



Reimagine digital trust in capital markets

Reinforcing investor trust

kpmg.com/in

Foreword by KPMG in India

Capital markets play a crucial role in the economic growth of a country by mobilizing and allocating capital that a growing economy needs. We know that transparency, fairness, efficiency and competitiveness are crucial for a dynamic and vibrant capital market, and trust is its bedrock.

In last few decades capital markets have undergone a significant transformation supported by ever evolving technology. We saw adoption of technology advancements like increase in computing power and high-speed networks powering the initial transformation and are now witnessing further transformation leveraging breakthrough technologies like artificial intelligence, blockchain, quantum computing and 5G. The technology adoption has at one end empowered investors across all age groups to participate in capital markets, bringing investment opportunities at their fingertips. While, at other end enabled all stakeholders in this ecosystem i.e., stock exchanges, depositories, clearing corporations, brokers and information providers in offering services that are efficient, fit-for-purpose and at lower cost. The decade has also seen emergence of fintech that have created new vistas of investing as well as brought new challenges.

The hyper digitalisation of capital markets characterised by automation, interconnectivity across value chain, real-time (or near real-time) processing also poses risks related to security, resiliency, transparency, responsible use, reliability of the ecosystem, which raise questions about trust. In light of this, there is an urgent and continuous need for developing holistic capabilities to ensure that trust in the capital markets is sustained and enhanced. The need for developing these capabilities assumes national and global level importance due to rapidly changing threat environment particularly in cyber security including non-traditional cyber threats emanating from organised crime, globally interlinked supply chains, etc. As technology advancement continues to drive transformative changes at an accelerated pace, it is imperative that trust stands resolute.

The Indian capital markets during its evolution and rapid growth have faced various threats and challenges, which have led to disruption in trade activities, cybersecurity incidents, etc. impacting investor confidence. Market participants, including stock exchanges, clearing corporations, depositories and other market intermediaries, have continuously

been engaged in revamping their business and operations models, strategies, technology setup and SOPs to ensure that ecosystem manifests robust security, resiliency, transparency and thereby uphold investor trust. We believe that digital trust is no longer just a technology matter, but a golden thread that runs through an organisation to enable it to operate with greater responsibility, transparency, efficiency, and security.

As Central Depository Services (India) Limited (CDSL) celebrates its 25th year we present you this report highlighting digital transformation journey in the capital markets industry i.e., democratisation of market access, shorter settlements, higher disclosure norms, decentralised account structure, integration into the global economy and emerging future opportunities. The report then delves into newer technology capabilities vis. artificial intelligence, blockchain, web 3.0, 5G, etc. and ever-increasing challenges to the tenet of digital trust particularly around cyber security. The report explores opportunities enabled by the digital technologies for building a secured and trusted environment. The report also captures key themes discussed in the cyber security symposium - Reimagine digital trust in capital markets held on 7 October 2023.

In this journey, taking cue from Government of India's initiative of Aatma Nirbhar Bharat, आत्मनिर्भर भारत (self-reliant India), particularly around digital public infrastructure, we believe that enhanced cyber security capabilities also need to be indigenously built. The focus should be on entire ecosystem i.e., national, capital market industry, organisational and societal level, as cyber Aatma Nirbhar Bharat, आत्मनिर्भर भारत (self-reliant India) shall support laying the foundation of trust and contributing to our confident march ahead in reaping benefits of a vibrant digital capital markets.

In support of our shared vision of digital trust by design, through this report KPMG in India contributes to building a cyber resilient and self-reliant digital India.



Akhilesh Tuteja

Global Cyber Security Leader,
KPMG International Partner

Foreword by CDSL

India, the land of diversity, is undergoing a profound transformation. Our nation is experiencing unprecedented growth and emerging as a formidable force on the global stage. The recent successes, such as the Chandrayaan-3 lunar mission and our remarkable performance at the Asian games, underscore India's arrival and enduring presence. This growth extends to our capital market, with a surge in digital transactions and increased participation.

At the heart of this remarkable growth in our securities market is a deceptively simple yet profound concept—a five-letter word called trust. Trust is not a static notion; it is a dynamic and ever-evolving force that demands perpetual nurturing and reimagining. It is the power to unite, to shape, and to secure. To truly understand the potency of trust, we need only turn to the timeless inspiration of Lord Krishna, who, in his unwavering commitment to upholding trust in dharma, took on the role of Arjun's charioteer. His actions transcended conventional boundaries, teaching us that trust knows no limits and that individuals can be the driving force behind transformative change.

This potent emotion finds its resonance in our capital markets, where digital trust forms the invisible foundation that underpins our financial landscape. CDSL is not just custodian of wealth but also the guardian of trust for millions of Indians. This trust stretches far and wide, touching the lives of Information Technology (IT) professionals in Pune, women entrepreneurs in Kerala, dedicated army servicemen in the Siachen, elderly citizens in the bustling streets of Kolkata, and countless others who entrust us to safeguard their hard-earned savings and investments.

However, trust doesn't stand alone; it is intricately linked with technology and security. Trust and security are inseparable companions, each dependent on the other. This unique relationship has propelled us to achieve remarkable feats:

- Witness the astounding rise in demat accounts, from a mere 30 million to an astounding 139 million^I in a mere four years
- Observe the extensive participation in our securities market, reaching a staggering 98 percent^{II} of India's pin codes, encompassing tier 1, tier 2, and tier 3 towns

- Recognise the regulatory shift that has mandated demat as the sole mode of share transfer in under 25 years.

While these innovations present remarkable opportunities, they also expose us to new and evolving threats. What was once considered mere technology has now evolved into sentient beings, with artificial intelligence, machine learning, and quantum computing offering immense potential but also posing sophisticated threats in the hands of bad actors. Therefore, safeguarding trust is no longer a choice; it is a moral imperative. Robust cybersecurity in our capital markets is the need of the hour.

In this age, we must harmoniously blend tradition and technology.

This new era of digital transformation unveils India's unparalleled growth story, and it is our shared responsibility to secure it. As we embark on this journey, we delve into the intersection of this growth and digital transformation, exploring not only the opportunities it presents but also the critical role of Digital Trust in securing the future of our capital markets.

This collective effort extends beyond safeguarding wealth or enabling technology; it is our contribution to empower Aatmanirbharta, आत्मनिर्भरता (self-reliance) in the Indian capital markets, empowering every Aatmanirbhar Niveshak, आत्मनिर्भर निवेशक (self-reliant investor). As we embark on this journey, let us remember that trust is the driving force behind our progress, and it is our sacred duty to safeguard it for the generations to come.

Together, as we pave the way for a secure and prosperous digital future for our beloved Bharat, I extend my heartfelt gratitude for your unwavering commitment and dedication to this vital cause.

Jai Hind!



Nehal Vora

MD and CEO,
Central Depository Services (India) Limited

I. Annual Report 2022-23 SEBI, 07 August 2023; Statistics, CDSL update, CDSL, 31 December 2023; NSDL update, NSDL, 31 December 2023;
II. Annual report 2022-23 : CDSL, 17 November 2023



-TheBombay.doodler

An artist's interpretation of CDSL's cyber security symposium held on 7 October 2023 at Mumbai, India

Contents

Executive Summary	6
1. Future is here and what's beyond	8
2. Powering the future	16
3. Risks and challenges	20
4. Managing digital trust by outpacing threats	28
5. Opportunity for India & the World – “AatmaNirbhar Bharat”	36
6. Symposium highlights	42
Glossary	49

Executive Summary

Capital markets serve as a mechanism for the economic development and wealth creation of a country by enabling capital formation and capital inflows required to fuel innovation, growth and prosperity. In recent decades, the Indian capital markets have undergone remarkable transformation riding on the opportunity provided by the country's increasing global importance and disruptive power of digital technology. This evolution has positioned Indian capital markets as a significant player on the global stage, with market capitalisation exceeding INR 373 trillion in listed securities and attracting significant foreign investment of over INR 50 trillion into the Indian equity markets as of H1 2023¹. The growth has been fueled by increased participation of the institutional segments such as foreign portfolio investments, foreign direct investments, private equity, venture capitalists, mutual funds, alternative investment funds, insurance etc., coupled with rapidly increasing retail participation.

The rise of technology-led transformations such as investing using mobile app, T+1 settlement, extended trading hours, direct market access (DMA), electronic KYC (eKYC), electronic delivery instruction slip (eDIS), electronic margin (eMargin), margin pledge mechanism, instant payments, real-time market news, etc. in capital markets have drawn in investors to greater participation in both value and volume terms. If the number of demat accounts can be treated as a source indicator of investor interest, then the last two years itself have witnessed the number of investors accounts swell from approximately 55 million+ to 139 million+ in a population of 1.4 billion².

India is witnessing continuous innovation in the market with introduction of new products and capabilities by not only existing participants but also by India's growing fintech companies. The potential of digital technology has been a keen focus for Securities and Exchange Board of India (SEBI),

encouraging continuous innovations like introduction of optional T+0 and near instantaneous settlement of trades³.

The industry is also embracing cutting-edge technologies like artificial intelligence (AI), blockchain, 5G, and web 3.0. These technologies empower investors to make well-informed trading decisions, automate critical processes, enhance efficiency, and reduce risks. Together, they open a realm of possibilities, fostering a capital market landscape that thrives on innovation.

However, as transformative technologies become mainstream, custodians of the new age digital assets need to address emerging and increasing risks that potentially may impact trust in the capital markets. It should foster stakeholders to confidently participate in wealth creation and country's growth. Thus, stakeholders across the spectrum – government, regulators, industry, organisations, technology participants and society – need to intensify efforts to make components of digital trust i.e., cyber security, reliability, responsible use and transparency central themes as the golden thread across the ecosystem. Core to this endeavour is to build ecosystem wide cyber security measures with focus on investors to build and sustain against emerging threat actors like crime syndicates and state actors. A good example to emulate on building security by design is from Formula-1 racing, wherein safety measures are meticulously designed and integrated into the system (aka racing cars) from the very beginning to protect against accidents.

The Government of India, under the AatmaNirbhar Bharat, आत्मनिर्भर भारत (Self-reliant India) initiative, is determined to build foundational capabilities. With a rich talent pool, strong government support, and an innovation-driven culture, India is poised to make substantial contributions in addressing global challenges.

1. All India Market Capitalization, BSE, 9 January 2024

2. Annual Report 2022-23 SEBI, 07 August 2023; Statistics, CDSL update, CDSL, 31 December 2023; NSDL update, NSDL, 31 December 2023;

3. Consultation paper on 'Introduction of optional T+0 and optional Instant Settlement of Trades in addition to T+1 Settlement Cycle in Indian Securities Markets, SEBI, 22 December 2023

With digitalisation, the increasing instances of data breaches and technology disruptions are impacting trust among businesses, investors, and other stakeholders. As per 2023 Ponemon report, the average cost of data breach in India is INR 179 million⁴. It is important to strengthen cyber security landscape from the macro level to the micro level to ensure the safety, security and stability of the capital markets and thereby uphold the currency of trust. At national level, government and regulators need to enhance investment to build Aatmanirbharta, आत्मनिर्भरता (self-reliance) in cyber security through fit for purpose laws and regulations, skilled and at scale human capital, indigenously designed and built infrastructure. The capital markets industry should enhance focus on cyber security, embrace transparency and ethical adoption of digital technologies, and promote public – private partnerships to build investor awareness. On the organisational level, a top-down approach should be followed and the board should ensure regulatory compliance while mitigating third party risks.

At societal level, it is imperative to enhance digital and cybersecurity literacy and awareness of consumer protection mechanisms available to instill confidence.

In this journey India would play active role in building collaboration to fight global cybercrime and offer scale capabilities for a better and cyber safe world and investing.

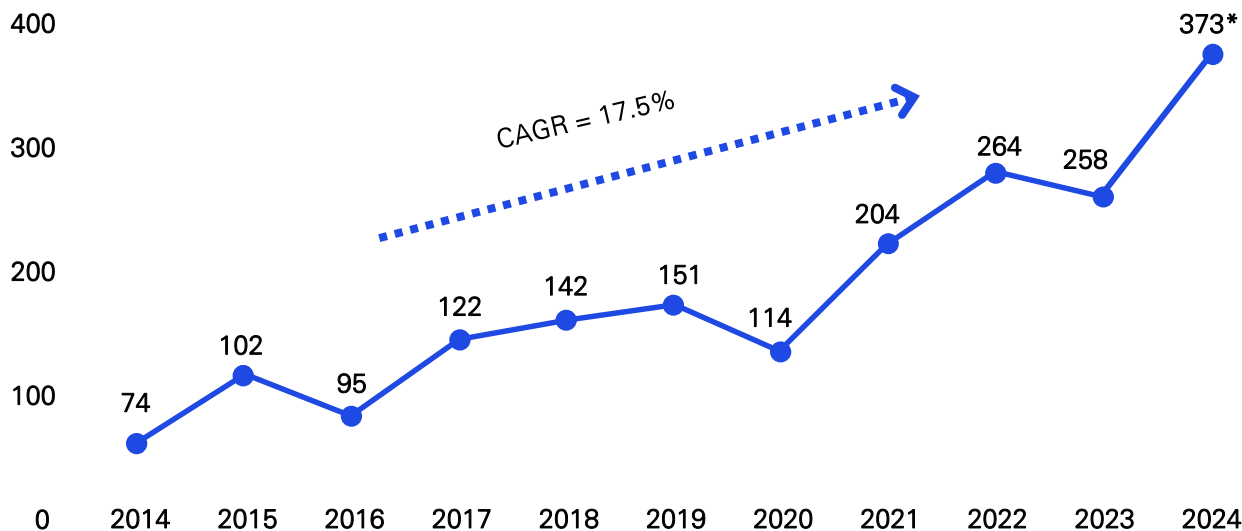
4. Cost of Data Breach Report 2023, Ponemon Institute, July 2023

1 Future is here and what's beyond



The capital markets serve as a significant contributor to the economy, enabling identification of investment opportunities and provision of resources that fuel innovation, growth, and wealth creation. The Indian capital markets have undergone a remarkable transformation to emerge as a significant player on the global stage—currently ranked as the 4th largest, with a market capitalisation exceeding INR 373 trillion in listed securities⁵. Below is the graph indicating the market capitalisation of listed companies for the last 10 years.

