www.pwc.in

Securing the cashless economy

ASSOCHAM
INDIA

pwc

Message from PwC

Sivarama Krishnan
Leader, Cyber Security
PwC India

Cyber security—the protection of valuable intellectual property, business information and financial transactions in digital form against theft and misuse—is an increasingly critical issue. Given the increasing pace and complexity of threats and the clear focus on realising a more cashless economy, we must adopt approaches to cyber security that will require much more engagement from the industry, academia, governments, security establishments and civil society to protect critical business information without constraining innovation and growth.

Until now, cyber security has been treated primarily as a technology issue. This has to change. With technology traversing industries, organisations and indeed governments, it can no longer be just be a technology issue.

Innovation, disruption and technological advancement are constantly changing our lives. More sophisticated threats and attacks are being unleashed, with the same technology being exploited to bring individuals, organisations, governments—and indeed nations—to their knees. The need of the hour is a comprehensive, progressive and forward-looking cyber security strategy at the national level which bridges people, processes and technology, and requires us to deal with questions of technology, law and privacy.

As the nation stands at the cusp of a digital revolution, our work as technologists, strategists and captains of industry is clearly cut out. We need to focus on the basics that will help keep the growth story on course and ensure that India adopts the right cyber security stance.

As more value migrates online and corporations adopt more innovative ways of interacting with customers and other partners, the cyber security challenge will only become more complex. Through this knowledge paper, we have tried to highlight areas that needs to be re-examined. When addressed properly, these areas shall help us protect interconnected systems and assist organisations in India in building strong defences against cyberthreats, thus fostering organisational growth in this digital age.

Message from ASSOCHAM

Babu Lal Jain
Co-Chairman ASSOCHAM
National Council on Cyber Security

I am pleased to announce that ASSOCHAM is organising a workshop on 'Securing the cashless economy' with participation from the Government, leading industry experts and other key stakeholders.

Post-demonetization, all forms of digital payments have achieved record numbers of transactions. This is certainly a positive signal if we intend to move towards a cashless economy. But the speed of technological development and its integration into our economy far supersedes the speed of defence mechanisms that can mitigate cyberattacks. Today, cyber security is reactive in nature, which brings in the fundamental question of safety on the new payment platforms.

Cyber security is an evolving challenge. Companies, customers, and the government must collectively participate to mitigate cyberattacks and minimise their damage.

Globally, most countries are facing a shortage of professionals with the expertise, training and motivation needed to deal with cybercriminals, and India is no exception. What we urgently need is serious effort in capacity building and setting up high-end cyber labs that are capable of critically inspecting every IT component before these are deployed in critical infrastructure across industry sectors.

Our prime minister recently asked people to embrace the digital cashless world, reiterating that digitisation of economic activities is here to stay. We all share a collective responsibility of building a safe and secure digital infrastructure.

I hope the workshop is a great success.

Message from ASSOCHAM

D. S. Rawat
Secretary General
ASSOCHAM

The demonetisation initiative of the Government of India is likely to increase the speed of development and deployment of digital services, thus enabling the transition towards a cashless economy. With Digital India, the foundation for transforming India into a digitally empowered and knowledge economy has been laid.

There is an ever-growing threat to the economy, financial sector, key government departments and infrastructure set-up, which in turn leaves internal security at risk. Therefore, ASSOCHAM believes that our Hon'ble Prime Minister's vision of a cashless economy can only be truly fulfilled with adequate measures for cyber security.

We at ASSOCHAM have been discussing and deliberating with the concerned authorities and stakeholders on the need for security compliance and a legal system for effectively dealing with internal and external cyber security threats.

ASSOCHAM is privileged to be a member of the Joint Working Group on Cyber Security set up by the National Security Council Secretariat (NSCS), Government of India, a member of the Cyber Regulation Advisory Committee and of the Joint Working Group on Digital India—both of which were set up by the Ministry of Communications and IT, Government of India.

ASSOCHAM is committed to creating more awareness about cyber-related issues and this background paper, jointly prepared by PwC and ASSOCHAM, is a step in that direction. We congratulate the team on their efforts.

Finally, we convey our best wishes for the success of the ASSOCHAM Workshop on 'Securing the cashless economy' and hope that it provides more insight into the emerging cyber-related challenges and appropriate solutions for further securing cyberspace.

Securing the cashless economy

'We carried out a secret operation [demonetisation]; it was 10 months of work involving printing new notes and announced it on November 8.'

– PM Narendra Modi at the foundation stone laying ceremony of the greenfield airport at Mopa plateau in Goa (November 2016).

Introduction

The recent demonetisation move has had a huge impact on various sectors of the Indian economy and has significantly impacted the way people transact in daily life. From midnight of 8 November 2016, 500 INR and 1,000 INR notes ceased to be considered as legal tender. While the government's aim was to prevent the counterfeiting of currency, black money, tax evasion and terrorism funding, demonetisation also had an impact on the way people bank in India.

Clearly, the step involved a lot of planning and entailed measures that were taken under utmost secrecy. However, with the announcement coming into effect, 86% of the total currency (amounting to 14 trillion INR) in circulation was abruptly revoked from the economy. [1] In addition, restrictions were imposed on the amount which customers could withdraw and deposit through platforms such as bank branches and ATMs.

