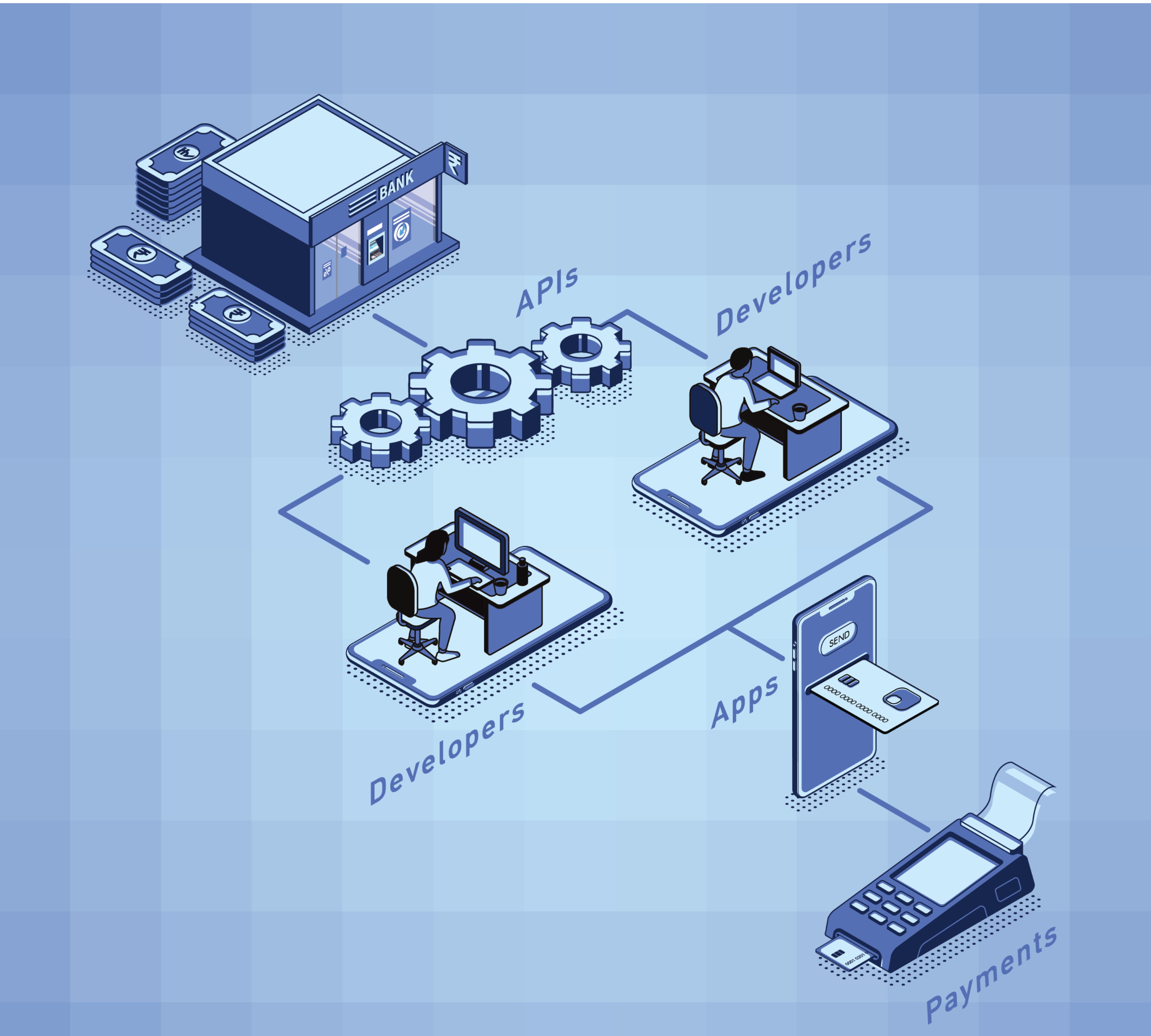
GATEWAY HOUSE
INDIAN COUNCIL ON GLOBAL RELATIONS

SWIFT INSTITUTE

A CYBERSECURITY AGENDA FOR INDIA'S DIGITAL PAYMENT SYSTEMS

Sameer Patil, *Fellow, International Security Studies Programme*
& **Sagnik Chakraborty,** *Researcher, Cybersecurity Studies Programme*



PAPER NO. 20 | SEPTEMBER, 2019

A Cyber Security Agenda for India’s Digital Payment System

Sameer Patil, Fellow, International Security Studies Programme
& Sagnik Chakraborty, Researcher, Cyber Security Studies Programme

PAPER NO. 20 I SEPTEMBER 2019

GATEWAY HOUSE
INDIAN COUNCIL ON GLOBAL RELATIONS
भारतीय वैश्विक संबंध परिषद्

GATEWAY HOUSE
INDIAN COUNCIL ON GLOBAL RELATIONS

Executive

Executive Director, Manjeet Kripalani
Director, Neelam Deo
CEO and Director of Research, Akshay Mathur

Publications

Website and Publications Manager, Aashna Agarwal
Editor, Manjeet Kripalani
Editor, Nandini Bhaskaran
Editor, Christopher Conte
Cover Design, Debarpan Das
Layout Design, Daniella Singh

Gateway House: Indian Council on Global Relations

@GatewayHouseIND

@GatewayHouse.in

For more information on how to participate in Gateway House's outreach initiatives, please email outreach@gatewayhouse.in

Printed in India by Airolite Printers.

TABLE OF CONTENTS

LIST OF TABLES:

About the Authors

__Sameer Patil__ is Fellow, International Security Studies Programme, Gateway House. Prior to this, he was Assistant Director at the National Security Council Secretariat in the Prime Minister's Office, New Delhi, where he handled counter-terrorism and regional security desks. Sameer has written extensively on various aspects of national security, including counter-terrorism, cyber security, the Kashmir issue, India-Pakistan and India-China relations. He is also a dissertation advisor at the Naval War College, Goa.

__Sagnik Chakraborty__ is a Researcher in Cybersecurity and Manager of the Management Office at Gateway House. His work focuses on technology and national security. Sagnik is a software engineer by profession with more than nine years of experience in the IT industry. Prior to Gateway House, he worked with Tata Consultancy Services. He has held various roles in his IT career, starting from a developer to a consultant and an operations & product manager. He is interested in cyber security, fintech, business analytics and disruptive technologies.

Acknowledgements

SWIFT INSTITUTE

This project was funded by the SWIFT Institute.

The views and opinions expressed in this paper are solely those of the authors. SWIFT and the SWIFT Institute have not reviewed the paper, and the views expressed in it do not necessarily reflect those of either SWIFT or the SWIFT Institute.

This paper is based on desk research and analysis, interviews with government and law enforcement officials who handle cyber-security issues, financial regulators, representatives of banks, payment gateway companies and cyber security professionals.