Growth in market capitalization (in INR trillion) in the past decade



Source: Handbook of Statistics of Indian Economy, RBI, December 2023; All India Market Capitalization, BSE, 9 January 2024

* As of January 2024

Notably, India has garnered recognition as an attractive investment destination, bolstered by the ease of doing business, a progressive regulator - Securities and Exchange Board of India (SEBI), presence of two of the world's largest exchanges, namely National Stock Exchange of India Limited (NSE) and BSE Limited (BSE), leading depositories – Central Depository Services (India) Limited (CDSL) and National Securities Depository Limited (NSDL) and a host of other participants.

Pivotal developments in capital markets include establishment of decentralised structure i.e., recording or accounting (Depositories), trading (Exchanges), clearing and settlement (Clearing corporations), introduction of shorter settlements, advent of interoperability, introduction of UPI payments, settlement guarantee funds, mass scale investor education, tech driven solutions which has enhanced safety and transparency in the market. In this journey the depositories have played a critical role in facilitating dematerialisation of securities, enabling digitalisation of investor interaction across the value chain and increasing transparency in the market.

Indian capital markets have emerged as a distinct ecosystem due to decentralisation, investor-centric innovation and technology driven approach. The

markets are uniquely structured, with exchanges, clearing corporations, and depositories facilitating operations. This decentralisation has not only promoted transparency and risk mitigation but also empowered investors with greater control and confidence in the ecosystem.

The introduction of technology enabled products/ services such as seamless online account opening through eKYC, digital payments using UPI, digital B2C authorisation, eMargin, margin pledge mechanism and many similar initiatives have revolutionised the Indian investment landscape, placing power firmly in the hands of investors. It has not only made capital markets more accessible but also instilled trust in the financial ecosystem.

One striking measure of this transformation is the remarkable growth in retail market participants. In just a decade, the number of demat accounts have surged from 21 million+ to 139 million+⁶. The growth is further mirrored in the expansion of market capitalisation, increase in trading volumes, and the growth in benchmark indices like the Nifty and Sensex. CDSL became the first depository in India to cross 100 million active demat accounts as of November 2023⁷.

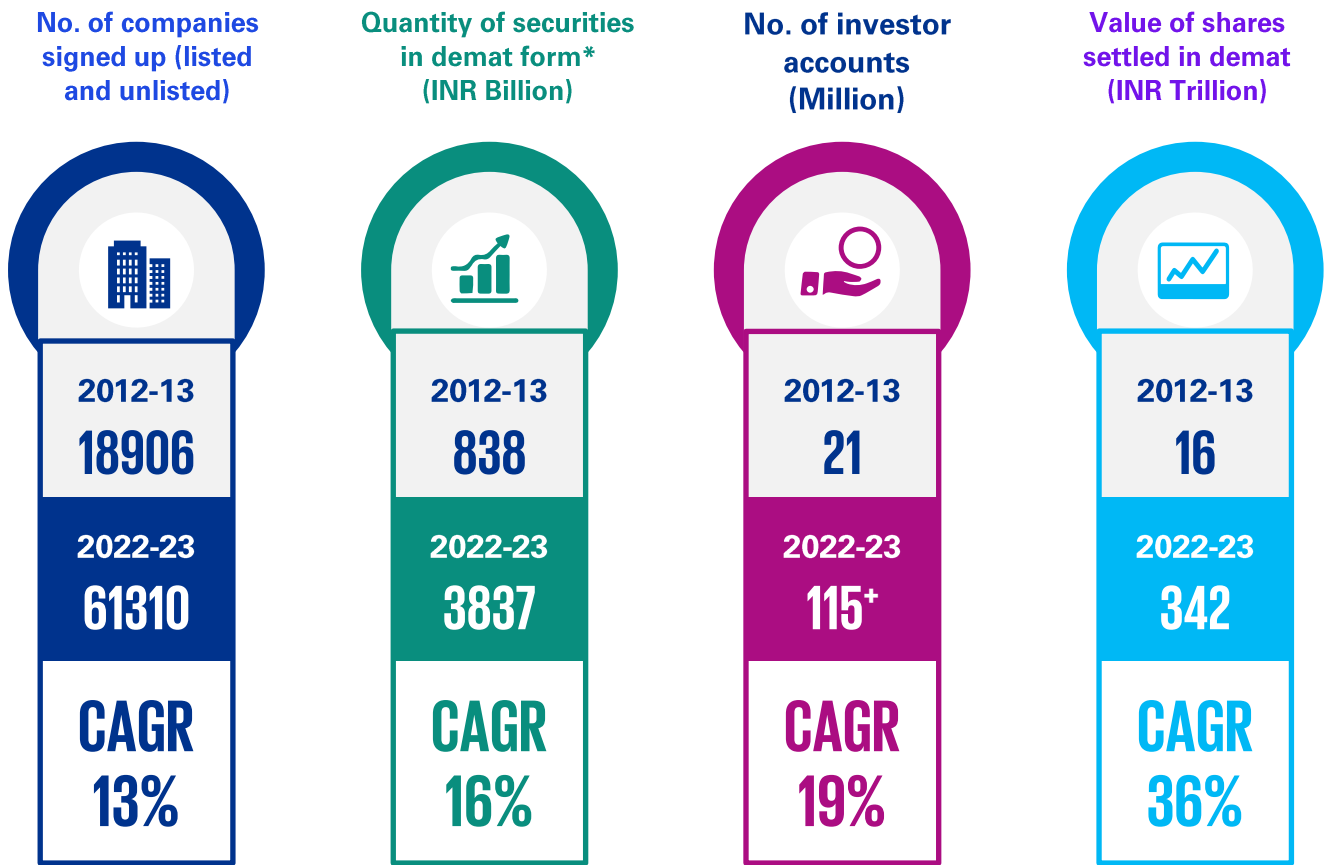
5. All India Market Capitalization, BSE, 9 January 2024

6. Annual Report 2022-23 SEBI, 07 August 2023; Statistics, CDSL update, CDSL, 31 December 2023; NSDL update, NSDL, 31 December 2023;

7. Central Depository Services (India) Limited website, CDSL, November 2023

The evolution of Indian depositories, during the last 10 years in terms of accounts, companies, etc., is depicted below:

Figure: Depository statistics for 2013 vs 2023



Source: Annual Report 2012-13, SEBI, August 2013; Annual Report 2022-23, SEBI, August 2023; Statistics, CDSL update, 31 December 2023; Statistics, NSDL, 31 December 2023;

*Securities include common equity shares, preferential shares, mutual funds, debentures and commercial papers + 139 million as of 31 December 2023

Indian capital markets have continually evolved through introduction of newer products and capabilities such as stocks futures, options, index futures, smart order routing, faster settlement (T+1), eDIS, DMA, etc. These products and services have not only enabled innovative investment opportunities, but also aided in enhanced risk management like lower settlement risks, better hedging of risks, greater participation in governance, etc.

The significant digitalisation and rising awareness amongst the investors are expected to drive further increase in participation. The increase in market value, digitalisation, investor participation (including retail investors) is raising inherent risks as well as being target for cyberattacks. A safe, responsible and secure digital ecosystem is the currency of trust amongst the participants, and especially investors.

The decade to shine?

In an increasingly globalised world, Indian capital markets are going through remarkable digital transformation, harnessing cutting-edge technologies like cloud computing, big data analytics, artificial intelligence, mobile applications to elevate efficiency, transparency, security, and innovation. Embracing digital platforms such as Aadhaar, Digilocker, Unified Payments Interface (UPI) has facilitated swift and cost-effective transactions, expanding market access to a diverse customer base, including in rural and semi-urban areas. This decade will continue to witness accelerated digitisation.

Today's investors can seamlessly access capital market investment opportunities at their fingertips, thanks to multiple and customised investment platforms, instant payments, real-time market news, and stock advisories. Powered by a growing economy, thriving company valuations, political stability and technological advancements, investors are gaining confidence in the Indian market.

It is, therefore, imperative to safeguard this democratised ecosystem from potential emerging

risks and cyber threats by embedding the “currency of trust” into the design and reinforce safety and security of investor wealth and society at large.

1.1 Emerging digital trends in capital markets

Capital markets serve as potent catalyst for economic growth and wealth generation. Their core purpose is to facilitate the alignment of the investee with the investors on their respective risk preferences for various financial instruments, thus creating symbiotic investment opportunities. Recognising the significant contribution of capital markets, the G20 agenda also emphasises their potential in channelling finances not only in the corporate sector but also to critical areas like infrastructure and SMEs. The G20 agenda recognises the key role capital markets can play in mobilising an estimated INR 640-800 trillion annual investment, required for developing countries to achieve the sustainable development goals (SDGs) by 2030⁸.

As the landscape of capital markets is rapidly evolving wherein the emerging digital technologies are driving transformative developments and innovations in the capital markets worldwide, top trends amongst these are:

- Disruption by fintech
- Increased market interconnectivity
- Decentralisation using web 3.0

1.2 Disruption by fintech

Capital markets ecosystem comprises a wide range and network of intermediaries, including trading platforms, interdealer brokers, clearing houses, securities depositories, securities services firms, information providers, and data and analytics companies across the country. The rapidly evolving landscape of capital markets is witnessing accelerated disruption, ushering in significant innovative changes for the future.

Digital is integral to how we live and work. Ensuring the security of the enterprise, the individual and the capital market participants is now a part of every boardroom

Ms. Neelam Dhawan

Independent Director, ICICI Bank Limited, Hindustan Unilever Ltd, Capita PLC, Fractal Analytics Pvt Ltd and Yatra Online Inc

8. Capital Markets, The World Bank, 31 August 2022

Fintech are transforming various aspects of the capital markets ecosystem, enhancing efficiency, accessibility, security and convenience for market participants and investors. Also, market infrastructure institutions (MIIs) in India have increasingly embraced fintech solutions to streamline operations, improve market infrastructure and deliver innovative services. Fintech solutions while being positively disruptive have also added a new scale and type of risk management that regulators are seeking to administer, in the interest of the markets.

Notable fintech driven innovation within Indian capital markets are:

Online trading platforms



Fintech offer user-friendly online trading platforms, empowering retail investors to engage in real-time trading of stocks, securities, derivatives, and commodities. These platforms feature advanced charting tools, technical analysis, algo trading, and robust transaction execution, providing investors with greater control over their investment portfolios. Recognising the risk that these trading platforms bring in, SEBI brought in scale-based regulation for brokers offering large platforms designated as Qualified Stock Brokers (QSBs). With effect from 1 July 2023, 15 brokers have been designated as QSB⁹.

CAS



Consolidated Account Statement (CAS) offers investors a comprehensive overview of their holdings across diverse financial instruments and platforms. It consolidates information from various sources like mutual funds, stocks, and bonds into one accessible statement, simplifying the process for investors. This clarity enables better decision-making and more effective financial planning. CAS encourages transparency and convenience in the investment landscape, empowering investors with enhanced control and comprehension of their portfolios.

eKYC



Aadhaar-based eKYC verifies identity electronically through Aadhaar-based authentication. The benefits include instant proof of identity and address to the service provider, eliminating the need for tedious in person verification and single point of change management.

eDIS



Electronic Delivery Instruction Slip (eDIS) introduces a digital approach to transferring securities, replacing traditional paper slips. It allows investors to sell shares without Power of Attorney (POA). This shift reduces manual handling, leading to faster processing and fewer errors. It also enhances transparency and security in transactions. eDIS aligns with the industry's move towards digitisation, promising more efficient and accurate operations.

eMargin pledge



eMargin pledge is a process whereby investors can electronically pledge their stocks to the broker in return for a collateral margin that can be utilised for trading. As the stocks do not leave investor's demat account the risk of misuse of investor funds and/or securities is eliminated.

9. Exchanges designate 15 stockbrokers as QSBs with enhanced obligations, ENTPNEWS, 3 March 2023

1.3 Increased market interconnectivity

Amid financial market globalisation, markets worldwide are becoming increasingly automated and interconnected. Electronic trading platforms, information-sharing networks, and cross-listing arrangements have enabled integration, offering investors a plethora of options to trade securities across different stock exchanges, including foreign stocks and securities. Dynamic transformation of settlement systems leveraging technological breakthroughs like India's adoption of T+1 settlement of stocks provides for better liquidity management. It also reduces operational and counterparty risks thereby furthering investor interests.

Formal linkages amongst stock exchanges through partnerships, alliances, or direct connections with other exchanges enabled by cross-border trading is also on the rise, exemplified by the stock connect programs between London Stock Exchange (LSE) and Shanghai Stock Exchange (SSE), as well as the Hong Kong Stock Exchange (HKEX) and exchanges in Shanghai and Shenzhen.

Since July 2023, GIFT NIFTY (previously SGX Nifty) derivatives contracts, previously traded on the Singapore Stock Exchange, have begun trading on NSE IX, GIFT City, India¹⁰. This arrangement not only makes India a seamless global destination, but also

exempts transactions from Securities Transaction Tax (STT) and Commodities Transaction Tax (CTT) for trades executed at GIFT City.

The interconnectedness amongst capital market ecosystem enables wider market access, but also necessitates enhanced cyber security measures. The interconnected environment gives a wider target to perpetrators wherein cyber security incident affecting one stakeholder, could impact the whole value chain across markets.

1.4 Decentralisation using web 3.0

The emergence of web 3.0 is set to make a substantial impact on India's capital markets, presenting countless advantages and opportunities for various stakeholders. Web 3.0 and blockchain technologies are projected to add an impressive INR 90 billion by the year 2032¹¹.

In the context of web 3.0 and decentralised finance (DeFi), composite wallets assume a crucial role within capital markets. These advanced wallets offer users distinctive functionalities, enabling seamless trading of stocks. In the Indian capital market context digital payments are being widely used for trading of stocks. India is targeting to implement real time settlement along with instant payments by 2024.

Some of the features of web 3.0 in the context of capital markets are provided in the diagram below:

Figure: Web 3.0 and its features

Asset tokenisation

Enables the tokenisation of assets in Indian capital markets, including stocks, bonds, and real estate.

Improved accessibility

Provides decentralised, permissionless platform which allows Individuals to participate in capital markets without relying on traditional intermediaries, making it easier for retail investors to enter the market.

Data analysis and market insights

Provides accurate data in real-time, giving investors better insights for informed decision making. This will help support the growth of data analytics and algorithmic trading strategies in India.

