

Cyber Risks in Digital Transformation

Dr. K. Srinivasa Rao

*Former General Manager, Bank of Baroda & Adjunct Professor,
Institute of Insurance and Risk Management, Hyderabad*

Email: kembais@gmail.com

ABSTRACT

As financial institutions, especially banks, rely more on technology for service delivery and customers become increasingly engaged with digital banking, the risk of cyber threats grows due to enhanced vulnerabilities. Cyber risk refers to the potential financial losses institutions face from technology breaches, customer fraud, operational disruptions, or reputational damage caused by digital system disruptions or data breaches. When customers are targeted for identity theft, they may fall prey to cybercriminals' tricks, eroding trust in digital banking systems. Hence, reinforcing protective controls against cyber risks is of much greater significance for taking digital banking to the masses.

A cyber-attack is a plan to cause "system failure" or an "external risk event" that disrupts the bank's ability to operate. Such cyber risk events are legally and broadly treated as an Operational Risk. Thus, amid the intensity of digital dependence, Cyber Risk Management has matured into its own highly specialized discipline, with dedicated CISOs equipped with "Cyber control Rooms" and data dumps and heatmaps constantly buzzing on the dashboard.

Banks may lack iron domes – invincible firewalls to safeguard their internal technology architecture, leaving them vulnerable to cyber threats. Therefore, management of Cyber risks calls for exploring all operational risk control tools, more importantly, the institutionalization of the Risk Control and Self-Assessment (RCSA) framework, as upside risks could increase the capital charge component, serving as a buffer against operational risks.

Before diving deep into the changing forms and intensities of cyber risks, a glance at the evolving and deepening digital banking system will be pertinent for connecting the dots of digital transformation (DT). Unless the density of DT is well understood, the cyber risks and their impact cannot be fully assessed. Along with DT, securing digital modes and educating users will be equally important for financial intermediaries providing digital banking services.

1. PROGRESS OF DIGITAL TRANSFORMATION

The DT of the domestic banking system began in the 1980s with the use of standalone automated ledger posting machines (ALPMs), a modest start that later evolved into the standalone computerization of bank branches in the early 2000s. The real benefit of DT came with the adoption of interoperable technology, which enabled anytime, anywhere banking through the Centralized Online Real-time Environment (CORE) banking model sometime between 2005 and 2010.

Different Public Sector banks (PSBs) adopted the CORE banking system at different points in time, based on their internal capacity, among other factors, to invest in technology, while new-age private banks entered the banking sector as part of bank reforms from 1992 onward, setting standards for technology exploration in the banking system. This helped PSBs upgrade their technology to compete with private peers and onboard new customers to the technology mode. The demographic shift and the tilting of the customer base towards Gen Z and millennials prompted PSBs and old private banks to adopt technology more quickly to stay competitive in the sector, thereby accelerating DT.

The formation of strategically important institutions such as the Institute for Development and Research in Banking Technology (IDRBT) in 1994, the Indian Financial Network (INFINET) in 1999, and the National Payments Corporation of India (NPCI) in 2008 enabled the proliferation of technology-driven alternative services. It enabled remote banking services, where traffic for payment and settlement transactions increased much faster as a daily requirement.

The merits of DT lie in its strategic shift from a traditional, branch-centric model to a virtual, technology-first ecosystem accessible remotely, anytime, anywhere. It is not just about “going paperless,” but about reimagining the entire banking lifecycle—from customer onboarding to credit underwriting—using centralized data analytics and intelligence inputs.

By now, the digital penetration has moved from being an “alternative” channel to the primary mode of engagement for over 70% of urban and 45% of rural Indians.

2. PHASED DIGITAL TRANSFORMATION

Thus, the journey of DT can be briefly categorized into three distinct phases. (1) Along with the introduction of Standalone Computers and MICR (Magnetic Ink Character Recognition) for automatic clearing of cheques, the mid-2000s saw banks migrating to centralized databases by using core-banking solutions (CBS). Centralized data centres and forming disaster recovery centres for standby data protection that were built to preserve customer and operational data.

The RBI introduced remittances through RTGS/NEFT systems between 2004 and 2005, professionalizing fund transfers. Internet banking (1996) began with ICICI Bank taking the first step to introduce it in India, soon followed by others.