After the announcement of demonetisation, multiple guidelines were issued by RBI. Banks had to implement changes such as setting withdrawal limits, changes to cash management applications, core banking applications, coupled with the ability to report additional data to the regulators. Banks also had to push system integrators to incorporate these changes in the various systems such as core banking systems, ATM switches and cash inventory management overnight.

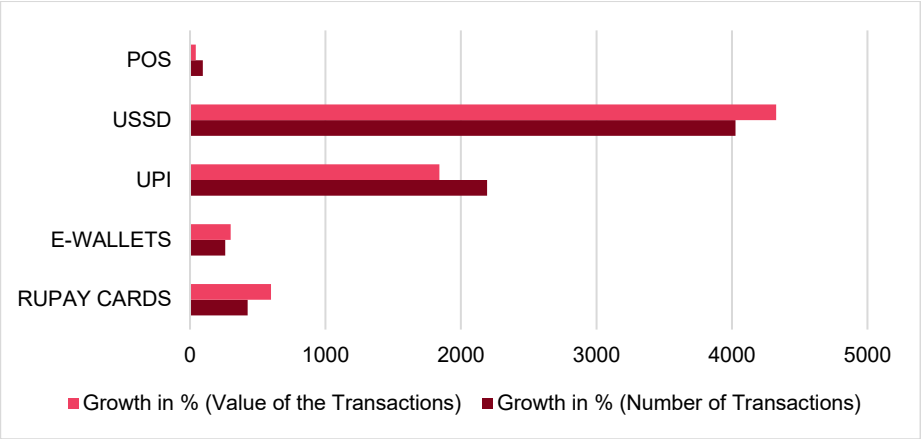
The ATM has been the key enabling technology for dispensing funds. Due to the change to note dimensions, recalibrating the machines and making them operational became the need of the hour. Because this was a covert operation, the ATM supporting industry was unable to recalibrate machines overnight. Further, more than two lakh ATMs across the country had to be recalibrated with the help of just a few thousand technicians. The fact that only a few machines were up and running, together with low cash availability, led to a domino effect. The entire population faced a severe cash crunch, which led to banks and ATMs being thronged by customers. The replacement of old notes took longer than expected, and hence, routine low-value transactions were severely affected.

Simultaneously, replacing a large amount of cash over a 50-day period put humongous pressure on the banking system. This led to the adoption of alternative technology platforms. As a result, both the number and value of transactions through these platforms saw a huge surge. For example, the value of transactions through e-wallets witnessed 301% growth during the period from 8 November to 27 December 2016. The number of transactions through POS saw a massive 95% increase during the same period. Further, the number of transactions through RuPay cards shot up by 425%.[2] The government also announced some incentives for going cashless. For example, it was announced that no service tax will be charged on digital transactions up to 2,000 INR. Digital payments made for buying petrol and diesel were given a discount of 0.75%. The suburban railway network also announced a discount of up to 0.5% to customers for monthly or seasonal tickets booked through digital transactions. In addition, life and general insurance policies and renewal premiums on public sector undertaking (PSU) insurers' websites provided an 8% and 10% discount, respectively. For payments at toll plazas on national highways using RFID card/Fast Tags, a discount of 10% was made available to users in the year 2016-17.

[1] *http://www.business-standard.com/article/economy-policy/86-of-currency-by-value-in-india-are-of-rs-500-rs-1-000-denominations-116110801416_1.html*

[2] *Ministry of Electronics and Information Technology*

% Growth inDigital Transactions



Comparative analysis of digital payments during the demonetisation phase (8 November 2016 to 27 December 2016)

	Number of transactions per day		Value of transactions per day (in INR)	
Platform	08 Nov 16	27-Dec-16	08-Nov-16	27-Dec-16
RuPay cards	3.8 lakhs	20lakhs	39.17 crore	274 crore
E-wallets	22 lakhs	79 lakhs	88 crore	353 crore
UPI	3,721	85,283	1.93 crore	38 crore
USSD	97	4001	1 lakh	49 lakhs
POS	50.2 lakhs	98.1 lakhs	1,221 crore	1751 crore

Source: Ministry of Electronics and Information Technology

By 30 December 2016, old 1,000 INR and 500 INR notes worth around 13 lakh crore INR were deposited back in the banking system. However, the rate at which new notes were infused into the economy was much lower. Clearly, the shortage of notes has led to people considering cashless avenues for transactions. Although the journey to creating a cashless economy remains an ongoing one, there have been several milestones along the way, led by RBI and supported by banks and the other players in the financial infrastructure system.

The government has been consistently investing in various reforms for greater financial inclusion. Therefore, after the demonetisation move, the economy was ready with the infrastructure required to take the leap towards a cashless society. During the last few years, initiatives such as Jan Dhan accounts, Aadhaar-enabled payment system, e-wallets and National Financial Switch (NFS) have cemented the government's resolve to go cashless.