Smart contracts for efficiency

Leverages smart contracts on the Web 3.0 platform to automate and streamline transaction processing.

Crowdfunding and fundraising

Enables startups and SMEs to raise capital directly from global investor pools using Initial Coin Offerings (ICOs) or Security Token Offerings (STOs). This could open up new opportunities for capital formation for innovative Indian startups.

Decentralised exchange

Enables peer-to-peer trading, reduce brokerage costs, and increase transparency thus giving investors more control over their assets



10. SGX Nifty Renamed as GIFT Nifty on July 3, Groww, 02 August 2023

11. Indian Web3 industry to reach \$1.1 billion by 2032, India today, 14 March 2023

The transformative power of emerging technologies in terms of expanding investor base, seamless interconnectivity, straight through and automated operations is providing India a very powerful catalyst to drive its ambitions of becoming one of the foremost economies in the world. It is crucial that currency of trust is embedded into this emerging ecosystem and coordinated efforts are taken up to effectively guard against the challenges thrown by cyber attackers.

1.5 New offerings to the investors in India

Indian investors are being presented with new opportunities and developments, expanding their horizons for portfolio diversification, risk management and fostering stable returns. India is the first jurisdiction in the world to move towards T+1 settlements. Now, the concept of instant settlement (T+0) isn't that far away. Among emerging avenues in India, notable ones include:

Securitised products - secondary market: While the securitised products market in India is relatively nascent, it offers the advantage of tailoring portfolios and optimising capital deployment in the broader financial landscape. By adopting tokenisation and composite wallets, the securitised products market will become more transparent and safer for the investors.



ESG linked products: The ESG market is poised to witness tremendous growth and therefore also bringing in newer risks. In January 2023, India issued its first tranche of sovereign green bonds worth INR 80 billion¹².

Carbon trading stands out as a dominant market-based approach in the fight against climate change. Several countries in the Asia Pacific, are moving toward introducing requirements and guidelines for financial institutions to address climate-related risks. The Indian Government is presently making strides towards establishing the Indian carbon market (ICM) as a pivotal platform to develop a national framework for decarbonising the Indian economy. The recent Ministry of Power's 2023 Carbon Credit Trading Plan (CCTP) aims to create an internal marketplace for tracking and trading carbon credits.



Instant settlements: Looking ahead, capital market securities regulators, central banks and governments are modernising security trading and payment systems through the adoption of instant settlement, payments and digital wallets, aimed at improving the speed, accessibility, and security of transactions. Exploring securities tokenisation and central bank digital currencies (CBDCs), promises to revolutionise settlements by making them instantaneous. SEBI published a consultation paper in December 2023, proposing a move towards optional T+0 and near instantaneous settlement of trades¹³.



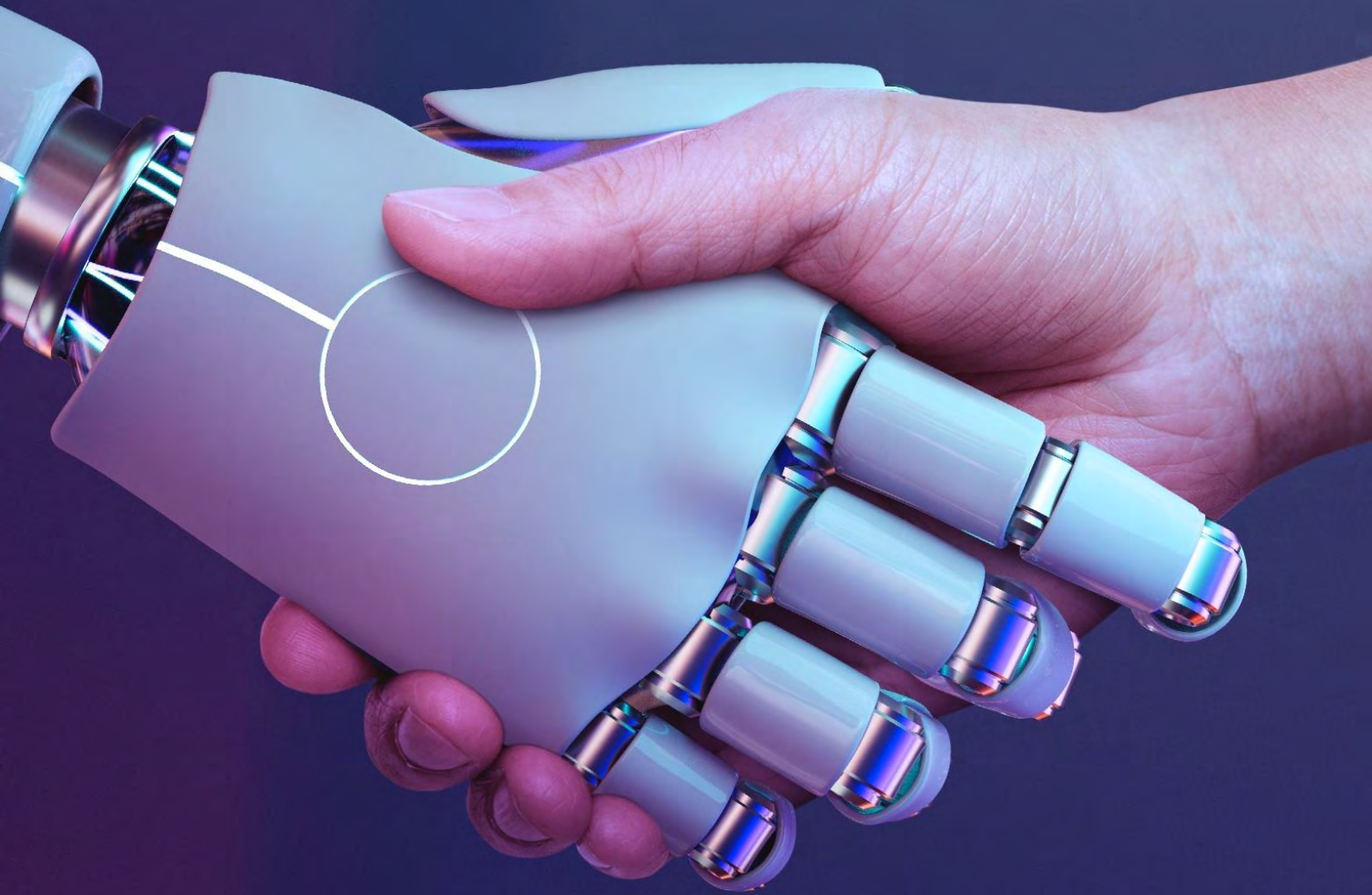
We discuss about underlying technologies that are powering this digital transformation in the next chapter.

12. India incorporates green bonds into its climate finance strategy, World bank blogs, Farah Imrana Hussain and Helena Dill, 12 June 2023

13. Consultation paper on 'Introduction of optional T+0 and optional Instant Settlement of Trades in addition to T+1 Settlement Cycle in Indian Securities Markets, SEBI, 22 December 2023



2 Powering the future



As the wave of ground-breaking innovations and differentiated product offerings shape global consumer preferences, it is important to look at the foundation on which these advancements thrive. Beyond the limelight of trends lies the vital role played by underlying technologies, quietly propelling transformative changes.

For over a decade, cloud technologies have influenced the provision and consumption of computing services. They have democratised availability of affordable, dependable, flexible, agile and adaptable computing solutions, lowering the barriers to entry while also bringing in more efficiency. Cloud adoption remains an ongoing trend as businesses strive to maintain a competitive edge and now is a pivot on which new advancements run.

A remarkable leap in technology is artificial intelligence (AI), orchestrating dramatic changes in the world of trading. It empowers investors to make more informed trading decisions, extract fresh insights, and automate critical processes resulting in heightened efficiency, burgeoning opportunities, and a notable decline in associated risks.

Blockchain is surmounting diverse challenges and inefficiencies through its inherent transparency, automation, and risk reduction capabilities, while opening disruptive opportunities for capital markets.

Yet another game-changer is extreme networking powered by technologies like 5G that is propelling us into seamless and ubiquitous connectivity at an astonishing pace ensuring interconnectedness across the ecosystem. Its unparalleled speed, remarkably low latency, and expansive capacity have engendered a fertile ground for a novel ecosystem like web 3.0, immersive hyperconnected world, etc. contributing to innovations in the capital markets while opening a future replete with untold promises.

2.1 The AI revolution in the trading world

Artificial intelligence (AI), has introduced an era of advanced computational capabilities, fundamentally reshaping the trading landscape. Hedge funds and high-frequency trading (HFT) firms are leveraging AI to improve trading decisions and execute data-driven trades in real-time. Retail traders are also embracing AI-powered platforms for investment guidance.

The impact of AI on trading spans across various domains. Algorithmic trading, fueled by machine learning algorithms, enables automated systems to swiftly execute trades real time, based on predefined rules and market conditions, outpacing human traders. Predictive analytics empowers traders to generate valuable insights into price movements, market trends, and volatility through the analysis of diverse data sources, thereby improving decision-

making and risk management strategies.

Organisations are applying deep neural capabilities that can understand nonlinear and complex data relationships, and thereby unlock accurate and faster predictions.

AI models play a pivotal role in risk management by identifying anomalies, detecting market manipulation and fraud, and continuously monitoring real-time trading activity, fostering a secure and compliant trading environment. AI-driven high-frequency trading strategies process real-time market data at microsecond levels, uncovering hidden opportunities and capturing small value creation opportunities beyond human capabilities.

Market surveillance, facilitated by AI, proactively prevents market abuse, ensuring fair and transparent trading practices through extensive analysis of trading data. AI techniques optimise investment portfolios, considering factors such as risk tolerance, market conditions, historical data, and investment goals to recommend ideal asset allocation and diversification strategies that adapt to changing market conditions.

Another subset of AI, natural language processing (NLP), analyses unstructured data from news articles and social media, extracting relevant market insights. This offers traders a deeper understanding of market sentiment and the potential impact of news-driven events on asset prices.

Advancement in AI in form of generative AI with its ability to create new content reports, synthetic data has potential to revolutionise capital markets. Generative AI tools can assist in better decision making by sifting through the loads of data to share insights and trends. It can automate pre and post trade tasks by making significant contribution in faster generation of high-quality research reports, building financial models, etc. It can also help in enhancing personalised services by generating suggestive investment portfolio for investors. Generative AI is still in its early stages, and it is crucial that any gen AI service is thoroughly tested to address challenges around reliability and accuracy of outcome.

A recent survey-based report by KPMG Australia and The University of Queensland identifies AI risks pertaining to cybersecurity and privacy breaches, manipulation and harmful use, loss of jobs and deskilling, system failure, the erosion of human rights and inaccurate or biased outcomes. And overall, cybersecurity and privacy risks are the leading concerns globally.

As capital markets adopt more advanced and innovative AI enabled capabilities, it is important to ensure that robust risk management, especially cyber security requirements are secured by design.

2.2 Blockchain binding the market together

Blockchain technology in simple terms is a “chain of blocks” distributed across a decentralised network of users (nodes) wherein a user can add transactions or programs (like smart contract) without need for a central authority (or controlling unit). Each node maintains the chain of blocks that is encoded using cryptographic techniques such that need for centralised control is obviated by a codified consensus mechanism. The technology intrinsically brings in capabilities of straight through processing, common non-repudiable data (and code), self-contained event driven actions thereby unleashing huge possibilities.

Blockchain initiatives are making significant strides to enhance capital markets infrastructures, fostered by governments, stock exchanges, and other stakeholders seeking to improve transparency, efficiency, and security. The inherent immutability of blockchain technology instils greater trust and accountability in transactions.

As it continues to evolve, blockchain is expected to catalyse financial market innovation, revolutionising transaction recording and verification processes in various ways. For instance, transparency and trust in capital markets have long been significant challenges. However, blockchain technology emerges as a game-changer, offering a decentralised and transparent ledger that records and verifies transactions in real-time. By eliminating intermediaries, blockchain reduces delays, errors, and costs while enhancing the integrity of transactions. The complex and cumbersome clearing and settlement processes can be streamlined and automated through blockchain implementation, driven by smart contracts that execute and settle transactions without

intermediaries, thereby increasing operational speed and efficiency while reducing counterparty risks. A blockchain embedded programmable contract (smart contract) significantly reduces the risk of settlement default due to inaction.

Blockchain’s potential to tokenise assets enhances market liquidity, enabling fractional ownership and trading of previously illiquid assets, presenting new investment opportunities. The benefits extend to issuers and market infrastructures, with blockchain enabling easier, cheaper, and faster access to capital through programmable digital assets and securities. Regulatory compliance also benefits through blockchain’s real-time transaction visibility and automated reporting, simplifying adherence to compliance rules.

Blockchain-based identity solutions strengthen know your customer (KYC) processes and anti-money laundering (AML) efforts. Additionally, blockchain technology paves the way for decentralised exchanges (DEXs), fostering peer-to-peer trading, increased privacy, and security by eliminating central authorities.

Central banks across the globe along with market regulators are looking to encourage securities settlement by leveraging wholesale Central Bank Digital Currency (CBDC). The recent trials with wholesale digital rupee have been providing experience to build for faster and seamless settlement while integrating with existing market infrastructure.

While blockchain technology is ushering in tremendous innovations, it is subject to cybersecurity risks like insecure coding, data privacy, consensus mechanisms and on interfacing off-chain data/ systems, which needs to be comprehensively addressed by ensuring security at a design level.



2.3 5G transforming the digital ecosystem

5G technology bears profound implications for both capital markets and the development of web 3.0, cutting the turf for transformative changes in these domains. In the capital markets ecosystem, 5G's low latency and high-speed capabilities promise faster and more efficient trading, enabling reduced transaction times for majority of participants. Also, real-time market data dissemination becomes seamless, empowering investors and traders with up-to-date information for making informed decisions and timely trades.

5G's widespread connectivity enables a hyperconnected ecosystem which ensures access to capital markets from diverse locations, democratising participation among a broader range of stakeholders. The integration of the internet of things (IoT) into 5G networks offers real-time data on a variety of areas like asset movement and provenance across supply chain and tokenised carbon units e.g., for a power plant thereby empowering market participants with deeper insights as well as transparent investment opportunities.

Built upon its foundation of increased bandwidth and enhanced reliability, 5G facilitates high quality video conferencing alongside support for augmented reality (AR) and virtual reality (VR) technologies, fostering a truly immersive environment for data visualisation and collaborative interactions among its users.

