Digital payments- Analysing the cyber landscape

Risk Consulting

April 2017

KPMG.com/in

Foreword

The pace of shift to digital payments has significantly increased with the strong move towards cashless economy. This shift wouldn't have been possible without several factors that influence the growth and proliferation of digitalisation, including:

- An ever increasing mobile phone penetration
- Lower cost of service delivery
- Banks discouraging customers to visit branches
- Unorganised sector supporting the digital economy
- Demonetisation

Adoption of digital payments is visible when country's Honourable Prime Minister, Shri Narendra Modi, launched a mobile application, Bharat Interface for Money, popularly referred to as, BHIM, two months after announcing demonetisation and this mobile application, created a world record of sorts when it was downloaded more than 17 million times in less than two months. Other channels such as Immediate Payment Service (IMPS), has witnessed growth of 97 per cent with about 72 million transactions. Country's leading mobile wallet service provider has ~150 million users as of today.

While the macro factors clearly indicate favourable environment for digital payments, which is also being supported by the approach being taken by regulator, however, several challenges remain though for having attain the state where country truly becomes digital-

- Feature phones continue to be widely used in rural India, which make it a tad difficult – not impossible to transact,
- Patchy digital connectivity in parts of India
- Acceptance and change in mind set
- Lack of awareness and
- Most important security in transacting.

Bitcoin based financial infrastructure is expected to bring a revolution just like the internet. In future, bitcoins could be the means of exchanging and trading. The Reserve Bank of India is taking a precautionary view on the cryptocurrency and RBI regulations don't permit bitcoin to be prepaid payment instrument[1].

Keeping pace with the growth of digitisation, the cyber threats are not far behind. As many as 11,592 cases of cybercrime were reported across India in 2015. The growth in cybercrime coupled with proliferation of digital economy is as close as it can get to a death-knell, if not dealt appropriately.

In this Thought Leadership, titled 'Digital Payments – Analysing the cyber landscape', we examine the digital payments ecosystem from a lens of readiness of framework for adopting the technology, emergence of new industry (Fintech), security and preventive measures that an Indian citizen needs to take before taking a leap of faith in the digital world, and measures to avoid frauds. While we unremittingly build our defences, it is our strong belief that cybersecurity is the only panacea for immunity in the digital age against cybercrimes.

Mritunjay Kapur
Partner and Head
Risk Consulting

Mritunjay heads the Risk Consulting practice at KPMG in India. He has over 20 years of experience in consulting and advising across sectors, business solutions, and geographies. At KPMG, Mritunjay is not only one of the senior members of the India Leadership Team, but also an active member of the Global Risk Consulting Steering Committee responsible for stratgising and driving our Risk Consulting business, globally. In terms of industry associations, Mritunjay is the Chairman for ASSOCHAM's National Committee on Internal Audit and Corporate Fraud.

1. RBI maintains a no-no but India's bitcoin demand is shooting, The Indian Economist, 08/02/2017

Executive summary

Government of India's recent demonetisation in November 2016 and the 'Digital India' initiative, launched in 2015 have provided substantial boost to the country's digital ecosystem. With initiatives such as 'DigiShala', the government aims at building a conducive ecosystem for 'cashless economy'; other initiatives such as the National Optical Fibre Network (NFON) and introduction of Unified Payments Interface (UPI), Bharat Interface for Money (BHIM- internet based mobile application) can help support in faster adoption and transition to digital payments.

However, this sudden surge and change in end user profile has led to various challenges in the digital payment ecosystem. Cybersecurity is one of the most critical challenges faced by stakeholders of the digital payment ecosystem. With more and more users preferring digital payments, the chances of getting exposed to cybersecurity risks such as online fraud, information theft, and malware or virus attacks are also increasing. Lack of awareness and poor digital payment ecosystem are some of the primary reasons that have led to the increase in these attacks.

A robust regulatory framework, an effective customer redressal framework, fool proof security measures to enable confidence and trust, incentives for larger participation and benefits similar to cash transactions i.e. ease of use, universal acceptability, perceived low cost of transaction, convenience and immediate settlement, are some measures that can help ensure long-term success for digital payments.

We conducted a survey to understand India's perspective on the cybersecurity concerns around digital payments. Below are the key findings from the survey -

Cashless payment

Nearly **88 per cent** respondents prefer cashless payment over cash payment, with **48 per cent** using digital payment for more than **75 per cent** of their transactions.

Ease of doing payments

Ease of doing payments is one of the key factors for users to move towards digital payments.

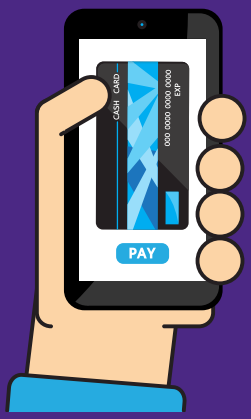
Around **90 per cent** of the people are unaware that the government runs a 24*7 TV channel 'DigiShala' to guide people and help them adopt digital payments.

Security concerns

As high as **88 per cent** of respondents expressed their will to adopt digital payment, however security concerns and lack of awareness act as key barriers.

End devices

All respondents cited security of end points/ devices being used for digital payments as a major concern.

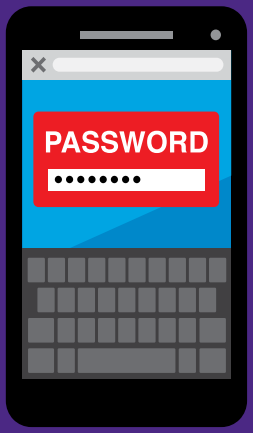


Strong cashless ecosystem

About **78 per cent** of respondents opined that availability of strong cashless ecosystem is essential for enhanced adoption of digital payments.

One-time password

Dual factor authentication such as card and Personally Identified Number (PIN) as well as one-time password based transactions should be used to strengthen security in digital payments and gain customers confidence.



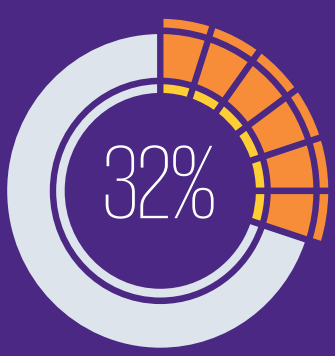
About the survey

We recently conducted a survey with an aim to provide the industry with a reference point that sheds light on key aspects such as acceptance, barriers, challenges and awareness of digital payments ecosystem post demonetisation. This survey seeks views from various customers and users across different sectors on cybersecurity in digital payment ecosystem post demonetisation. The content of the survey is derived from the responses of the participants and is complemented by insights from our experts in cyber forensic.

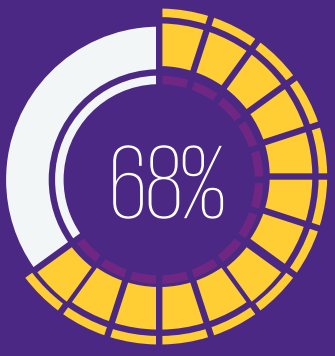
An overview of the demographics of survey participants

Profile of the participants

The survey saw over 320+ participants across age groups and different sectors who are the end users of digital payments platform in India.



Female



Male

Age of respondents

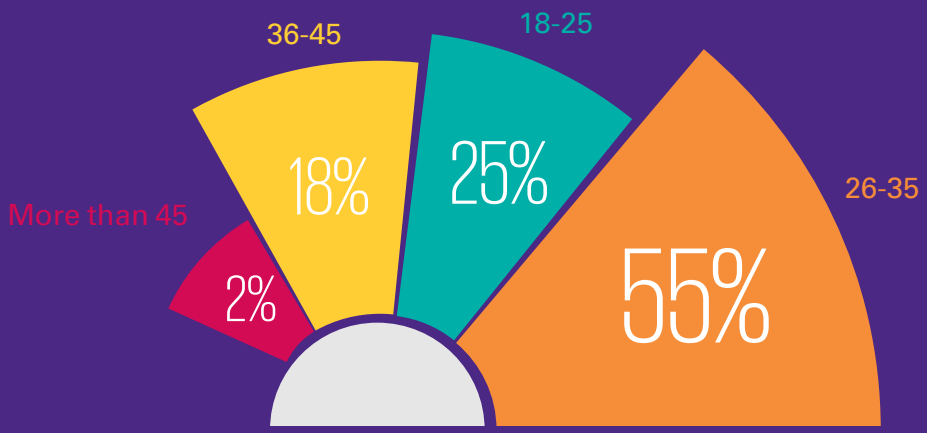


Table of contents

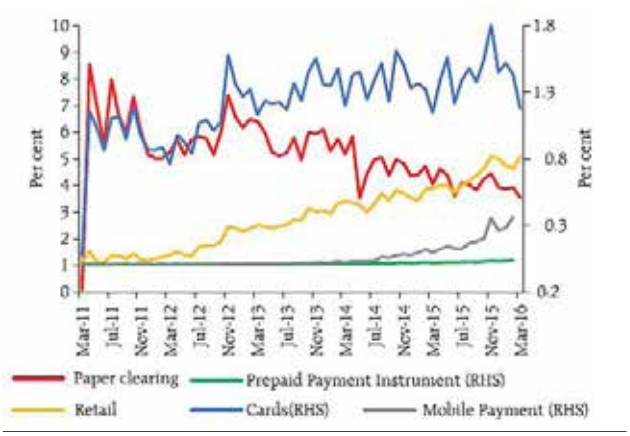
Digital payments in India

The digital payment landscape in India is undergoing a massive transformation. Indian consumers have shown tremendous affinity to digital technologies, with growth rates for mobile phones and e-commerce adoption far outstripping rates in developed economies. The Government of India's 'Digital India' initiative aimed at transforming India into a digitally empowered society and knowledge economy is expected to further accelerate awareness, availability and adoption of digital technologies.

As highlighted in the Ministry of Finance's Committee report on Digital Payments published in December 2016, financial inclusion is one of the foremost policy challenges facing India today. As of 2014, approximately 53 per cent of India's population had access to formal financial services. In this context, digital payment acts as a key enabler for accelerating financial inclusion. In fact, troves of insights available through customers' payment transaction patterns can be leveraged to offer fit-for-purpose products and solutions.