On its part, RBI along with National Payments Corporation of India (NPCI) leveraged technology and introduced newer avenues for banking with the overall objective of improving customer experience, security and ease of transactions. The evolution of India's financial infrastructure can be divided into three phases:

1 First phase of technology initiatives

- 1984: Introduction of Magnetic Ink Character Recognition (MICR) technology
- 1987: First ATM installed in Kolkata
- 1988: Computerised settlement operations at clearing houses of RBI
- 1998–2000: Core banking software

2 Second phase of technology initiatives

- 2001: Internet banking
- 2004: National Financial Switch (NFS)
- 2004–2005: Real Time Gross Settlement (RTGS), National Electronic Funds Transfer (NEFT)
- 2007 : Mobile banking
- 2008: Cheque truncation systems

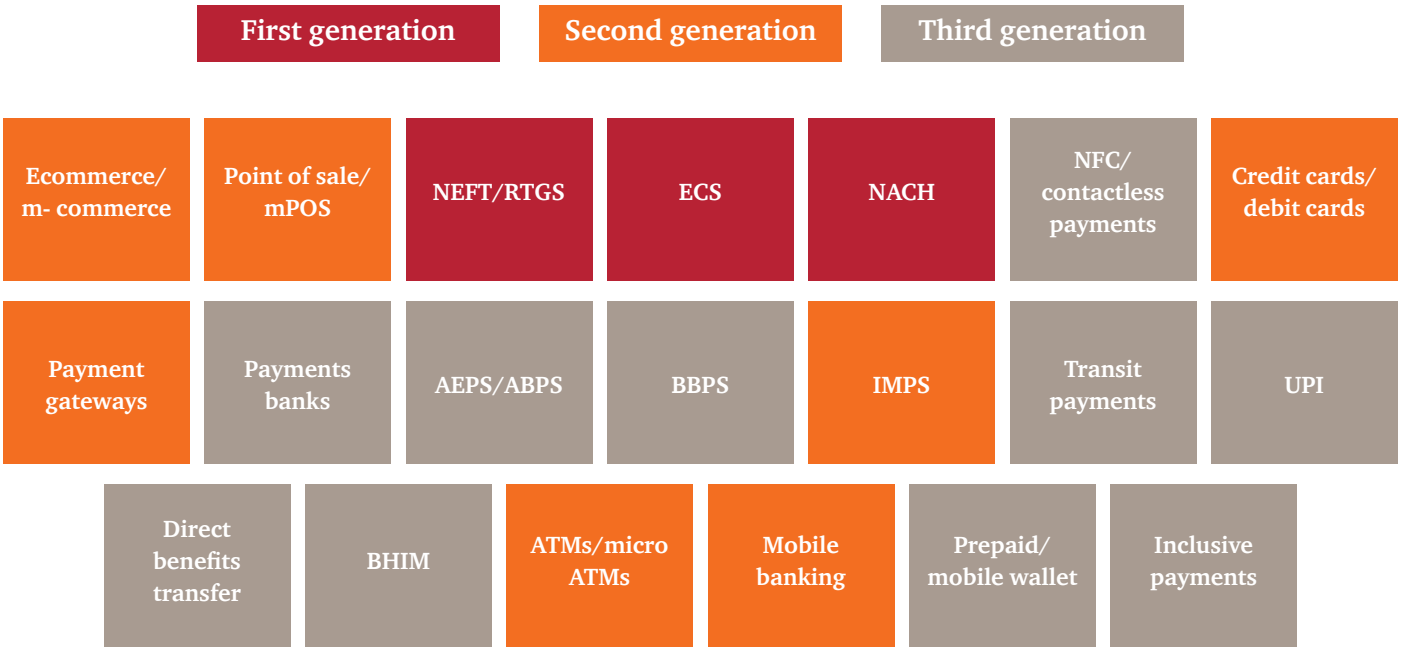
3 Third phase of technology initiatives

- 2010: Immediate Payment Service (IMPS)
- 2012: Adoption of ISO 20022 messaging standard in the Next Generation RTGS (NG-RTGS) system
- 2014: Jan Dhan Yojana, National Unified USSD Platform, RuPay Card, Bharat Bill Payment System (BBPS)
- 2016: Unified Payment Interface (UPI), payment banks, mobile wallets,
- 2017: Bharat Interface for Money (BHIM) app

'Scrapping these notes has opened other avenues to make payments. Download apps of banks and e-payment options. Shopkeepers can keep card swiping facilities and everyone can ensure they pay safe using their credit and debit cards. If not a 100% cashless society, I request you to make India "less-cash society".'

– PM Narendra Modi during his address to the nation on 27 November 2016

Three generations of digital payments



With the evolution of the financial infrastructure ecosystem, the digital platforms available for payments have been transformed. Financial inclusion has gained prominence as the banking system flourished and various platforms were adopted in India.

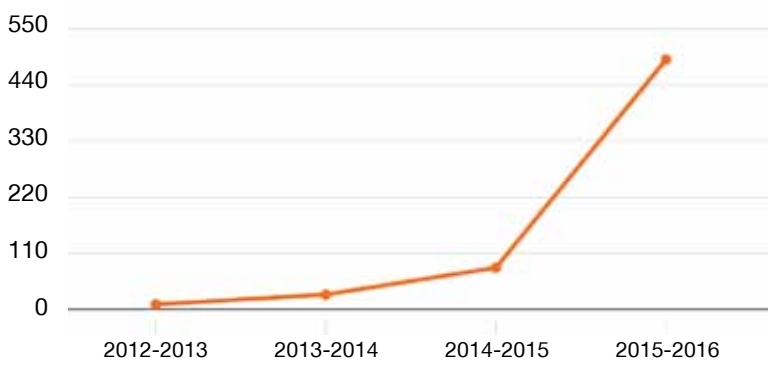
With the rise of technology in the financial infrastructure ecosystem came a greater flow of funds. Today, financial inclusion is seen as a realistic dream because of mobile and smartphone penetration across the country.

