure that standards for information and network-security protocols adhere to globally consistent security-by-design principles. Currently, India lacks device-level cyber-security standards (as per the MeitY CRS scheme). India should actively try to expedite developing and establishing cyber-security standards for this, as per the ITU[276] or the Common Criteria ISO standards. The STQC testing labs presently follow outdated information-security benchmarks. It is necessary to update this as soon as possible to avoid perpetuating ecosystem insecurity.

- To enhance testing for cyber resilience, the setting up of the Telecom Security Test Lab under the TEC should be expedited. The template for this lab can be similar to the German Trust Centre, which collaborates with testing facilities from various foreign jurisdictions. For critical sectors such as digital payments, the Telecom lab must strive to collaborate with international testing labs of payments organisations such as the EMVCo.

- The BIS, the STQC and the TEC should seek to promote wider consultation processes in standardising information and IT security, as done by the national standard setters in the US and Germany. The proposed multistakeholder payments advisory council can be an avenue through which Indian institutions gain payments-related insights on cyber-security standards.

- India's current strategy in participating at relevant International SSOs must be reconsidered, as it is insufficient in its current form. The government must accelerate collaboration with experts from the payments industry to identify strategies to promote Indian perspectives on cyber-security in such foreign fora. Policymakers should adopt approaches similar to countries such as Germany, Australia, China, Japan and South Korea.

- India must proactively participate in various international working groups. Policymakers can promote the interests of the entire digital-payments ecosystem (beyond banks and the NPCI) and create avenues to increase the country's international presence.

[275] http://www.standards.org.au/StandardsDevelopment/Developing_Standards/Pages/National-Sector-Managers.aspx.

[276] https://www.itu.int/en/ITU-T/studygroups/2017-2020/09/Documents/ITU_FGDFS_SecurityReport.pdf.

RESHAPING NATIONAL CYBER-SECURITY STRATEGIES

The current NCSP was adopted under a prior regime and does not reflect policy priorities such as Digital India; the Smart Cities Mission; the push for digital financial inclusion; and next-gen technological movements, e.g. the Internet of Things (IoT) and artificial intelligence. Moreover, the capacity-building provisions of the policy were designed based on five-year targets (starting 2013).[277] Even normatively, the NCSP appears incomplete as it does not address how Indian cyber-security strategies can be augmented by engaging the international community. While the NCSP refers to needs relating to greater bilateral and multilateral arrangements; greater cooperation with international law enforcement agencies, judicial systems and security agencies like CERTs; and creating mechanisms for technical dialogue -- these provisions have lacked specificity or defined processes to further such goals.[278] Thus, it is now time for India to update its NCSP to reflect current technological and ecosystem realities, and provide special emphasis on challenges relating to the international dimension of the cyberspace. Alternatively, policymakers across departments can collaboratively develop (with stakeholder inputs) a sectoral cyber-security plan (under the Digidhan Mission) along the lines of the US' 2015 strategy for its financial sector.[279] Such a policy, if consultatively developed, could create mutual goals, raise trust and expedite India's security efforts. It could also be used as a tool to help define processes to secure critical nodes and infrastructure specific to digital payments. Any cyber-security policy—overarching or for payments—should incorporate the best practices enlisted below:

- **Sunset Provision:** Similar to the UK government's National Cyber-Security Strategy (2016–21),[280] a new policy should only be applicable for a specific time period. Additionally, it should be subjected to periodic reviews to ensure that cyber-security efforts keep pace with technological advancements.

- **Standardisation:** Promoting "Security-By-Design," based on the ISO Common Criteria Product Assurance Certification (Singapore Cyber-Security Strategy, 2016[281]).

- **International Dimension:** Countries such as Singapore and the UK tie up with international white-hat hackers, e.g. CREST, to set up penetration and accreditation facilities. Moreover, the US specifies that financial-sector security requires international cooperation (see FS-ISAC).

- **Capacity-Building Strategies:** The UK's strategy relies on market-driven solutions, such as cyber-risk insurance for SMEs, to adopt good cyber-security practices. The UK has implemented a citizen-facing capacity-building programme (Cyber Aware) and a cyber essentials platform to shield SMEs from low-level exploits. In the financial sector, the US' sectoral framework helps SMEs adopt appropriate cyber-security safeguards. The OECD espouses the benefits of introducing security labels to products and services to better inform the market and promoting cyber-security insurance markets.[282]

[277] Objective 8.