In the realm of web 3.0, 5G's high-speed and extensive connectivity accelerates the adoption of decentralised applications, blockchain-based smart contracts, and peer-to-peer networks. Integration with IoT devices in web 3.0 ecosystems facilitates autonomous machine-to-machine communication and decentralised data sharing, enabling innovative business models centred around IoT data monetisation.

The hyper connectivity based on 5G technology shall tremendously increase integration of IoT products where vulnerabilities are quite prevalent due to inadequate security in design, patching or misconfiguration. 5G networks enable significant ability to bring data close to client devices leading to increase in edge computing (IoT devices also can be considered part of edge computing), increasing attack surface and security complexity.



3 Risks and challenges



As elaborated earlier, the accelerated progress of capital markets is driven by the emergence of cutting-edge technologies, but it is not devoid of challenges. In the 2022 annual report published by Financial Stability Board (FSB), an international body of central banks and financial regulators that promotes global financial stability, it was noted that cyber incidents are rapidly increasing in frequency and sophistication, and growing interconnectedness of the financial system is leading to spill over effects across borders and sectors¹⁴. This emphasises the fact that custodians of digital assets who embrace the technological paradigm shift must also proactively address distinctive risks and adeptly navigate the expanded threat landscape that accompanies it.

Unique risks emerging from introduction of any new

technology initiate a cycle of challenges. These risks are further amplified by the complex interconnectedness among organisations and their third-party entities, traversing the entire supply chain. Over time, repercussions of these risks become evident, thereby exposing their potential impact on the investor/end user, organisations, and even nation-states. Regulators and governments diligently oversee this cycle, and the extent of their scrutiny is directly correlated to severity of the adverse effects stemming from these emerging technologies.

It is also crucial to recognise that the risks and challenges differ at national, capital market, organisational and societal levels, requiring tailored strategies and awareness efforts to mitigate them effectively.



At the national level, the proliferation of these technologies raises concerns about cybersecurity threats, as they become integrated into critical infrastructure and national security, potentially exposing nations to cyberattacks and espionage. Governments face the constant challenge of establishing and enforcing comprehensive laws, regulations, standards and institutions to develop and safeguard financial infrastructure, data and citizens.



At the level of capital markets, the emerging digital technologies not only amplify existing risks but also bring newer risks to the capital markets and expose investors to such risks. Adoption of new technologies in a transparent and responsible manner while ensuring resilience and data protection at its core, is challenging. Regulatory uncertainties often arise as these technologies outpace existing frameworks, creating uncertainty among market participants and impacting investments and market dynamics. In the absence of public-private partnership, compliance with evolving cybersecurity regulations and reporting requirements can be complicated and resource intensive.



Within organisations, the rapid obsolescence of existing technologies and business models is a pressing challenge, requiring constant adaptation to remain competitive. Also, dependence on third parties exposes organisations to supply chain risks. The shortage of skilled professionals in emerging technology fields poses talent acquisition and retention difficulties, resulting in increased labour costs. Additionally, the vast data requirements of emerging tech raise concerns about data privacy, security, and compliance with data protection regulations.



At the societal level, concerns about exposure to risks of cybercrime and unethical use of troves of data being collected has risen. This has sparked debates about societal action along with national, industry and organization level action. The challenge that also includes maintaining investor confidence requires while raising public awareness about cyber risks, aiming to protect the interests of the broader society.

14. Promoting Global Financial Stability-2022 FSB Annual Report, Financial Stability Board, 16 November 2022

3.1 New tech accompanied by newer risks

3.1.1 Artificial intelligence









As artificial intelligence (AI) gains traction within capital markets, it brings along a set of associated risks encompassing data privacy, need to maintain a balance between the legacy systems and the new edge solutions, intellectual property, bias and fairness, misinformation, and malicious use. For instance, the 17th edition of “The Global Risks Report 2022” published by the World Economic Forum (WEF), highlighted a new risk from “ransomware as a

service”, allowing even non-technical criminals to execute attacks, a trend that is foreseen to intensify due to artificial intelligence (AI)-powered malware. Moreover, it also highlighted that artificial intelligence was among the areas with the least established or effective international risk mitigation efforts¹⁵.

The reliance on extensive data for training AI models exposes them to data poisoning and model manipulation attacks, while also raising concerns about the environmental impact due to the utilisation of non-renewable energy sources to support the complex computational requirements.

Impact on capital markets

Emerging risks from the adoption of AI

 <p>Data manipulation</p> <ul style="list-style-type: none"> • Malicious alteration of training or input data • False predictions, misleading trading algorithms, erroneous investment decisions 	 <p>Adversarial attacks</p> <ul style="list-style-type: none"> • Manipulating input data to deceive or mislead the AI model • Unauthorised access, compromised market insights, incorrect trade executions 	 <p>Model theft or replication</p> <ul style="list-style-type: none"> • Unauthorised access or replication of proprietary AI models • Financial losses, competitive disadvantage, loss of intellectual property 	 <p>Model bias/discrimination</p> <ul style="list-style-type: none"> • Biased outcomes due to biased or incomplete training data • Unfair practices, market inefficiencies, regulatory non-compliance
 <p>Insider threats</p> <ul style="list-style-type: none"> • Abuse of privileged access or manipulation by authorized insiders • Manipulation of algorithms, unauthorized access to sensitive financial data 	 <p>Lack of explainability</p> <ul style="list-style-type: none"> • Difficulty in interpreting and understanding AI model decisions 	 <p>Regulatory compliance</p> <ul style="list-style-type: none"> • Legal consequences, reputational damage, financial penalties • Failure to comply with relevant regulations and standards • Regulatory compliance challenges, reduced trust in AI-driven decisions, legal implications 	 <p>System integration vulnerabilities</p> <ul style="list-style-type: none"> • Unauthorized access, disruption of trading activities, compromised data integrity, financial losses, market instability • Weaknesses in integrating AI systems with existing infrastructure

15. The Global Risks Report 2022 17th Edition, World Economic Forum, 11 January 2022









3.1.2 Blockchain

Blockchain has demonstrated significant potential in introducing innovative financial tools to enhance the efficiency, transparency, and accessibility of capital markets, however, several challenges remain. These challenges include addressing scalability issues, cybersecurity risks, establishing regulatory frameworks, ensuring interoperability, and achieving

standardisation. Blockchain is widely used today for cryptocurrencies, and according to data from Chainalysis, in 2021 and 2022, INR 275 billion and INR 316 billion, respectively, were stolen in crypto hacks¹⁶. These figures, when extrapolated to the increasing use cases of blockchain in capital markets, provide a fair indication of the scale of challenges that need to be addressed.

Impact on capital markets

Emerging risks from the adoption of blockchain based systems

 <p>Smart contract vulnerabilities</p>	 <p>Privacy challenges</p>	 <p>On-Off blockchain integration risks</p>	 <p>Lack of interoperability</p>
<ul style="list-style-type: none"> • Flaws in blockchain-based smart contracts • Exploitation of vulnerabilities, unauthorized manipulation of transactions, financial losses, contract disputes 	<ul style="list-style-type: none"> • Difficulties in ensuring user privacy • Exposing transaction details, compromising investor confidentiality, regulatory non-compliance 	<ul style="list-style-type: none"> • Inadequate understanding of risks at integration points • False 'trust' in the system, increased attack surface, data inaccuracy 	<ul style="list-style-type: none"> • Difficulties in integrating diverse blockchain platforms • Incompatibility, data fragmentation, hindrance of cross-platform transactions
 <p>Data integrity issues</p>	 <p>Scalability issues</p>	 <p>Vulnerabilities in wallets</p>	 <p>Consensus protocol vulnerabilities</p>
<ul style="list-style-type: none"> • Risks to the accuracy and validity of data stored on the blockchain • Manipulation of data, fraudulent transactions, compromised audit trails 	<ul style="list-style-type: none"> • Limitations in the scalability of blockchain networks • Slow transaction processing, congestion, bottlenecks in capital market activities 	<ul style="list-style-type: none"> • Security weaknesses in blockchain wallets • Unauthorized access, theft of digital assets, financial losses 	<ul style="list-style-type: none"> • Weaknesses in the consensus mechanism of the blockchain • Disruption of network operation, compromise of transaction validation, potential for alternate chains









16. 2022 Biggest Year Ever For Crypto Hacking with \$3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers, Chainalysis, 1 February 2023

3.1.3 5G

5G networks, with their high-speed and ubiquitous connectivity, have accelerated the adoption of web 3.0 technologies, fostering remarkable growth in the capital markets as discussed earlier. The widespread implementation of 5G also significantly amplifies exposure surface and therefore potential impact of

cyberattacks. Now, more than ever, an attack on one of the hyperconnected entity can have a ripple effect on numerous entities, in turn leading to extensive disruptions in critical services, financial losses for individuals and businesses, compromise of privacy and personal information, erosion of trust in digitally enabled economy, and potential concerns for national security.

Emerging risks from the adoption of 5G

 <p>Increased attack surface</p>	 <p>Supply chain risks</p>	 <p>Network slicing vulnerabilities</p>	 <p>Edge computing risks</p>
<ul style="list-style-type: none"> Expanded network infrastructure and connected devices Increased potential for cyberattacks, data breaches, disruption of trading activities 	<ul style="list-style-type: none"> Risks associated with complex supply chains in 5G networks Compromised components, introduction of malicious software, disruption of critical financial systems 	<ul style="list-style-type: none"> Vulnerabilities in network slicing implementation Data breaches, unauthorized access, disruption of critical financial systems 	<ul style="list-style-type: none"> Security risks associated with edge computing infrastructure Compromised edge devices, unauthorised access to sensitive financial data, disruption of financial operations
 <p>Denial-of-Service (DoS) attacks</p>	 <p>Lack of data privacy and confidentiality</p>	 <p>Interoperability challenges</p>	 <p>Insider trading and market manipulation</p>
<ul style="list-style-type: none"> Overwhelming the network with a high volume of traffic Service disruptions, slowdowns, hindrance of critical financial transactions 	<ul style="list-style-type: none"> Risks associated with the transmission and storage of sensitive data Unauthorised access, interception, data breaches, compromising investor confidentiality 	<ul style="list-style-type: none"> Challenges in integrating diverse systems and protocols Security vulnerabilities, misconfigurations, exploitation by attackers, disruption of financial operations 	<ul style="list-style-type: none"> Exploiting low latency for fraudulent activities Insider trading, market manipulation, regulatory non-compliance

3.2 Evolving 3rd party risks

The dynamic and ever-changing landscape of third-party risks has become a major area of concern for capital markets. This concern arises primarily due to the increasing reliance of market participants on intricate relationships with third-party service providers and partners to facilitate their operations.

One recent cyber-attack that exemplified this concern occurred in June 2023. In this attack, carried out by a Russian ransomware gang named LockBit, the target was a semiconductor manufacturing company's supplier. This attack resulted in the leak of information pertinent to the initial setup and configuration of servers. LockBit demanded a hefty INR 5.8 billion ransom, threatening to publish stolen data if their demands were not met¹⁷.



In the area of technology services, the third-party market, marked by intense competition, is increasingly being controlled by a handful of entities (e.g., cloud service providers) that deliver crucial services to a majority of the capital market participants, thereby amplifying repercussions of any failures at the service providers. This concern also extends to software supply chain security and reliability, as organisations in the capital market heavily depend on software components, libraries, and various other software development services offered by these external vendors or suppliers.

For instance, in late 2021, a software supply chain attack targeted Log4j, a widely used Java-based logging utility. This vulnerability, known as Log4Shell, exposed millions of computers to significant risks, including data theft, exposure of login credentials, and the potential installation of additional malicious software. Given the extensive use of Log4j by individuals and organisations, this vulnerability posed a grave threat to a vast number of users and businesses¹⁸.



As the range of third-party involvement expands, it introduces more complexity, which in turn poses challenges for organisations to uphold visibility and control over the governance and security practices of lower-tier vendors.

The widespread adoption of AI has led capital markets to increasingly depend on third-party AI applications for functions such as chatbots and forecasting capabilities. However, as these AI models heavily rely on diverse datasets for training and decision-making, risks associated with data inaccuracy, bias, and lack of transparency have become pressing concerns for the heavily regulated capital markets.

Use of blockchain applications in capital markets often involves utilisation of oracles to interact with external data sources and systems. Should these oracles be compromised or provide inaccurate information, it can undermine integrity of blockchain-based processes and introduce operational and financial risks.

The adoption of 5G in capital markets necessitates reliance on various vendors for network equipment and services. This exposes capital markets to supply chain risks, including vendor lock-in, limited competition, and potential vulnerabilities in the vendor's products or infrastructure.

As mentioned earlier in this section, the emergence of risks from new technologies extends throughout the entire supply chain, consequently impacting third-party risk landscape too.