Another major leap in DT came with the introduction of digitally driven Centralized Know Your Customer (CKYC) information under the Prevention of Money Laundering Act (PMLA)-2002, through the Central Registry of Securitization, Asset Reconstruction and Security Interest of India (CERSAI), formed in 2011-12, initially meant to record borrowers’ mortgages, which was extended to undertake CKYC.

Thus, in 2012, CERSAI’s mandate was expanded to include the registration of security interests arising from the assignment of accounts receivable under the Factoring Act,

2012. In January 2016, its role was further expanded to cover security interests in movable and intangible assets, as well as all other types of mortgages.

Subsequently, CERSAI began serving as a repository for CKYC data management, and CKYC became operational in July 2016 for Reporting Entities regulated by RBI, SEBI, IRDAI, and PFRDA. Once an individual obtains a 14-digit CKYC registration no, it can be used by any regulated entity as valid KYC, so that repeated KYC is not needed to identify the person. This has served as a foundation for KYC validity, speeding up DT. So far, 103 crore CKYC records have been registered with CERSAI, serving millions of customers and lakhs of entities – a digital foundation. Going forward, the Central KYC Record Registry (CKYCRR) will be accessible to individuals to check KYC status once the infrastructure is ready by 2027.

Phase (2) witnessed the Infrastructure Revolution, notably after the 'Digital India' mission was launched in 2015, which moved banking from computers to mobile phones and made it inclusive. The public digital infrastructure has been another pillar supporting the DT in the financial system. The convergence of Aadhaar (Identity), e-KYC (Paperless onboarding via CERSAI), and UPI (Payments) acted as a massive booster, forcing millions to learn digital payment tools for convenience. The UPI app, introduced in 2016 by NPCI, transformed mobile numbers into bank accounts, making payments as simple as sending a text message.

Phase 3 experienced the entry of AI & the "Hyper-Digital" Era (2021 – 2026), driven by the challenges posed by COVID-19. It accelerated "Video KYC," and many financial intermediaries began moving towards digital loan processing, particularly targeting retail borrowers.

To promote user safety, the RBI launched a public directory of Digital Lending Apps (DLAs) on its website, starting from July 1, 2025. This list includes all DLAs operated by RBI-regulated entities. It serves as the official, verifiable record of legitimate lending apps in India—those supported by an RBI-registered bank or NBFC. Currently, the directory lists about 1,200–1,500 registered DLAs associated with regulated entities.

Google removed more than 4,700 illegal loan apps from the Play Store over two years following a policy change that only allows apps associated with regulated lenders. The introduction of the concept of banks setting up Digital Banking Units (DBUs) to provide unmanned, full-fledged virtual banking services in brick-and-mortar locations, with 100% self-service and paperless operations, has been a recent innovative model for delivering services digitally.

3. IMPACT OF DIGITAL TRANSFORMATION

Since 2005, DT has been pursued in mission mode as banks adopted interoperable technology. The first non-branch banking infrastructure was an ATM. By March 2026, ATMs numbered 2,65,000, exceeding the 1,65,000 bank branches. Micro ATMs (handheld

devices) reached 16.5 lakh; debit cards totalled 104 crore; credit cards 12 crore; QR codes and sound boxes at merchant outlets reached 57 crore; and digital banking units numbered 84.

The expanded digital infrastructure has resulted in a remarkable surge in digital transactions. The increasing volume and funds processed through digital channels highlight technology's essential role in payment and settlement systems. From 2014 to 2024, digital transaction volumes expanded 38 times, with the total value more than tripling. The CAGR during this period was 52.5% in volume and 13% in value.

Over the past five years, volumes increased by 6.6 times and values by 1.6 times—corresponding to a five-year CAGR of 46% and 10%, respectively. This represents not just incremental growth but a fundamental change in how customers use the digital payment system for their financial transactions.

The current digital payments landscape encompasses a wide range of tools, including credit and debit cards, rapid payment platforms such as UPI, IMPS, NEFT, RTGS, digital wallets, mobile applications, and online banking. Traditional paper-based methods have also been digitized—cheques are now processed via the Cheque Truncation System (CTS) and the National Automated Clearing House (NACH), which greatly accelerates fund transfers. In CTS, only images of cheques are transmitted electronically, removing the need to physically transport the cheques.