[278] See Strategy M.

[279] "Financial Services S 2E0 Ct1 O5 R- Specific," FSSCC, FBIIC, 2015, accessed 9 January 2018, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-financial-services-2015-508.pdf.

[280] "NATIONAL CYBER SECURITY STRATEGY 2016-2021," National Cyber Security Centre, UK government, 2016, accessed 9 January 2018, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf.

[281] "SINGAPORE's CYBERSECURITY STRATEGY," Cyber Security Agency of Singapore, 2016, accessed 9 January 2018, https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf?la=en.

[282] "CYBERSECURITY POLICY MAKING AT A TURNING POINT," op. cit.

Resolving Localisation

Cyber-security strategies (sectoral or national) must reflect the cross-border aspect of the cyberspace. However, the current NCSP fails to provide specific strategies for effective international cooperation. It is important for India to effectively engage with international frameworks that enable cyber-crime investigation. At the same time, the government must recognise that traditional routes under Mutual Legal Assistance Treaty (MLAT) and Letters Rogatory (LR) frameworks remain inefficient.[283]

Srikrishna Recommendations

The B.N. Srikrishna Committee Report on data protection considers 'localisation' a tool that can facilitate seamless law-enforcement access to data to tackle cyber-attacks and cybercrime.[284] At the same time the report concedes that a preferable route is one where nation states work towards a regime which facilitates information sharing.[285] Indeed, the report states this as a preference due to the overwhelming costs associated with data localisation; the manner in which localisation undercuts the value of internet economies through cloud computing-based service models; and the potential adverse impact a balkanised internet could have on civil liberties.[286] Moreover, localisation can also weaken technological security, as it leads to the concentration of risks to a specific geography. Moreover, it also contributes to suboptimal development of cybersecurity solutions/strategies as a considerable amount of such processes is via dynamic intelligence sharing/big data analytics within different offices, businesses and industries often located across jurisdictions.

Unfortunately, Chapter VIII of the Srikrishna Committee's DPB (Sections 40 and 41) adopts a protectionist approach to cross-border transfers of personal data. Specifically, it mandates all personal data[287] to have one serving copy within Indian servers. The Bill also allows for certain categories of "critical personal data," which can only be stored and processed domestically. However, despite such local storage mandates, the Bill provides for a highly regulated/monitored framework[288] to allow for any cross-border exchange of Indian data in foreign servers (Section 41).

Recommendations:

Given complex (economic and socio-political) trade-offs, a national cyber-security policy can provide an impetus for change and push Indian authorities to improve the country's cross-border law enforcement capabilities, whilst preserving the inherent fabric of digital markets and digital payments. Two specific frameworks that Indian authorities should consider are:

Budapest Convention on Cyber Crime (CETS No.185): It is the world's first and largest multilateral cyber-crime treaty, with 60 ratifications.[289] Designed by the Council of Europe in 2001, it strives to harmonise national cyber-security laws and form a basis for international cooperation. India is one of the few major non-signatories to the convention, even though it is considered a major instrument for cross-border cyber-crime investigations and for securing e-evidence. The convention has established a dedicated "Cloud Evidence Group," which explores solutions for governments/authorities to access evidence stored on cloud servers in foreign jurisdictions.[290] In

[283] https://www.orfonline.org/research/hitting-refresh-india-us-data-sharing-mlat/.

[284] http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf, 88.

[285] http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf, Page 88.

[286] http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf, Page 93-96.

[287] The Central Government may exempt certain categories of personal data from this requirement (Section 40(3)).

[288] Standard Contract Clauses or Intra-Group Schemes; Central Government and DPA approved list of certain international jurisdictions, sectors and organisations; For situations of "necessity"; and with requisite consent of data principals.

[289] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=WI0CsBtT.

[290] https://www.coe.int/en/web/cybercrime/ceg.

accordance with its terms of reference, the group is developing terms for an optional protocol to enable law-enforcement access to data stored in foreign servers.