According to TRAI, as on 30 September 2016, 82 out of 100 citizens in India owned a mobile phone. The evolution of the telecom ecosystem has occurred at an opportune time, given that call and data rates are decreasing significantly, along with the prices of smartphones, further propelling the shift to a cashless society. Also, initiatives like USSD and the *99# service have ensured that non-smartphone users are also on board the cashless wave.

Demonetisation has given an impetus to e-wallet services. Mobile wallets have witnessed a massive rise in app downloads. With programmes for financial inclusion, digitisation of the economy and increased use of smartphones, online transactions are already quite popular among the urban Indian population. The result has been that leading mobile wallets have witnessed growth of upwards of 100% in app download numbers and have similarly seen an increase of upwards of 400% increase in wallet recharges.

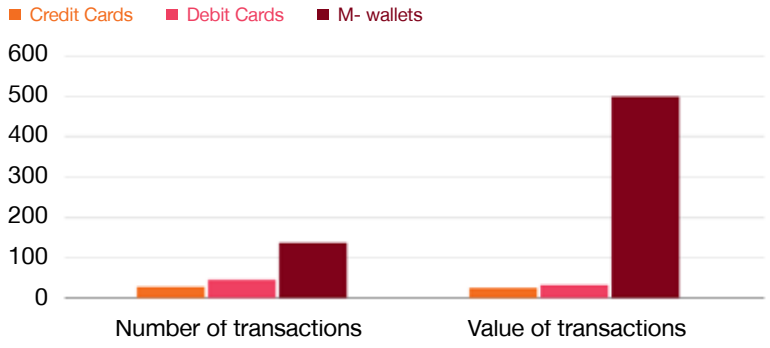
This smartphone revolution has led to the emergence of e-commerce, m-commerce and other services, including app-based cab aggregators, who encourage digital payments for use of various services. The value-added services such as cashback, bill payment facilities, loyalty points, rewards and ease of use have promoted increased usage of such digital platforms.

Transactions carried out through mobile wallets (Rs, billion)



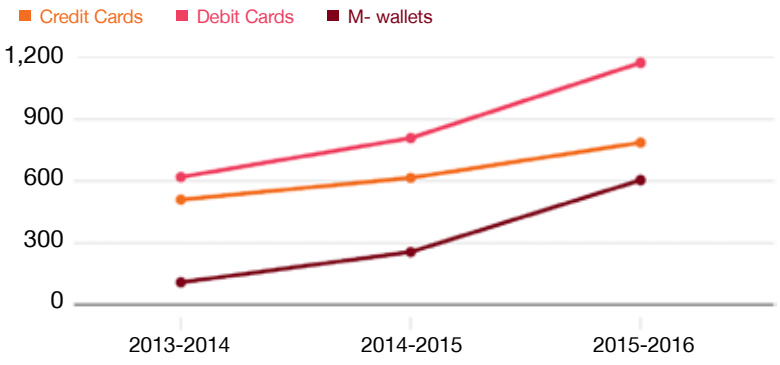
Data: Reserve Bank of India

Growth of different payment methods between 2014-2016(%)



Data: Reserve Bank of India

Number of transactions *(in millions)*



Data: Reserve Bank of India

3X increase in the download of a leading mobile wallet app within 2 days of the demonetisation announcement

1 million: Number of newly saved credit and debit cards within two days of demonetisation announcement

100%: Day-on-day growth in customer enrolment with leading mobile wallets after demonetisation

30%: Increase in app usage and 50% increase in the download of wallets backed by leading banks

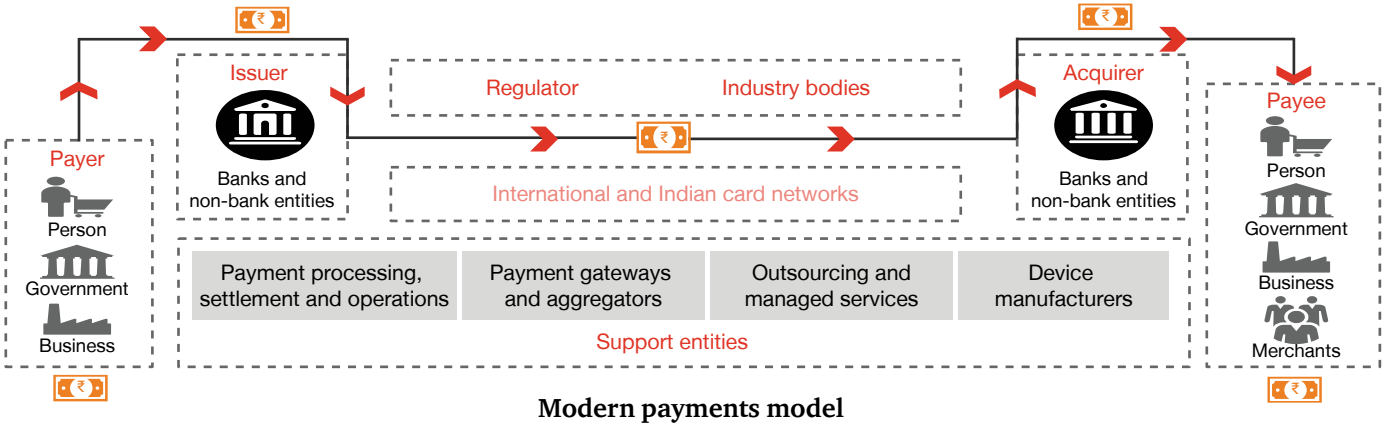
Given the changes initiated by the government, the steps taken by RBI and the digital channels that have opened up, the entire financial ecosystem in India has changed. While traditional brick and mortar banks and banking operations will still be relevant, it is important to note that a shift of value to digital platforms is already occurring and is set to increase. These developments have given rise to a modern payment model.

