National Cyber Security Strategy 2020

DSCI submission

Submitted by

Data Security Council of India

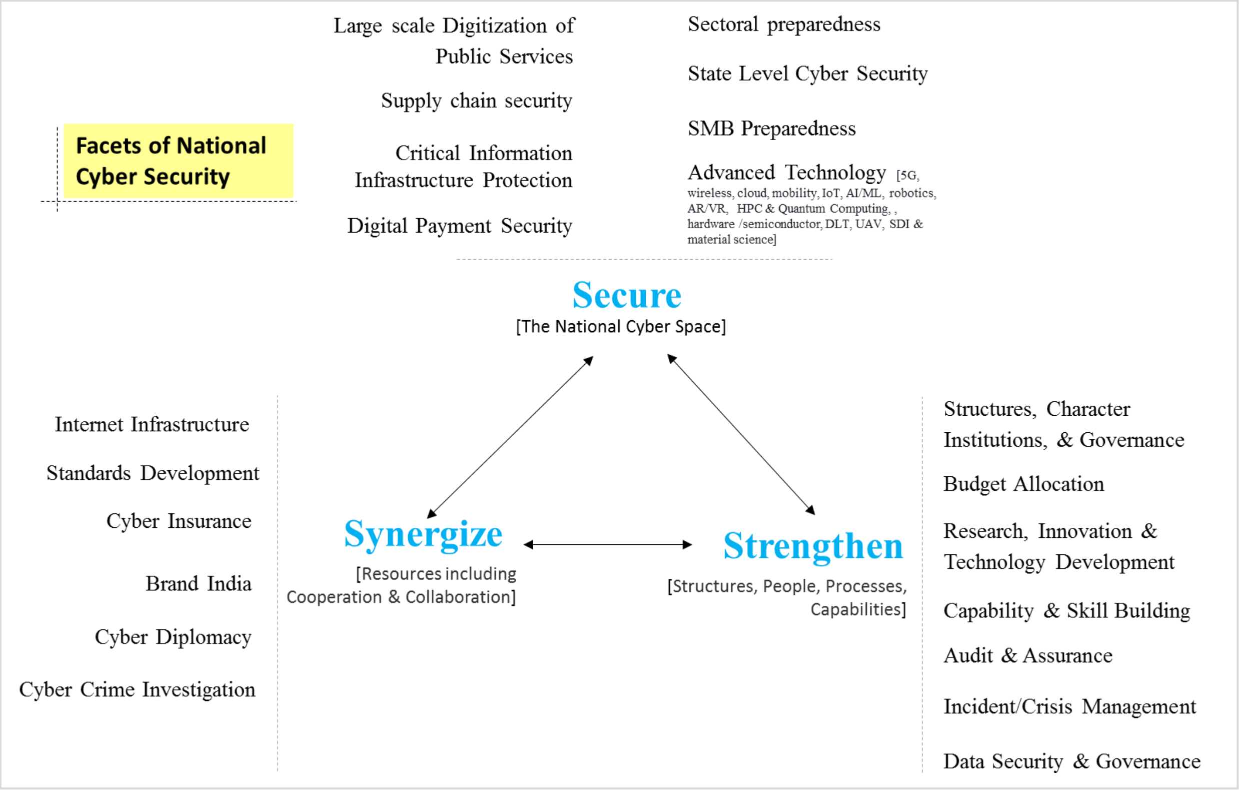
A NASSCOM® Initiative

DSCI
PROMOTING DATA PROTECTION

Executive Summary

India’s digital economy is growing rapidly, and technology adoption is in every facet of human intervention. According to recent report by McKinsey Global Institute, India is the second-fastest digital adopter among 17 most digital economies of the World. India’s core digital sectors accounted for about $170 billion-or 7 percent of GDP in 2017–18, and this is expected to grow to 8%-10% of our GDP by 2025[1].

With rapid digitization comes the challenges of the risks posed by technology. The most recent attacks targeted our critical infrastructure sectors – nuclear plant and space agency and these attacks have exposed India’s preparedness in Cybersecurity.


Facets of National Cyber Security
Large scale Digitization of Public Services
Supply chain security
Critical Information Infrastructure Protection
Digital Payment Security
Sectoral preparedness
State Level Cyber Security
SMB Preparedness
Advanced Technology [5G, wireless, cloud, mobility, IoT, AI/ML, robotics, AR/VR, HPC & Quantum Computing, , hardware /semiconductor, DLT, UAV, SDI & material science]
Secure
[The National Cyber Space]
Internet Infrastructure
Standards Development
Cyber Insurance
Brand India
Cyber Diplomacy
Cyber Crime Investigation
Synergize
[Resources including Cooperation & Collaboration]
Strengthen
[Structures, People, Processes, Capabilities]
Structures, Character Institutions, & Governance
Budget Allocation
Research, Innovation & Technology Development
Capability & Skill Building
Audit & Assurance
Incident/Crisis Management
Data Security & Governance

This report provides detailed coverage of **21 areas** that will ensure a safe, secure, trusted, resilient, and vibrant cyberspace for India’s prosperity. Key highlights of the report are as follows:

- Concerted and well-thought-through effort for ensuring security right from design to entire phases of life cycle of large-scale digitization of public services projects