International Data-Sharing Arrangements: While the above framework relies on principles of mutual assistance as under MLAT frameworks,[291] international conversations are now focusing on data-sharing arrangements for law-enforcement access. One such framework is articulated under the US' recently enacted Clarifying Lawful Overseas Use of Data (CLOUD) Act,[292] designed to enable easier law-enforcement access to data stored across borders through *direct data-sharing arrangements*. The amendments under the CLOUD Act specifically enable foreign states to make binding requests for direct law-enforcement access to data held by companies located in the US, upon execution of bilateral executive agreements. To be eligible for this, India's data-protection standards and civil-liberties framework must be sufficient as per the US Attorney General's assessment. The UK–US Data Sharing Agreement forms a template for future executive agreements authorised under the Act. The EU and the US are currently negotiating an agreement. Similarly, the EU's Proposal on European Production and Preservation Orders envisions a direct data-sharing arrangement, such that courts can demand electronic evidence from entities holding data in other member countries.[293]

[291] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008156l, Article 27.

[292] https://www.congress.gov/bill/115th-congress/house-bill/4943.

[293] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final - 2018/0108 (COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:225:FIN.

Annexure 1: Sectoral Institutional Approaches to Secure Digital Payments

Jurisdiction	Sectoral Treatment
Singapore[294]	■ In August 2017, the Monetary Authority of Singapore established a Payments Council to help develop its e-payment society. The council comprised 20 representatives across banks, PSPs, clearing houses, businesses and trade associations.
Brazil	■ In Brazil, security frameworks only supervise PSPs identified as carrying "systemic risk," which leaves out schemes that do not impose risks affecting the regular functioning of retail payments systems, i.e. closed-loop payment cards. Another criterion is the volume of transactions over the concerned payments service. Such a regulatory approach is to promote the development of market penetration while also preserving the security and efficiency of markets.[295]
Canada[296]	■ Canada lacks a comprehensive framework, and applicable laws or standards are based on the type of PSP. For instance, financial institutions must comply with consumer-protection obligations as imposed by the sectoral regulator. Non-financial institutions that facilitate digital payments must comply with generic consumer-protection regulations. ■ Industry associations establish standards for secure deployment of various types of payments mechanisms, e.g. the NFC. Such standards include the design of payment applications, device standards, and best practices with respect to collection and storage of personal data. Additionally, the Canadian general data protection law (PIPEDA), if implemented, cannot override sector-specific data-security requirements.
Other International Practices	■ Payment supervisory authorities in jurisdictions such as Spain, Canada and Japan have developed security requirements in cooperation with other national authorities.

[294] Monetary Authority of Singapore, "MAS Establishes Payments Council," 2017, accessed 9 January 2018, http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-Establishes-Payments-Council.aspx.

[295] "Online And Mobile Payments: Supervisory Challenges To Mitigate Security Risks," op. cit.

[296] "Online And Mobile Payments: Supervisory Challenges To Mitigate Security Risks," op. cit.

Annexure 2: International Approaches to Securing Digital-Payments Ecosystems

Jurisdiction	Policy/Regulatory Approach
Singapore	■ The Monetary Authority of Singapore (MAS) has a set of non-binding "Technology Risk Management Guidelines,"[297] detailing risk-management best practices for financial institutions. The primary goal is to enable system security, reliability, resilience and recoverability. The regulator also identifies the importance of robust authentication to secure transactions. ■ The country allows institutions the flexibility to adapt its guidelines based on an entity's prevailing risks. Key elements of the MAS guidelines include board-level risk-management frameworks; effective internal-control and risk-management processes; periodically updated IT policies for risk mitigation and secure information-system assets; and risk assessment. ■ The MAS endorses taking insurance cover for aspects such as recovery and restitution costs. ■ Risk identification should examine internal and external networks; hardware; software interfaces; risk assessment on the basis of threat and vulnerability matrices; risk treatment on the basis of risk tolerance; and robust incident handling and risk escalation. Additionally, companies should maintain comprehensive disaster recovery plans, conduct vulnerability assessments and penetration testing, implement security-patch management procedures, and effective access controls (principle of "least privilege"). ■ Security measures should also be taken for data at rest and data traversing across networks. In particular, confidential information requires appropriate encryption with adequate key strength. Based on the criticality of IT, infrastructure entities must consider installing network-security measures such as firewalls and intrusion-detection systems. ■ Interoperable-payments ecosystems carry a higher degree of risk and require better security approaches, e.g. stronger encryption algorithms in line with international standards. The MAS recommends the adoption of strong monitoring and surveillance mechanisms to check for abnormal activities on the basis of transaction velocity. It also endorses the adoption of two-factor authentication for online payments and strong card-authentication mechanisms such as Dynamic Data Authentication (DDA) and Card Data Authentication (CDA). ■ The MAS urges businesses to undertake comprehensive cyber audits.