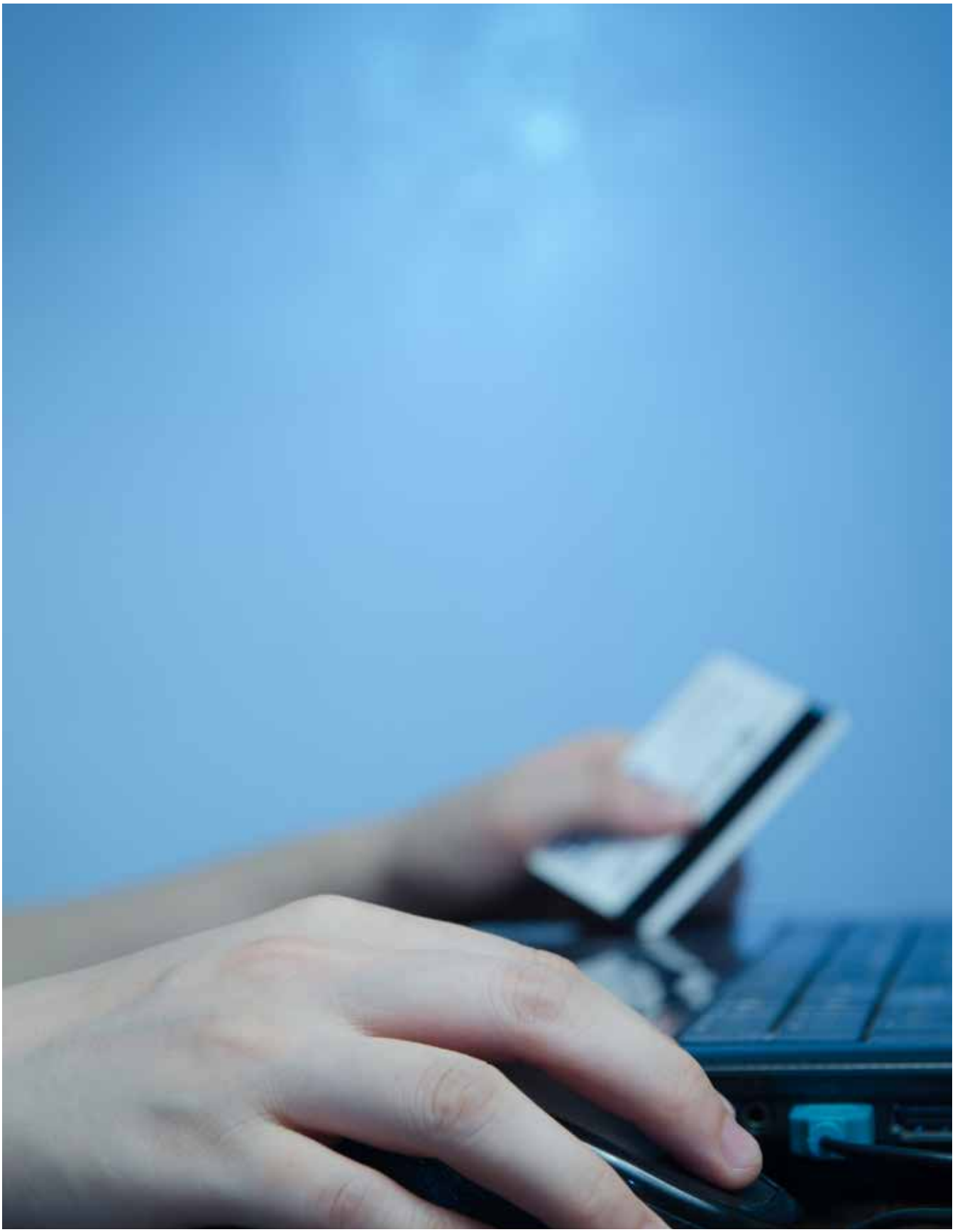
As per Reserve Bank of India's 'Financial Stability Report of 2015-16', share of electronic transactions as part of total transactions in volume terms moved up to 84.4 per cent from 74.6 per cent, accounting for more than 95.2 per cent in value terms. While majority of these are because of inter-bank RTGS and CCIL transactions, share of retail electronic payments and mobile payments is steadily increasing.

The chart depicts the share of various categories of payments systems, excluding the RTGS and CCIL. It explicitly highlights the decreasing trend of paper-based clearing and an increasing trend of various digital modes.

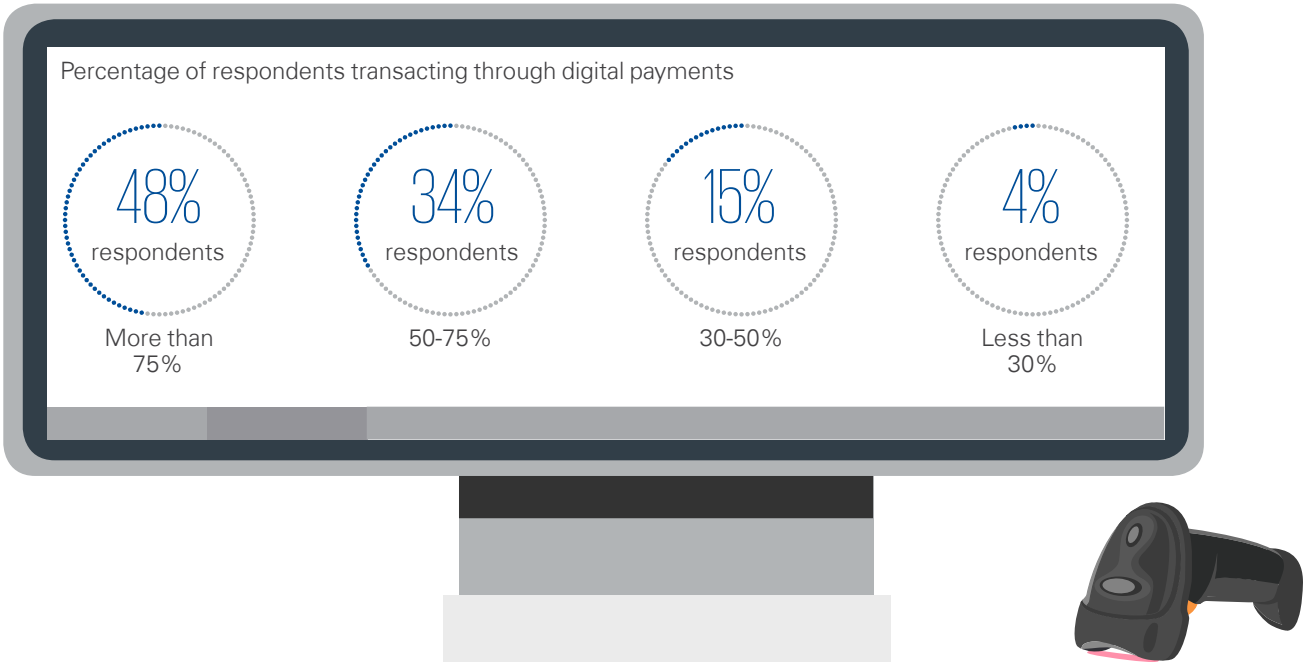


Source: RBI - Financial Stability Report of 2015-16

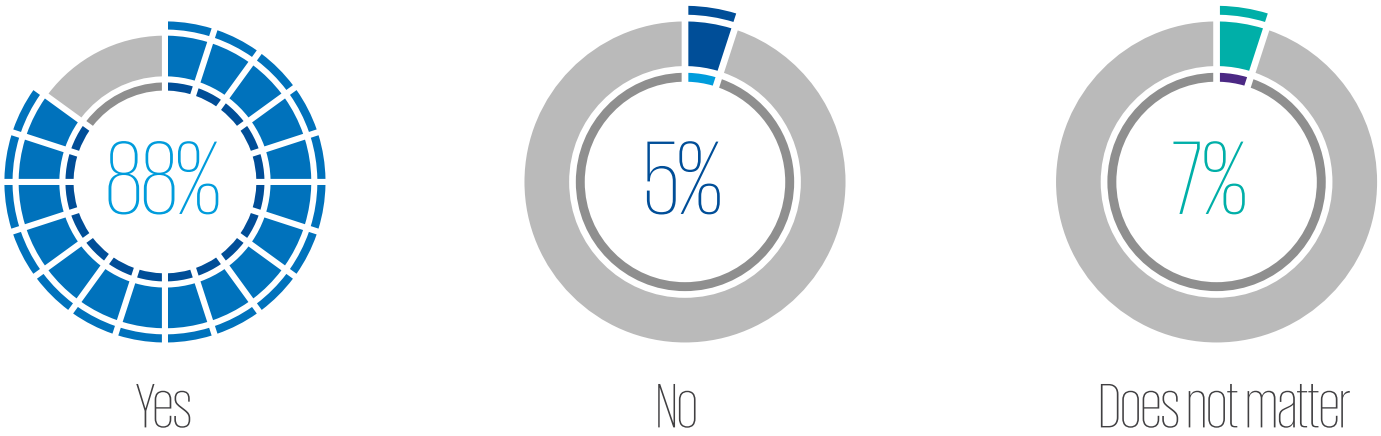
In fact, the share of retail electronic transactions (i.e. excluding RTGS) is approximately 12 per cent with cheque (10 per cent) and cash (78 per cent) covering the rest of the retail payment space.



Our study indicates that 88 per cent respondents prefer cashless payment over cash, with 48 per cent using digital payment for more than 75 per cent of their transactions.



Will you prefer cashless payment over cash payment



The recent demonetisation introduced by the government in November 2016, and following drive towards launch of policy level changes (such as merchant and consumer reward programmes for using digital payments instruments) and assets (e.g. BHIM mobile application) has turbo charged the digital payment adoption landscape.

It would be fair to say that the existing adoptions levels and several macroeconomic factors indicate that ingredients for successful creation of a thriving digital ecosystem are rapidly falling in place in India.

The digital payment ecosystem in India

Digital payments comprises payment transactions carried out using a variety electronic modes such as cards, mobile or internet based set ups, to send and receive money. The ecosystem consists of buyer (customer), seller (merchant, service provider) and Payment Service Provider (PSP) that enables transfer of money from buyer to seller for the product/service availed.

The PSPs in India consist of both bank and non-bank players. As of July 2016, PSP segment had 44 authorised Pre-Paid Payment Instruments (PPIs) including mobile wallets, prepaid cards providers and eight authorised payments banks, eight authorised cross-border money transfer operators and eight authorised white-label Automatic Teller Machines (ATM) operators.

These PSPs offer a variety of digital payment modes – from traditional ones such as National Electronic Funds Transfer (NEFT), National Electronic Clearing Services (NECS)/ Automated Clearing House (ACH), bank cards (credit, debit, pre-paid), internet banking, mobile banking to newer ones such as wallets (PPIs), Aadhaar Enabled Payment System (AEPS), Immediate Payment Service (IMPS), UPI, Bharat Bill Payment System (BBPS), and now AadharPay and India QR code.

Undoubtedly, mobile instruments as the form factor and technology are driving innovation and adoption. Banks and non-banks are now rolling out products driving adoption on mobile platform.

In this context, increasing availability of mobile phones (internet enabled mobile phone are expected to cross 500 million by 2020) and ubiquitous availability of data network infrastructure, further rollout of 3G and 4G network, and large merchant ecosystem are critical enablers, and require coordinated effort from industry, government and regulators.

As per RBI's report, 'Vision-2018', a four pronged strategy focusing on regulations, robust infrastructure, effective supervisory mechanisms and customer centricity has been adopted to push digital payments in the country. The policy initiatives such as simplified Know Your Customer (KYC), removal of Two Factor Authorisation (2FA) for small value transactions, recent disincentives for cash transactions, lowering of digital payment costs and building infrastructure such as National Optical Fibre Network (NFON) and standardisation such as UPI, BHIM (internet based mobile application) will help in adoption and usage of various modes of digital payment.

These enabling mechanisms along with relentless innovation driven by PSPs and technology service providers (such as FinTech, etc.) provides to launch customer centric and easy to use products, ecosystem of large number of merchants and customers shall continue to drive onslaught of digital payment on cash and other modes of non-digital payments.

The Reserve Bank of India's report, 'Payment and Settlement Systems in India: VISION-2018' highlights vision statement as-'Building best of class payment and settlement systems for a 'less-cash' India through responsive regulation, robust infrastructure, effective supervision and customer centricity' which revolves around following five contours:

Coverage – by enabling wider access to a variety of electronic payment services

Convenience – by enhancing user experience through ease of use and of products and processes

Confidence – by promoting integrity of systems, security of operations and customer protection

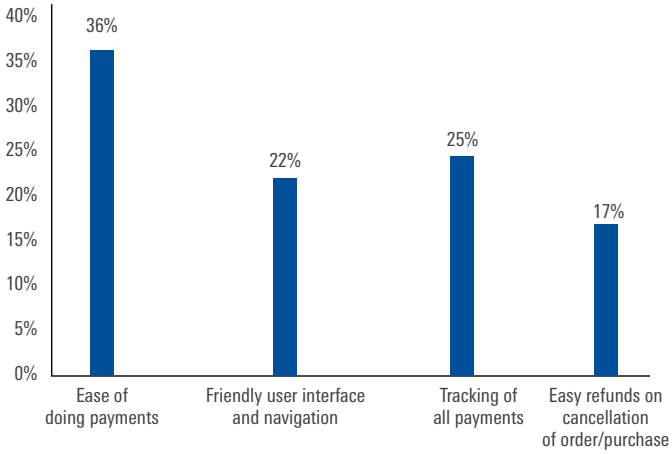
Convergence – by ensuring interoperability across service providers

Cost – by making services cost effective for users as well as service providers

The long-term success for digital payments would be contingent of convenient and easy to use mode, a robust regulatory framework, an effective customer redressal framework, fool proof security measures to enable confidence and trust, incentivizes larger participation and benefits similar to cash transactions i.e. ease of use, universal acceptability, perceived low cost of transaction, convenience and immediate settlement.