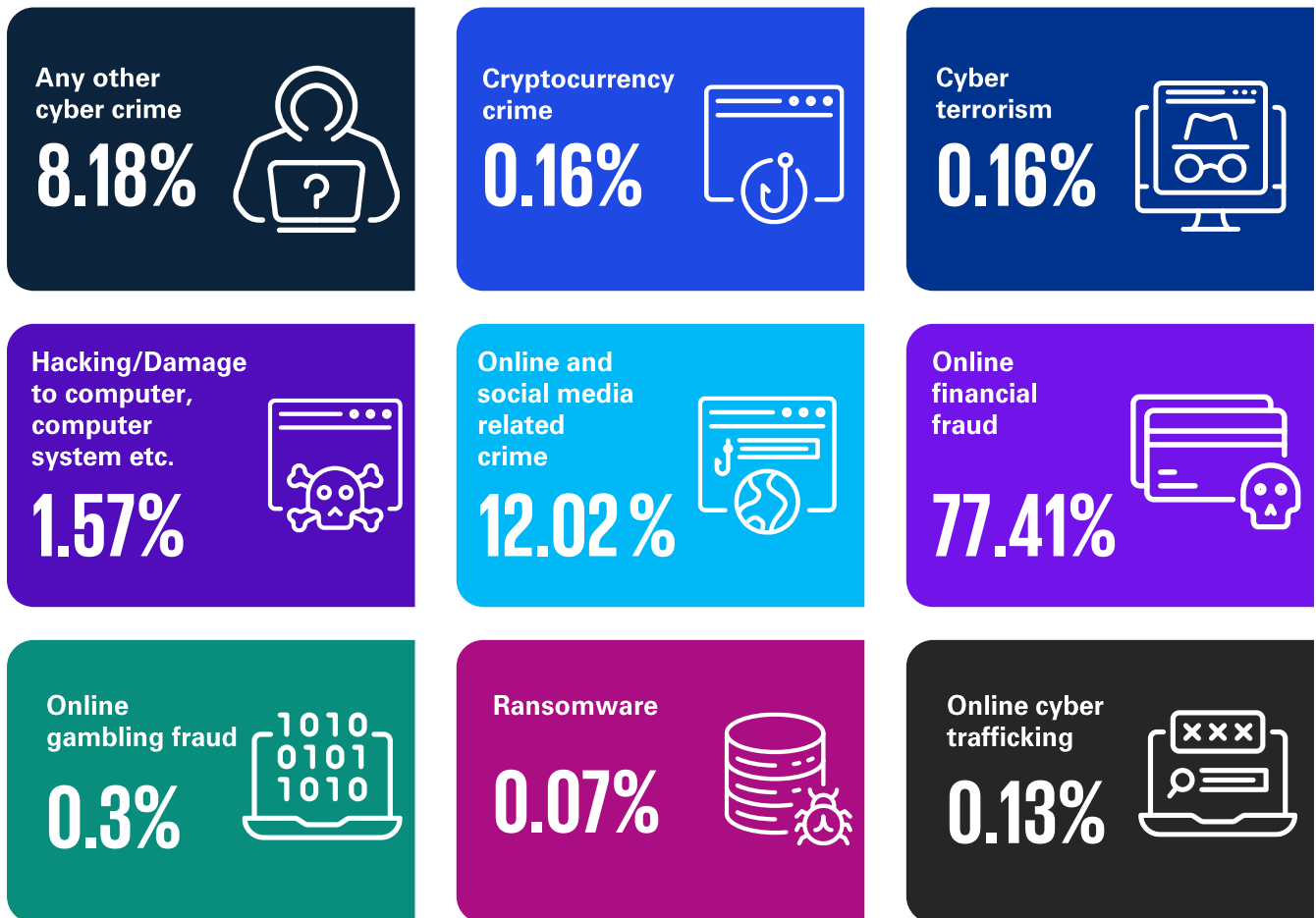
17. TSMC confirms data breach after LockBit cyberattack on third-party supplier, TechCrunch, Carly Page, 30 June 2023

18. The Log4j Vulnerability: Millions of Attempts Made Per Hour to Exploit Software Flaw, The Wall Street Journal, David Uberti, James Rundle, Catherine Stupp, December 2021

3.3 Cyber fraud and money laundering

The fast-paced adoption of new technology also has profound implications on account of risks arising from increasing instances of cyber fraud and money laundering. In 2022 alone, the INTERPOL helped member countries intercept nearly INR 16.5 billion in criminal proceeds from cyber-enabled fraud¹⁹. These advanced technologies have also provided cybercriminals with powerful capabilities to execute sophisticated attacks, deceiving both individuals and systems.

Cybercrime distribution trend in India



Source: A deep dive into cybercrime trends impacting India, FCRF, September 2023

In their recent comprehensive whitepaper titled “A Deep Dive into Cybercrime Trends Impacting India”, the Future Crime Research Foundation (FCRF), a non-profit startup incubated at the Indian Institute of Technology (IIT) Kanpur, observed that financial frauds constituted over 75 per cent of cybercrimes in the country between January 2020 and June 2023. Notably, almost 50 per cent of these cases were related to UPI and internet banking. Social media-related crimes accounted for 12 per cent of online offenses, encompassing subcategories like cheating by impersonation, cyberbullying, sexting, email phishing, and more²⁰.

The emergence of AI-generated deep fakes has enabled cybercriminals to engage in impersonation and identity theft. In January 2023, a US family became a victim of a “virtual kidnapping” scam where the attacker mimicked the voice of their 15-year-old daughter using AI and pretended to have kidnapped her, demanding a ransom of INR 82 million in return²¹.


19. Annual Report 2022, INTERPOL, June 2023

20. A Deep Dive into Cybercrime Trends Impacting India, FCRF, September 2023

21. ‘Mom, these bad men have me’: She believes scammers cloned her daughter’s voice in a fake kidnapping, CNN, Faith Karimi, 29 April 2023

Generative AI algorithms can craft convincing phishing emails that evade traditional email filters, while ML algorithms can analyse stolen login credentials and mimic human behaviour, bypassing security measures like CAPTCHAs or behavioural analysis systems. Additionally, AI-powered bots can automate social media attacks, including the dissemination of malicious links, manipulation of public opinion by fake news, and perpetration of fraudulent activities. Generative AI has also brought our attention to large language models (LLMs) being used for criminal purposes such as WormGPT and FraudGPT²².

Similarly, blockchain while ushering in significant innovative opportunities has also brought about newer risks. One such risk is about scammers orchestrating initial coin offerings (ICOs) for fictitious investment opportunities that promise attractive returns and luring unsuspecting individuals into such schemes, and then vanishing with their funds.



An example of such ICO scam was BitConnect, which claimed to be an open-source cryptocurrency guaranteeing investors 40 percent returns. Unfortunately, it turned out to be a Ponzi scheme that cost its investors INR 200 billion²³.

Metaverse and composite wallets are also being misused for money laundering. Criminals convert illicit funds into virtual assets and mix them with legitimate funds and transactions to obscuring origins of the illicit funds.

Mobile traffic in India has witnessed an astounding growth rate of about 15 times in the past five years. By the end of 2027, it is projected that 5G will represent nearly 40 per cent of mobile subscriptions, which is roughly 500 million subscriptions. However, these impressive figures also expand the attack surface for cyber fraud and money laundering, consequently amplifying the challenges faced by the country, capital market industry, organisations, and society at large.

22. WormGPT and FraudGPT – The Rise of Malicious LLMs, Trustwave, Arthur Erzberger, 8 August 2023

23. BitConnect Founder Indicted in Global \$2.4 Billion Cryptocurrency Scheme, Office of Public Affairs, U.S. Department of Justice, 25 February 2022 Office of Public Affairs



4 Managing digital trust by outpacing threats



Digitalisation and transformation enabled by emerging technologies have led to capital markets becoming more accessible, efficient, interconnected and offering greater variety of products and services. India's growth and key contribution that capital markets play has made upholding trust, a foundational requirement. It would be correct to say that similar to how a strong and stable currency is valuable in trade, a solid and sustainable foundation of trust is invaluable for fostering investor confidence and healthy growth in the capital markets.

Also, while technology changes and trends come and go, trust must stand resolute, unaffected by the rapidly evolving risk landscape.

In the upcoming sections, we embark on an exploration of the constituents of digital trust,

emerging technologies and innovative strategies, particularly in the field of cyber security, to uphold trust.

4.1. Currency of digital trust

In the context of digital trust, "currency of trust" would symbolise the confidence in the outcome for investors, and it comprises following attributes - security and reliability, accountability and oversight, and transparent and responsible use. A strong currency of trust means that investors are more willing to participate in the market, leading to greater liquidity and stability. We explore how these attributes especially cyber security and resiliency, have become ever more critical as the digital world is being increasingly characterised by near absence of human touch and complexity of digital environment.

Data is the new oil, but trust is an evergreen engine - capital markets are no exception to this rule.

- Mr. J.V.N. Subramanyam, IAS

Director, Department of Economic Affairs (DEA), Government of India

4.1.1 Security and reliability

In today's digital age, reliable functionality, secure communication and protection of information have become paramount. However, increasing instances of data breaches and technology disruptions are impacting trust among businesses, investors, and other stakeholders. As per 2023 Ponemon report, the average cost of data breach globally is INR 343 million and average cost of data breach in India is INR 179 million²⁴.

Just as a fortress is built with strong walls, guarded gates, watchtowers, and security personnel, trust needs to be protected with multiple layers of defence. These layers cohesively work to create a secure and reliable environment for trust to thrive.

The digital security ensures dependable service levels

by minimising the potential for disruptions in the ecosystem. With the increasing complexity of the digital realm and volume of users, there is a need for assurance and information regarding the reliability and security of the ecosystem. This creates a dynamism where either trust in secure and dependable systems flourishes in a virtuous cycle or dwindles in a vicious cycle, due to mistrust in unsecure or unreliable technologies.

As digital ecosystem and services have become the primary mode of service delivery for most users, any form of disruption, or degradation in these services via breach in cyber security can have significant losses for the individual, participants, and the wider landscape. Therefore, ensuring security, and reliability within the digital realm is of utmost importance for the capital markets ecosystem.

24. Cost of Data Breach Report 2023, Ponemon Institute, July 2023

4.1.2 Accountability and oversight

The importance of governance on use of digital technology in capital markets industry organisations is witnessing a remarkable surge. This is evident by the heightened statutory and capital markets regulatory scrutiny surrounding various digital risk domains. As a result, organisations are facing mounting pressure to exhibit improved oversight in their efforts to uphold social responsibility.

The regulators are demanding faster, detailed and automated reporting of digital risks particularly on cyber security and technology resilience. For example, increased requirements for reporting material incidents to the market as evidenced by SEBI circulars as well as recent SEC rulings.

These developments are intended to bridge information gaps that may exist amongst capital market players, technology providers and end users, ultimately fostering a sense of trust and confidence on digital technology enabled transformative changes that capital markets are undergoing.

4.1.3 Transparent and responsible use

The digital world is characterised by faceless, touchless, and highly automated (and now autonomous) ecosystem. The digital technologies bring in innate power to amplify both the righteousness/malice as well as accuracy/error. It is crucial to build and implement measures to effectively safeguard against these challenges, which have emerged as major risks in an increasingly AI enabled digital ecosystem.

Organizations need to build capabilities to considering risks throughout the lifecycle i.e. from model design,

training and testing to learning and continual improvement. Particular attention needs to be given to data across training, testing and live usage such that AI does not bring bias as well as lack of explainability in the service. The risk management measure need to consider many third-party tools (including for cyber security) that are integral components of the digital service offerings world. Critical information like training data, cyber security posture of the solution is not readily available to capital market stakeholders for making informed decisions. Establishing transparent and effective communication is important for a trusted and reliable ecosystem. While, internal accountability measures are crucial for ensuring responsibility, truly ethical and responsible organisations go beyond and create avenues for redressal when their technologies inadvertently cause harm to external stakeholders. These external avenues serve as critical checks, particularly when an organisation falls short of its aspirations for inclusive, ethical, and responsible use of technology. By embracing such external opportunities for redressal, capital market participants (including technology providers) can demonstrate their dedication to rectifying any unintended consequences and mitigating potential harm, further solidifying their reputation as trustworthy and conscientious actors in the digital landscape

4.2 Elevating digital trust

In this fast -growing and digitalising Indian capital market space, traditional approach to cybersecurity is no longer sufficient. We are witness to the struggle in keeping reasonable security over the modern capital markets landscape.

Trust of people in digital transactions in this century is critical and is vital for financial transactions. Steps taken by our depositories to continuously enhance and finetune their cyber-security mechanisms have been an important pillar in the recognised robustness of Indian systems.

- Dr. Deepak B Phatak,
Professor Emeritus, IIT Bombay



"Security by design" has emerged as a strategic imperative to fortify India's capital markets against cyber risks. Security by design entails embedding cybersecurity into the core of all operations and decision-making processes, making it an intrinsic part of the financial ecosystem's DNA at the national, capital market, organisational and societal levels. In the following section we will look at some trust initiatives taken at different levels.

4.2.1 Recognising cybersecurity as a strategic imperative

The first step towards a "trustworthy" posture is acknowledging that it must be a strategic priority for all stakeholders. Such a recognition from government and regulatory authorities, financial institutions, technology service providers and investors shall go a long way in allocation of adequate resources to address potential threats and challenges effectively.

4.2.2 Embedding security and resiliency into the core of financial operations

In Formula-1 racing, engineers meticulously design and integrate safety features into the car from the very beginning to prevent accidents. Similarly, to build a secure and robust financial ecosystem, cybersecurity and technology resiliency must be seamlessly integrated into the entire landscape, starting from the planning phase of policies, regulations, rules and guidelines, determining financial products, services, and infrastructure. This proactive approach helps reduce risks and safeguard critical assets. Postponing cybersecurity until the end is like focusing solely on speed during the race without ensuring the car's safety features are in place – it increases the risk of crashes and compromises the overall performance. Security and resiliency need to be seen as an enabler and not a constraint.

The Digital Operation Resilience Act (DORA) released in the UK provides a good framework for improving resilience of the financial sector against digital disruptions. DORA mandates that robust assessment frameworks that quantify cyber risk, enable organisations to identify potential vulnerabilities and allocate resources effectively. The legislation sets a benchmark globally for risk quantification and resiliency measures.

The recent SEBI guidelines titled "Guidelines for MIIIs regarding Cyber security and Cyber resilience" circulated on 29 August 2023, mark a significant stride forward²⁵. It underscores the regulator's recognition to safeguarding market integrity and investor trust by building a more cyber resilient capital market ecosystem.

Digital trust by design calls for proactive measures in identifying, assessing, and mitigating cybersecurity and technology risks. Regular risk assessments, threat modelling, and vulnerability assessments are critical components of this approach. Additionally, decision-makers must have access to actionable real-time threat intelligence and observability of operating vitals to make informed choices that align measures with the evolving risk landscape.

It is high time that organisations give importance to cyber resilience as cyber incidents have become part of life and exist irrespective of the industry. The systems/processes must be resilient enough to deal with ongoing incidents. Effective cyber threat management and incident response are vital components of a robust cybersecurity strategy for organisations in the capital markets sector. As cyber threats evolve and become increasingly sophisticated, organisations must adopt proactive measures to identify, detect, and respond to potential security incidents.

Implementing a comprehensive cyber threat management program involves continuously monitoring the threat landscape, conducting vulnerability assessments, and implementing robust security controls. Organisations can leverage threat intelligence feeds, security information and event management (SIEM) solutions, and advanced analytics to detect and respond to threats in real-time. Regular penetration testing and red team exercises can also help identify potential vulnerabilities and strengthen the security posture.

Last but not the least, organisations must have a well-defined incident response plan in place. This plan should outline clear roles and responsibilities, communication protocols, and steps for containment, eradication, and recovery. By having a structured and tested incident response process, organisations can minimise the impact of security breaches, reduce downtime, and ensure the preservation of critical data and systems.