** Additional research inputs for this paper were provided by Aditya Phatak, Chandni Jindal and Gayatri Bafna.*

List of abbreviations:

AEPS: Aadhaar-Enabled Payment System

APT: Advanced Persistent Threat

BHIM: Bharat Interface for Money

CERT-IN: Computer Emergency Response Team-India

CISO: Chief Information Security Officer

DDoS: Distributed Denial of Service

IB-CART: Indian Banks-Center for Analysis of Risks and Threats

IT: Information Technology

NCIIPC: National Critical Information Infrastructure Protection Centre

NCSP: National Cyber Security Policy

NFS: National Financial Switch

NPCI: National Payments Corporation of India

MHA: Ministry of Home Affairs

PoS: Point of Sale

PPI: Prepaid Payment Instruments

RBI: Reserve Bank of India

SWIFT: Society for Worldwide Interbank Financial Telecommunication

UPI: Unified Payments Interface

Executive Summary

In the span of a mere decade, the Indian economy has gone from being cash-based to being heavily reliant on digital payment systems. This transition has been driven by domestic initiatives such as the Unified Payments Interface, IndiaStack, Aadhaar-Enabled Payment Systems and mobile wallets. These have brought many visible and worthwhile changes, such as greater convenience, financial inclusion, transparency in transactions, substantial tax revenue and wider scope for financial technology to come into its own. But the growing digitisation of payment systems also has brought greater threats, perpetrated by hackers, organised criminal syndicates and, in some cases, foreign governments. Indian regulators and the payment industry have focused on tackling these threats.

This paper analyses India's payments industry and reviews trends in cyber-attacks on its payment infrastructure. It maps the system's vulnerabilities and channels to explain how attacks may arise. It also includes a review of existing policy measures and cyber-security standards. The paper argues that in order to secure its digital payment systems, India will need to expand its efforts by focusing on data protection, information sharing, cyber hygiene and cyber attack attribution. A safe and secure payment system will increase citizens' confidence and strengthen the digital economy.

India's policy push towards digital payments makes it an important global actor in the digital economy. Therefore, a greater emphasis is needed on threat mitigation and vulnerability-patching to ensure resilience of the payment systems and a greater level of cyber security. This paper makes the following recommendations for action on three levels: government, business and diplomatic.

Government

- Make reporting of data breaches mandatory
- Expedite creation of CERT for the financial sector
- Adopt a phased approach to local data storage requirements for the payments industry
- Expand cyber hygiene education initiatives

Business (industry)

- Create a payment-industry platform for information-sharing
- Enable consumers to control data through a consent dashboard

Diplomatic (global)

- Negotiate preferential and conditional data-sharing agreements with like-minded countries
- Articulate a normative framework for cyber-attack attribution

1. Introduction

In just 10 years, India has gone from having a cash-based economy to one that primarily relies on digital payment systems. Successful implementation of the JAM trinity (the Pradhan Mantri Jan-Dhan Yojana initiative to make basic financial services available to all, linkage of Aadhaar national identity cards to government subsidy payments and promotion of mobile payment systems) have contributed to this transformation. So have private sector-led and government-supported innovations like the IndiaStack software platform and the Unified Payments Interface (UPI) real-time payment system.

The shift towards digital payments has reduced corruption, increased transparency and tax revenue, and created more opportunities for financial technology innovation. But it has emerged at a time of expanding cyber threats to payment systems, as demonstrated by cyber crimes committed by organised criminal syndicates and rogue state actors. The targeting of more than 100 banks and other financial institutions in 40 countries (mostly in Europe) by Carbanak, a criminal syndicate led by a Spain-based mastermind, demonstrates this growing threat; through a malware attack on banks, this syndicate stole more than €1 billion between 2013 and 2018.[1]

In other cases, foreign governments have used proxies to target states' governmental and commercial computer networks, and to engage in cyber crime for profit. This is evident in the case of the North Korea-backed Advanced Persistent Threat[2] (APT) 38 cyber operation, which repeatedly targeted bank payment systems.[3] Data breaches of the government Office of Personnel Management[4] and the Marriott International hotel corporation in the United States also have been attributed to malicious state actors.[5]

Although India has taken extensive cyber security measures, its digital payment infrastructure continues to lack resilience. Data-breach reporting and vulnerability disclosure are voluntary, business trust in government is low, the competitive business environment works against cooperation, and technical and forensic capacity remains inadequate.

This paper analyses India's payments industry and trends in cyber-attacks on its payment infrastructure; maps the system's vulnerabilities and recommends measures to plug them; and reviews existing policy measures and cyber security standards.

2. India's digital payment system

In the last decade, India's regulators and payment industry participants have taken important initiatives in the digital payments arena. In 2009, 56 major state-owned and private-sector banks set up the National Payments Corporation of India[6] (NPCI) to manage retail payment systems. This was followed in 2012 by launch of RuPay[7] – an Indian brand for retail electronic payments. The NPCI developed the Unified Payments Interface (UPI) for facilitating real-time fund transfers between bank accounts by using mobile numbers, QR codes, Aadhaar numbers or virtual payment addresses mapped to individual bank accounts. A key enabler was seeding of personal and biometric Aadhaar data with individual bank account information. Transactions executed through the authentication of Aadhaar data gave rise to the Aadhaar-enabled Payment Systems (AEPS). The demonetisation exercise in November 2016 gave a significant boost to AEPS and UPI-based transactions.

Table 1: India's Digital Payment Modes

Aadhaar-Enabled Payment System (AEPS)	
Unified Payments Interface (UPI)-based applications	Mobile applications for payment and related transactions
Micro-ATM	Modified Point of Sale (PoS) terminals used by the business correspondents of any bank to make tranactions
*99# service	Mobile banking service based on the Unstructured Supplementary Service Data (USSD) communication protocol – a communications technology used by mobile phones for payment transactions
BHIM Aadhaar Pay	UPI-based mobile application for merchants to receive payments from customers over the counter through Aadhaar authentication
Non-AEPS payment systems	
Prepaid Payment Instruments	Digital applications that store consumer payment information and carry out payment transactions. Commonly known as 'mobile wallets' such as PayTM, MobiKwik and Oxigen
PoS terminal	Payments made at retail establishments using debit or credit cards on physical equipment
Online banking	Mobile or internet-based banking applications for payment transactions and other banking services

Source: Source: Gateway House research

Statistics from the NPCI show that these services have been growing rapidly. Monthly transactions on UPI, for instance, crossed the Rs.1 trillion mark in December 2018.[8]

Crypto-currencies such as Bitcoin are not part of the growing payment system in India. Given the wide fluctuations in their value, the Reserve Bank of India (RBI) has warned Indian citizens not to trade or use such currencies. In 2018, the RBI also prohibited banks from providing financial services to crypto-currency exchanges. Yet such exchanges continue to flourish due to growing interest among Indians. The RBI's concern about crypto-currencies is reaffirmed by the security establishment's apprehension about the use of these currencies in digital black markets for selling and buying contraband and narcotic substances.[9]

3. Cyber risks to India's digital payments

A review of the major data breaches involving Indian computer networks (Table 2) since 2010 shows that financial sector and government servers have been targeted the most for unauthorised access to sensitive payments data. In the most serious incident, sophisticated malware was injected into India-based servers of Hitachi Payment Services (a payment subsidiary of Hitachi Ltd. Japan) in 2016, enabling unauthorised access to a vast store of Indian debit-card data. The malware, which remained undetected for a long time,[10] resulted in losses totalling Rs.1.3 crore and forced 19 Indian banks to replace 3.2 million debit cards.[11]

Bad actors are hacking into payment systems not just by attacking centralised databases, but also by targeting individual users and banking professionals to gain access to restricted Indian computer systems illegally – widely known as "social engineering" attacks. For instance, in 2016 hackers gained access to the payment systems of the Union Bank of India,[12] one of the country's largest public-sector banks, after an employee mistakenly responded to a phishing email that then installed the malware in the bank's servers.[13] This allowed hackers to siphon $170 million from its foreign-exchange accounts. Timely intervention by the bank retrieved the stolen money in its entirety; in many other cases, stolen money was only partially recovered, as in the case of a breach in 2018 at the private-sector City Union Bank,[14] or lost without a trace, as in the case of fraud in 2018 at Cosmos Bank, a cooperative bank.[15]