Ease of use: Based on our survey, ease of doing payments is one of the major contributors for users to move to digital payments. We believe this can be a key enabler to encourage people to opt for digital banking/payments.

Factors enhancing use of digital payment



It is important to design use cases with optimal transaction flows and information exchange to simplify payment transactions. Similarly, while measures around information security and data privacy are essential, it is crucial to achieve the trade-off with customer convenience. Few prevalent measures are the relaxation of 2FA for online payments below INR2000. Adoption of Aadhaar for authenticating online transactions and its usage for KYC can further encourage the use of digital payments in India.

Technology enhancements and innovations: Increasing penetration of mobile phones, ubiquitous connectivity, alternate modes of authentication such as voice and biometrics and adoption of cloud and Internet of Things (IoT) are the technologies that can shape the way for future transaction in India. Unified Payments Interface (UPI) can be further refined to enable a large scale adoption of digital payments in India by overcoming current short falls e.g. integration of various service providers such as banks and other financial institutions on this platform and uniform customer experience.

Merchant adoption: The depth and breadth of merchant participation are significant determinants for adoption of digital payments. Merchants need to be encouraged with sufficient incentives for them to actively contribute to the growth of the digital payment ecosystem. Merchant discount rate and other transaction charges on digital payments are in the process of being rationalised and a new regime of transaction charges based on high volume and low charges is expected to be rolled out. Special care is being taken of small and rural merchants, for instance, one of the largest public sector bank has proposed zero transaction/ MDR charges on such terminals.[1]

Awareness: While there has been a significant uptake of digital payments, there is still a considerable amount of work that needs to be accomplished. There should be continuous focus on educating customers and merchants on the advantages of digital transactions. Awareness campaigns regarding security best practices, ease of usage and grievance redressal forums for issues in digital payments can go a long way to increasing adoption.

Enhanced customer service: An effective and efficient customer service mechanism is one of the critical components for increased adoption. A digital payment ecosystem comprises of number of players – telecom operators, payment gateways, banks and regulators. It is important to clearly define the roles and responsibilities of all stakeholders. Effective customer handling will be one of the primary drivers for adoption and all stakeholders need to ensure that consumer interests are paramount in their operating and business models. The following need to be looked at:

- Institutionalise mechanism for handling customer complaints/grievances
- Establish chargeback and dispute resolution process

Fit for purpose offerings: The payment transaction data collected by PSPs can be used by them to provide customised deals and offers to the customers, thereby influencing their buying pattern.

Through security: It is imperative for the security architecture to ensure confidentiality, integrity, authenticity and non – reputability. Robust encryption measures for communicating customer and payment information between stakeholders should be established along with periodic risk management analysis, security vulnerability assessment of the application & network.

Kunal is a Partner with IT Advisory, KPMG in India. He leads IT Advisory focus towards financial services sector. Kunal has more than 13 years of experience in providing IT advisory and assurance services.

Kunal Pande
Partner
IT Advisory

1. SBI waives MDR charges for small merchants for one year, The Economic Times, 09 January 2017

Digital payments - Adoption, acceptance and barriers

With the entire clamour on demonetisation and the endeavour to move from hard currency to digital, it would be interesting to ponder if we have done something like this in the past. As it turns out, we have done it quite a few times before. In the last 2 centuries, we went from using gold/silver coins to bank notes, subsequently to paper currency. In the last century itself we moved from the 'anna' system to the 'paise' system. Just the same way that paper currency espoused the ideals of our country for the last 60 years namely the Ashok Chakra and the face of the father of the nation, it's only logical that the next wave would be digital and electronic payments which is a reflection of how we live today.

Which brings me to the question, what are the barriers to digital payments? Probably because we have been using it in its current form for the last 70 years. While there have been many attempts to bring in financial discipline via bank accounts, credit cards, pre-paid cards, post office accounts but the robust system of cash based transactions has continued to thrive alongside the banking system. In some ways the longevity and association, it becomes a part of our culture, from money in the hand, under the table, in polythene bags, in sweet boxes and sometimes in garlands. There are a number of people not just habituated by incentives to keep the status quo.

November 8, 2016 however may have proved to be a watershed moment in every Indian's life. One that may well be remembered as a BD (Before Demonetisation) and AD (After Demonetisation) event.

The intent, implementation and readiness (or lack thereof) have received extensive coverage and commentary but it showed us that in the tomorrow's world, it could be difficult to escape an indelible electronic money trail.

There were many developments that quietly led up to support the digital payments phenomenon-

- India has the third largest internet user base in the world, with more that 300 million users[1]. Nearly 50 per cent i.e. 150 million users are mobile-only internet users. This may be a significant number from an absolute perspective but it still represents only 19 per cent of population using internet and even lesser percentage using mobile internet. These numbers have to increase substantially if digital payments have to make the impact they promise.
- The Government of India has taken upon itself to create an ecosystem for cashless digital economy. This means fostering an environment conducive for growth and innovation in the FinTech industry. The Indian FinTech software market is forecasted to touch USD2.4 billion in the year 2020 from the current USD1.2 billion[2].
- The RBI has also responded to the growing trend in its report, 'Vision 2018' – where it states that new policies with focus on electronic payments will influence the trends in electronic payment systems in the country.[3]
- The government's focus on banking for the unbanked through schemes such as the 'Jan Dhan Yojana' where 200 million unbanked individuals were brought into the banking sector. Also, the extension of Aadhaar to pension and Provident Fund has helped in financial inclusion.[2]
- The banking industry has also seen mobile and internet banking transactions increase to 27 per cent overall transactions in April 2016, an increase from 8 per cent in March 2012. There has also been an increase in card based transactions.[3]
- There has been significant growth in the e-commerce market place. India's e-commerce market (revenues) grew from USD 3.8 billion in 2009 to USD 23 billion in 2015.[4] The trends of online shopping are also tending significantly towards mobile devices.
- Since the government's demonetisation announcement, Indian bitcoin adoption has been on the rise. Indians are likely to adopt crypto currencies in the form of bitcoins. For bitcoin to gain adoption and become the foundation of a new global financial system, companies should continue to innovate and make it easier for consumers to buy, hold, and spend bitcoin*.

1. Mobile Internet users in India to double by 2017, says study, Live Mint, 24 March 2017
2. Fintech in India – A global growth story, KPMG in India- NASSCOM, June 2016
3. RBI's Vision 2018 zeroes in on electronic payments, Live Mint, 24 March 2017
4. E-Commerce Industry will cross $38 bln mark by 2016; Indian e-commerce market set to grow by 67% in 2016: study, ASSOCHAM India, 01 January 2016

* The 5 Phases of Bitcoin Adoption, The Market Oracle, 30 December 2014

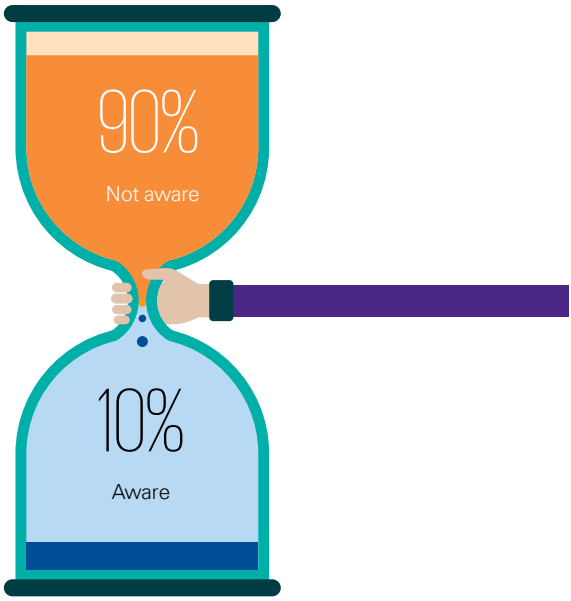
The volumes should expand dramatically so that large merchants can start accepting payment in bitcoin. Awareness for bitcoin should be spread along with these developments. Blockchain is a fundamentally more scalable, reliable, and secure solution than the then, and even the present day, payment processing technologies used by some of the biggest processors and gateways in India.

There is however a need to step back and take note of what it means in our everyday life. Can the digital payments industry be really inclusive?

- The digital world could not escape the disparities we see in the real world. According to a survey by Pew Research Centre in February 2016, only 12 per cent of older respondents (aged 35 and above) used the internet occasionally or own a smartphone. This was in comparison to 34 per cent of millennial (aged between 18 and 34).
- While there is an exponential growth in the e-commerce market, cash on delivery is still the most preferred mode. In 2015, 45% of online shoppers preferred cash over card based or digital payments.[5] This trend has not reversed post demonetisation.
- The divide extends to education levels where only 9 per cent with lower education levels are online, as compared to 38 per cent who have higher education levels. A gender gap was also noted where 17 per cent of women and 27 per cent of men reported internet and smart phone usage. What may be particularly worrying is that the disparity between the digital haves and have not's may widened faster with rapid changes in technology.[6]
- The comparison with a cash based economy will weigh digital payments down. In a cash based transaction, the cost of the transaction is not transferred to the customer. In a cash-less transaction, the merchants pass on the transaction charge to the customer. While the government intervened during demonetisation, eventually the PSP will charge fees to make margins.
- Also, KYC requirements are disparate. The threshold for KYC requirements for a digital transaction is lower than that for an over the counter cash transaction.

Based on our survey, 90 per cent of the respondents said they were unaware of the government's 24*7 TV channel, 'DigiShala' that guides people for using digital payment modes.

Government's cashless lessons on 'DigiShala'



With these issues, the larger question is who is responsible and accountable for a cashless economy. The government and RBI have clearly stated that cashless economy is the way forward. In this scenario, we need to answer some important questions:

- Is there adequate governance mechanism and public policy intellect to cope with the impact of digital/cyber terrorism and warfare?
- Are the three pillars of our democracy i.e. legislature, executive and judiciary skilled and ready to take on the challenges of cybercrime?
- If the economy runs on digital, should our government report on cyber security performance?
- Do companies have an obligation to their customers and investors to be transparent on their cybersecurity performance?

These questions are just some that need to be answered for a thriving yet secure digital economy.