This framework is primarily based on the Payment and Settlement Systems Act of 2007, which empowered the RBI to create the current infrastructure. According to this law, Payment System Operators (PSOs) are responsible for core functions like routing, clearing, and settlement. Meanwhile, Payment Service Providers (PSPs) manage the customer-facing aspects, including wallet applications, payment gateways, and merchant onboarding. With the rise in transaction volumes, the risk of cyber fraud has also increased. The growing reliance on digital technologies has further broadened the scope for cyberattacks.

Such digital banking transformation comes in the backdrop of the massive Financial Inclusion (FI) efforts. The (FI) Index stood at 67 in March 2025, up from 53.9 in March 2021 and rising from its base index of 43.4. The RBI's half-yearly Digital Payments Index stood at 551 in September 2025, up from a base of 100 in March 2018. More and more services are moving to digital modes, intensifying the DT. As the user base increases, ensuring operational efficiency and safety of the network becomes challenging for regulated entities. Despite adopting the latest versions of software, the systemic vulnerability cannot be undermined.

4. TECHNOLOGY ARCHITECTURE

The foundational technology architecture is undergoing rapid transformation to accelerate DT in line with state-of-the-art technology, improving operational efficiency and enabling

faster delivery of safe and secure services to end users. Before the cyber risks are pinpointed to the institutional technology platforms, it will be interesting to understand their multi-layered architecture, which can explain the enormity of the vulnerabilities and the massive protective layers institutions must provide to ensure the safety of digital banking with equally strong and invincible firewalls.

The technology architecture is developed and innovated over a period of time by its alignment with the developments of the latest versions of technology, but shall constitute certain essential system configurations comprising (i) Core Digital Hardware Infrastructure – Data centres and computer application servers, database servers, disaster recovery centres/data backup systems. (ii) Core banking and payment hardware – Hardware security modules, Crypto processor, mechanism for encryption, decryption, authentication, and digital signing, mainframes, and payment switches. (iii) Network perimeter hardware – enables wire transfer, loan approval process, bank transactions, and trading algorithm runs across a network that could be targeted in a cyber-attack. (iv) End-User, Branch & Self-Service Hardware – hardware such as ATMs, POS terminals in merchant networks, and teller desktops at branches are the service outlet infrastructure forming a distributed attack surface against which protections are needed. (v) Cloud, Edge & Mobile Infrastructure – financial entities use hybrid or fully cloud-based infrastructures, providing greater flexibility and scalability. Edge and IoT devices include branch cameras, sensors, smart infrastructure, and customer mobile devices (banking apps), providing last-mile digital connectivity to users.

In this dynamic digital infrastructure, the entities will need to protect Data Centres, Core Banking & Payment Hardware, the connecting network, ATMs, branches, and endpoints, building a robust system to develop resilience against cyber threats and monitor cloud security. Despite every possible measure, financial services globally experienced 1,735 attacks per week in 2025—a 15% increase from 2024—and further threats continue to loom. To achieve further DT, financial institutions will need to effectively address the following types of cyber threats, accounting for their nuances and evolving forms.

5. CYBER RISKS TO INSTITUTIONS

As DT rapidly moves bank customers to a technology-first model, exposure to cyber risks increases for both institutions and their users. Among the key cyber risks are those to the technology infrastructure of regulated entities. While there are innovative methods of cyber-attacks on the digital hardware, software, and firmware that could potentially disrupt the services or compromise internal controls, where the hackers can jeopardize the services in many ways, yet the most common threats to regulated entities include

5.1 Ransomware & Ransomware-as-a-Service (RaaS)

Numerous reports indicate that ransomware incidents in the financial sector reached 451 in 2025, a notable increase from the previous year. This escalation demonstrates the

increased maturity of ransomware-as-a-service (RaaS) platforms and the more advanced extortion tactics employed. Attackers now use a combination of encryption, data theft, public shaming, and direct pressure on executives and clients to successfully bypass firewalls that are regularly tested for vulnerabilities.

Rather than launching random attacks, cybercriminals target sensitive organizations, often high-profile ones such as banks and credit unions, to extract large ransom payments. The sanctity of data leaves organizations helpless in certain situations, as access to it is blocked and held by cybercriminals. This is despite institutionalizing system audits, vulnerability testing, and ethical hacking exercises to protect systems against external cyberattacks.

5.2 Social Engineering through Phishing Attacks

Beyond digital modes used for operational purposes in banking and financial services, technology is also used for routine administrative tasks. Taking advantage of this, cybercriminals use phishing as the leading initial attack vector, accounting for approximately 16% of breaches and now surpassing stolen credentials.