[3] *http://www.trai.gov.in/WriteReadData/PressRealease/Document/Press_Release_120_30_12_2016.pdf*

Modern payment model

The financial infrastructure ecosystem is no longer closed due to the inclusion of more players like payment networks and digital platforms. The issuers will be banks and other financial institutions providing wallet services and acquirers will be service providers who will receive payments on behalf of the issuers.

Flexibility of transacting will be a critical success factor for all the digital platform service providers in order to ensure and enhance customer experience. With the emergence of e-KYC, it is no longer necessary to know your customer/payer physically as the payments model has evolved to beat limitations related to physical presence. Due to the emergence of new players, the payments ecosystem has become less of a 'physical presence required' banking and more of a 'faceless' payments ecosystem. Ecosystem players will continue to emerge in the modern payments model. The payer and payee can perform transactions through endpoints like smartphones and tablets. That being said, interoperability has become realistic due to payment gateways and aggregators.



Modern payments model

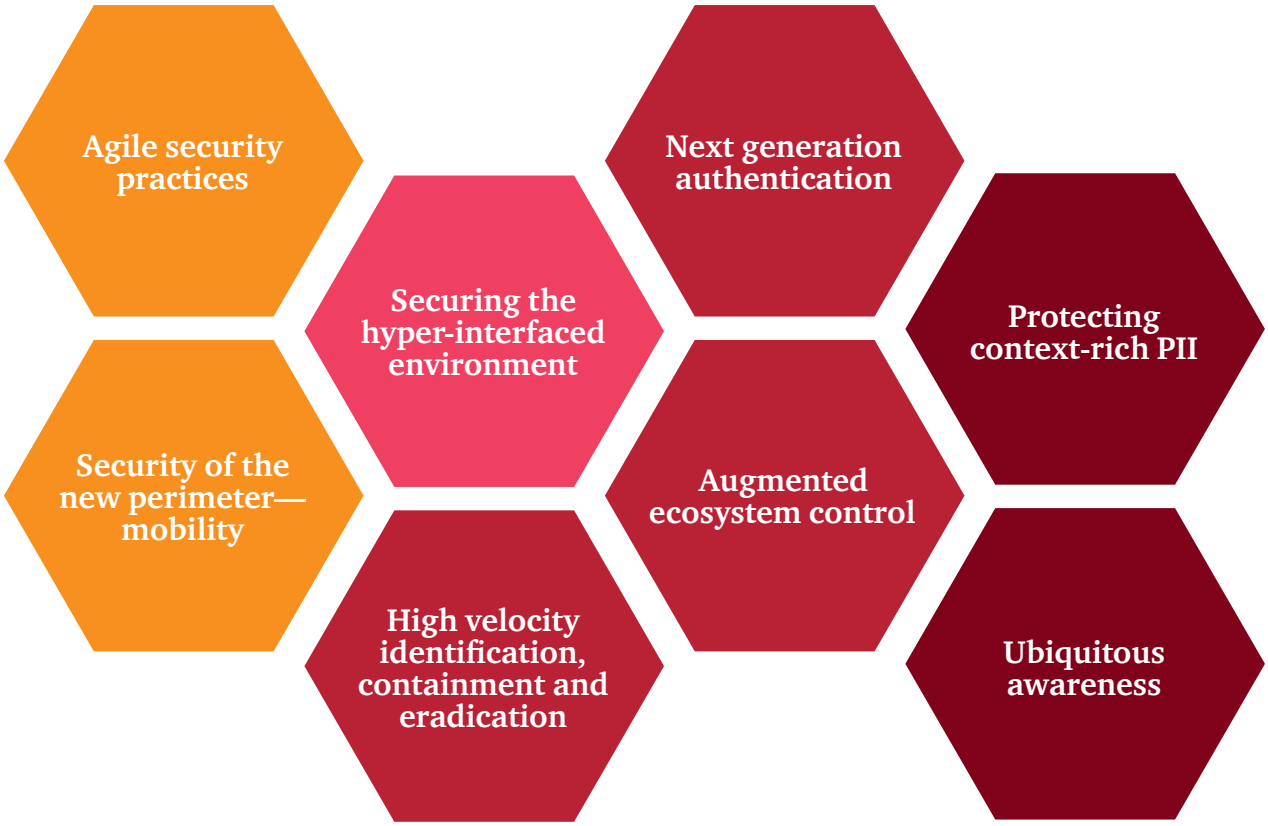
During this speech at the Global Citizen Festival (19 November 2016), Prime Minister Modi referred to the classic song by Bob Dylan: 'We better get out of the way as indeed the times they are a changing.' Thus, it is quite clear that the cashless economy is very much a thing of the near future in the Indian economy.