[29] "TECHNOLOGY RISK MANAGEMENT GUIDELINES," Monetary Authority of Singapore, 2013, accessed 9 January 2018, http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf.

Jurisdiction	Policy/Regulatory Approach
European Union	■ Data-security requirements under the EU's new General Data Protection Regulation (GDPR) embrace risk-based approaches, which correspond to the level of risks of data-processing activities.[298] Regulators are supposed to undertake risks analysis by evaluating the possibility and severity of an adverse incident, with nature, scope and context being important factors. Severity under the GDPR regime is based on factors such as the significance of economic damage (Recital 60a). Under this regime, financial losses can be perceived as less harmful than losses revealing intimate and personal details about individuals. Specific to the EU's Revised Payments Services Directive (PSD2): ■ In November 2017, the EC released Regulatory Technical Standards for strong customer authentication (under Article 98, PSD2), for digital payments after a widespread consultative process.[299] These measures were developed to protect the confidentiality and integrity of payments-related security credentials and the need for common and secure open standards of communication across various service providers in payments value chains. ■ The standards are developed keeping in mind framework objectives to enhance security, promote competition, protect consumers, facilitate technological and business-model neutrality, and allow innovation for consumer experience. The authentication procedural framework includes transaction-monitoring mechanisms. It notes that authentication codes must be dynamic in nature (and no specific technology should be made mandatory), and these codes can include validation through OTPs, digital signatures or other cryptographically underpinned validity assertion. ■ The SCA is based on principles of knowledge, possession and inherence. These elements should be independent of one another, where a breach of one does not compromise the reliability of other layers. Anonymised payments instruments are not subject to the same technical SCA requirements. ■ Security exemptions can be made for the SCA on the basis of (1) risk, (2) amount, (3) recurrence and (4) channel of payment. ■ The PSD2 also allows for exemptions for low-value contactless payments at PoS, which take into account a maximum number of consecutive transactions or a fixed maximum value of consecutive transactions, without applying strong customer authentication. ■ Such exemptions can be based on real-time transaction risk analysis, which can identify low-risk payments. The framework deems it appropriate to exempt PSPs of SCA requirements if they adopt effective, risk-based mechanisms to ensure fund and personal-data security. It states that if transactions cannot be quantified as low-risk, PSP should revert to the SCA.

[298] "The Risk-Based Approach In The GDPR: Interpretation And Implications," accessed 9 January 2018, https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdf.

[299] European Commission, "COMMISSION DELEGATED REGULATION (EU) No …/.. Of XXX Supplementing Directive 2015/2366 Of The European Parliament And Of The Council With Regard To Regulatory Technical Standards For Strong Customer Authentication And Common And Secure Open Standards Of Communication," 2017.

Jurisdiction	Policy/Regulatory Approach
Austria, Brazil, and Netherlands (FINCONET)	■ According to the International Financial Consumer Protection Organisation's global study on digital-payments security,[300] Austria takes a risk-based approach to digital-payments security. As per the report, regulators prioritise assessment of payment systems that are prone to incidents or suffer from higher exposure. ■ The report observes that Brazilian authorities have delegated the responsibility of security to PSPs. Outcomes suggest that businesses were afforded the requisite flexibility to manage their risks better, and there have been fewer instances of fraud. ■ Additionally, risk-mitigation strategies in the Netherlands have been found to benefit from automated transaction-monitoring mechanisms.
United States	■ NIST, in its latest draft of a framework to critical infrastructure cyber security,[301] observed that to secure increasingly connected ecosystem networks, policy frameworks must identify "flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks." ■ This shows that policy approaches take into account cost-effectiveness on the basis of business models, seeking to economically incentivise good cyber-security practices and incorporate cyber-risk management into overall organisational risk-management processes. ■ NIST holds that risk-based approaches ensure network security, as more effective investment decisions are made with better measurements of risks, costs and benefits of cyber-security strategies. ■ NIST acknowledges that SMS-based authentication processes are vulnerable to both social and technical security threats.[302]
OECD	■ In the context of consumer protection in the financial sector, the OECD holds that regulatory and supervisory frameworks must be responsive to new designs, products and technologies.[303]
Saudi Arabia	■ The Saudi Arabian Monetary Agency has imposed comprehensive online-security regulations to prevent data misuse or theft. This includes two-factor authentication for all online payments, transaction notifications to account holders, and regulations to ensure mobile-application security. Their security frameworks also include 14 risk-management principles.[304]

[300] "Online And Mobile Payments: Supervisory Challenges To Mitigate Security Risks," op. cit.