India has not publicly attributed these cyber security incidents to state actors. But anecdotal and technical evidence from private cyber-security firms suggests the involvement of state actors in some of these hostile acts. FireEye, an American cyber-security consulting company, has reported that a cyber operation, codenamed 'APT30', targeted the Indian government and commercial servers to harvest sensitive military and business data as part of a decade-long espionage operation, most likely state-sponsored.[16] Similarly, the modus operandi followed in the attack on Cosmos Bank suggests the involvement of North Korea's 'APT38' operation.[17]

Table 2: Major cyber security incidents involving Indian computer networks

Year	Incident	Implications
2010	Stuxnet infections of Indian computer systems	Part of a global attack, the malware-infected computer systems across India, including computer systems at power plants and oil pipelines in Gujarat and Haryana. No other major disruption was reported.
2015	Foreign espionage operation focused on government and commercial computer networks	A decade-long espionage operation through the APT30 vector, carried out by a China-based group that was most likely state-sponsored. The data harvested was political, economic and military. The APT30 utilised the same tools, tactics and infrastructure for 10 years, exposing a major vulnerability in critical computer networks.
2016	DCNS data breach	Designs and data on India's Kalvari-class submarines, along with those of Malaysia and Chile, were leaked from the French shipbuilder DCNS, which was involved in submarine-building projects. The breach reportedly revealed confidential stealth capabilities of submarines. Commercial rivalry was suspected to be behind the data breach.

Source: Source: Gateway House research based on official data and media reports

Table 2: Major cyber security incidents involving Indian computer networks (Continued)

Year	Incident	Implications
2016	Breach in Union Bank of India's foreign exchange account	Successful phishing attack activated malware that gave hackers access to payment-processing codes that were used to steal $170 million. Timely intervention resulted in retrieving the entire amount. After observing a trend in such attacks on banks, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which facilitates inter-banking payment transactions, launched a Customer Security Programme to expand information sharing about emerging cyber threats within the industry.
2016	Malware attack on the Hitachi Payment Systems	Malware compromised the payment infrastructure, resulting in the data breach of approximately 3.2 million debit cards. This is the biggest data breach in Indian history, resulting in losses totalling Rs. 1.3 crore.
2017	Bank of Maharashtra fraud	Fraudsters exploited software vulnerability in the UPI application for an unauthorised fund transfer. This caused the Bank of Maharashtra a loss of Rs.25 crores, which was partially recovered.
2017	'WannaCry' and 'Petya' ransomware attacks	Part of the global attack, the 'WannaCry' ransomware affected many government and commercial systems in India, but not many infections were officially reported. Some estimates put the number of infections at 48,000 computers. The Petya ransomware attack most prominently hit the container terminals of APM Terminals Mumbai, at India's biggest container port, the Jawaharlal Nehru Port Trust.
2018	Breach at City Union Bank	Cyber criminals hacked into the bank's payment systems to steal $2 million. The bank managed to retrieve $1 million.
2018	Cosmos Bank fraud	The bank lost Rs.94 crores due to a malware attack that authorised fraudulent transactions, with ATM withdrawals being reportedly made in 28 countries.

Source: Gateway House research, based on official data and media reports

Even as such attacks are rising, a gap in data on the extent of cyber-crimes in India prevents a uniform statistical assessment. The National Crime Records Bureau, which compiles data on criminal cases in India, reports that India recorded 12,317 cases of cyber-crimes nationally in 2016.[18] This includes technical crimes (computer infection through virus, disruption of computer network) as well as computer-enabled ones (cheating, forgery, destruction of electronic evidence etc.). However, these statistics are likely on the low side, since reporting on cyber-security incidents and data breaches is voluntary in India. India's law-enforcement agencies and judiciary are proactively enhancing their capacity to process and investigate cyber-crimes, but their ever-increasing sophistication makes this a daunting task given a lack of adequate forensic skills and training. This inadequate capacity is reflected in the low conviction rate for cyber-crimes: in 2015, only 253[19] people were convicted, while many cases remain pending with the police and judiciary.

3.1 Tracking vulnerabilities, channels and perpetrators

Based on interviews with representatives of banks, payment-gateway companies, and cyber-security professionals, this paper has attempted to map specific cyber vulnerabilities and channels in the payment system (Table 3). The section below illustrates them.

Table 3: Vulnerabilities, channels and perpetrators

Where (Node)	Why (Vulnerability)	How (Channel)	Who (Perpetrator)	What (Implication)
Aadhaar-Enabled Payment System (BHIM app, BHIM Aadhaar pay)				
UPI applications	• Biometric data • Centralised data storage • Lack of patched system (computer with outdated software)	• DDoS attack • Malware injection	• Adversarial states • Organised criminal syndicates • Hackers' collective • Individual hackers • Terrorist groups • Hacktivists • Rogue employees	• Identity theft • Doxing (leaking of personal sensitive and financial data for coercion)
Customer's bank	• Lack of environment patch update hygiene • Insider threat	• Malware injection • APT • Internal network sniffer • Man in the middle attack		• Data breach • Fraud and economic loss • Data breach
Receiving bank	• Lack of environment patch update hygiene • Insider threat	• Malware injection • APT • Internal network sniffer		• Data breach • Fraud and economic loss • Loss of proprietary financial data • Cyber-enabled espionage • Loss of reputation

Source: Source: Gateway House research

Table 3: Vulnerabilities, channels and perpetrators (Continued)

Where (Node)	Why (Vulnerability)	How (Channel)	Who (Perpetrator)	What (Implication)
***99# (Unstructured Supplementary Service Data) service**				
USSD gateway (GSM mobile *99#)	• Deficient cyber hygiene • Lack of or insufficient encryption	• Social engineering attack • Man in the middle attack	• Adversarial states • Organised criminal syndicates • Hackers' collective • Individual hackers • Terrorist groups • Hacktivists • Rogue employees	• Data breach and loss • Identity theft • Doxing
Customer's bank	• Lack of patched system • Insider threat	• Social engineering attack • Malware injection • APT • Internal network sniffer • Man in the middle attack		• Data breach • Fraud and economic loss • Data breach
Receiving bank	• Lack of environment patch update hygiene • Insider threat	• Malware injection • APT • Internal network sniffer		• Data breach • Fraud and economic loss • Loss of proprietary financial data
Prepaid Payment Instruments/Mobile wallets				
Customer's mobile wallet	• Lack of Two-Factor Authentication	• SIM card swapping and cloning • DDoS attack • Fake wallet apps	• Adversarial states • Organised criminal syndicates • Hackers' collective • Individual hackers • Terrorist groups • Hacktivists • Rogue employees	• Identity theft • Disruption of service • Doxing • Economic loss
Payment gateway or switch	• Lack of or insufficient encryption	• Man in the middle attack • DDoS attack		• Data breach
Payment processor	• Lack of or insufficient encryption	• Man in the middle attack • DDoS attack		• Data breach
Customer's bank	• Lack of patched system • Insider threat	• Malware injection • APT • Internal network sniffer • Man in the middle attack		• Data breach • Fraud and economic loss
Issuing bank	• Lack of environment patch update hygiene • Insider threat	• Malware injection • APT • Internal network sniffer		• Data breach • Fraud and economic loss