Security in Cashless Economy

With more platforms being included in the banking ecosystem, the sources of transaction origination will see a significant increase, which means cyberthreats will continue to evolve. Moreover, cyberthreats will only rise as India is seeing a shift towards a cashless economy. With more time to detect and time to respond to these attacks, the return on investments for cyberattacks is greater in emerging markets like India as compared to developed markets like the US.[4] The types of cyber security incidents such as phishing, scanning, website intrusions and defacements, virus code and denial of service attacks will continue to grow.

As the country is experiencing a digital revolution, the impact of this transformation makes it imperative for financial service players to revisit their cyber security resilience. The number of incidents occurring in banking systems has increased in the last five years. In the month of October 2016, an ATM card hack hit Indian banks, affecting around 3.2 million debit cards.[5] Hence, efforts are needed to enhance cyber security as businesses and citizens embrace this new digital wave.

Undoubtedly, for the players in the financial services ecosystem, it's not business as usual. A collective effort is needed to ensure preparedness for the new cashless economy. We believe that the areas below will have to be re-examined to ensure adaptive and real-time cyber defence. While data will be at the core, the network perimeter will extend to end devices. Faster development will demand agile security. More intelligent transaction monitoring will have to be carried out as part of continuous surveillance. Crisis response and recovery strategies will have to step up along with the increased digital footprint. Security awareness of all the stakeholders will be a vital pillar of a secure cashless society.



[4] As per data collected by CERT-In, cyber security incidents are seeing a steady rise, with a total of 39,730 incidents reported in the first 10 months of 2016, as against 44,679 and 49,455 observed during the years 2014 and 2015 respectively.

[5] http://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms

1. **Agile security practices:** For financial services players, faster development and roll-out of the services will be a critical success factor. Accordingly, all technology development and refresh will be delivered using an agile development framework. Security in this context can no longer be a standalone post-facto toll gate. Security assessment and **testing will need to be embedded into the agile development life cycle.** Agile security testing methods based on **automation will have to be adopted**. In many ways driving, a paradigm shift is needed in the way security testing is undertaken today.

2. **Securing the hyper-interfaced environment:** The new era will call for hyper-interoperability across different value chain players. In order to enable this, each ecosystem player will need to create multiple application programing interfaces (APIs). While this will deliver a seamless experience to customer, there is also a risk of malware injection through such APIs. With faster proliferation of interfaces, **protecting APIs will become critical to ensure malware and persistent threats do not propagate** through such untrusted/ untested APIs.

3. **Next generation authentication:** In the new cashless world, frauds will be driven mainly by impersonation and will become a daily affair. Accordingly, the need for stronger authentication of transactions will gain significance. The current techniques of authentication based on location and timing will no longer be adequate. **Adaptive authentication will need to be embedded into the heart of transaction** processing. Next generation authentication will use triangulation techniques while considering larger data sets including the nature of transaction, merchant type and transaction channel.

4. **Protecting context-rich personally identifiable information (PII):** The new generation data marts will not be limited to traditional transactions and account-related information but will have enriched data insights such as spending patterns, patterns of digital platform usage, preferences and other person-specific information sets. In an integrated ecosystem, such data sets may be stored, transferred or shared with third parties for revenue generation opportunities. Both regulators and organisations will be obligated to invest in strong processes and technology to prevent the misuse of context-driven rich PII. While traditional controls such as data masking and encryption will need to be enhanced, **capabilities to hunt down any misuse of PII** will have to be built by organisations.