[301] "Framework For Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, 2017, accessed 9 January 2018, https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf.

[302] Paul A. Grassi et. al., "Digital Identity Guidelines," NIST, 2017, accessed 9 January 2018, https://pages.nist.gov/800-63-3/sp800-63b.html.

[303] "G20 HIGH-LEVEL PRINCIPLES ON FINANCIAL CONSUMER PROTECTION," 2011, accessed 9 January 2018, http://www.oecd.org/daf/fin/financial-markets/48892010.pdf.

[304] "Online And Mobile Payments: Supervisory Challenges To Mitigate Security Risks," op. cit.

Annexure 3: Mapping India's Participation/Collaboration in Relevant Standard-Setting Organisations

International Bodies	Indian Participation
International Standards Organisation (ISO)/ International Electrotechnical Commission (IEC)	**ISO** ■ Standards are developed through multistakeholder processes. Technical Committee participants comprise experts nominated by national standards organisations, e.g. the BIS. ■ Relevant security standards developed include ISO 20022 and ISO 27001. The ISO has constituted a technical committee (ISO/TC 68/SC 2), which seeks to address financial services security. ■ India, represented by the BIS, is one of the 54 participating countries in an ISO/IEC joint technical committee pertaining to "IT security techniques." However, anecdotal evidence suggests that India's participation remains poor. ■ In addition to the Technical Committee, the ISO works with specific sectoral associations or "organisations." The lack of Indian representation here is a lost opportunity for the Indian industry to bring forth its perspective on global-standardisation discourse. **IEC** ■ BIS is one of the 60 members of the IEC. ■ It created the "ISO/IEC JTC 1/SC 27," which deals with IT security techniques; the BIS is a participating member. ■ The ISO/IEC 27001 and 27002 provide standards for information security management.
European Telecommunications Standards Institute (ETSI)	■ The ETSI produces globally applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies. ■ It comprises industry players, governments and regulatory bodies. ■ It includes three Indian members, namely, C-DOT (Governmental), HCL Technologies, WIPRO. ■ The Telecommunications Standards Development Society, India (TSDSI) signed a cooperation agreement with the ETSI in April 2015. ■ The collaboration between the two organisations now happens at the level of the Global Standards Collaboration (GSC) initiative, where TSDSI is a full member. The GSC fosters cooperation amongst standards organisations from across the world, to facilitate the exchange of information on standards development, build synergies and reduce duplication of work. ■ The ETSI has over 800 members from 67 countries. ■ Any company or organisation with an interest in creating telecommunications and related standards can become an ETSI member, including universities, research bodies, associations and public authorities, as well as industrial companies of all sizes. ■ The ETSI is part of the Web Payments Charter group of W3C.

International Bodies	Indian Participation
EMVCo	■ The EMVCo has nine working groups (including mobile payments and security) and numerous task forces, which are responsible for developing and publishing the EMV specifications and evolving and managing EMVCo's testing and approval processes. These groups consist of payment systems staff, who are subject-matter experts. ■ The EMVCo engages with various regional and global organisations to receive input and share perspectives on areas of mutual interest. These organisations include the NFC Forum, the Global Platform, the GSMA, the PCI-SSC, the AFSCM, the APSCA, the ACT Canada, the ETSI, the European Payments Council, the Smart Card Alliance and the EMV Migration Forum. ■ The NPCI is the EMVCo's technical and business associate. It can provide inputs and receive feedback on detailed technical and operational issues connected to the EMV specifications and related processes. It can also offer inputs on strategic business and implementation issues related to the use of the EMV specifications.
PCI-Security Standards Council (SSC)	■ Its five founding members include American Express, Discover, JCB, MasterCard and Visa. ■ It has eight affiliate members, comprising regional and national organisations, which define standards and influence the adoption of digital payments. They actively participate in standards-development processes. ■ The NPCI was recently admitted as an affiliate member. ■ Other members include: the Australian Payments Clearing Association; the Cartes Bancaires (France's National Interbank Network and represents the interests of over 100 PSPs), the Dutch Payments Association, the Pan Nordic Card Association (association of banks and financial institutions across Scandinavian states), the Interac (non-profit Canadian Interbank Network), the Cartao Elo (owned by Bank of Brazil), and the MIR (Russia's National Payment System).
Fast Identity Online (FIDO) Alliance	■ The Alliance aims to develop scalable, interoperable, open-source and two-factor authentication for the digital-payments industry. ■ The FIDO Alliance has established the FIDO2 Project, which aims to build the Universal Second Factor (U2F) to create interoperable and scalable authentication solutions **that offer a password-less experience**. It will be based on the W3C Web Authentication specifications. ■ One of its primary goals is to improve transaction security, which leads to reduced risk, less churn and enhanced customer loyalty. ■ Currently, it has no Indian representation.