Source: Source: Gateway House research

Table 3: Vulnerabilities, channels and perpetrators (Continued)

Where (Node)	Why (Vulnerability)	How (Channel)	Who (Perpetrator)	What (Implication)
Point of Sales Terminal and Micro-ATM				
PoS terminal	• Deficient cyber hygiene	• Card cloning • Digital black markets • Social engineering attack	• Adversarial states • Organised criminal syndicates • Hackers' collective • Individual hackers • Terrorist groups • Hacktivists • Rogue employees	• Financial data loss • Identity theft • Doxing • Data breach
Payment processor	• Lack of or insufficient encryption	• Man in the middle attack		• Data breach
Acquiring bank	• Lack of environment patch update hygiene • Insider threat	• Malware injection • APT • Internal network sniffer		• Data breach • Fraud and economic loss
Payment brand's network	• Lack of or insufficient encryption	• Man in the middle attack		• Data breach
Issuing bank	• Lack of environment patch update hygiene • Insider threat	• Malware injection • APT • Internal network sniffer		• Data breach • Fraud and economic loss
Online banking				
Customer's bank website	• Deficient cyber hygiene • Rooted devices or apps	• DDoS Attack • SIM card swapping • Social engineering attack	• Adversarial states • Organised criminal syndicates • Hackers' collective • Individual hackers • Terrorist groups • Hacktivists • Rogue employees	• Financial data loss • Identity theft • Disruption of service • Doxing
Customer's bank	• Lack of environment patch update hygiene • Insider threat	• Malware injection • APT • Internal network sniffer		• Data breach • Fraud and economic loss • Data breach
Receiving bank	• Lack of environment patch update hygiene • Insider threat	• Malware injection • APT • Internal network sniffer		• Data breach • Fraud and economic loss • Loss of reputation

Source: Source: Gateway House research

Table 3: Vulnerabilities, channels and perpetrators (Continued)

Vulnerabilities	
Biometric data	Compromise of the biometric data such as fingerprints and iris can potentially result in spoofing of identity.
Centralised data storage	Centralised storage of data is often described as a 'honey pot', which entices users to hack into the databases.
Lack of patched system	Outdated and vulnerable systems, if not patched adequately in time, can be sitting ducks for cyber-attacks.
Insider threat	Former and/or current employees who have access to critical information, including financial and customer data, can expose banks to cyber-attacks.
Lack of or insufficient encryption	Lack of or insufficient encryption of transiting data, using protocols such as SSL or TSL, can expose it to interception.
Lack of cyber hygiene	Many Indian internet users, being first-generation users, lack knowledge of safe practices – do's and don'ts – to protect themselves.
Two-Factor Authentication (2FA)	If the customer's mobile phone is not secure enough, 2FA can be used to permit fraudulent transactions.
Unsecured mobile phones	Internet use in India is driven by low-end mobile phones, which come with even lower security standards, making them vulnerable to hacking.

Channels	
Distributed Denial of Service (DDoS) attack	An attack technique in which multiple computer systems are used to target a single system such as a payment server, internet banking website or mobile application, by overloading it with superfluous traffic and rendering it inoperative.
Malware injection	Malware dispatched by hackers to infect individual systems or a large network, by targeting existing software vulnerabilities, especially on unpatched systems.
APT	Sophisticated hacking technique used to penetrate a network and remain undetected for an extended period of time, harvesting sensitive personal and financial information.
Internal network sniffer	Technique used to capture data, when it is being transmitted over a network, especially unencrypted data like usernames and passwords.
Man in the middle attack	Attack technique, where saboteurs steal data during transit to carry out fraudulent payment transactions.
Social engineering attack	Attack technique that lures individuals to divulge confidential information or perform actions to gain privileged access to restricted systems.
SIM card swapping	Tactic, where a hacker tricks a mobile carrier to switch a user's phone number, to a SIM card owned by the hackers; this is then used to steal sensitive personal and financial information and also for 2FA.
Fake wallet apps	Mobile wallet apps which replicate the original genuine apps to prompt users to divulge wallet passwords, private keys and other sensitive personal financial information.
Carding	Frauds committed with stolen but active credit cards.
Digital black markets	Digital black markets offer easy access to computer hacking tools, software vulnerability data, social engineering attack tools and software.

Source: Source: Gateway House research

Payment industry representatives have cited deficient cyber hygiene – practices to ensure safe online behaviour – as the weakest security link in payment systems. The success of social engineering techniques – phishing and vishing (using telephones to trick individuals into divulging critical personal or financial information) – demonstrates why cyber hygiene is critical. Anecdotal evidence suggests hackers deploy social engineering techniques to target bank employees as seen in the case of the Union Bank of India breach in 2016.

A related concern is software piracy. Cyber criminals are adept at exploiting vulnerabilities in pirated software to install and spread malware such as keyloggers (which collect login details and passwords through keystrokes). According to Microsoft, more than 80% of new personal computers, loaded with pirated software in Asia (including India), are infected with malware.[20]

As India's dependence on digital payment systems deepens, particularly through the UPI, AEPS and mobile wallets, the vulnerabilities cited here are expanding the threat landscape. The payments industry has enthusiastically adopted the latest technology to cater to an expanding customer base, while paying attention to cyber security in response to a push from regulators. However, both regulators and companies are playing catch-up with the growing threats.

Sometimes cyber-security compliance is treated as a mere formality. Many organisations tend to resort to quick fixes and compliance window-dressing in lieu of comprehensive threat management. In many cases, notwithstanding awareness of cyber threats, compliance with cyber regulations is difficult due to inadequate budgets and lack of cyber security expertise in senior management. Moreover, some organisations believe that a grave cyber incident that could imperil their business is unlikely, and many rely excessively on insurance to cover any losses caused by cyber incidents.

A cyber-attack on the payment system potentially could be devastating for individual users and businesses.

For individuals, the risks include data breaches, identity theft, fraud and economic loss, and a form of cyber blackmail called doxing, in which a person's confidential or publicly available personal and financial data are made public for coercive purposes. Businesses are equally at risk, vulnerable not just to potential fraud but also loss of proprietary financial data – and hence, future business opportunities. A debilitating cyber-attack on financial infrastructure, such as banks and payment systems, can lead to economic loss or disruption of service, and potentially even set off a recession, if not mitigated. In 2017, the U.S. consumer credit reporting agency, Equifax, lost more than $3 billion in stock market value after it reported a data breach.[21] Beyond the economic costs, loss of reputation and potential liability are even more serious risks. American insurance company, Anthem, was forced to pay $115 million to settle consumer claims over a 2015 data breach that exposed records of approximately 78.8 million consumers.[22]

For victimised nations, potential risks include economic loss, cyber-enabled espionage (as has been seen in the case of APT30), loss of strategic data, and disruption or degradation of services. Most importantly, such attacks hamper expansion of digital payment systems as they diminish citizens' confidence in them. The volatile security situation around India makes the country particularly vulnerable to such cyber malfeasance by hostile state actors. Bridging these vulnerabilities requires fundamental steps related to information sharing, data protection and reporting of cyber security incidents.

4. The regulatory landscape for digital payments

Indian regulators have implemented several policy measures in response to ever evolving challenges to the security of digital payment systems.

The Information Technology (IT) Act, 2000 (amended in 2008) and the National Cyber Security Policy (NCSP) of 2013 provide the guiding policy framework for cyber security and digital payment systems in India. In 2015, the Indian government created the post of National Cyber Security Coordinator to deal with cyber security issues.[23]

The IT Act and the NCSP have been supplemented by specific guidelines, advisories, technical frameworks and standards from other government bodies and departments focusing on data protection, mobile banking, regulation of mobile wallets, critical infrastructure protection, encryption and crypto-currencies (see Table 4 in the Appendix).