4.2.3 Embracing cyber risk quantification - What gets measured gets done

Cyber risk quantification (CRQ) looks at different costs involved in a cyber-attack and segregates them into useful metrics. These costs are basis of any effective cyber strategy. Cyber-attacks if not addressed timely might result in reputational loss, operational loss, financial loss and legal penalties.

Cyber risk can be meaningfully quantified by identifying losses associated with business interruption, data exfiltration and regulatory costs. CRQ helps in making better business decisions using risk-based cybersecurity investments and initiatives, helps in monitoring of crown jewel assets.

25. Guidelines for MIIIs regarding Cyber security and Cyber resilience, SEBI, 29 August 2023

Cyber risk cost = Business interruption cost + Data exfiltration cost + Regulatory cost + Recovery and response cost

Business interruption cost

Business interruption cost =
Process revenue per hour x
Time to recover from the attack



Data exfiltration cost

Data exfiltration cost =
Number of records x cost
per record

Regulatory cost

Cost associated with
regulatory fines and penalties

Recovery and response cost

Cost involved in recovery
and timely response

4.2.4 Implementing robust governance frameworks

As capital markets embrace emerging digital technologies, governance becomes ever more crucial to ensure responsible and secure implementation. Governing new technologies involves establishing policies, frameworks and controls that enable organisations to leverage the benefits of technology while managing associated risks effectively.

One aspect of technology governance is establishing clear policies and guidelines for the adoption of emerging technologies such as artificial intelligence (AI), blockchain, quantum computing/encryption and 5G. For example, AI frameworks require careful governance to ensure ethical use, data privacy, explainability, low bias and security. As organisations adopt AI algorithms that make important decisions that impact trading strategies, risk management measures, and customer interactions, they must establish robust governance frameworks that promote transparency, accountability, and fairness to not only uphold trust but also comply with ever increasing regulatory requirements.

The emergence of risks (local and cross border) and their consequential impacts on capital markets have

led to an increase in regulatory scrutiny across various societal aspects, including privacy, security, ethics, transparency, and competition.

In the realm of AI, regulatory frameworks are being built to govern the development and deployment of AI systems, particularly high-risk applications. For instance, in April 2021, the European commission proposed the “EU Artificial Intelligence Act”, aimed at regulating AI systems. The United States Government has also initiated efforts in regulating AI and ML technologies, with NIST releasing guidelines for AI risk management and standards development²⁶. Proposed bills such as the “Algorithmic Accountability Act” and the “Facial Recognition and Biometric Technology Moratorium Act” address concerns surrounding bias, privacy, and facial recognition technology. Similarly, the Chinese Government has released guidelines for AI ethics and data security to promote responsible AI development. The challenges arising out of these acts are felt by institutions which are present cross border, as the regulatory norms are not uniform. This adds to franchise risks, besides additional costs and compliances.

26. AI Risk Management Framework, NIST, 26 January 2023



Regarding the adoption of 5G, several countries have implemented or proposed national security review mechanisms to ensure the security and protection of critical infrastructure from potential cyber threats, especially in sectors like finance that heavily rely on secure and reliable networks. Regulatory bodies like the Federal Communications Commission (FCC) in the United States have regulations in place to govern the deployment and operation of 5G networks. These regulations cover aspects such as spectrum allocation, network infrastructure standards, and compliance with privacy and security requirements.

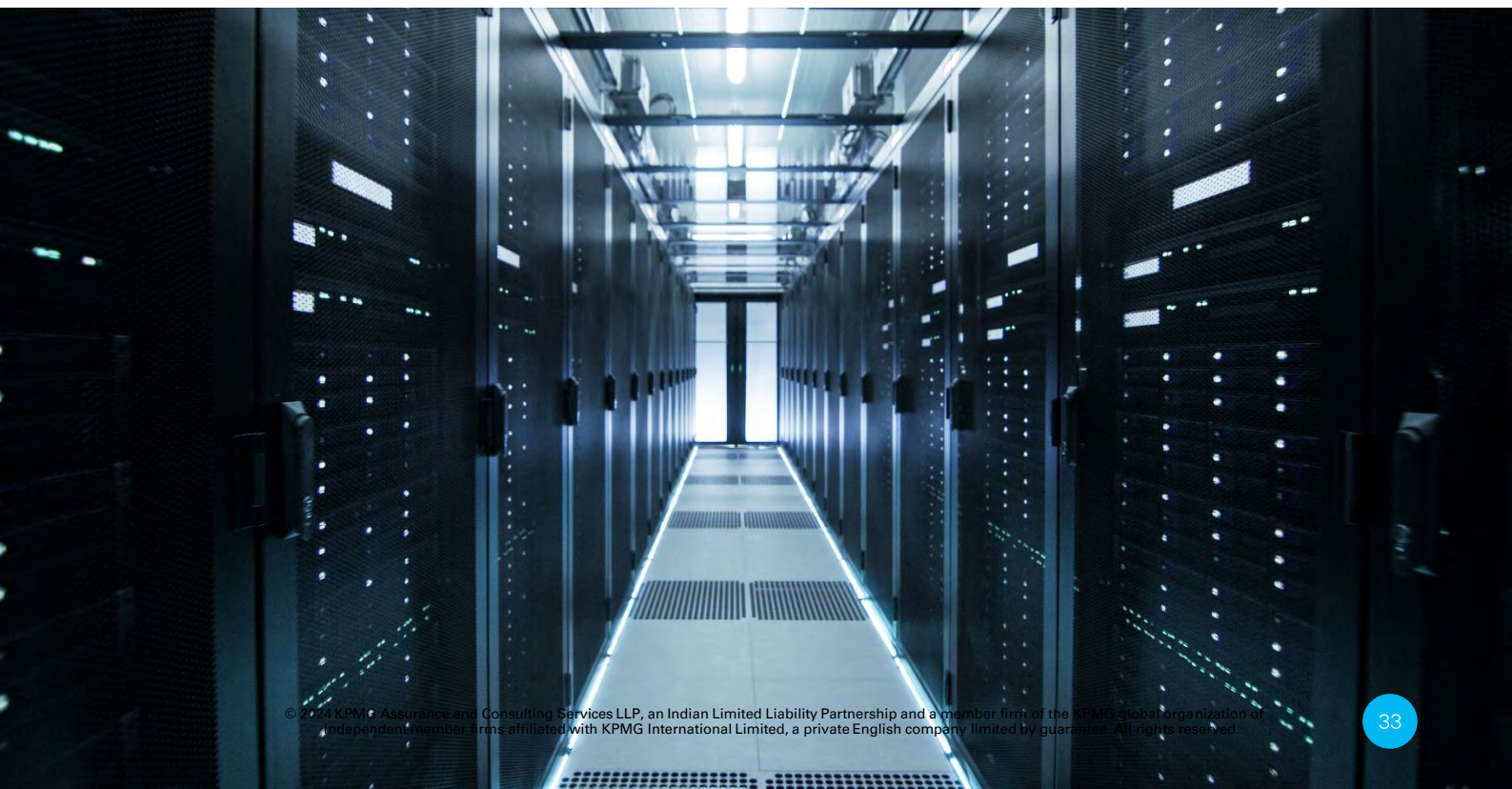
In March 2023, The US Government released the national cybersecurity strategy which also emphasises on the importance of securing next generation technologies through its endeavours such as the national artificial intelligence initiative and the national strategy to secure 5G. A key element of such upcoming regulations/guidelines is the mandatory checks for malware in infrastructure and the need to procure infrastructure from trusted suppliers.

India has been in the forefront of regulating emerging technologies while also providing a habitable environment for their sustainable growth. In India, the AI and emerging technologies division of the Ministry of Electronics and Information Technology (MeitY) is actively promoting the advancement of cutting-edge technologies through various initiatives. It has established four committees in the country to develop a policy framework for AI. The Indian Government has also launched the AIRAWAT project (AI Research, Analytics, and Knowledge Dissemination Platform) to provide a common compute platform for AI research and knowledge assimilation. In March 2020, the STPI APIARY, a centre of entrepreneurship in blockchain technology, was set up in collaboration with MeitY, STPI, Govt.

of Haryana, and several other private entities, to identify and evaluate blockchain based startups and host them in the STPI Gurugram incubation facility. The Securities and Exchange Board of India (SEBI) issued a circular in 2022 outlining "Operational guidelines for 'Security and Covenant Monitoring' using Distributed Ledger Technology (DLT)", which was a follow-up to the first circular in 2021 titled "'Security and Covenant Monitoring' using Distributed Ledger Technology". Moreover, in June 2023, the Reserve Bank of India (RBI) published a report titled "Chapter 3: Regulatory Initiatives in the Financial Sector", delving into decentralised finance (DeFi) and its impact on financial stability.

Notably, the newly published Digital Personal Data Protection Act (DPDPA) in India shall be the overarching regulation, influencing all areas of emerging technologies, over data privacy concerns. Factors such as accountability, transparency, data minimisation, fairness, accuracy, and lawful processing of personal data have been reflected in the DPDPA.

It is important to acknowledge that regulatory framework for emerging technologies is in a state of rapid development, and regulations pertaining to AI, blockchain, and 5G can differ from one country or region to another, thereby adding new challenges. The given examples illustrate the initial efforts made to tackle the distinctive challenges and risks associated with these technologies. Nevertheless, these examples also emphasise that adhering to regulatory changes can be intricate. This is where regtech plays a vital role, utilising emerging technologies to streamline responses and automate governance and reporting procedures, providing a solution to this complexity.



4.3 Enhanced security by leveraging emerging technology

The emerging technologies have also offered in innovative opportunities to enhance trust and security posture. In this section we discuss following such key opportunities - smart contracts, strong identity and access management and zero trust, self-sovereign identity security and post quantum encryption.

4.3.1 Smart contracts: Enhancing digital trust in capital markets

Smart contracts, enabled by blockchain technology, have emerged as a powerful tool to enhance digital trust in capital markets. These self-executing contracts automate and enforce the terms of agreements, eliminating the need for intermediaries and reducing the risk of human error. A prime use case for smart contracts in the capital markets sector is trade settlements. Traditionally, the settlement process involves multiple intermediaries, manual verification, and reconciliation of trade details. This process is time-consuming, prone to errors, and lacks transparency. By leveraging smart contracts, the settlement process can be streamlined and automated, significantly enhancing transparency, reducing settlement time and minimising risk of errors.

For instance, consider a scenario where two financial institutions engage in a trade of financial instruments. With the implementation of smart contracts, the terms of the trade are coded into a blockchain-based smart contract. The smart contract automatically executes the trade based on predefined conditions, verifies the ownership and availability of assets, and triggers the settlement process. As a result, the settlement is executed in a secure, transparent, and efficient manner, reducing counterparty risk, and enhancing operational efficiency.

4.3.2 Strong identity and access management (IAM) and zero trust (ZT)

Strong IAM based on multiple factors and entity behaviour can enable fine grained and context aware access. Implementation of strong IAM capabilities like biometric authentication, hardware tokens or one-time password to access trading platforms and continual behaviour monitoring can reduce the risk of unauthorised access to these platforms. Although, such IAM frameworks provide a sturdy foundation, increasing complexities of modern trading systems necessitate consideration of solutions such as zero trust and zero knowledge proof (a cryptographic instrument) for securing access.

The ethos of zero trust introduces an epoch of continual risk appraisal. Through the meticulous

scrutiny of access patterns and behavioural tendencies, any semblance of abnormal activities can be promptly unearthed and subsequently mitigated. With zero knowledge proof, individuals and traders can authenticate their identities without resorting to the disclosure of sensitive data and substantiate their credentials without revealing the finer details of trading strategies or comprehensive portfolio particulars, consequently fortifying against identity-related transgressions.

4.3.3 Self-sovereign identity security: Empowering data privacy

Self-sovereign identity security represents a paradigm shift in the way individuals manage and control their digital identities. It empowers individuals with the ability to maintain ownership and control over their personal data, enabling secure and privacy-preserving interactions in the capital markets sector. India has taken a step in implementing secured pseudo self-sovereign identity. MeitY under its Digital India initiative of providing citizens a secure document access platform on a public cloud, built DigiLocker a digitalisation service that provides storage space for digital version of such as academic mark sheets, driving license, vehicle registration certificates etc. and other identity proofs. As per DigiLocker national statistics in December 2023, currently 226 million users are registered with 6.28 billion issued documents.

One notable use case for self-sovereign identity security in the capital markets sector is customer onboarding and KYC processes. Traditional onboarding processes often require individuals to provide extensive personal information to financial institutions, raising concerns about data privacy and security. With self-sovereign identity, individuals can create and manage their digital identities using decentralised identity (DID) systems. Consider a scenario where a brokerage firm is onboarding a new client. Instead of requesting the client to provide numerous identity documents, the firm can leverage self-sovereign identity to streamline the process. The client can create their digital identity using a DID system, storing their personal data locally on their devices. The firm can then request specific attributes or credentials from the client for verification, such as proof of address or proof of income, without the need for the client to disclose their complete personal information. These attributes are cryptographically signed by trusted issuers, ensuring their authenticity. As a result, the client retains control over their personal data and can selectively disclose only the necessary information, enhancing privacy and minimising the risk of data breaches.

Self-sovereign identity can facilitate secure and efficient cross-border transactions in the capital markets sector. With traditional identity verification processes, individuals often encounter delays and complexities when conducting transactions across different jurisdictions and traditional identity verification procedures are susceptible to cyber attacks. Self-sovereign identity simplifies the verification process by providing individuals with portable and globally recognised identities. This allows them to prove their identity and access financial services across borders without the need for repetitive and time-consuming identity verification processes and using passwords. By reducing friction in cross-border transactions, self-sovereign identity promotes efficiency, fosters financial inclusion, and strengthens the integrity of global capital markets.

To encourage wider adoption and interoperability of self-sovereign identity systems in the capital markets sector, collaboration among financial institutions, regulatory bodies, and technology providers is essential. Establishing common standards, interoperable protocols, and trusted credentials, issuers can create a robust ecosystem that empowers individuals while maintaining regulatory compliance and security.