Phishing campaigns, business email compromise (BEC), and invoice fraud schemes now use AI-generated content that is both accurate and fluent, making them harder to detect with traditional email filters. Employees often succumb to these tactics and inadvertently download malicious files, putting the organization at considerable risk.

To overhaul digital banking security, the RBI issued a directive requiring all commercial and licensed banks to migrate their official corporate websites and net banking portals from generic top-level domains (such as .com or .co.in) to the exclusive 'bank.in' domain. The migration deadline was set for October 31, 2025.

5.3 Distributed Denial of Service (DDoS) Attacks

DDoS attacks are among the most formidable cyber threats to enterprises. They can hinder customer interactions with financial services by delaying or halting access to websites and apps. These attacks may also interfere with communications between financial firms and third-party providers or employees by blocking access altogether.

The data shows a 105% increase in DDoS attacks in 2025, primarily due to coordinated hacktivist efforts targeting major financial platforms and services. These short, intense bursts—often dozens in a single day—have challenged the DDoS mitigation capacities of financial institutions. As a result, enterprises must allocate more resources to strengthen their defences against such powerful cyber-attacks.

5.4 Disruption of Vendor Services

Technology systems face ongoing threats that could lead to disruptions and unauthorized control. In 2025, supply chain compromise was a factor in about 30% of cyber breaches in

financial institutions. Common entry points included file transfer solutions, managed service platforms, and API-based services, all of which have privileged access to sensitive data.

Organizations relying on outsourcing vendors face risks of disrupting their value chains. Supply chain attacks often target weak points in vendors, partners, and software providers that banks and FinTechs depend on daily. Institutions continuously seek ways to shield their controls from cybercriminals, engaging in an ongoing effort to enhance cybersecurity and resilience.

5.5 Use of AI for Cyber-Attacks

Cybercriminals are increasingly leveraging AI tools to execute a variety of attacks against organizations. By 2025, threat actors had integrated AI into different stages of their attack cycle, such as reconnaissance, identifying vulnerabilities, and activities after gaining access.

Automated vulnerability scanning powered by machine learning has reduced the time between vulnerability disclosure and active exploitation. Additionally, advanced malware can now adapt its behaviour dynamically during runtime, responding to security measures, which makes signature-based detection more challenging and extends dwell times.

5.6 Insider Threats

Though by exception, insiders could collaborate in cyber-attacks. Malicious insiders, whether recruited or acting independently, can provide direct access to sensitive data and systems within financial institutions.

Many social media platforms have emerged as a prominent means for advertising and recruiting insider services targeting the financial sector. Misleading information and malicious content with a nexus to disgruntled individuals can harm companies. Social engineering tools use innovative methods to digitally attack entities by obtaining clues from in-house personnel, though this is rare.

5.7 Advanced Persistent Threats (APTs)

Amid ongoing cyber-attacks, institutions should be ready to counter lingering cyber disruptions that can slow operational efficiency.

Accordingly, the financial institutions may face a significant increase in advanced persistent threats (APTs), which involve highly targeted, prolonged cyber-attacks aimed at stealing sensitive data or disrupting operations.

Nation-state-backed groups like Lazarus Group (North Korea) have demonstrated a broad range of targets, including cryptocurrency exchanges and financial institutions. Their campaigns are driven by financial profit, cyber espionage, and sabotage—employing sophisticated spear-phishing emails, malware disguised in image files, and watering-hole attacks.

5.8 Cloud Security Breach to Lead to Data Leaks

Data breaches and leaks increased by 73% in 2025, highlighting ongoing vulnerabilities in cloud security, identity management, and third-party ecosystems. Initial Access Brokers focus on infiltrating financial networks and selling access credentials to other threat groups, such as ransomware operators. They use methods such as phishing, malware that steals information, and exploiting remote desktop protocol (RDP) credentials. From April 2024 to April 2025, more than 6,400 posts related to financial-sector access were observed on criminal forums.

5.9 Inadequate Internal Controls to Manage AI Risks

In the AI age, building internal competency to face AI-driven attacks will be essential to stay competitive, but many entities do not invest in AI technology to mobilize such capacity.

Among organizations that faced AI-related security issues, 97% did not have sufficient AI access controls. Shadow AI refers to the unauthorized, unapproved, and unmonitored use of AI tools such as chatbots or code generators within a company. Employees frequently resort to shadow AI tools to enhance productivity, often bypassing official IT and security procedures, which can put organizations at risk.