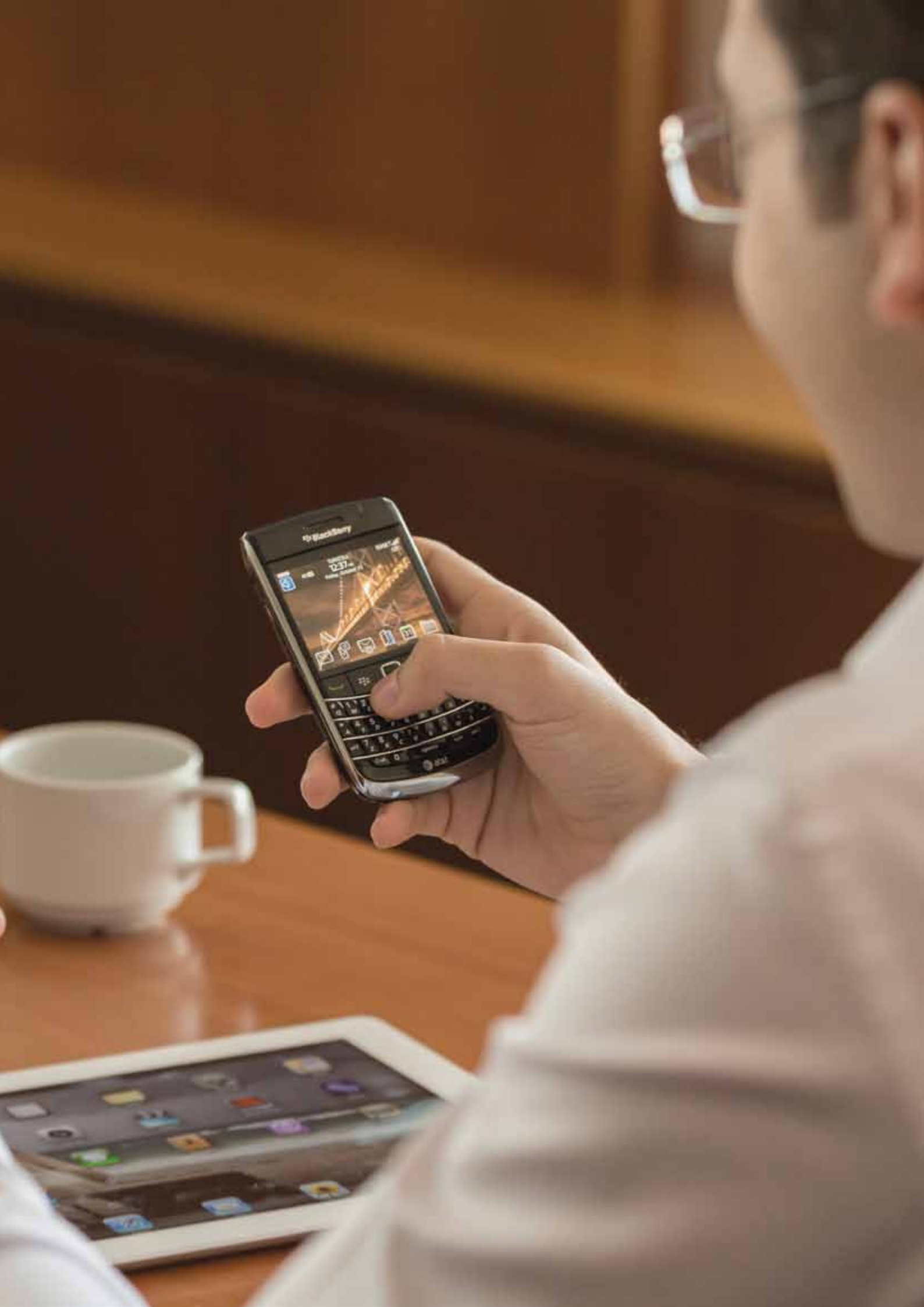
5. **Security of the new perimeter—mobility:** In the new digital/ cashless economy, mobility-based solutions will continue to gain prominence and, hence, security concerns will no longer be limited to the organisation architecture boundaries. Mobility will form a new perimeter of the organisation. In order to ensure endpoint **security containerised apps with built-in advanced persistent threat (APT)** capabilities will have to be developed. Controls for in memory data and additional controls like device certification will be considered. To ensure security of data in endpoints, there may be a requirement for guidelines to define the kind of sensitive data that end devices retain. Hence, the next generation financial infrastructure may involve the adoption of **advanced end-user device management solutions.**

6. **High velocity identification, containment and eradication:** Each consumer today is using multiple platforms and using services across the ecosystem. Any threat that impacts such a user can potentially proliferate and bring the entire financial services ecosystem to a standstill. As the ecosystem continues to be interconnected and overlapping, **cybercriminals will try to exploit possible lapses** and, hence, strategies need to be built to deal with such eventualities. Given this interdependence on the all the players of the financial ecosystem, it becomes crucial to **identify any anomaly at a pace which mirrors real time or near real time.** Once an anomaly is identified, containing it is of paramount importance before it spreads and crosses a point where the damages have transcended organisational boundaries and services. Response strategies will have to be quick and customised to meet various incident scenarios based on situational awareness. Further, these strategies will have to be orchestrated across own infrastructure and encompass various digital partners and other stakeholders.

7. **Augmented ecosystem control:** The new age enterprises will adopt the cloud for faster roll-out and to address non-linear growth. Technology partners could include start-ups, garage shops and large conglomerates, who come together to deliver end products. **The security boundaries of the various players will be extended to end users, third parties and other ecosystem partners.** Security controls will no longer be defined in contracts limited to uptime and resolution of vulnerabilities, but will actually be embedded in the partner ecosystem. The process for monitoring of parameters will also have to be integrated with the company's incident response framework.

8. **Ubiquitous awareness:** TThe cashless economy means that the stakeholder community will now not just be limited to internal stakeholders but will also include external as well as peripheral stakeholders (like merchants). With the influx of first-time users, users from various linguistic ethnic groups and users of different channels, the soft targets will be multifold. **The awareness theme for tomorrow will thus be multichannel, multilingual and multicultural**, and hence go beyond the scope of traditional programmes. Regulators may have to start thinking across industries and develop awareness programmes that addresses this need. Social media can be a key enabler to propagate awareness.