The Reserve Bank of India (RBI), as the principal regulator, has regularly released frameworks, guidelines and advisories for banks and other payment-system operators. It released a Cyber Security Framework for banks in 2016.[24] The framework instructed banks to adopt and implement cyber security policies with emphasis on organisational resilience and cyber hygiene. It also mandated banks to set up a Security Operations Centre (SOC) to detect cyber security incidents and report them to the Indian Banks-Center for Analysis of Risks and Threats (IB-CART), a one-of-its-kind mechanism in India for banks to share threat-related information. Notwithstanding the mandatory requirement of establishing the SOC, many smaller banks are still in the process of doing so.

In 2017, the RBI issued detailed guidelines for the country's 58 mobile wallet operators[25] for ensuring authentication of transactions and prevention of fraud.[26] It also directed these operators to audit their systems annually.[27]

The RBI also has mandated storage of payments data in India.[28] Some payment processors have opposed this provision, claiming it will disrupt their business operations.[29] [30] But senior police officials repeatedly have pointed to India's painful experience obtaining data that is stored outside India.[31] For well-known cyber incident cases such as WannaCry, there has been a seamless exchange of information, but for many daily occurrences of other cyber-crimes, it is difficult to replicate this cooperation. Varying legal practices add another layer of complication, despite the existence of Mutual Legal Assistance Treaties (MLATs).

The RBI is the chief regulator, but several other central government agencies and local units handle various dimensions of the cyber security of digital payments:

- Computer Emergency Response Team-India (CERT-IN) is the chief technical agency to deal with cyber threats. It operates a Botnet Cleaning and Malware Analysis Centre, also known as the Cyber Swachhta Kendra, to detect and prevent spread of malware infections on Indian computer networks.
- The Unique Identification Authority of India collects and manages Aadhaar data.
- The Standardisation, Testing and Quality Certification Directorate, among other things, certifies payment software and hardware for use in India.

- Reserve Bank Information Technology Private Limited, set up in 2017, focuses on cyber security, research, audit and assessment of RBI-regulated entities.
- The Institute for Development & Research in Banking Technology (IDRBT), established in 2014, disseminates information on cyber threats in the banking and financial sector.
- The National Critical Information Infrastructure Protection Centre, set up in 2014, is tasked with managing the cyber security of India's critical infrastructure, including the financial sector.

More specialised agencies are being planned. These include the Indian Cyber Crime Coordination Centre, which will monitor cyber-crimes, and a long-awaited Computer Emergency Response Team for the financial sector (CERT-FIN), which will report to CERT-IN.[32] Establishing CERT-FIN has been difficult as many smaller banks are yet to have Security Operation Centres to enable them to report cyber security incidents to it.

Paralleling regulatory measures on digital payments by the RBI and government, individual banks[33] are moving to comply with globally-accepted industry standards such as the Payment Card Industry Data Security Standard.[34] To secure inter-banking financial transactions, in 2016, SWIFT introduced a Customer Security Programme which focuses on the prevention of cyber-related fraud by improving information sharing within banks.[35] Under this, SWIFT has an advisory to banks, recommending the adoption of 29 rules (19 mandatory and 10 advisory) related to critical hardware, login credentials, incident response and identity management, among others.[36] SWIFT has also introduced a Payments Control Service whereby banks can screen payment instructions for any fraud or unusual activity before they are transmitted to other banks for fulfilling payments.

Yet, information sharing within government agencies, the government and industry remains a challenge. Moreover, India lacks an enforcement mechanism at the government level, and its digital payment industry is not equipped with a dedicated national cyber security incident-reporting platform. The IB-CART, set up for reporting cyber threats, only covers the banking sector. Mobile wallet providers, which constitute a critical and growing part of the financial system, have no dedicated mechanism through which to report cyber security incidents, such as fraud or data breaches, other than to report them to the local police stations, where enforcement and punitive action are weak.[37]

5. Recommendations for securing digital payment systems

India's policy push for digital payments makes it an important global actor in the digital economy. It must put greater emphasis on threat mitigation and vulnerability-patching to ensure resilience of payment systems and a greater level of cyber security.

This requires action on three levels: government, business and diplomatic.

5.1 Government

a. **Make reporting of data breaches mandatory.** Data-breach reporting and vulnerability disclosure currently are voluntary. The government must require industry to report data breaches and cyber security incidents immediately. The requirement can be phased. First, industry should be required to make initial, limited reports to regulators within standard periods of time, laid down in consultation with the financial sector and payments industry. More detailed reporting for release in the public domain can follow, again subject to a time limit decided in consultation with the industry. Additionally, businesses that have previously experienced cyber-attacks should be asked to file regular cyber-security reports to the regulators; for this, an online national reporting platform like the Ministry of Home Affairs' portal for citizen reporting on cyber-crimes will be suitable. Such reporting also can cover industry compliance, along with the multiple advisories and frameworks established by the RBI, CERT-IN and other government agencies.

b. **Expedite creation of CERT for the financial sector.** In the 2017-18 budget, the government announced plans to establish a CERT for the financial sector,[38] but this goal has not yet been realised. The central CERT-IN continues to provide support through its regular advisories, but a specialised, sectoral CERT is urgently needed to generate actionable intelligence on emerging cyber threats proactively, monitor suspicious network activity, identify threat vectors and pinpoint malicious actors.

c. **Adopt a phased approach to local data-storage requirements for the payments industry.** Experience gained in criminal investigations shows Indian regulators and security agencies need to have on-demand and timely access to payment processing-related data whose security is in question. In major cyber-crime cases like the WannaCry ransomware attack, countries have seamlessly exchanged data, but it is difficult to replicate similar cooperation on data exchange involving small-scale cyber crimes, which are equally vicious. Therefore, the government should persist in its demand that the payment industry store its India-related payment data in India, where regulators can get quick access to it. China already has required firms to store data locally. In implementing this recommendation, India should adopt a phased approach in order to ensure compliance. It also should create incentives, such as tax benefits, to encourage the payment industry to store data locally. This ought to be complemented by expeditious implementation of a data-protection legal framework, as proposed by the Justice Srikrishna Data Protection report; this will regulate collection and storage of data as well as define penalties for violations.

d. **Expand cyber hygiene education initiatives.** User awareness of cyber risks is crucial to the prevention of attacks. The government has taken multiple steps on cyber hygiene education, including the Pradhan

Mantri Gramin Digital Saksharta Abhiyan,[39] which is specifically aimed at countering phishing emails and vishing. It is necessary to expand this effort by: (i) focusing on emerging technologies, cloud services, multiple-factor authentication, encryption etc.; (ii) instilling a culture of cyber hygiene and cyber safety (a replicable example is a nationwide school project launched in Italy for digital literacy[40]); and (iii) focusing on information-sharing security practices for government departments in handling data, especially Aadhaar-related data.