International Bodies	Indian Participation
World Wide Web Consortium (W3C)	■ Open to all types of organisations (including commercial, educational and governmental entities) and individuals. ■ The MeitY and the NPCI represent India at the W3C. ■ The Web Payments Working Group and Web Payments Interest Group are set up for easier and secure payments. ■ NPCI does not participate in either of these payment-standards development processes. The Centre for Development and Advanced Computing, under the MeitY, has four representatives assigned for the Web Payments Interest Group. Thus, India misses out on the FIDO2 conversation, which could be a solution for low-digital literacy countries.
Internet Engineering Task Force	■ The platform is open source. ■ Governments or corporations cannot register; only individuals can. ■ Indian stakeholders should track IETF developments for the emergence of technical best practices.

AUTHOR'S NOTE

On 09 October 2017, the National Institute for Transforming India (or NITI Aayog), in partnership with the Observer Research Foundation (ORF) convened a consultation with stakeholders to outline a roadmap for securing India's digital financial sectors. The discussion was chaired by NITI Aayog's Dr VK Saraswat. The inputs received from the discussants were of immense value in shaping this report. The names of the stakeholders and the organisations which they represented at the time of the consultation are as follows:

- Amrit Pradhan, *Vodafone India*
- Ashish Aggarwal, *National Institute of Public Finance and Policy*
- Bedavyasa Mohanty, *ORF*
- Karthik Ramanathan, *Mastercard*
- Madhulika Srikumar, *ORF*
- Mahavir Jindal, *Amazon Pay*
- Meghna Bal, *ORF*
- Prem Kumar Gurnani, *State Bank of India*
- Ravi Aurora, *Mastercard*
- Rohan Mishra, *Mastercard*
- Saikat Datta, *Centre for Internet and Society*
- Samir Saran, *ORF*
- Saurabh Singh, *CISCO*
- Shagufta Kamran, *US-India Strategic Partnership Forum*
- Shubh Soni, *ORF*
- Subba Rao Katta, *Airtel Payments Bank*
- Udbhav Tiwari, *Centre for Internet and Society*
- Umesh Jagga, *Wipro*
- Vivan Sharan, *Koan Advisory Group*

This report would not have been possible without support from Mastercard. In particular, I would like to thank Mr Ravi Aurora and Mr Rohan Mishra of Mastercard for their technical support throughout the process. My gratitude as well to Ms Madhulika Srikumar and Mr Bedavyasa Mohanty, both of ORF, for their guidance and support in finishing the research for this report. Any errors in this report should solely be attributed to the author.

The Indian government has outlined a target of creating a US$1-trillion digital economy by 2025. Digital payments are an important component of this target and a national payments mission (‘Digidhan Mission’) has been initiated under the aegis of the Ministry of Electronics and Information Technology (MeitY). As this process continues, the security framework for the system of digital payments must be simultaneously constructed. One clear objective of the *Digidhan Mission* is to secure the entire digital-payments ecosystem, which includes reviewing the efficacy of current institutional and security frameworks. This report contextualises the various moving parts within digital payments and broader policymaking arenas to propose a forward-looking cyber-security strategy for the sector.

Observer Research Foundation
20, Rouse Avenue Institutional Area
New Delhi – 110002
contactus@orfonline.org
+91 11 35332000, 43520020

Koan Advisory
B6-1, Second Floor, DDA Commercial Complex
Safdarjung Enclave, New Delhi – 110029
contactus@koanadvisory.com
+91 1141834471