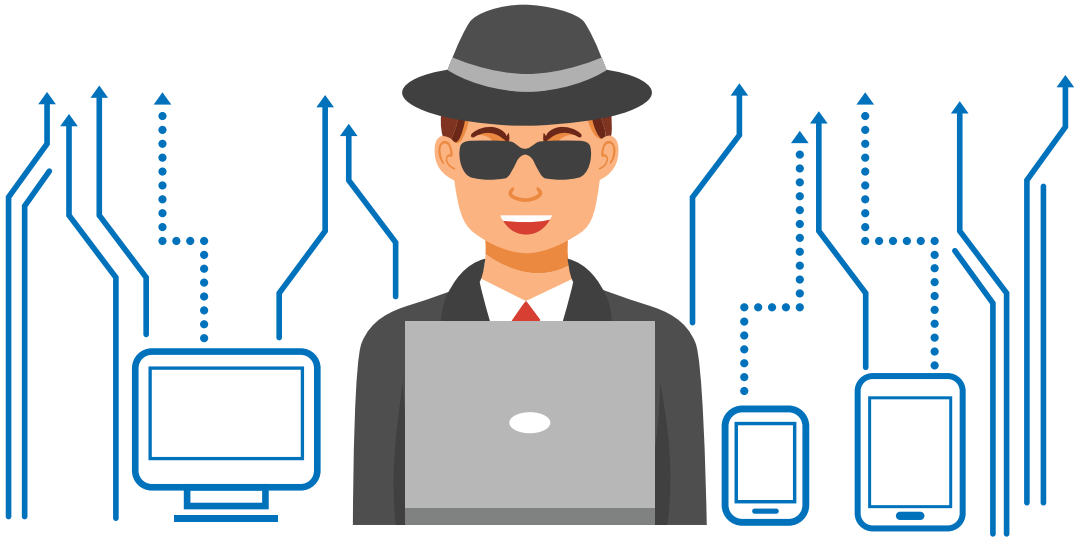
Abhijit Varma
Partner
IT Advisory

Abhijit is a Partner with IT Advisory, KPMG in India. Abhijit has more than 15 years of experience in developing and building cybersecurity solutions in a wide variety of areas including security governance, policies and standards, privacy and business continuity. He also leads the Business Intelligence and Analytics team for KPMG in India, focused on delivering high quality information, helping clients improve the quality of their decision-making processes.

5. E-Commerce Industry will cross $38 bln mark by 2016; Indian e-commerce market set to grow by 67% in 2016: study, ASSOCHAM India, 01 January 2016
6. Only 17% Indians own smartphones: survey, Live Mint, 24 March 2017

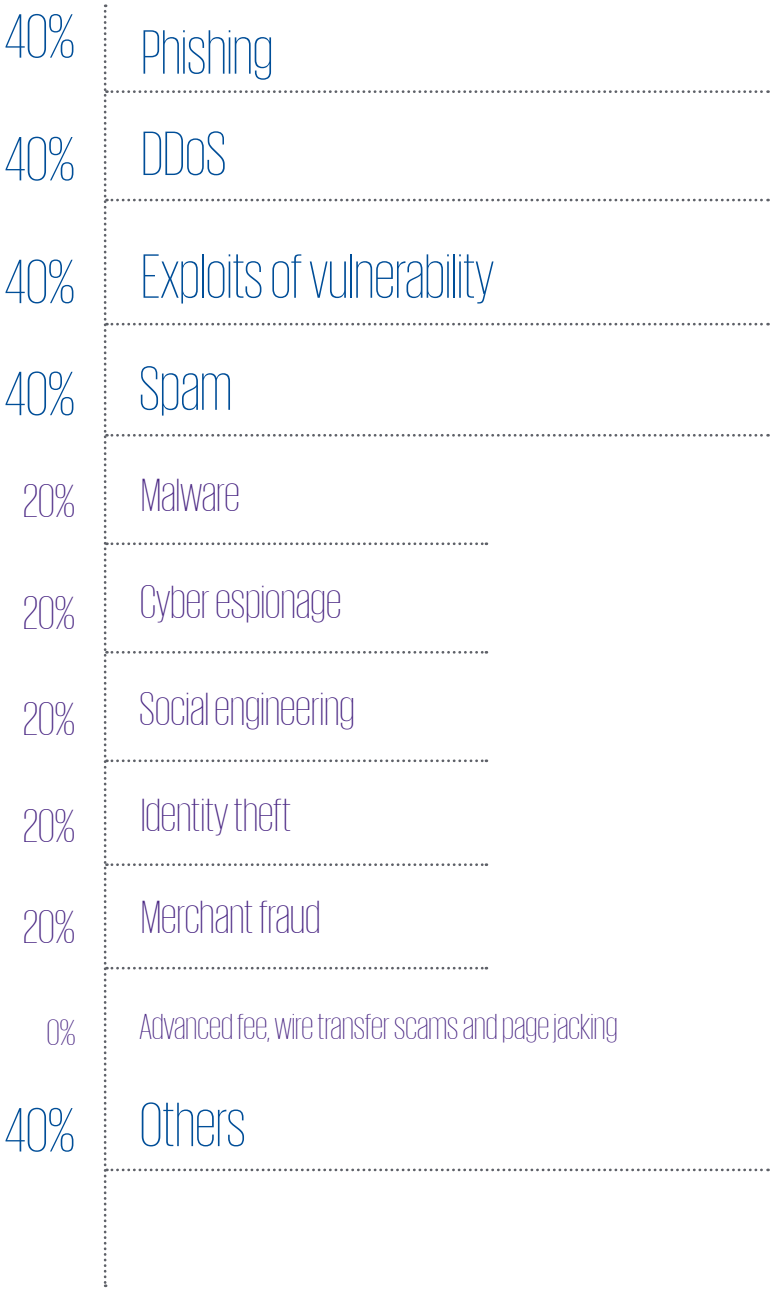
Security in digital payment and associated ecosystem

Last few years have witnessed many high impact cybersecurity attacks, globally, across sectors such as healthcare, e-commerce, telecom, financial services, government services, manufacturing, and hospitality causing far reaching implications and establishing cybersecurity as one of the top business risks. Our study, which included inputs from global CEOs, indicates that cybersecurity risk has climbed to become top three risks where CEOs would like to invest. The magnitude of risk has exponentially increased with enhanced adoption of digital channels by businesses to interact with customers and capture of information across industries.



Cyber risk is not limited to geographical boundaries and corporates in India have been fairly exposed to this risk. Our study indicated that nearly 72 per cent of organisations witnessed some form of cyberattacks. The attacks have accentuated with significant drive on adoption of digital payment channels over the last six months with phishing, Distributed Denial of Service (DDoS) and spam being most widely used attack vector.

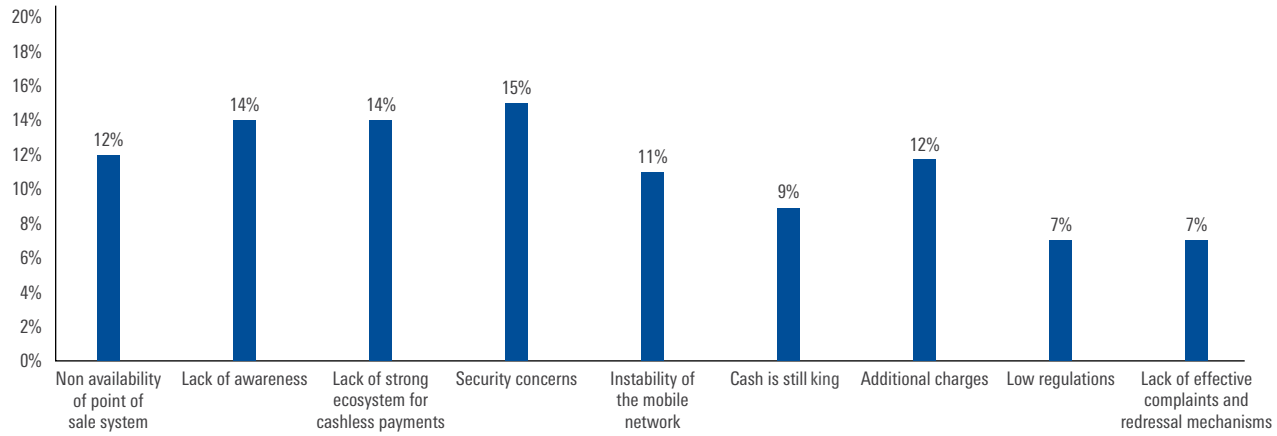
Nature of cyberattacks faced by organisations on digital payments channels



Nearly 88 per cent of our survey respondents preferred to adopt digital payment channels; however, our study also highlights the following two major causes that act as barriers for adoption-

- Cybersecurity
- Awareness

Digital payment: Barriers of growth



Cybersecurity risk – Reality check

Proliferation of digital channels along with increased data access covering the remote locations in India, has led to significantly high number of users having internet access.

The current decade has witnessed significant changes and innovations in digital payments channels and with emergence of FinTech the transformation shall continue at even more rapid pace.

While this has led to multiple customers to use digital channels, however, at the same time it has also led to increased cyber-risk exposure.

'Cyber Swachhta Kendra' (CSK)

Established in February 2017, the Botnet Cleaning and Malware Analysis Centre, CSK, operated by Indian Computer Emergency Response Team (CERT-IN) focuses on desktop and mobile device security. The Union Minister of Electronics and Information Technology, Ravi Shankar Prasad mentioned this as an important milestone in various initiatives taken on cyber-security.

There are multiple solutions which have been released, including solution on desktop security ('USB Pratirodh') and mobile device security (focused on Android™[1] based mobile phones, called 'M-Kavach').

This is a step which has been taken by CERT-IN to address the increased number of incidents being reported (more than 50,300 incidents reported in 2016) and is also part of the government's 'Digital India' initiative, under the Ministry of Electronics and Information Technology.

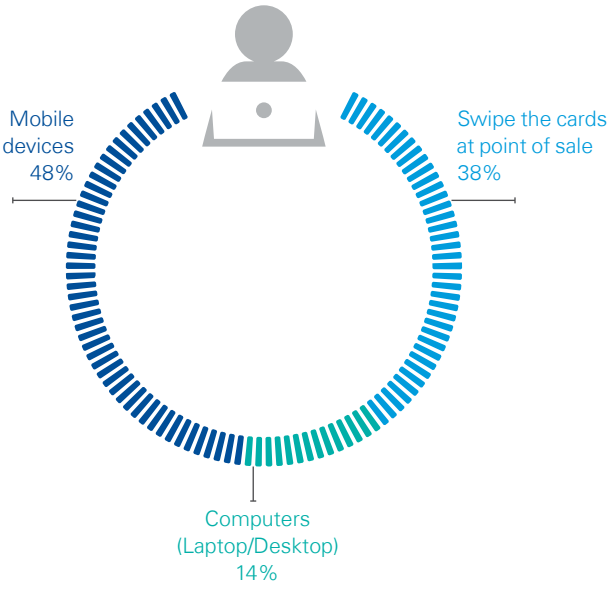
1. Android is a trademark of Google Inc

These could be attributed to:

Security measures on end user devices

Users today are accessing digital channels through multiple devices, and our study indicates that nearly 48 per cent of the users prefer using mobile phones.

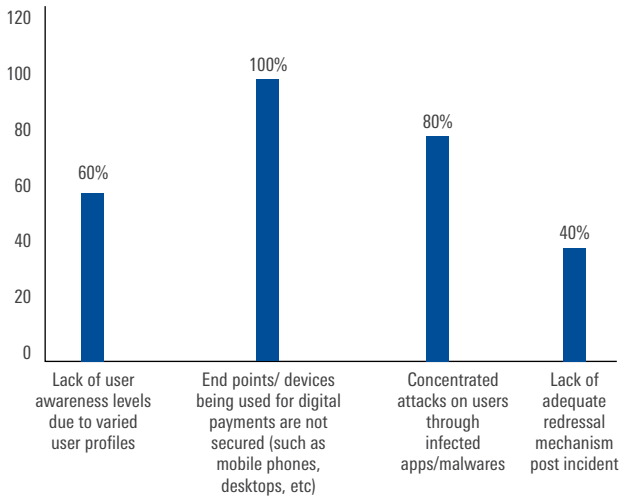
Preferred mode of digital payment transactions



Smart phones have emerged as a preferred mode for carrying out digital payments since it enables communication – anytime, anywhere, provide applications for ease of access. While doing transactions/business is more convenient by the use of mobile devices, it also exposes individuals and organisations to cyber security risks such as online fraud, information theft, and malware or virus attacks. These may happen because of the any of the following:

- ***Inadequate security measures on devices –*** Smart phones with internet access are exposed similar to traditional computers from security perspective, however, these devices are normally not secured through various security tools – such as antivirus, anti-phishing, anti-malware, etc. This exposes the users to cyber security risks. All our survey respondents uniformly cited security of end points/devices used for digital payments as a major concern.