5.2 Business (industry)

a. **Create a payment-industry platform for information sharing.** India's banking industry already has IB-CART for sharing information about cyber security incidents among banks. This platform can be extended to enable the entire digital payment industry to share classified, unclassified and open source information on cyber-attacks and threat vectors. The model can be along the lines of the Ministry of Home Affairs' Multi-Agency Centre, which enables security agencies to share counter terrorism-related information on a real-time basis.[41]

b. **Enable consumers to control data through a consent dashboard.** The concept of a consent dashboard, mentioned in the Justice Srikrishna Data Protection report, can be applied in determining how customers use card payment systems. Payment processors like MasterCard, Visa and RuPay can create a dashboard that explicitly identifies websites such as e-commerce sites, where users have saved their card details and other data. An option to manage – review, modify or delete – this data through such dashboards will ensure that consumers have more control over it.[42] This needs to be accompanied with implementation of the 'data minimisation' principle[43] by which companies do not store sensitive data they no longer need and do not give third parties access to it.

5.3 Diplomatic (global)

a. **Negotiate preferential and conditional data-sharing agreements with like-minded countries.** Ensuring cyber-crime investigators timely access to data is critical. Much sharing currently happens bilaterally through Mutual Legal Assistance Treaties or international treaties such as the Budapest Convention on Cybercrime (which India opposes and therefore did not sign).[44] India can explore data-sharing agreements with countries aligned to its cyber diplomacy objectives and its cyber-crime investigations. Such agreements can be similar to the proposed U.S.-UK data-sharing agreement, which will require technology companies based in either country to provide information requested by law enforcement agencies in either the U.S. or UK.[45]

b. **Articulate a normative framework for cyber-attack attribution.** Attributing a cyber attack to a specific actor has technical, legal and political dimensions. In many instances, despite work at technical levels, attribution has not happened at legal and political levels for multiple reasons.[46] India has not yet publicly attributed a cyber attack to a state or non-state actor. However, as the frequency and intensity of cyber attacks from adversarial state actors is soaring, India should explore enunciating the elements of such attribution, like technical analysis of threat vectors, the role of non-state actors and applicable legal frameworks.

6. Conclusion

The expansion of India’s digital economy hinges upon a safe and secure payment system. India is yet to see a major state-sponsored cyber attack on its payment systems, but medium-and small-scale attacks have revealed the potential chinks in its armour. Payment industry players and regulators have over the years sought to patch these vulnerabilities. But if certain fundamental measures related to information sharing, reporting of data breaches, cyber hygiene and data protection are not taken, then ensuring resilience of digital payment systems will remain a difficult proposition. In light of the ever-expanding cyber threat landscape in general, regulators and those operating within the payment industry will need to adopt a proactive approach to identifying threat vectors and malicious actors. Secure digital payment is vital for consumer confidence. If this security concern does not get due attention, expansion of the digital economy will face significant impediments.

7. Appendix

Table 4: Supervisory and regulatory measures for securing the digital payment eco-system in India

Table 4.1: Indian regulations governing digital payments

	Title	Details
Acts and policies	Information Technology Act, 2000 (amended in 2008)	The act is the primary legal framework to deal with Information Technology (IT)-related matters in India. It has provisions on data protection, methods for encryption and information security practices. It also spells out types of offences related to information technology.
	Payment and Settlement Systems Act, 2007	This act provides for the regulation and supervision of payment systems in India, including electronic systems. The Ministry of Finance has proposed to amend the act, taking note of growth in the fintech sector and the expanding role of non-banking institutions in providing payment services.
	National Cyber Security Policy, 2013	The policy provides the overarching regulatory framework for cyber security issues. It has provisions for protection of IT systems, including mobile and payment gateways. The policy advises every organisation to appoint a Chief Information Security Officer for cyber security-related issues.
	Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016	The act spells out various dimensions related to the implementation of Aadhaar-linked subsidies and other government benefit schemes. It also has provisions on the use and protection of personal and biometric information by the Unique Identification Authority.
Draft Bills and policies	Draft National Encryption Policy, 2015 – withdrawn	The draft policy had supported use of cryptography for encrypting transactions and communications for individuals, businesses and government. It was subsequently withdrawn because of its impractical provisions and concerns over privacy.
	Financial Data Management Centre Bill, 2016	The bill proposes establishment of a data centre, which will act as a repository of all financial regulatory data. The centre will provide this data to the Financial Stability and Development Council for further analysis.

Source: Gateway House research, based on data obtained from the respective Indian government agencies

Table 4.1: Indian regulations governing digital payments (Continued)

	Title	Details
Frameworks, guidelines and advisories	RBI Advisory on Virtual Currencies, 2013	The advisory asserts that the creation, trading or use of virtual or crypto-currencies as a medium of payment are not authorised by any central bank or monetary authority. It cautioned about likely financial, operational, legal, customer protection and security-related risks from these currencies.
	NCIIPC Guidelines for the Protection of National Critical Information Infrastructure, 2015	The guidelines lay down the criteria for identifying critical information infrastructure. They enumerate 35 essential controls involving planning, implementation, operations, disaster recovery/business continuity planning and reporting, and accountability for protecting the critical infrastructure.
	CERT-IN Advisory CIAD-2016-0070 Securing Mobile Banking, 2016	The advisory explains various threats to mobile banking and prescribes best practices for mobile phone users to secure their phone and transactions.
	CERT-IN Advisory CIAD-2016-0069 Safeguarding Smart phones against Cyber Attacks, 2016	The advisory describes potential attack vectors for mobile phones and prescribes best practices for users to secure their phones.
	RBI Cyber Security Framework in Banks, 2016	The framework advises banks to implement various cyber-security measures for building organisational resilience, including putting in place a bank board-approved cyber-security policy. It also mandates banks to report cyber incidents to the RBI's Cyber Security and Information Technology Examination cell.
	RBI Master Circular – Mobile Banking transactions in India – Operative Guidelines for Banks, 2016	This circular requires banks to put in place risk mitigation and other measures. It also mandates the use of Two-Factor Authentication (a process where the user authenticates an ongoing payment transaction by providing an additional credential) for mobile-banking transactions.
	RBI Directive on Security and Risk Mitigation measures – Technical Audit of Prepaid Payment Instrument issuers, 2016	It advises Prepaid Payment Instrument issuers to carry out system audits and take appropriate measures against phishing attacks.
	UPI Procedural Guidelines, 2016	The guidelines lay down various security risks in the operation of the UPI and steps to mitigate those risks.

Source: Gateway House research, based on data obtained from the respective Indian government agencies

Table 4.1: Indian regulations governing digital payments (Continued)

	Title	Details
Frameworks, guidelines and advisories	RBI Policy Guidelines on Issuance and Operation of Prepaid Payment Instruments in India, 2017	The guidelines require Prepaid Payment Instrument issuers to put in place appropriate information and data-security infrastructure and systems for authentication of transactions and prevention of fraud. They also require issuers to have information security policies approved by their boards.
	Ministry of Electronics and Information Technology Guidelines for the Chief Information Security Officers (CISOs), 2018	These guidelines illustrate key roles and responsibilities for the CISOs in all the government agencies and private organisations. These focus on cyber hygiene, access management and mapping of organisations' IT networks.
	RBI's Basic Cyber Security Framework for Primary (Urban) Cooperative Banks, 2018	Similar to the 2016 cyber security framework for banks, this framework advises each urban cooperative bank to adopt a cyber security policy approved by its board and a cyber crisis management plan. It also mandates the banks to report all unusual cyber security incidents to the RBI's Department of Cooperative Bank Supervision.
	RBI Directive on Storage of Payment System data, 2018	The directive mandates payment companies to store transaction-related data locally in India to ensure better monitoring. It says that data on the foreign parts of transactions can be stored in the relevant foreign countries.
	RBI notification on prohibition on dealing in Virtual Currencies, 2018	The notification bars entities regulated by the Reserve Bank from dealing in virtual currencies or providing any related services.