4.4 How should the ecosystem respond?

In the capital markets sector, cybersecurity is complex and ever-changing. To effectively address challenges and share best practices, collaboration and partnerships are crucial. Organisations should engage with industry peers, regulatory bodies, technology vendors, and cybersecurity experts to exchange

insights, share threat intelligence, and develop industry-wide standards.

Industry consortiums, information-sharing platforms, and cross-sector partnerships play a significant role in enhancing cybersecurity capabilities. By pooling resources and intelligence, organisations can collectively strengthen their defences against cyber threats and establish a more resilient security posture.

Collaboration with regulatory bodies ensures compliance with industry-specific regulations and guidelines. Engaging in open dialogue with regulators fosters a proactive approach to cybersecurity and demonstrates a commitment to a secure financial ecosystem.

Leveraging technology vendors and cybersecurity service providers augments security capabilities. Specialised vendors offer cutting-edge technologies, threat intelligence, and expertise in implementing and managing cybersecurity solutions, helping organisations stay ahead of evolving threats.

Investing in training and awareness programs for employees is essential. Human error and lack of cybersecurity awareness contribute to security incidents and breaches. Training should cover common threats, safe browsing practices, and adherence to security policies. Specialised topics for developers, system administrators, and security teams should also be included. Regular training sessions, workshops, and cyber drills including phishing exercises reinforce best practices and foster a security-conscious culture within the organisation.



5 Opportunity for India & the World – “AatmaNirbhar Bharat”

India's digital journey began in the early 2000s. The country's increasing reliance on digital technologies and the growing use of the internet have propelled the establishment of systems that streamline transactions. The Indian Government initiated the development of digital and foundational capabilities in-house, leveraging skilled resources in line with the AatmaNirbhar Bharat, आत्मनिर्भर भारत (Self-reliant India) initiative. This initiative aims at reducing import dependency and promoting domestic production and innovation, holds significant potential for India and the world, particularly given the fundamental changes in the capital markets threat landscape in India.

In addition to AatmaNirbhar Bharat, आत्मनिर्भर भारत, the Indian Government has launched various initiatives, including Make in India, Startup India Seed Fund, Startup India Initiative, and Startup Leadership program, all geared towards nurturing innovation and entrepreneurship in the technology sector. These encompass the Startup India program, fostering a favourable environment for startups, and Digital India initiative, striving to connect every citizen to the internet.

The Government has developed several world-class digital capabilities indigenously, including one of the largest biometric ID system known as Aadhaar²⁷, one of the largest rural broadband project named Bharatnet²⁸, a robust digital physical infrastructure, a data sharing framework called Data Empowerment and Protection Architecture (DEPA), paperless governance initiative named DigiLocker, the Unified Payments Interface (UPI) for instant payments, autonomous Indian regional navigation satellite system known as NavIC, among others.

The industry has made remarkable strides, becoming a global leader in information technology services. The growth is exemplified by India's rapidly expanding ecosystem with approximately 68,000+ startups and 100+ unicorns, with combined valuation of INR 30+ trillion²⁹. India now ranks as the world's third-largest startup ecosystem having raised about INR 940+ billion³⁰ in 2023. These startups have created 768,000+ jobs over last six years²⁹.

Recognising importance of cybersecurity, the Indian Government has taken initiatives to strengthen cybersecurity laws in the country. The focus has shifted towards cyber to enhance trust among stakeholders. India is determined to achieve self-reliance in the field of cybersecurity. A recent example in this is, the development of Maya OS by the Ministry of Defence in collaboration with the Defence Research and Development Organisation (DRDO), the Centre for Development of Advanced Computing (C-DAC), and the National Informatics Centre (NIC). Maya OS is created with aim to use indigenous systems for protecting India's defense

system's sensitive information³¹.

In the subsequent section, we discuss cyber landscape in India with a focus on capital markets and journey that country needs to embark for being self-reliant "Aatmanirbhar, आत्मनिर्भर" in the cyber security space considering the criticality of digital ecosystem for capital markets and the country as a whole.

5.1 Cyber landscape in India

In recent years, the country has witnessed a surge in cyberattacks, targeting government agencies, private companies, and even healthcare institutions. According to CERT-In, ransomware incidents in India increased by 53 per cent in 2022³² compared to the previous year. The most impacted sectors were the information technology and IT-enabled services, followed by finance and manufacturing. In 2022-2023, approximately 50 government websites were hacked, and eight data breaches were reported³³.

The threat landscape in India has evolved, driven by the proliferation of consumer-facing digital devices, increased cloud adoption, and the simultaneous use of endpoints, IoT devices, and consumer gadgets. As India digitises further, the threat landscape naturally expands. Various components of the ecosystem, including hardware, applications, and networks, are increasingly vulnerable, with endpoints being particularly at risk. Strengthening controls such as Endpoint Detection and Response (EDR) and User and Entity Behaviour Analytics (UEBA) on endpoints is essential.

The 2023 union budget emphasises strengthening digital infrastructure in alignment with national data governance policies, aiming to create a secure channel for anonymous data access. The Government has allocated around INR 6 billion to enhance India's cybersecurity infrastructure³⁴.

In addition to favourable government initiatives, India boasts a sizable and growing pool of skilled tech talent renowned for their expertise in software development, IT consulting, and customer support. This talent reservoir has empowered Indian companies to assert a strong global presence. Moreover, the number of engineering colleges and universities in the country continues to increase, further enriching this talent pool.

Indian companies are demonstrating a growing commitment to innovation by developing and implementing cutting-edge technologies. Among these developments, Indian firms are actively involved in creating and deploying artificial intelligence (AI) solutions across diverse applications. Riding on the information technology and now startup ecosystem, India is witnessing expansion of indigenous capabilities in cybersecurity arena, including startup ecosystem.

27. Decentralised Identity: A safe protector for managing digital identity faces hurdles, The Economic Times, Surabhi Sarada, 23 September 2023

28. Bharatnet Project, Universal Service Obligation Fund, Department of Telecommunication, Govt. of India, August 2023

29. Indian Tech Startup Funding Report 2023, INC 42, 29 December 2023

30. Indian startups raised more than \$11 Bn in 2023: Report, Entracker, Harsh Upadhyay & Shashank Pathak, 30 December 2023

31. What is Maya OS, the indigenous Windows replacement for India's defense systems?, Indian express, Zohaib Ahmed, 19 August 2023

32. Cybersecurity threat. Ransomware incidents up by 53% in India: CERT-In, The Hindu business line, 14 April 2023

33. 50 government websites hacked, 8 data breaches in 2022, says IT Minister Ashwini Vaishnav, Times of India, 4 February 2023

34. Budget 2023 | India allocates over Rs 600 crore to improve cybersecurity infra, MSN, Pihu Yadav, 1 February 2023

5.2 Building currency of trust in the Indian capital markets

In an increasingly interconnected world, India is geared to capitalise on its potential with advancement in technology. With the vision to become a major player in global capital markets and cultivate a thriving and innovative ecosystem, India's journey requires strengthening its cybersecurity measures. This involves safeguarding critical digital assets, sensitive data, and individual privacy through

substantial investments and effective defences against cyber threats. Prioritising robust encryption, promoting cybersecurity awareness, and fostering public-private collaborations fortify India's digital security landscape.

India needs to take several strategic steps to build a cybersecure future. The nature of cyber risk requires response at national, capital market, organisational and societal level. Key initiatives for each level include the following:

1. National level/regulatory level



- **Comprehensive cybersecurity framework:** Establish and enforce robust cybersecurity laws, regulations and standards covering,



- **Need for interoperable regulations:** As capital markets play an important role in financial services sector, the participants are expected to adhere to regulatory requirements from primary regulators like SEBI, and also other statutory bodies/acts (RBI, Companies Act 2013, Contract Act). However, the cyber attackers on the other side can attack any sector, impacting the whole ecosystem including the Financial Services sector. Therefore, there is need for interoperable and robust regulation to bring consistency in regulations across wide participation.



Common cyber taxonomy:



While there are certain regulations/ standards and industry usage, which comes with wide variations of terms. In this era of growing cyber threats, cyber risk requires fast/ real time response. There is a need for consistent and common cyber taxonomy to be developed to improve information sharing across governments, regulators and industry participants.

Differential requirements:



As capital markets participants manage technology setup of varied size, complexity and strategic importance differential scale-based cyber security and resilience regulations should be established. A good initiative in this direction is such differentiated regulations released by SEBI for MIIIs and QSBs.

Comprehensive framework for critical organisations:



Regulators can build framework for identifying critical organisations in capital markets sector similar to Navratnas and Maharatnas in PSU sector and compile robust rules/ requirements for them.

2. Capital markets industry level



Ecosystem wide cyber stress testing: Encourage cyber stress testing for all critical stakeholders of the ecosystem. Guidelines like NIS2 requirements from EU can be considered for making assessment and reporting mandatory. The stress test should cover not just regulated entities but also critical service providers and stakeholders enabling the capital market ecosystem.



Public-private partnerships: Encourage collaboration between government agencies, financial institutions, and cybersecurity experts to enhance the resilience of capital market systems.



Incident response capabilities: Develop and implement incident response capabilities to minimise impact in the event of cyberattacks on capital market infrastructure.



Investors education: Promote cybersecurity awareness among investors, educating them about potential risks and safe online practices when participating in capital markets.

In the ever-evolving landscape of capital markets, trust is the currency of the digital age. At SBI Securities our relationship with customers goes beyond transactions; it's built on lifelong trust. With this CDSL's initiative on cyber security, it is time we as an industry come together to reimagine and reinforce the foundations of trust, forging a path to a more secure and innovative financial future for our customers.

- Mr. Deepak Kumar Lalla,
Managing Director & Chief Executive Officer, SBICAP Securities

3. Organisational level



Deeper engagement at board level – Cyber security and resiliency is a business risk and requires deeper attention of “**Those in charge with governance**”. Organisation should have annual cyber security strategy sessions, and cybersecurity training, including table-top drill for board to enhance its awareness and effectiveness of oversight.



Effective communication strategy – Cyber incidents require precise and expeditious communication to stakeholders from regulators to customers and from partners to industry peers. The strategy needs to comprehensively cover variety of cyber incidents and be implemented such that it can be effectively operationalise in case of a cyber security incident.



Managing third party risks – Organisations rely on third parties comprising technology product suppliers, service providers, Fintech for a significant part of the business activity. A comprehensive framework comprising policy, standards and procedures, effective contractual arrangements, 360-degree governance and monitoring across lifecycle is crucial to manage risks emanating from such third parties. Amongst third parties more attention is needed around cloud services, SOC services, fintech’s and those handling personal data.



Reduction of attack surface – Organisations need comprehensive cyber security program to identify crown jewels, minimise data proliferation/storage, minimise access provisions, and institute robust testing to consistently maintain effective cyber defence



Capability for faster detection and response – Organisations must adopt security by design practices, build comprehensive monitoring and correlation capability augmented by external threat intelligence, use threat hunting to early identify cyberthreats. It is essential to regularly test the detection and response capability by methods like red teaming exercise to proactively identify changes and enhancements needed.



Practice response and recovery – It has been quite often seen that practically, response and recovery procedures do not remain effective in real time, due to insufficient coverage of cyber breach scenarios and confidence on the plans. It is crucial to have comprehensive set of response and recovery playbooks, period cyber simulation covering all stakeholders.



Regulatory compliance: Ensure that organisations adhere to cybersecurity regulations, conduct regular security assessments, and report incidents promptly.

4. Societal level



Digital literacy

Launch nationwide digital literacy programs to educate citizens, especially youth and seniors, about online risks, safe browsing, and responsible digital behaviour.



Consumer awareness

Build awareness about consumer protection and other cyber security laws that provide safeguard to individuals from fraudulent online schemes and cybercrimes.

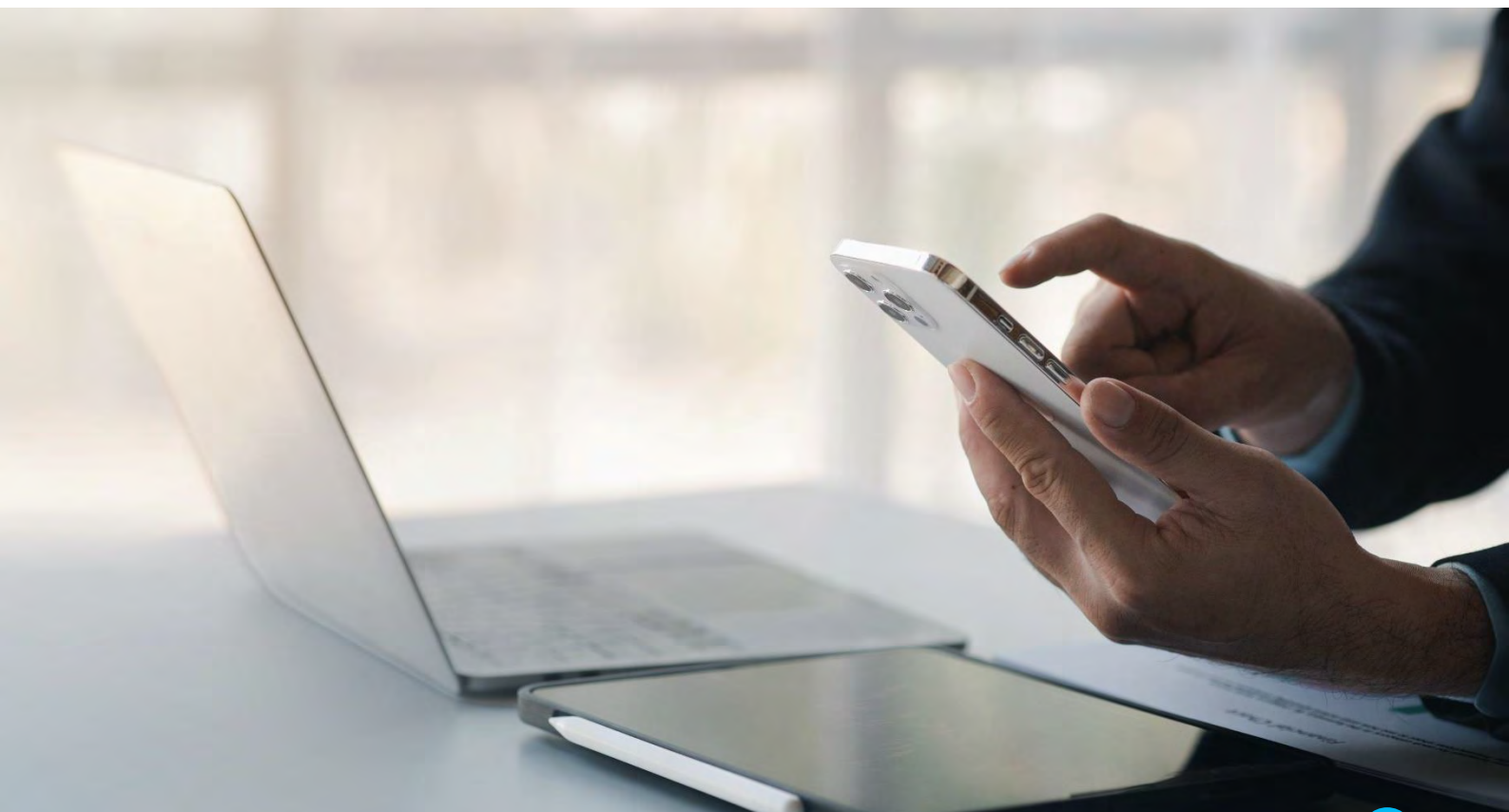


Community engagement

Engage communities in initiatives that promote cybersecurity awareness and best practices, fostering a culture of collective security.