Key reasons for security incidents



- ***Cracked applications installed on devices –*** Users have multiple applications installed on their mobile phones, which also includes the 'cracked' applications that may have access to information across the device. These applications potentially access financially sensitive information and pass on to attackers. Our study indicates that nearly 58 per cent respondents considered the usage of One Time Password (OTP) to be a secure mechanism; however, information such as OTP can be accessed by malicious applications installed on mobile phones, which have access to user's messages or calls.
- ***Vulnerable/unpatched operating systems –*** India has a mix of users having smart phone with Android™ (76.85 per cent) and Apple™[2] operating system (2.33 per cent).[3] The nature of some of these operating systems are extremely open which supports collaboration, but also exposes large set of users to potential security issues.

2. Apple is a trademark of Apple INC., registered in the U.S. and other countries
3. Market share held by mobile operating systems in India from January 2012 to December 2016, The Statistics Portal

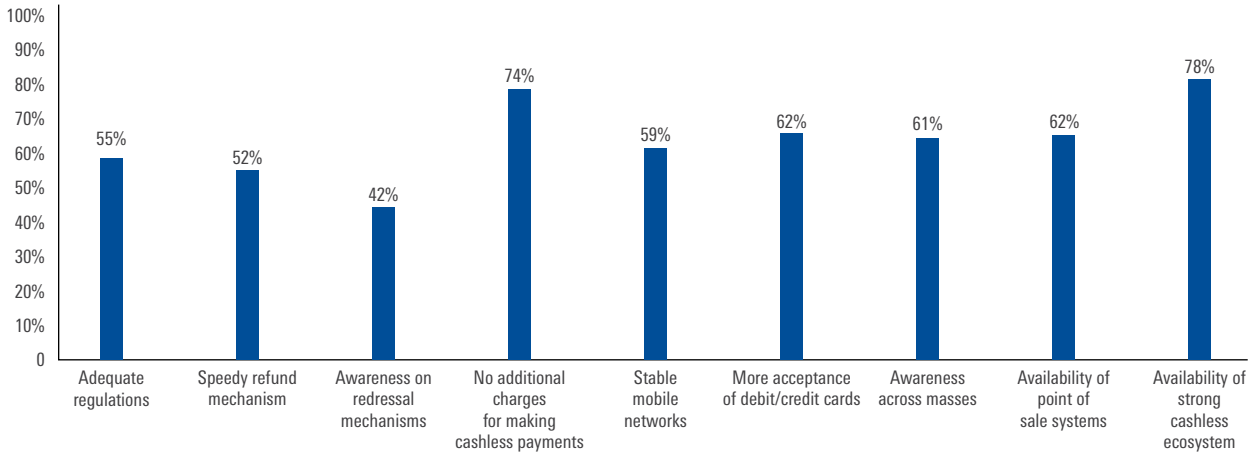
Security by design for digital payment products

- The demand for accessing digital payment channels has increased significantly post the demonetisation drive in the country. While this provided an opportunity to service providers, the demand of solutions led to design and launch of multiple products during short period, which may lead to security controls not being designed comprehensively.
- One of the leading mobile wallet providers had to roll back the product, since there were concerns raised on security measures.[4]

Large ecosystem with multiple variables

According to our survey, availability of strong cashless ecosystem is essential for enhanced adoption of digital payments.

Digital payments: Factors to enhance adoption



Digital payment ecosystem is evolving at a rapid pace as India is embracing digital and technological advancements. The value chain of entire ecosystem is large and growing, which exposes it to cybersecurity risks. The key variables include:

- ***Data interfaces across the products:*** Products are required to have multiple interfaces with other services/ applications and most of the products have multiple Application Program Interface (APIs) for this purpose. There is high possibility that these APIs may be exposed to untested/ untrusted interfaces, which may lead to compromise of security measures.
- ***Third party service providers:*** There is lot of information exchange that happens with third parties, and overall security levels are based on the weakest link in the chain. Recent incidents related to debit card security compromise were attributed to security attack on third party service provider.
- ***Lack of perimeter:*** The ecosystem being large with multiple data interfaces, devices and systems, has led to undefined perimeter for the environment. Enforcing adequate security controls in such an environment causes its own challenges.

User awareness

Lack of end user awareness has emerged as one of the main causes for attacks being successful. Attackers continue to exploit lack of awareness through various social engineering attacks, which include identity impersonation, phishing sensitive information, etc.

4. Paytm rolls back app POS service: Will it affect the brand?, Moneycontrol, 25 November 2016

Regulation – Are we doing enough to address cybersecurity risks?

One of the key drivers for deploying adequate cybersecurity measures has been the regulatory requirements. Our study indicates that 55 per cent respondents believe that the adoption of digital payments can be enhanced once there are 'adequate regulations' governing the digital payments in country. This calls for a need to adopt a more proactive approach to build a robust regulatory framework.

The RBI has been monitoring the changing risk posture due to cybersecurity and have drawn regulations to be implemented by organisations across sectors to strengthen user's confidence in digital transaction. Recently issued cybersecurity regulations include:

- Banks to have comprehensive and robust cybersecurity framework
- Technical cybersecurity audit of Prepaid Payment Instrument (PPI) issuers

The regulations are enforcing PSPs to ensure that there is a minimum baseline of security controls.

One of the potential emerging areas is where devices (post adoption of IoT) shall carry out payments and our study indicates that more than 65 per cent of users are keenly looking forward to such technologies; this however needs to be commensurated by appropriate regulations.

Conclusion

The changing nature of cybersecurity attacks such as web application attack, ransomware, reconnaissance, DDoS attack clearly establish cyber-risk as new reality and also positions it as one of the top business risks today.

Country has adopted digital payment channels with significant increase in volume (and value) of transactions, however, any significant security incident can have adverse impact on the usage of this channel.

It is imperative to have structured approach to security, with following key components:

Security strategy and governance

- Design and implement robust cybersecurity frameworks
- Identify 'crown jewels' and protect them
- Establish adequate measures for protection from third party risks
- Evaluate the changing threat landscape and align risk treatment strategies
- Empower the users through enhanced security awareness

Security defence and transformation

- Establish robust measures for establishing user identity and authentication for transactions
- Establish advanced authentication measures, such as risk based/adaptive authentication
- Deploy adequate technical and security measures to deal with 'cyber warfare'

Cyber response

- Establish comprehensive cyber and incident response plan
- Conduct regular cyber drills to enhance preparedness

Atul Gupta
Partner
IT Advisory

Atul is a Partner with IT Advisory, KPMG in India. Atul has more than 16 years of experience in IT advisory assignments and leads the cybersecurity practice at KPMG in India and is also an active member of KPMG's global initiative on cybersecurity.

Preventive measures in digital payment to avoid fraud

Background

Over the last two decades, the world has seen rapid strides in technology and communication. In the digital world, cybercrime is evolving rapidly, making it one of the biggest threats to businesses, individuals and governments.

Traditionally, fraudsters have targeted all payment vehicles and digital payments are no different. Traditionally, risks in digital payments include loss of revenue, brand reputation, denial of services, theft of services or currency, money laundering as well as transaction frauds.

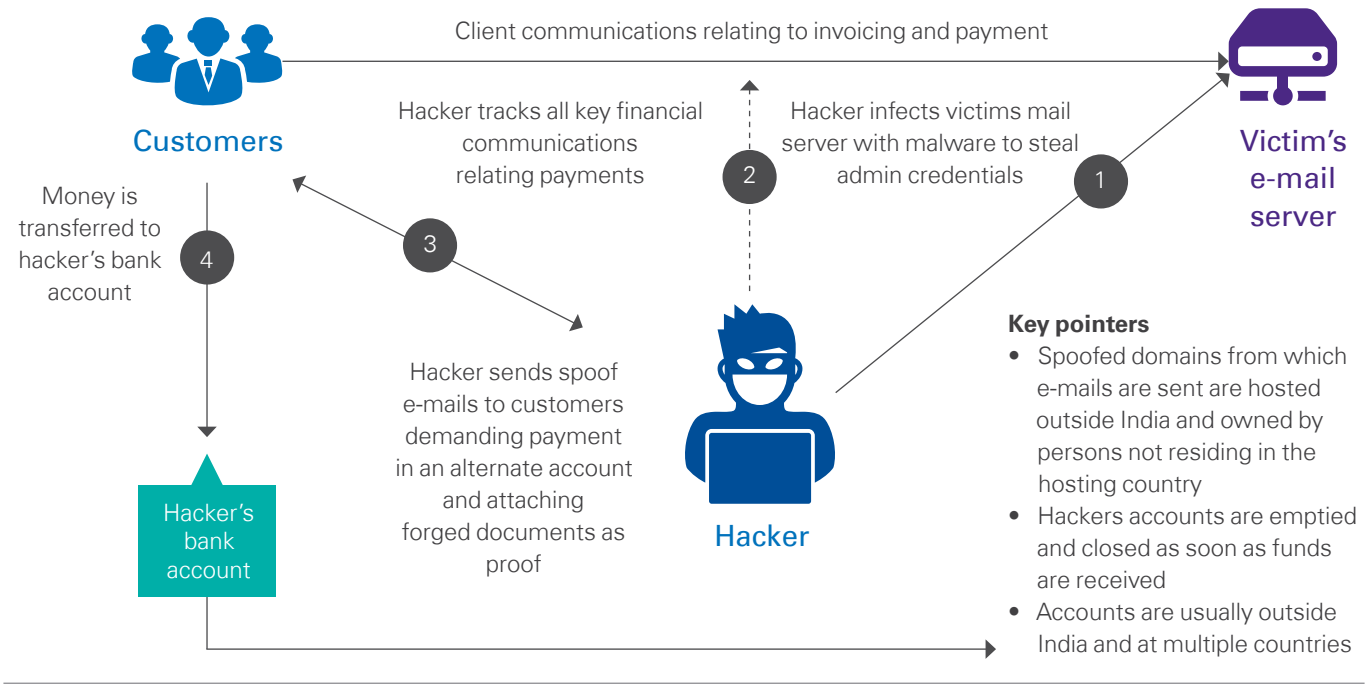
Traditional threats versus latest threats

Traditionally, bank frauds happen due to risks around identity theft, phishing, unauthorised transactions, and fraudulent transactions and so on. However, criminals are gradually becoming more sophisticated in their use of advanced tools and techniques. They now employ malware infections, remote code execution, and man-in-the-middle of transactions as well as system vulnerabilities to perform unauthorised as well as fraudulent transactions. Fraudsters exploit zero day vulnerabilities or alternative payment methods such as digital wallets as well as government initiatives such as UPI have paved way for newer techniques to perform digital frauds.

A few illustrations of the cyber frauds prevalent in India are as under:

Fund diversion attacks: These type of attacks are becoming increasingly prominent in India, where more and more companies with export businesses are targeted. The typical modus operandi of this attack involves infecting computers of key personnel in accounts receivables department or the companies e-mail server with a view to obtain the credentials of their e-mail accounts. By using Trojan, the cyber fraudster stealthily monitors the e-mail flow between the victim and the customers over a period of months. At an opportune time, the hacker strikes by impersonating the victim and directly communicating with the customer, asking them to remit funds into an account of his choice, which is instantly emptied out using an international laundering syndicate.