Source: Gateway House research, based on data obtained from the respective Indian government agencies

Table 4.1: Indian regulations governing digital payments (Continued)

	Title	Details
Committees	Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (Gopalakrishna Committee), 2011	Its report focuses on the use of IT in the banking sector and recommends various steps concerning IT governance, information security and its audit, IT operations, IT services outsourcing, cyber fraud, business continuity planning, customer awareness programmes and legal issues.
	Committee on Digital Payments (Watal Committee), 2016	Its report proposed structural reforms – legislative and regulatory – for promoting digital payments.
	RBI Inter-disciplinary Standing Committee on Cyber Security, 2017	The committee is mandated to review existing and emerging cyber threats and suggest measures to strengthen cyber security and resilience.
	Working Group on Computer Emergency Response Team in the Financial Sector, 2017	The report of the Working Group discussed cyber threats to the financial sector and modalities of setting up a dedicated CERT unit for the financial sector. It also discusses the criticality of cyber hygiene.
	Committee of Experts to deliberate on a data protection framework (Srikrishna Committee), 2017	This committee, set up by the Ministry of Electronics and Information Technology, focused on protection, processing and storage of data. Its report identified various data protection principles, including the 'right to be forgotten' among others. It also recommended data localisation for critical personal data.
	Committee on Deepening of Digital Payments, 2019	The committee, set up in 2019, reviewed the functioning of digital payment systems in India, and suggested that the government lead the effort on digitisation of payments, expand the payment infrastructure and widen access to digital payments.
Information-sharing mechanism	Indian Banks – Center for Anaysis of Risks and Threats, 2014	Managed by the IDBRT, this centre conducts cyber drills for various banks and trains bank personnel in dealing with cyber-attacks. It also shares and disseminates information associated with the bank's critical infrastructures and technologies.

Source: Gateway House research, based on data obtained from the respective Indian government agencies

Table 4.2: Other extant governing frameworks and standards applicable to digital payments

Measures	Details
SWIFT Customer Security Programme	This programme intends to improve information sharing within the banking industry, enhance SWIFT-related tools for customers and provide a customer security control framework. The framework has mandatory and advisory security controls for SWIFT's customers. Under this, SWIFT has published multiple bulletins, covering cyber prevention and detection measures. Other than this, SWIFT has also introduced in-network payment screening utility, called the Payments Control Service. It enables SWIFT's customers to screen payment instructions before transmission to counterparties, to detect any illicit or unusual message flows. SWIFT has also worked with other stakeholders, such as law enforcement agencies and incident response teams, to ensure rapid identification of financial institutions targeted by cyber criminals.
Payment Card Industry Data Security Standard (PCI-DSS)	PCI-DSS standards lay down technical and operational requirements for payment transactions and for hardware and software used in those transactions.

Source: Gateway House research, based on data obtained from the respective organisations

8. Notes and References

1. Europol, Mastermind behind EUR 1 billion cyber bank robbery arrested in Spain, 26 March 2018, <https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain> (Accessed on 26 January 2019).

2. Advanced Persistent Threat refers to an attack campaign undertaken by cyber saboteurs or hackers to establish an unauthorised and prolonged presence in a network to mine sensitive or confidential data.

3. Fraser, Nalani, Jacqueline O'Leary, Vincent Cannon and Fred Plan, 'APT38: Details on New North Korean Regime-Backed Threat Group', FireEye, 3 October 2018, <https://www.fireeye.com/blog/threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html> (Accessed on 12 January 2019).

4. Perez, Evan, 'FBI arrests Chinese national connected to malware used in OPM data breach', CNN, 24 August 2017, <https://edition.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html> (Accessed on 15 June 2018).

5. Balsamo, Michael, 'China suspected in huge Marriott data breach, official says', Associated Press, 13 December 2018, <https://www.pbs.org/newshour/world/china-suspected-in-huge-marriott-data-breach-official-says> (Accessed on 26 January 2019).

6. National Payments Corporation of India, About us, <https://www.npci.org.in/about-us-background> (Accessed on 19 August 2018).

7. RuPay, Milestones, <https://www.rupay.co.in/milestones> (Accessed on 21 June 2018)

8. Data from the NPCI. See National Payments Corporation of India, Statistics, <https://www.npci.org.in/statistics> (Accessed on 5 February 2019).

9. Patil, Sameer, Partnering for Prosperity: India-Canada Collaboration to Curb Digital Black Markets (Mumbai: Gateway House, Indian Council on Global Relations, 2019), <https://www.gatewayhouse.in/india-canada-digital-black-markets/> (Accessed on 12 March 2019), p. 4.

10. Hitachi, Final investigation report completed; Hitachi Payment Services suffered breach due to sophisticated malware attack in mid-2016, 9 February 2017, <https://www.hitachi-payments.com/src/HPY%20Press%20Release_V9.pdf> (Accessed on 21 June 2018).

11. National Payments Corporation of India, Statement pertaining to press reports on debit card compromise, 20 October 2016, <https://www.npci.org.in/sites/default/files/Statementpertainingtopressreportsondebitcardcompromise.pdf> (Accessed on 15 June 2018).

12. Gopakumar, Gopika and Leslie D'Monte, "How Union Bank was hacked and got its money back", LiveMint, 18 April 2017, <https://www.livemint.com/Industry/xuBJNapRGBrtl05iEAvsYO/How-Union-

Bank-was-hacked-and-got-its-money-back.html> (Accessed on 19 August 2018).

13. Phishing emails are emails which appear to be sent by genuine people or organisations. These emails entice the users to click on a link which will take them to fraudulent websites or to download attachments that install malware or ransomware on their systems, enabling them to harvest personal data or steal login credentials.

14. CNBC-TV18, "City Union Bank cyber attack: Successfully retrieved/block money in 2 out of 3 cases", 19 February 2018, <https://www.moneycontrol.com/news/business/companies/city-union-bank-cyber-attack-successfully-retrievedblock-money-in-2-out-of-3-cases-2510837.html> (Accessed on 26 January 2018).

15. Cosmos Bank, "Official press release regarding the unfortunate attack on the Indian Banking Sector", <https://www.cosmosbank.com/press-release/> (Accessed on 20 August 2018).

16. FireEye, 'APT30 and the Mechanics of a Long-Running Cyber Espionage Operation', April 2015, <https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf> (Accessed on 21 June 2018).

17. FireEye, 'APT38: Un-usual Suspects', <https://content.fireeye.com/apt/rpt-apt38>, (Accessed on 21 May 2019), p. 5.

18. National Crime Records Bureau, Ministry of Home Affairs, Crime in India 2016, <http://ncrb.gov.in/StatPublications/CII/CII2016/pdfs/NEWPDFs/Crime%20in%20India%20-%202016%20Complete%20PDF%20291117.pdf> (Accessed on 19 August 2018).

19. p. 417

20. Ibid, p. 435.

21. Gantz, John F. et al, 'The Dangerous World of Counterfeit and Pirated Software', IDC, March 2013, <https://news.microsoft.com/download/presskits/antipiracy/docs/IDC030513.pdf > (Accessed on 26 January 2019).

22. Eisen, Ben, 'Equifax Loses More Than $3 Billion in Market Value', The Wall Street Journal, 11 September 2017, <https://blogs.wsj.com/moneybeat/2017/09/11/equifax-loses-more-than-3-billion-in-market-value/> (Accessed on 26 January 2018).