These measures and initiatives shall help India enhance its cybersecurity posture, safeguard its capital markets, and contribute to the development of a secure and innovative digital ecosystem.

India's commitment to achieving self-reliance in the realm of cybersecurity is evident through the launch of several key initiatives. The National Cyber Security Policy and National Cyber Security Strategy underscore India's determination to enhance its cybersecurity capabilities and lead as a global authority in this critical domain. Also, the country's ultra-large scale provides it an unparalleled opportunity to build world scale capabilities. The standards, products and innovations by Indian companies, startups and government therefore shall also help reinforcing India's influence in the journey towards safety and security of capital markets across the world.



6 Symposium highlights



Industry leaders, regulators, academicians and CXOs from India and various parts of the world recently came together for an essential discussion centered on the pressing cybersecurity challenges looming over the financial ecosystem. Coinciding with CDSL's 25th-anniversary celebration, the organisation initiated an event, named The cyber security symposium on theme - "Reimagine: Digital Trust in Capital Markets."

This symposium provided an exclusive platform for exploring the evolving landscape of digital trust in the context of capital markets, offering attendees:

- Deep insights from prominent experts in the field
- Thought-provoking discussions on critical issues

- Detailed exploration of the latest global cybersecurity trends

The event started with talks by the guest of honours and address by the chief guest, which set the right tone. The inaugural sessions were followed by a combination of three presentations and four panel discussions. The panel discussions focused on following:

- Protecting India's rising digital economy
- "Aatmanirbharta" in cybersecurity ecosystem
- Staying ahead of the curve
- What keeps board members awake at night?



Trust is a 5 letter word which symbolically eludes to that fist of the five fingers. A fist is a testament of power of unity demonstrating, incredible strength that trust can bring when we stand together. Trust is not static concept it requires continuous care and reinforcement, it needs to be reimaged constantly.

Mr. Nehal Vora,
Managing Director & Chief Executive Officer,
Central Depository Services (India) Limited (CDSL)



Insights from chief guest

Cyber security is not only the intrusion of data that is done by outsiders, but it is about sanctity of data, access and security of data.

Dr. Deepak B Phatak,
Professor Emeritus, IIT Bombay



Insights from guests of honour

The future of cyber security is be found on a wide range of principals that includes security by design, counterintelligence, regulations, proactive vigilance, cyber hygiene, automation and recoverability.

Mr. S. Ramadorai,
Former Chief Executive Officer and
Managing Director, Tata Consultancy Services (TCS)

Trust is fundamental for economic exchanges in financial markets, influencing transaction costs and market efficiency. Trust symbolizes stability and resilience. Therefore, cybersecurity is crucial for maintaining trust and prevent disruptions in the market.

Mr. K. Rajaraman,
Chairperson, International Financial Services Centres Authority (IFSCA)

Cyber resilience is identified as a crucial aspect in ensuring quick recovery from cyber-attacks. Collaboration and cooperation between stakeholders, including regulators, market intermediaries, and experts, are vital for staying ahead of cyber threats and safeguarding the trust of investors.

Mr. Kamlesh Chandra Varshney,
Whole-Time Member,
Securities and Exchange Board of India (SEBI)

Panel I - Protecting India's rising digital economy

Digital economy has contributed significantly to growth of capital markets and has also enabled in wider participation across society. Establishing digital trust through cyber and data protection measures will be pivotal for sustained adoption and innovation that shall continue driving economic growth leveraging digital channels.

Mr. Atul Gupta,

Partner - Digital Trust, Head- Cybersecurity services,
KPMG in India

India is transforming from informal, low productive, cash economy to formal, high productive, cashless economy. Open Network to Digital Commerce (ONDC) is going to change how retail businesses are done, bringing prosperity into billion people lives.

Mr. J.V.N. Subramanyam, IAS

Director, Department of Economic Affairs (DEA),
Government of India

We look at everything as opportunity, it is important to look at everything as risk. Don't trust any digital interaction and sensitise as many people and create as much investor's awareness as possible.

Mr. Nithin Kamath,

Founder & Chief Executive Officer, Zerodha

AI can attack you, but AI can also protect you. Trying to create systems where you balance ease of use with security is a true technological challenge.

Mr. Raj Balakrishnan,

Managing Director, Co Head of India Investment
Banking, Bank of America Securities

We need to optimize effort going into security in terms of compliance and other requirements. We should focus on Innovation and security issues out of the emerging technology.

Mr. Vinayak Godse,

Chief Executive Officer,
Data Security Council of India (DSCI)

Expert opinion to enhance cyber capabilities from eminent speaker



Technology wields immense potential as a tool for enhancing cybersecurity, but it should be seen as an enabler rather than a standalone solution. The responsibility for its effective and efficient utilization rests with individuals.

Mr. Leeladhar Meena,

Director - West Zone, National Critical Information
Infrastructure Protection Centre (NCIIPC)

Panel II - "Aatmanirbharta" in cyber security ecosystem

How do I measure that I am resilient using 7c's – competence – know your assets, confidence – know your risks, connections – know your networks, confident – know your SOC operation, contribution – know your weakness, cope up – know your strengths, control – know your resiliency measures.

Mr. Avneesh Pandey,
Chief Information Security Officer,
Securities and Exchange Board of India (SEBI)

Cybersecurity need not be enemy of convenience; One need to develop solutions which make it easy for every participant to participate in effective and efficient manner. ensuring Digital forensic readiness is the need of the hour in fast changing digital world.

Dr. Gaurav Gupta,
Additional Director - Ministry of Electronics &
Information Technology (MeitY), Government of India

Money is business of trust and trust is what makes people try new things, adopt new things, consistently migrate to newer capabilities.

Mr. Kunal Shah,
Founder, CRED

Robust cybersecurity is fundamental for protecting currency of trust in the capital markets. 'Aatmanirbharta' is needed at national, industry, organisation as well as societal level. At national level incentivising startup ecosystem and at organisation level adopting cybersecurity by design are key.

Mr. Kunal Pande,
Partner - Digital Trust, Digital Risk Security and
Governance, KPMG in India

In a digital age, cyber security cannot be taken as an event. It's a life cycle. Life cycle means this is going to be with you all the time. For an event you prepare differently than for a life cycle.

Mr. Sandeep Bhardwaj,
Chief Operating &
Digital Officer, HDFC Securities

There are no tools to figure out misinformation and disinformation in social media, at the scale that is required before something drastic happens in the market. This is where we need aatmanirbharta and have to start working and looking at this space seriously as going forward this will be a major issue which needs to be addressed.

Dr. Sanjay Bahl,
Director General,
Indian Computer Emergency Response Team (CERT-In)

Expert opinion to enhance cyber capabilities from eminent speaker



Building a strong cybersecurity culture within an organization involves a collective understanding of security goals, effective communication, and continuous innovation to keep defenders engaged and excited about tackling evolving challenges. Cyber defence necessitates 24/7 situational awareness, stress testing, and investing in innovative AI and ML solutions.

Dr. Durga Dube,
Executive Vice President and Group Head - Information Risk
Management and Cyber Security, Reliance Industries Limited

Panel III - Staying ahead of the curve

Going digital is inevitable, security needs to be looked at a 360 degree view point. Secure the nation, secure the enterprise and secure the individual.

Mr. Anil Valluri,
Managing Director & Vice President, Palo Alto Networks

There's a paradigm shift with cyber incidents. Response is equally important as Prevention.

Mr. Nehal Vora,
Managing Director & Chief Executive Officer,
Central Depository Services (India) Limited (CDSL)

Security evolves continuously. What is secure today isn't secure tomorrow. We need to have a mindset.

Mr. V. V. Balaji,
Chief Technology Officer, ICICI Bank

Complying to regulatory standards is not enough. Organisations need to have robust risk frameworks.

Mr. Charles Jacco,
Principal, U.S. Information Protection and
Global Cyber Security Financial Services
industry lead, KPMG in the U.S.

With the plethora of security products, the need of the hour is secure products.

Mr. Ramachandra Kulkarni,
Managing Director - Technology Risk, Goldman Sachs

Panel IV - What keeps the board members awake at night?

“

Prevention is shifting towards detection, and companies are learning that prevention is worth the investment. There's no one-size-fits-all in security.

Mr. Akhilesh Tuteja,
Global Cybersecurity Leader,
KPMG International Partner

“

Protection of data and business continuity is important.

Mr. Deepak Kumar Lalla,
Managing Director & Chief Executive Officer,
SBICAP Securities

“

Act before you need to act, because if you need to act, maybe it's too late to act.

Ms. Irina Ghose,
Managing Director, Microsoft India

“

It is essential to include cyber security in enterprise risk management framework and focus on the proactive strategy of managing a cyber breach.

Ms. Neelam Dhawan,
Independent Director, ICICI Bank Limited,
Hindustan Unilever Ltd, Capita PLC, Fractal
Analytics Pvt Ltd and Yatra Online Inc.

“

All data in a MII is not the same. Personal information is more valuable. Different levels of protection must be offered to different kinds of data and the board should be aware of this.

Prof. Umesh Bellur,
Public Interest Director,
Central Depository Services (India) Limited (CDSL)



Glossary

AI	Artificial Intelligence	FCA	Financial Conduct Authority
AIF	Alternative Investment Fund	FCC	Federal Communications Commission
AIRAWAT	AI Research, Analytics, and Knowledge Dissemination Platform	FinCen	Financial Crimes Enforcement Network
AML	Anti-Money Laundering	GDP	Gross Domestic Product
AR	Augmented Reality	HFT	High Frequency Trading
AUC	Asset Under Custody	IAM	Identity and Access Management
B2C	Business to Consumer	ICO	Initial Coin Offering
BSE	BSE Ltd. (formerly known as Bombay Stock Exchange)	IOSCO	International Organization of Securities Commissions
CAGR	Compound Annual Growth Rate	KYC	Know Your Customer
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart	MeitY	Ministry of Electronics and Information Technology
CBDC	Central Bank Digital Currencies	MII	Market Infrastructure Institutions
C-DAC	Centre for Development of Advanced Computing	NCIIPC	National Critical Information Infrastructure Protection Centre
CDSL	Central Depository Services (India) Limited	NIC	National Informatics Centre
CERT-In	Indian Computer Emergency Response Team	NIST	National Institute of Standards and Technology
CRQ	Cyber Risk Quantification	NLP	Natural Language Processing
CTF	Counter Terrorism Financing	NSE	National Stock Exchange of India Limited
CTT	Commodities Transaction Tax	RBI	Reserve Bank of India
DeFi	Decentralised Finance	SDG	Sustainable Development Goals
DEPA	Data Empowerment and Protection Architecture	SEC	Securities and Exchange Commission
DEX	Decentralised Exchanges	SEBI	Securities and Exchange Board of India
DID	Decentralised Identifiers	SIEM	Security Information and Event Management
DMA	Direct Market Access	SME	Small and Medium Enterprises
DORA	Digital Operation Resilience Act	SOP	Standard Operating Procedure
DPDP	Digital Personal Data Protection	TCS	Tata Consultancy Services
DRDO	Defence Research and Development Organisation	UEBA	User and Entity Behaviour Analytics
DSCI	Data Security Council of India	UPI	Unified Payments Interface
e-AGM	Electronic Annual General Meeting	VASP	Virtual Asset Service Providers
eDIS	Electronic Delivery Instruction Slip	VR	Virtual Reality
EDR	Endpoint Detection and Response	ZT	Zero Trust
eMargin	Electronic Margin		
EU	European Union		
FATF	Financial Action Task Force		

Acknowledgements

KPMG in India

Akhilesh Tuteja
Atul Gupta
Kunal Pande
Mridulla Khatri
Siddharth Durbha
Krishna Deepika Koduri
Gaurav Rout
Kartik Varma
Nisha Fernandes
Venkatesh R

Adfactors PR

Nijay Nair

CDSL

Nehal Vora
Amit Mahajan
Girish Amesara
Nayana Ovalekar
Rajesh Saraf
Ramkumar K
Vinay Madan
Akhil Wadhavkar
Ashwin Lalchandani
Sandhya Dubey

Pivot Management Consulting

Viraj Kulkarni



KPMG in India contacts

Akhilesh Tuteja

Global Cyber Security Leader
KPMG International Partner
E: atuteja@kpmg.com

Atul Gupta

Partner – Digital Trust
Head – Cyber Security Services
E: atulgupta@kpmg.com

Kunal Pande

Partner – Digital Trust
Co-Head Digital Risk and Cyber
E: kpande@kpmg.com

Siddharth Durbha

Director – Digital Trust
Digital Risk and Cyber
E: siddharthdurbha@kpmg.com

CDSL contacts

Nehal Vora

MD & CEO, Central Depository Services (India)
Limited (CDSL)

Vinay Madan

Chief Risk Officer, Central Depository Services
(India) Limited (CDSL)

Sandhya Dubey

Senior Manager, Central Depository Services
(India) Limited (CDSL)

kpmg.com/in

Follow us on:

kpmg.com/in/socialmedia



30 years
and beyond

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The views and opinions expressed herein are those of the quoted third parties and do not necessarily represent the views and opinions of KPMG in India.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011
Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2024 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only. (016_THL_1023_RV)