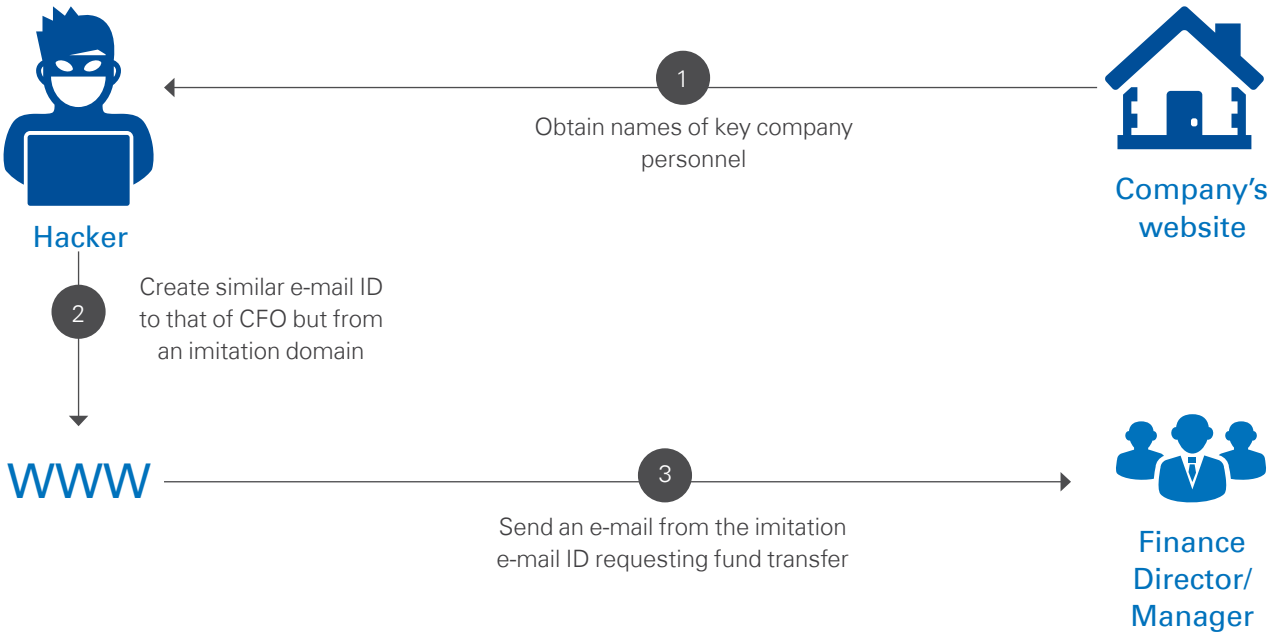
The modus operandi



Spear phishing: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organisation, seeking unauthorised access to confidential data or transfer of funds. As with the e-mail messages used in regular phishing attacks, spear phishing messages appear to come from a trusted source.

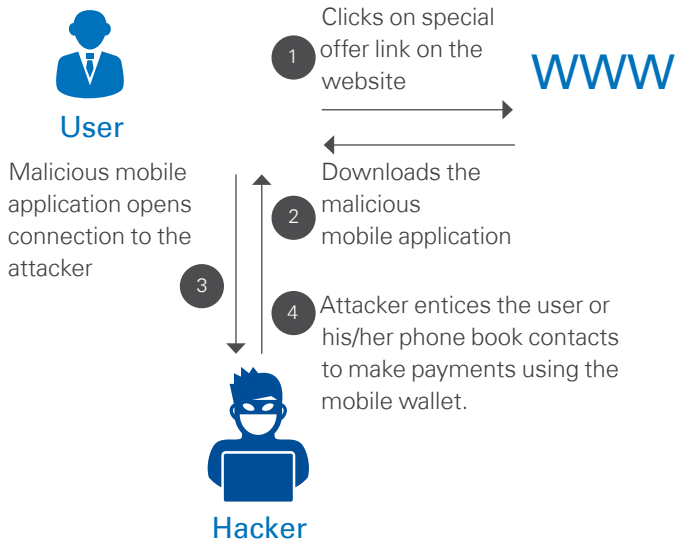
Companies within India are increasingly targeted with this type of cyber fraud/crime. The typical modus operandi of the fraudster is to first identify potential target companies and perform reconnaissance to gather information about the key personnel (usually from websites, social media sites). They then register a domain name that looks similar to the target's domain address. An e-mail account is hosted and forged e-mails posing to be CFO or CEO are sent to the finance Directors or Managers instructing them to perform fund transfer to an international bank account and charge the amount to admin expenses. Fraudsters typically target hundreds of companies with customised e-mails. A few corporates eventually do fall prey to this type of attack.

The modus operandi



Malicious mobile application based attacks: An increasing number of cases have been noted where mobile users are presented with attractive online offers and enticed into downloading and installing unknown mobile applications. Good majority of the users either always grant permission or simply do not know enough about the kind of consent they may have granted while installation of applications. In this way, malicious applications enter the mobile devices. Depending on the level of permissions these applications have been granted, the hacker connects to the user's mobile phone and entices/ demands the user or his/her contacts to make transfers through payment wallets.

The modus operandi



How forensic technology can help

While strategies of fraudsters have been evolving, so have the technologies and processes used for preventing, detecting and responding to frauds. Digital forensics is continuously evolving and numerous tools and methodologies are available with the forensic technology investigators to respond to payment frauds in an effective manner.

Cyber forensic experts can adequately identify, collect and preserve evidences in a manner that is presentable and acceptable in court of law.

Tools and methodologies allow forensic technology investigators to perform deeper collection and analysis of the evidences. Some of the activities that are typically performed by investigators to solve payment frauds are as below:

- Collection of evidences such as hard disk images, mobile phone images, server/desktop logs, firewall/security appliance logs in a forensically sound manner
- Recovering deleted evidences from the computer systems
- Analysing the data to identify traces of the fraud and its possible source
- Presenting the evidences in a manner acceptable in a court of law

While anonymity is still achievable by cyber criminals, tracing of the criminals is possible through detailed collection, preservation and analysis of evidence by forensic experts. The experts are able to track down the criminals by identifying IP addresses coupled with any other evidences left by the criminals in the data content and logs.

Cyber forensic and monitoring technologies

While it is evident that criminals prefer to carry out illegal activities using computing devices, making it hard for organisations and investigators to establish culpability. To detect cybercrime, organisations are increasingly leveraging on cyber forensics to know accurate facts of the incidences.

Cyber forensics encompasses the recovery and investigation of material found in digital devices, following standard procedures acceptable in a court of law. It is also used by private sector during internal corporate fraud investigations or intrusion investigations (for example, investigating a system breach that occurred from outside or loss of customer data).

Law enforcement agencies are required to increasingly cooperate among themselves to identify, track and extract evidences in order to capture criminals. Going forward, digital forensic evidence such as system logs and user identity details would be required along with the data from telecom, internet service providers, and cloud service providers such as IP address, GPS coordinates, for effective spatial and temporal analysis of the crime.

We should build data analytics capabilities that can handle increasingly huge volume of data. Data indexing and analytics platforms which can help in classifying information, identifying trends, performing keyword searches and visualising outlier data elements would need to be deployed.

Cyber forensic efforts are greatly enhanced if the organisations have appropriate audit trails and logging mechanisms established in its business environment. However, it is common for organisations to not have proper audit logging and monitoring practices implemented. Lack of system level audit trails generated at the time of business activities/transactions can hamper the investigation as cyber forensic can't recover something not created in the first place. It becomes difficult to propose/test hypothesis without having appropriate audit trails to substantiate the analysis.

Cybersecurity and securing digital payments infrastructure has emerged as one of the most important concerns for banks and payment service providers such as digital wallet providers. The sophistication and rapid growth of breaches, cybercrimes and digital payments fraud cannot be ignored. Corporates should bear in mind that an effective cybersecurity strategy, is not a onetime activity but a continuously evolving cycle of activities that need to be carried out at periodic intervals.

These include:

- Development of a Cyber Fraud Risk Management Policy Framework (including incident management, enhancement and assessment)
- Cyber fraud controls design and review
- Continuous monitoring systems
- Cyber forensic incident response and investigation.

Further, detective/monitoring technologies, verification of transactions, dual factor authentication for each and every transaction should be adequately configured for timely detection of fraudulent transactions and employing adequate countermeasures and corrective controls.

While the above is a sound framework for cyber risk management and protecting digital payments infrastructure for banks, wallet providers, processors, the key ingredients for success of such a framework are:

- Boards/senior management of organisations should take cognisance of the internal/external threats in their organisations
- Adequate support from the management
- Development of adequate cyber security and response mechanisms

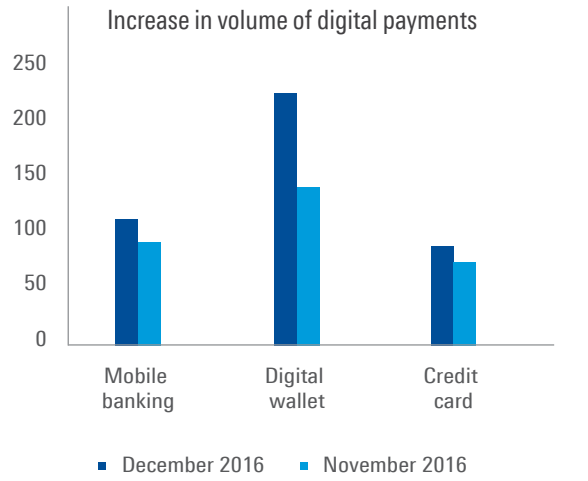
Last, the sustainability of such cyber risk management and digital payments protection programme requires tireless efforts to be put into creating and maintaining continuous awareness among end users, operators, processors, merchants as well as banks. As the saying goes, you are only as strong as your weakest link.

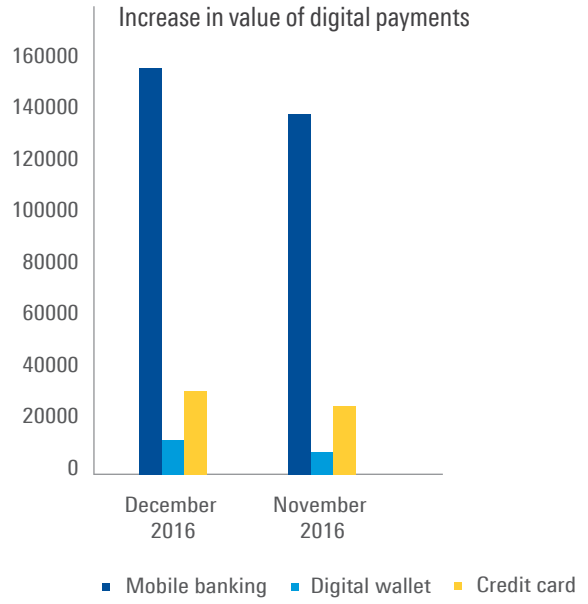
Sudesh Shetty
Partner
Forensic Services Investigation

Sudesh is a Partner with Forensic Services, KPMG in India. He has more than 15 years of experience in forensic and fraud investigation across life sciences, industrial, IT-ITeS, and consumer markets sector.