In conclusion, cyber security will continue to be a type of asymmetric warfare: Each organisation will face a multitude of cyber adversaries, and their ranks will grow and become more sophisticated. The new reality is that cyberattackers are sufficiently capable and motivated to break through the defences. Hence, organisations will have to develop novel preventive control mechanisms and significantly invest in reactive capabilities. We believe mastering the areas highlighted above will help financial services companies reach the forefront of the industry. This is because incorporating a more agile cyber risk management approach may enable them to more effectively harness the ongoing digital revolution to their advantage.



About ASSOCHAM

The Knowledge Architect of Corporate India

Evolution of Value Creator

ASSOCHAM initiated its endeavour of value creation for Indian industry in 1920. Having in its fold more than 400 Chambers and Trade Associations, and serving more than 4,50,000 members from all over India. It has witnessed upswings as well as upheavals of Indian Economy, and contributed significantly by playing a catalytic role in shaping up the Trade, Commerce and Industrial environment of the country.

Today, ASSOCHAM has emerged as the fountainhead of Knowledge for Indian industry, which is all set to redefine the dynamics of growth and development in the technology driven cyber age of 'Knowledge Based Economy'.

ASSOCHAM is seen as a forceful, proactive, forward looking institution equipping itself to meet the aspirations of corporate India in the new world of business. ASSOCHAM is working towards creating a conducive environment of India business to compete globally.

ASSOCHAM derives its strength from its Promoter Chambers and other Industry/Regional Chambers/Associations spread all over the country.

Vision

Empower Indian enterprise by inculcating knowledge that will be the catalyst of growth in the barrierless technology driven global market and help them upscale, align and emerge as formidable player in respective business segments.

Mission

As a representative organ of Corporate India, ASSOCHAM articulates the genuine, legitimate needs and interests of its members. Its mission is to impact the policy and legislative environment so as to foster balanced economic, industrial and social development. We believe education, IT, BT, Health, Corporate Social responsibility and environment to be the critical success factors.

Members – Our Strength

ASSOCHAM represents the interests of more than 4,50,000 direct and indirect members across the country. Through its heterogeneous membership, ASSOCHAM combines the entrepreneurial spirit and business acumen of owners with management skills and expertise of professionals to set itself apart as a Chamber with a difference.
Currently, ASSOCHAM has more than 100 National Councils covering the entire gamut of economic activities in India. It has been especially acknowledged as a significant voice of Indian industry in the field of Corporate Social Responsibility, Environment & Safety, HR & Labour Affairs, Corporate Governance, Information Technology, Biotechnology, Telecom, Banking & Finance, Company Law, Corporate Finance, Economic and International Affairs, Mergers & Acquisitions, Tourism, Civil Aviation, Infrastructure, Energy & Power, Education, Legal Reforms, Real Estate and Rural Development, Competency Building & Skill Development to mention a few.

Insight into 'New Business Models'

ASSOCHAM has been a significant contributory factor in the emergence of new-age Indian Corporates, characterized by a new mindset and global ambition for dominating the international business. The Chamber has addressed itself to the key areas like India as Investment Destination, Achieving International Competitiveness, Promoting International Trade, Corporate Strategies for Enhancing Stakeholders Value, Government Policies in sustaining India's Development, Infrastructure Development for enhancing India's Competitiveness, Building Indian MNCs, Role of Financial Sector the Catalyst for India's Transformation.

ASSOCHAM derives its strengths from the following Promoter Chambers: Bombay Chamber of Commerce & Industry, Mumbai; Cochin Chambers of Commerce & Industry, Cochin: Indian Merchant's Chamber, Mumbai; The Madras Chamber of Commerce and Industry, Chennai; PHD Chamber of Commerce and Industry, New Delhi and has over 4 Lakh Direct / Indirect members.

Together, we can make a significant difference to the burden that our nation carries and bring in a bright, new tomorrow for our nation.

D. S. Rawat
Secretary General
d.s.rawat@assocham.com

ASSOCHAM
INDIA

The Associated Chambers of Commerce and Industry of India
ASSOCHAM Corporate Office:
5, Sardar Patel Marg, Chanakyapuri, New Delhi-110 021
Tel: 011-46550555 (Hunting Line) • Fax: 011-23017008, 23017009
Website: www.assocham.org

About the authors

This knowledge paper has been co-authored by Siddharth Vishwanath, Amol Bhat, Priya Sawkare and Somaskandan Vinit. Siddharth Vishwanath is a Partner and leads the Financial Services focus for the Cyber Security practice. Amol Bhat is a Director with the Cyber Security practice and works with several banks.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

In India, PwC has offices in these cities: Ahmedabad, Bangalore, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in.

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity in separate lines of service. Please see www.pwc.com/structure for further details.

Contacts

Sivarama Krishnan
Leader, Cyber Security
sivarama.krishnan@in.pwc.com

Siddharth Vishwanath
Partner, Cyber Security
siddharth.vishwanath@in.pwc.com

Murali Talasila
Partner, Cyber Security
murali.talasila@in.pwc.com

Manu Dwivedi
Partner, Cyber Security
manu.dwivedi@in.pwc.com

Sundareshwar Krishnamurthy
Partner, Cyber Security
sundareshwar.krishnamurthy@in.pwc.com

PVS Murthy
Executive Director, Cyber Security
pvs.murthy@in.pwc.com

Hemant Arora
Executive Director, Cyber Security
hemant.arora@in.pwc.com

pwc.in

Data Classification: DC0