23. Pierson, Brendan, 'Anthem to pay record $115 million to settle U.S. lawsuits over data breach', Reuters,

24 June 2017, <https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML> (Accessed on 25 December 2018).

24. The National Cyber Security Coordinator reports to the National Security Advisor in the Prime Minister's Office.

25. Reserve Bank of India, 'Cyber Security Framework in Banks', 2 June 2016, <https://www.rbi.org.in/

scripts/BS_CircularIndexDisplay.aspx?Id=10435> (Accessed on 26 January 2018).

26. As of 29 March 2019, there are 58 mobile wallet operators in India.

27. Reserve Bank of India, 'Master Direction on Issuance and Operation of Prepaid Payment Instruments',

25 February 2019, <https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11142> (Accessed on 12 March 2019).

28. Reserve Bank of India, 'Security and Risk Mitigation measure - Technical Audit of Prepaid Payment Instrument issuers', 9 December 2016, <https://www.rbi.org.in/Scripts/BS_CircularIndexDisplay.aspx?Id=10772> (Accessed on 21 June 2017).

29. Reserve Bank of India, 'Storage of Payment System Data', 6 April 2018, <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0> (Accessed on 12 March 2019).

30. Kalra, Aditya, 'Exclusive: U.S. senators urge India to soften data localisation stance', Reuters, 13 October 2018, <https://in.reuters.com/article/india-data-localisation/exclusive-u-s-senators-urge-india-to-soften-data-

31. localisation-stance-idINKCN1MN0CJ> (Accessed on 25 December 2018).

32. Goel, Vindu, 'U.S. Credit Card Giants Flout India's New Law on Personal Data', The New York Times, 15 October 2018, <https://www.nytimes.com/2018/10/15/technology/visa-mastercard-amex-india-data-law.html> (Accessed on 25 December 2018).

33. Patil, Sameer, Interviews with Indian police officials, Mumbai, June 2017 and January 2019

34. Department of Economic Affairs, Ministry of Finance, Press Release on the Report of the Working Group for setting up Computer Emergency Response Team in the financial sector, 30 June 2017, <http://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf> (Accessed on 25 December 2018).

35. For example, the largest state-owned Indian bank, State Bank of India conducts regular information system and cyber security auditing of its IT systems. It has relocated its SWIFT centres in London and New York to India for better oversight and supervisory control. Similar auditing steps have been taken by the major private sector bank, ICICI Bank. It has also established 24x7 monitoring and surveillance of systems for any suspicious network activity. See State Bank of India, Building momentum for a transforming India: Annual Report 2017-18, 22 May 2018, <https://www.sbi.co.in/AR1718/assets/PDF/English/SBI-AR_2017-18.pdf> (Accessed on 12 March 2019), p. 54 and ICICI Bank, Partnering a dynamic India: Annual Report 2017-18, 7 May 2018, <https://www.icicibank.com/managed-assets/docs/investor/annual-reports/2018/annual-report-fy2018.pdf> (Accessed on 12 March 2019), p. 101.

36. Payment Standards Council, Maintaining payment security, <https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security> (Accessed on 25 December 2018).

37. SWIFT, "Customer Security Programme", <https://www.swift.com/myswift/customer-security-programme-

38. csp> (Accessed on 19 July 2019)

39. SWIFT, "Payment Controls", <https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/fraud-control/payment-controls> (Accessed on 19 July 2019)

40. National Crime Records Bureau, p. 435.

41. Department of Economic Affairs, Ministry of Finance, p. x.

42. Ministry of Electronics and Information Technology, Objective, <https://www.pmgdisha.in/about-pmgdisha/> (Accessed on 25 December 2018).

43. Livesay, Christopher, "Italy takes aim at fake news with new curriculum for high school students", National Public Radio, 31 October 2017, <https://www.npr.org/2017/10/31/561041307/italy-takes-aim-at-fake-news-with-new-curriculum-for-high-school-students> (Accessed on 25 December 2018).

44. This sharing happens virtually through a classified network as well as physically with daily meetings between concerned security agencies. Experience suggests that the daily meetings help to develop a rapport between the concerned officials, facilitating synergy between different agencies.

45. Ministry of Electronics and Information Technology, A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians: Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 2018, <https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> (Accessed on 12 March 2019), p. 38.

46. Warner, Mark R., Sen. Warner on Marriott Data Breach, 30 November 2018, <https://www.warner.senate.gov/public/index.cfm/2018/11/sen-warner-on-marriott-data-breach> (Accessed on 25 December 2018).

47. On India's position on Budapest Convention, see appendix 3 in Patil, Sameer et al, India-EU cooperation on cyber security and data protection, (Mumbai: Gateway House, Indian Council on Global Relations, 2016), <https://www.gatewayhouse.in/wp-content/uploads/2016/12/EU-India-Security-Dialogue-Cyber-Security.pdf> (Accessed on 21 June 2018), p. 20.

48. Nakashima, Ellen and Andrea Peterson, 'The British want to come to America — with wiretap orders and search warrants', The Washington Post, 4 February 2016, <https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america--with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html?utm_term=.f66aca6a387a> (Accessed on 12 March 2019).

49. Remarks by Marina Kaljurand, former Foreign Minister of Estonia, at the Globsec 2018 Bratislava Forum, 18 May 2018

9. Bibliography

Department of Economic Affairs, Ministry of Finance, Report of the Committee to study the Financial Data Management Legal Framework in India, 25 October 2016, <https://dea.gov.in/sites/default/files/FDMC%20Report%20along%20with%20draft%20bill_0.pdf> (Accessed on 12 March 2019).
Dejey and S. Murugan, Cyber Forensics, (New Delhi, Oxford University Press, 2018).

Gandhi, R., 'Evolution of Payment Systems in India: Or is it a Revolution?', Reserve Bank of India, 10 November 2016, <https://www.rbi.org.in/scripts/BS_ViewBulletin.aspx?Id=16563> (Accessed on 26 January 2018).

Gomzin, Slava, Hacking Point of Sale (New Delhi, Wiley, 2014).

Gulati, Ved Prakash and Shilpa Srivastava, Financial Technology Management, (Hyderabad, The Icfai University Press, 2008), Vols. I, II and III.

Khan, Harun, 'Customising Mobile Banking in India: Issues and Challenges', Reserve Bank of India, 11 October 2012, <https://www.rbi.org.in/Scripts/BS_ViewBulletin.aspx?Id=13650> (Accessed on 26 January 2018).

NITI Aayog, Digital Payments: Trends, Issues and Opportunities, July 2018, <https://niti.gov.in/writereaddata/files/document_publication/DigitalPaymentBook.pdf> (Accessed on 25 December 2018).

Reserve Bank of India, Report of the High Level Committee on Deepening of Digital Payments, May 2019, <https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/CDDP03062019634B0EEF3F7144C3B65360B280E420AC.PDF> (Accessed on 2 June 2019).

Reserve Bank of India, Payment and Settlement Systems in India: Vision – 2019-2021, 15 May 2019, <https://www.rbi.org.in/Scripts/PublicationVisionDocuments.aspx?Id=921> (Accessed on 2 June 2019).

Swire, Peter and Justin Hemmings, 'Recommendations for the Potential U.S.-U.K. Executive Agreement Under the Cloud Act', Lawfare, 13 September 2018, <https://www.lawfareblog.com/recommendations-potential-us-uk-executive-agreement-under-cloud-act> (Accessed on 25 December 2018).