Infographics: Digital payments and ecosystem

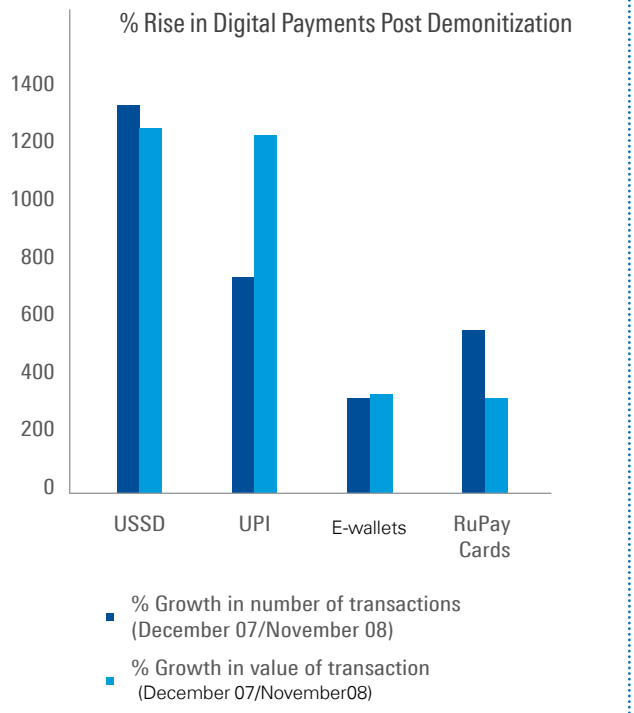
Rise in digital payments post demonetisation





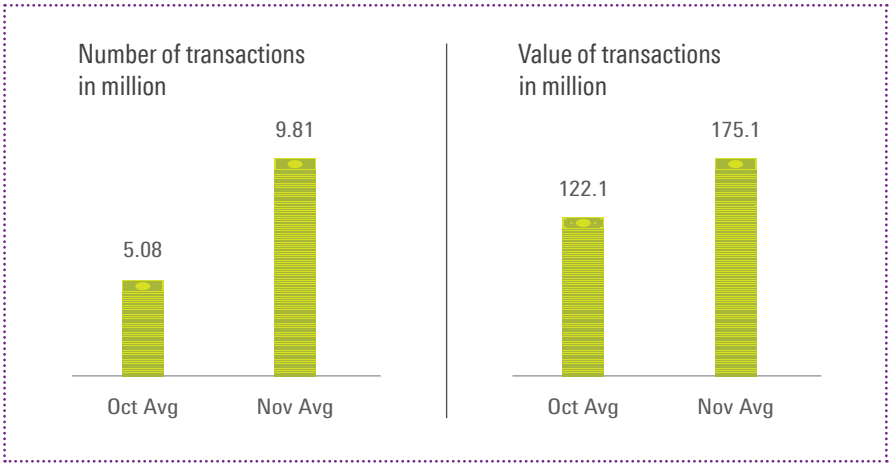
Source: Digital revolution cashes in on demonetization effect, Business Line, 12 February 2017

Growth in digital payments within **one month** of declaration of demonetisation



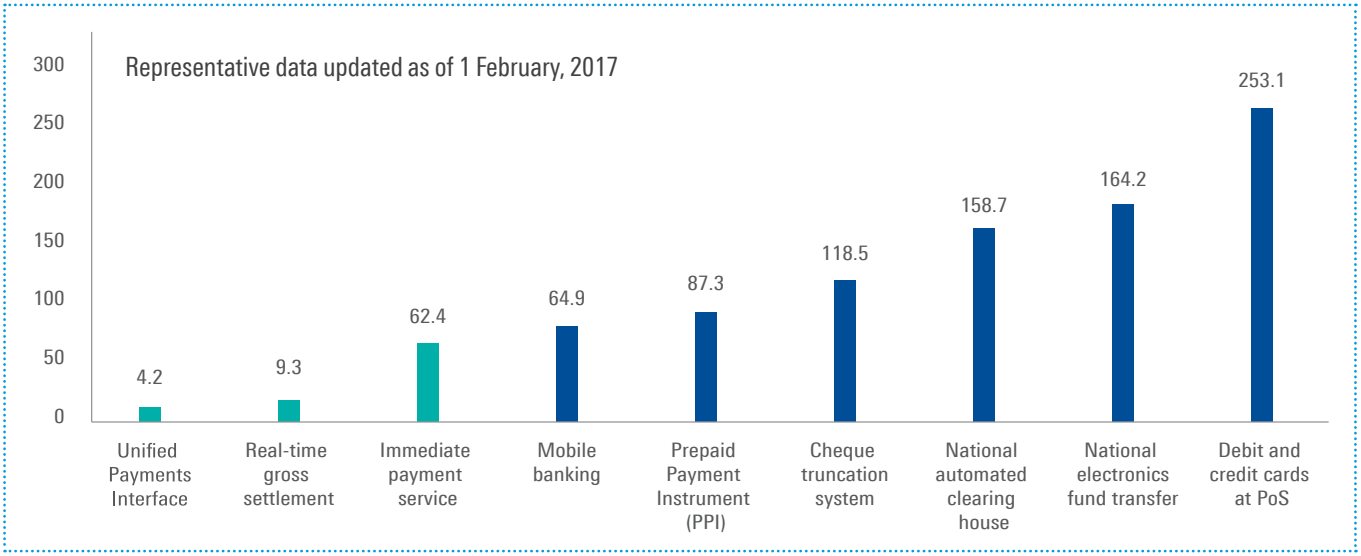
Source: Digital payments soar by up to 30% after demonetization, The Times of India, 10 December 2016

Upsurge in transactions from **Point of Sale (POS)** system post demonetisation



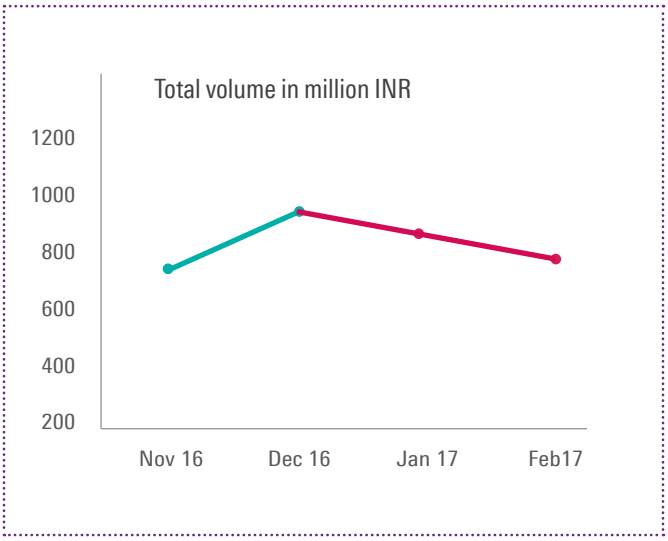
Source: Digital payments soar by up to 30% after demonetization, The Times of India, 10 December 2016

Volume of transactions using digital channels have **decreased** in the month of February 2017 as compared to December 2016

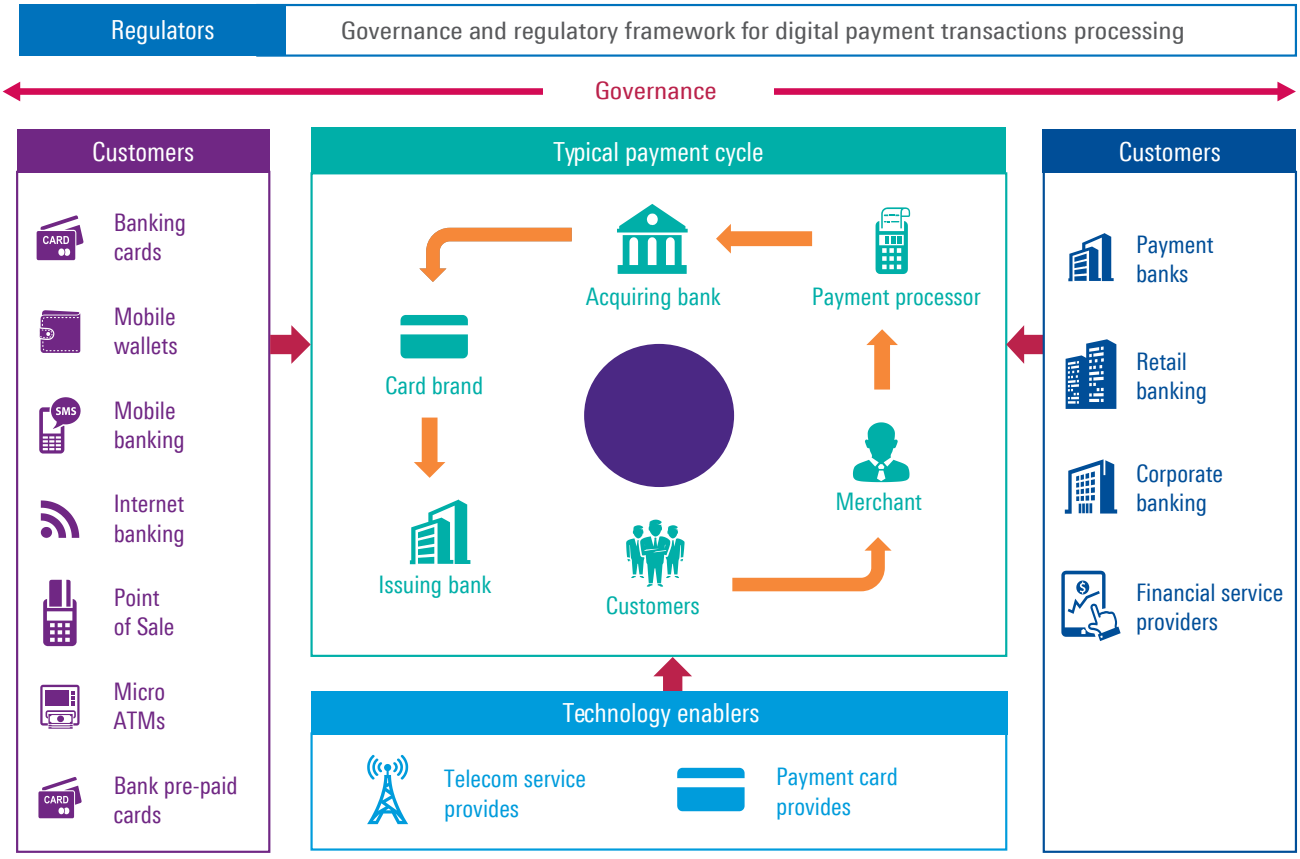


Source: Numbers speak: Digital payment volumes down 10%, reveals RBI data, Business Standard 7 February 2017

Digital payments have **decreased** in the month of January 2017 and February 2017