In 2025, about 20% of AI-related breaches involved shadow AI models or applications that were deployed without formal security assessments or governance.

5.10 Quantum Computing Threats (Emerging)

Quantum computing operates at a different level within the technology value chain, requiring current encryption methods to be adjusted for these new environments; failure to do so could threaten the stability of the technology framework.

Entities need to align with the measures specified in the EU's Digital Operational Resilience Act (DORA) to update their systems effectively. They should also evaluate if their current provisions support quantum-safe cryptographic methods, considering the potential future threat quantum computing poses to existing encryption standards. When handling Digital Transformation (DT), it is vital to upgrade standards and technology versions concurrently; neglecting this may elevate the risk of security breaches.

5.11 Collateral Risks of Geopolitical Attacks

In a connected world, geopolitical risks are rising. Growing global conflicts greatly raise cyber threats to the financial industry, including increased ransomware and phishing attacks. Regulators are calling on financial institutions to focus on essential cybersecurity practices, such as multi-factor authentication, managing privileged access, vulnerability management, and securing or disabling remote desktop protocols.

Thus, the cyber threat landscape for regulated financial entities spans opportunistic cybercrime (ransomware, phishing), state-sponsored espionage (APTs), systemic risks (supply chain, third party), and emerging threats (AI-driven attacks, quantum cryptography).

Investing in technology to adopt the latest versions is an essential part of managing cyber threats. Whether it is AI or quantum computing, entities should protect their technology infrastructure from cyber breaches that can jeopardize operational efficiency and service quality, especially when DT is fast penetrating and affecting a large number of users.

When considering cyber risks, the interconnected BFSI ecosystem's nature means that a single cyber-attack can cause widespread effects, impacting multiple entities beyond the original target. The financial industry handles over 15 billion UPI transactions each month and hosts more than 9,000 FinTech companies, ranking as the third-largest FinTech market worldwide. As digital payments lead the digital transformation, they are expected to reach \$3.1 trillion by 2028, creating an extensive attack surface due to the high concentration of financial activity on digital platforms.

5.12 Risks from Anthropic's Claude Mythos

Mythos is the newest model in Anthropic's Claude AI lineup, marking a significant advancement in AI, especially in cybersecurity. This general-purpose Large Language Model (LLM) is built to handle intricate, multi-step software engineering and security tasks efficiently. It also has the ability to identify zero-day vulnerabilities more quickly than human teams.

Zero-day vulnerabilities are security flaws in software, hardware, or firmware that are unknown to developers, giving them "zero days" to fix before attackers exploit them. These vulnerabilities can bypass security measures and increase the risk to the system.

Mythos stands out because of its capability to automatically identify critical vulnerabilities in popular software and infrastructure much faster than human researchers. It can also fix these issues when used defensively, but if misused maliciously, it could pose significant threats. Consequently, it is a very powerful tool with potential dangers.

Anthropic asserts that Mythos has uncovered significant flaws in major operating systems and web browsers, including vulnerabilities that went unnoticed for decades. The rapid and large-scale nature of these discoveries allows for timely fixes and enhances operational efficiency as a defensive measure.

This is a valuable contribution to AI research, but if misused, it could exploit the vulnerabilities Mythos aims to identify and fix. Therefore, regulators and regulated entities worldwide are worried that cybercriminals might weaponize it for cyber-attacks, transforming innovation into a new cyber threat.

After discussing the specific vulnerabilities of financial institutions that can delay Digital Transformation (DT), it's important to highlight some cyber threats arising from institutional weaknesses or users' limited digital literacy. These cyber threats to individual users, whether originating from institutions or independently, add another layer to the looming risk.

6. CYBER RISKS TO USERS

When navigating digital mode, users must be mindful of potential cyber risks. This includes keeping login IDs and passwords well-protected and changing them frequently and at random to ensure the safekeeping of their funds. There are unique methods of cyber fraud often used against customers, ranging from identity theft to digital arrests, AI-generated fakes to voice mimics.

Thus, in a highly interconnected digital ecosystem where open banking APIs and cloud-native frameworks are in use, vulnerabilities cannot be avoided. Digital banking has brought a tectonic shift in how banking services are delivered, but it has also exposed retail users, corporate clients, and financial professionals to a multi-vector threat landscape.

It calls for continuous upgrading of the protection layers on the technology platform, and users should educate themselves about potential cyber-attacks and how to respond to them. Stakeholder activism to fight cybercrime is essential to harness the full potential of the ongoing DT. While there are multiple innovative cyber threats in the digital ecosystem, they can be broadly grouped into the following.

6.1 Social Engineering Methods

Cyber fraudsters know that many customers are not fully aware of the nuances of protecting their identities. They can fall prey to conversations initiated by fraudsters, whose methods of engagement appear very genuine. Such natural-looking attacks exploit human psychology and behaviour rather than software vulnerabilities. Of late, cybercriminals have been using artificial intelligence techniques to bypass traditional anomaly detection systems.

Common cyber frauds targeting customers include phishing, vishing, and smishing. Digital arrest, swim swap, OTP frauds, UPI frauds, fake QR codes, screen-sharing frauds, counterfeit card fraud, ATM skimming, card-not-present overseas frauds where an OTP is not required, WhatsApp frauds, fake IPOs, and many other novel ways to defraud customers and usurp funds.

Cybercriminals even use generative AI to draft highly personalized, error-free emails or text messages that appear to be from regulatory bodies or banks. A rising sub-vector is Quishing (QR code phishing), which embeds malicious links in QR codes to bypass standard email filters and harvest credentials.

Fraudsters leverage voice and video deepfakes to bypass Know Your Customer (KYC) biometric verification or to execute corporate social engineering (e.g., impersonating an executive to authorize an urgent, high-value wire transfer).

Users face complex psychological manipulation, such as fake “customer care” numbers appearing in search results, calls from bank branches, extortion through staged accidents or kidnappings, or by creating emergency situations, and being lured into money laundering activities through mule accounts. As banking shifts heavily to mobile apps and decentralized interfaces, the entry points for malicious code have multiplied with a widely spread mobile banking culture.

Users are frequently tricked into downloading apps from unofficial sources. These malicious packages deploy infostealers or spyware that log keystrokes, intercept screen captures, and steal active session tokens.

Cyber criminals use automated bots, and threat actors test millions of leaked credential combinations across financial portals. Combined with SIM-swapping (intercepting cellular networks to steal OTPs), this allows attackers to gain full administrative control of user accounts.

Unsecured public networks or compromised routers allow attackers to intercept data packets between a user’s device and the banking server, capturing sensitive transaction details in real time. Devices having bank account linkage should refrain from using public networks to secure their systems. These threats target the backend stability, availability, and data integrity of financial institutions and FinTech platforms. Investing in customer education to impart digital literacy to protect them against cyber risks is essential, along with upgrading security features.

7. FRAUD RISK MANAGEMENT

The DT could have been more impactful if digital fraud had been better prevented. Despite improvements in digital fraud controls, the number of cases rose from 2.6 lakh in 2021 to 28 lakh in 2025. Correspondingly, losses increased from Rs. 551 crores to Rs. 22,931 crores in the same period. Although institutional safeguards are quite strong, they still require further strengthening.

The RBI progressively improved and layered fraud protection measures. It required an Additional Factor of Authentication (AFA)—usually an OTP—for all card-not-present transactions, like online payments. Magnetic stripe cards were replaced by EMV Chip and PIN technology, reducing cloning risks. Additionally, mandatory SMS and email alerts for all transactions enabled customers to identify unauthorized activity immediately.

Customer liability protection became a key element of RBI policy. If fraud happens because of the bank’s negligence or if a third-party breach is reported within three working days, the customer is not liable. Reporting within four to seven working days limits liability to

Rs. 10,000 for basic savings accounts. Banks were also required to offer 24/7 reporting channels—toll-free numbers, SMS, and apps—to report unauthorized transactions. However, these protections apply only if the customer’s identity remains secure.

The Positive Pay System added an additional verification step for high-value cheques, causing banks to re-verify cheque details before processing, which helps decrease the risk of cheque-cloning fraud.

Customers now possess detailed control over their payment methods. Using mobile apps, they can turn off international or e-commerce transactions and establish per-transaction and daily limits for UPI, cards, and net banking. These restrictions help minimize potential damage even if their credentials are compromised.

At the ecosystem level, the RBI established the Indian Digital Payments Intelligence Corporation (IDPIC) in October 2025. Unlike traditional bank monitoring, IDPIC leverages Big Data and AI to oversee the entire payment ecosystem in real time. Additionally, Mule Hunter.AI is a specialized tool created to detect mule accounts, which fraudsters use to layer and transfer stolen funds throughout the banking network.