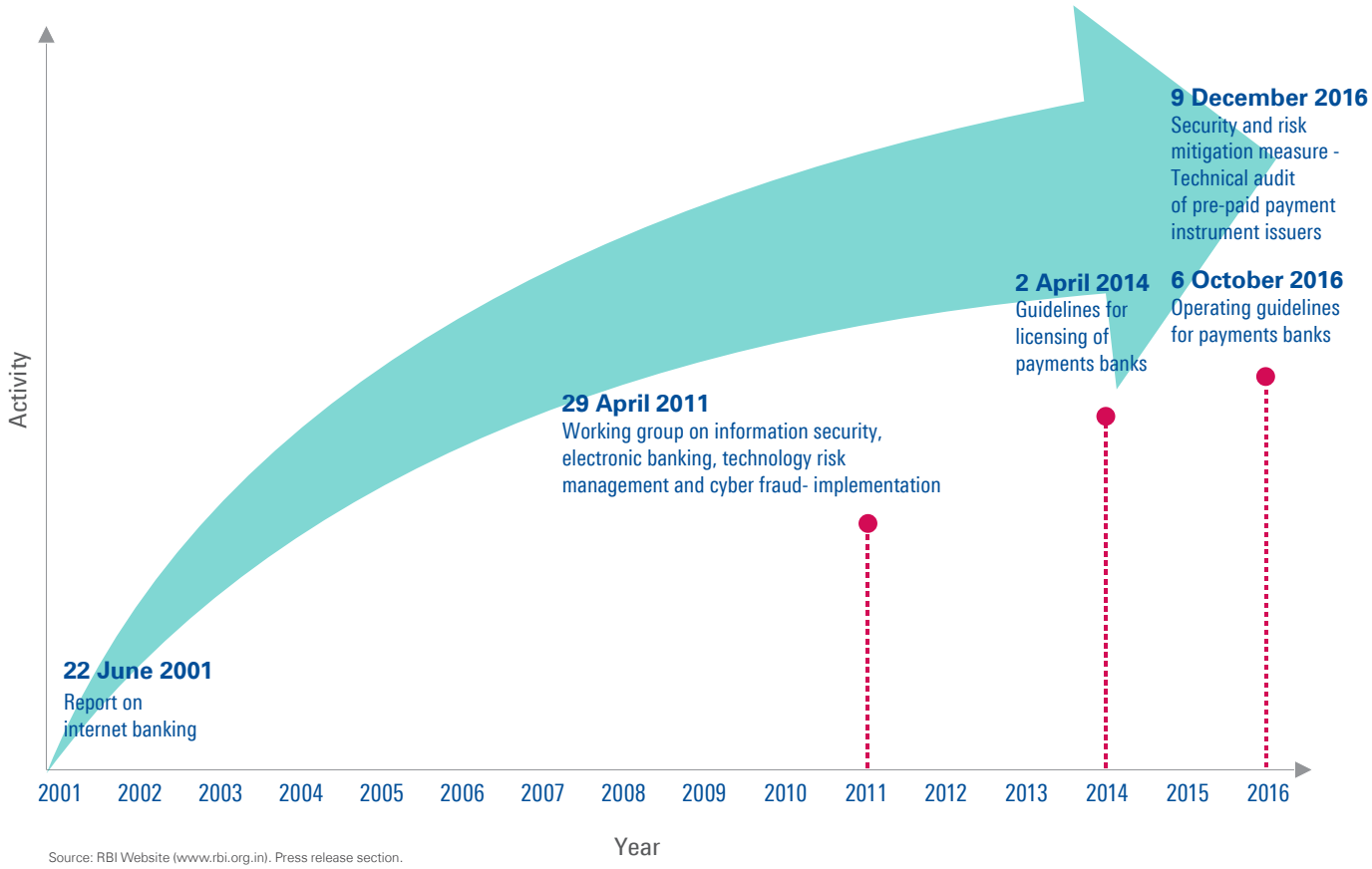


Digital payment - Ecosystem



Source: For illustrative purpose only, KPMG in India

RBI guidelines to strengthen digital payment ecosystem

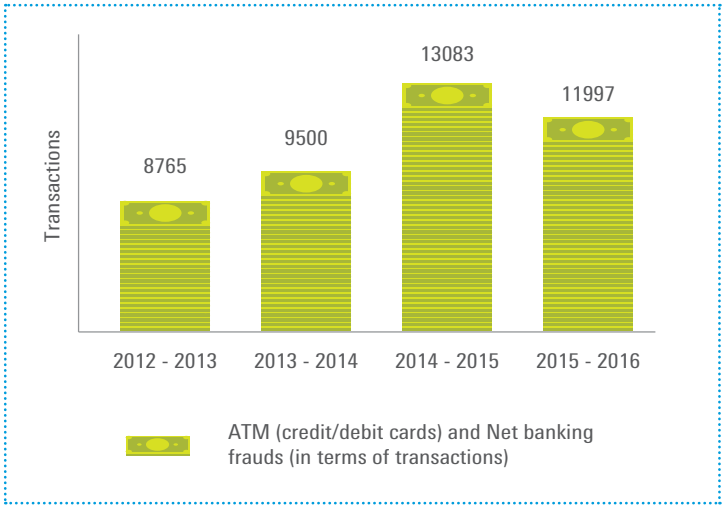


Source: RBI Website (www.rbi.org.in). Press release section.

Key legislations in India

1. Banking Regulation Act, 1949
2. Payment And Settlement Systems Act, 2007
3. Pre-paid Payment Instruments in India (Reserve Bank) Directions, 2009
4. Master Circular in 2014

Fraud spike



Source: 11,997 frauds related to credit, debit, net banking reported in Apr-Dec 2015; DNA Newspaper, 26 February 2016.

Keeping cybercriminals at bay

1. Users should treat their mobile phones as banks
2. Strong and unique passwords should be used on every websites
3. Operating systems, applications and anti-virus should always be up to date
4. Two-factor authentication should be enabled wherever available (particularly for e-mail and financial sites)
5. Link should be typed in the address bar of web browser instead of clicking on the links
6. Link or attachments sent from unidentified sources should be avoided
7. Connection should be secured by clicking the lock on the browser and the users should connect to the correct organisations
8. Accounts should be monitored for unauthorised transactions
9. Users should avoid sending financial or personal information by e-mail
10. Users should avoid clicking links or entering personal information on pop-windows

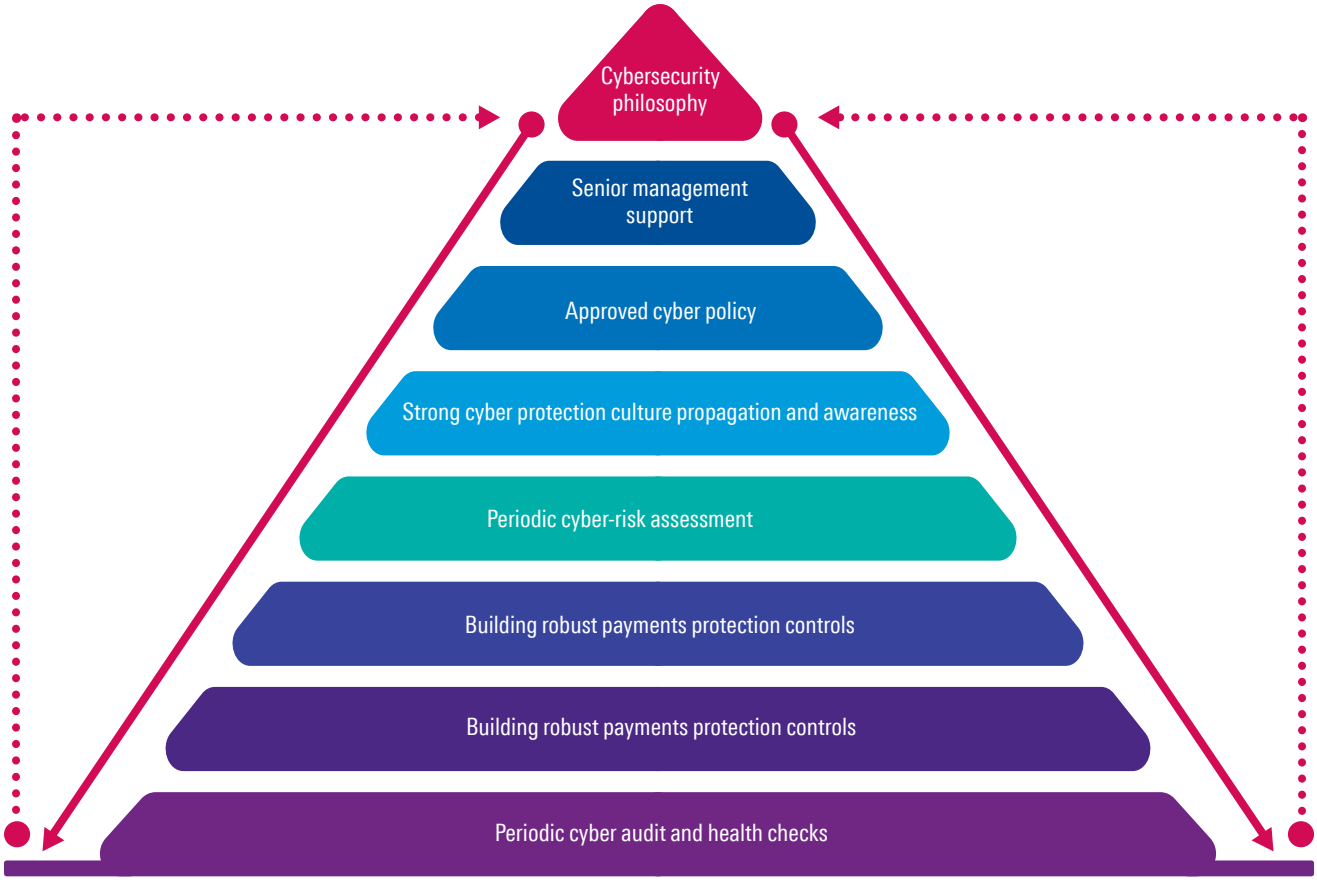
Way forward

With demonetisation, millions of Indians have enrolled for digital payments with mobile payments being the most preferred mode. With such surge in the volume and number of transactions, it is unlikely that the cybercriminals would not be interested. Hence, securing digital payments infrastructure becomes one of the most important concerns for banks and payment service providers such as digital wallet providers. With the use of online payments going up, the incidents on misuse of payments network and data theft are also on the rise.

Building a robust cybersecurity and digital payments protection programme – Our recommendations

Organisations should understand the potential threats of cyberattacks and install leading security architecture to ensure that the transactions are seamless and secure. We suggest the below digital payment protection programme for building robust cybersecurity mechanism:

- Developing a cybersecurity philosophy including protection from third party risks
- Engage senior management for their participation and support for effective implementation of philosophy
- Formulate an effective cyber policy with special focus on digital payments
- Develop strong cyber protection culture by conducting cyber awareness and trainings
- Perform periodic cyber risk assessments
- Build roust payment protection controls
- Perform periodic cyber audits and health checks



Source: For illustration purposes only, KPMG in India

People are the weakest link in the security architecture, hence security should be the shared responsibility of the organisations as well as the users of the digital platform. The end users should also proactively ensure that:

- They use strong, unique passwords
- Keep their operating systems, applications and antivirus up to date
- Enable 2FA, wherever available
- Avoid opening links or attachments sent from unidentified sources
- Ensure that the connection used during transacting is secure
- Monitor their accounts on regular basis to track for unauthorised transactions
- Avoid sharing any personal information over e-mail or call
- Avoid entering personal information on pop-up windows

As per our survey, nearly 90 per cent of the people are unaware of the government's 'DigiShala' initiative. Hence, the government should focus more on educating the customers as well as enforcing basic security standards for organisations. Also all the breaches should be mandatorily reported.

To conclude, the digital payment ecosystem needs to be strengthened, with organisations, users as well as government equally sharing the responsibility of securing the digital payment ecosystem.

Acknowledgements

Harshad Joshi
Hussain Rahat
Ishita Mogra
Jatin Rishi
Mubin Shaikh
Namrata Mehta
Priyanka Agarwal
Rishabh Rane
Ruchika Jaiswal
Sameer Hattangadi
Upalabadhi Singh

KPMG in India contacts:

Nitin Atroley
Partner and Head
Sales and Markets
T: +91 124 307 4887
E: nitinatroley@kpmg.com

Mritunjay Kapur
Partner and Head
Head Risk Consulting
T: +91 124 307 4797
E: mritunjay@kpmg.com

AkhileshTuteja
Partner and Head
IT Advisory
T: +91 124 307 4800
E: atuteja@kpmg.com

Atul Gupta
Partner
IT Advisory
T: +91 124 307 4134
E: atulgupta@kpmg.com

KPMG.com/in

Follow us on:
kpmg.com/in/socialmedia