The reality is: even a robust regulatory framework is ineffective if the end user remains unaware, inattentive, or sluggish in response. Customer vigilance serves as the final—and frequently the most critical—line of defence.

Starting April 1, 2026, two-factor authentication with a dynamic, risk-based second layer will be mandatory. Additional cybersecurity measures are being developed. The RBI aims to establish India as a leader in digital and real-time payments, guided by three principles: customer-centricity, safety-by-design, and interoperability. Achieving this will require improved technology and regulation, as well as a digitally literate public that is aware, vigilant, and capable of self-protection.

The REs, while protecting their internal technology architecture and firewall security, must also collaborate with other agencies to improve users’ digital literacy.

RBI and REs work together to build comprehensive structured financial literacy networks, beginning with district-level Financial Literacy and Credit Counselling Centres, expanding to block-level Centres for Financial Literacy (CFLs), and ultimately extending to villages through Business Correspondents (BCs) and State Rural Livelihoods Missions. These efforts focus on increasing grassroots awareness among bank customers regarding safe digital banking practices.

8. CONCLUSION

The discussion on the DT demonstrates the massive inroads the financial system has made in the last two decades, adopting state-of-the-art interoperable technology and providing last-mile digital connectivity through financial and digital inclusion. Virtual banking services could provide convenience and value to the users.

Financial institutions must continually sharpen their cyber threat intelligence framework to protect their internal technology architecture from cyber-attacks. It will need not only technological upgradation but also the imparting of knowledge to its workforce and the development of a competent talent pool to monitor digital infrastructure and realign controls to ensure system security and operational efficiency, keeping in view new forms of cyber tools that could threaten the system.

Extensive use of AI to protect may become incumbent upon advancing the DT. Besides the collaborative protective efforts of regulators and regulated entities, the inclusive participation of users for the safekeeping of institutions will become more important.

Only an alert and agile workforce across all three lines of defence in cyber risk management should work with all stakeholders to ensure the continued progress of DT in a safe and secure digital ecosystem.

REFERENCES

1. Bharadwaj, A, El Sawy, OA, Pavlou PA & Venkatraman NV (2013). Digital business strategy: Toward a next generation of insights. *MIS Q.* 37(2):471-482.
2. Chakrabarti R & Sharma M. (2023) Digital public infrastructure and inclusive growth: Evidence from India's transformation. *J Dev Stud.* 59(8):1245-1267.
3. Das, S. (2024) Digital public infrastructure and emerging technologies [Internet]. Bank for International Settlements. Aug 28 [cited 2026 Jan 15]. Available from: <https://www.bis.org/review/r240828p.htm>
4. Demirgüç-Kunt, A, Klapper, L, Singer, D & Ansar, S. (2022) The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID19. Washington (DC): World Bank Publications.
5. Gulati, M. (2016). Digital India: Challenges and Opportunities. *International Journal of Management, Information Technology and Engineering*, 4(10), 1-4.
6. Gupta, N., & Arora, K. (2015). Digital India: A Roadmap for the Development of Rural India. *International Journal of Business Management*, 2(2), 1333-1342.
7. Jani, J., & Tere, G. (2015). Digital India: A Need for Hours. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(8), 317-319.
8. Kedar, M. S. (2015). Digital India: A New Way of Innovating India Digitally. *International Research Journal of Multidisciplinary Studies*, 1(4).
9. Koregaonkar, K. T. (2016). Digital India: A Program to transform India into a Digitally Empowered Society. *International Journal of Business Quantitative Economics and Applied Management Research*, 2(9), 41-52. 14.
10. Schwab, K. (2016). *The Fourth Industrial Revolution*. World Economic Forum.
11. Turing, A. M. (1936). On Computable Numbers. Proceedings of the London Mathematical Society.

WEBSITES

1. <https://rbidocs.rbi.org.in/rdocs//PublicationReport/Pdfs/PAYMENTSVISION2028270326500316AFADEB47259CB970132BA01304.PDF>
2. <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/jun/doc2025630578601.pdf>
3. <https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2106794#:~:text=Currently%2C%20UPI%20is%20live%20in,Indians%20to%20make%20payments%20internationally.>
4. <https://claude.ai/chat/fda530ac-0879-4fde-887d-9ef826a167e0>