[1] Digital India: Technology to transform a connected nation, March 2019, McKinsey Global Institute

- Two-pronged approach for supply chain security, for product procured/deployed and product developed in India
- Empowered and resourced security function in critical information infrastructure sector, with specific attention to SCADA/OT security
- Index for sectoral preparedness and monitoring performance
- Given the urgency created by rising cyber threats, Government should carve out separate budget for cybersecurity
- Critical infrastructure protection demands fixing the structural problem by empowering security leadership and strengthening security in both IT and OT environment
- Synergize role and functions of various agencies and restructure them with role and functional responsibility aligned to the national strategy and execution blueprint
- Orchestrate all efforts of Government in bilateral, multilateral, regional cyber cooperation, and participation in Global forums and influence and drive the agenda aligned to India’s interests in Cyber Space and Security
- Bootstrap the Cyber Security Capability building program in states through central funding on lines of eGov
- Capacity building, managing risks arising from technology innovation, R&D and commercialization of insights, digitization of SMB sector, state and sector preparedness, data security governance and securing digital payments have become fundamentals of securing a nation and hence Government must leverage cybersecurity strategy 2020 to strengthen these fundamental components
- Attracting bright young minds to the field of cyber security through awareness, targeted campaigns, and providing enticing career opportunities.
- Incentivization contributions to for developing cybersecurity technology, development of training infrastructure, investing in the testing labs, active participation in technology standards making, demonstration of India’s capabilities in the global market, and for improving preparedness of SMB sector
- Calling for development of an index of preparedness of states in cybercrime investigations that would factor investment made, reach and scale of the effort, undertaken experimentations, timeliness in the resolution of the cases, and improvement in the conviction rate

Background

As India is on the way of becoming USD 1Tn economy, the Government of India is working towards updating its National Cybersecurity strategy in order to improve its position in the cyber space. While India has come a long way since it launched its policy in 2013, there are many new challenges that have emerged due to technology advancement. Our research suggests that between 2016 and 2018, India was second most-affected country due to targeted attacks and the average cost for a data breach in India has gone up to INR 11.9 Cr (USD 1.7 Mn). Additionally, in 2017 CERT-IN handled 53,117 incidents, while in 2018 the number was 2,08,456. The sudden rise in incidents can be linked to increased digitization of our economy. According DSCI's report on Cyber insurance, there are more than 560mn internet subscriber in India, with India becoming 2nd largest App market in the World. Recently, UPI transactions have crossed USD 14mn.

Global Cybersecurity Index for 2018 ranks India at 47th place globally, in its assessment covering 5 pillars (legal, technical measures, Organizational measures, capacity building and global collaboration). There is dire need for Government of India to intervene and help the sectors to improve cybersecurity posture of the country.

Scope

Data Security Council of India (DSCI), as an industry body has consolidated its perspective on the 2020 national cybersecurity strategy, in consultation with the enterprises from various sectors (Power, BFSI, Energy and IT/ITeS). The remaining document provides detailed perspective on various discussion points. This report is based on high-level submission that DSCI made on ww.ncss2020.nic.in website

The remaining report consolidates and present our view points, along with the inputs gathered from the industry.

Details of the Areas

Part 1: Secure

Large scale digitization of public services: Digitization efforts of India get global recognition due to innovative thinking, architectural experimentations, and the potential of scale. If security is not embedded in their design, well-thought-through in the deployment, and ensured in their operations, it would impact assured availability of services, and citizens trust in digital platforms and online services.

- Ensuring thinking of security in the early stages of design all digitization initiatives undertaken in the country
- Calling for empowered security roles and responsibilities in such projects and initiatives
- Promoting the culture of security authorization/clearances while deploying the solutions
- Developing institutional capability for assessment, evaluation, certification, and rating of the core devices used by the projects
- Advocating extensive assessment of devices, solutions, and architectures suggested, adopted, and implemented by such projects
- Mandating an advanced level of cybersecurity operations matching the scale and complexity of security challenges

Ensuring timely reporting of vulnerabilities and incidents in the devices and solutions adopted by the projects

Supply chain security: Rapid digitization of industry, including critical sectors, social spaces, and personal transactions on the one hand and country's aggressive efforts for Make-in-India on the other, demand a two-pronged approach for supply chain security. One, for procurement and deployment of products manufactured in the increasingly complex global supply chain. Second, for products developed or value-added in India.

- Continuous monitoring and mapping of the supply chain of the ICT and electronics products, ranking them for their criticality and evaluating country's contribution in them
- A close watch on technical capabilities developed in India and the role they are playing in the global supply chain. A systematic plan for enhancing India's role in the key supply chains by investing in critical technical capabilities
- Scale up India’s product testing and certification efforts in a time-bound mission mode way by dedicating desired resources and creating conducive investment and private sector participation in the area

- Adopt a risk-based approach by promoting the development of lightweight, agile, and dynamism mechanism for product testing that can co-exist with well-established schemes like common-criteria
- Promote and incentivize the public and private investment in testing labs and infrastructure and skill development that can serve both domestic and export market requirements
- Leverage the country's leadership in semiconductor design, ERnD (Engineering Research and Design) and emerging destination for deep-tech innovation for driving supply-chain security agenda globally at strategic, tactical and technical levels

Critical Information Infrastructure Protection: The increased focus of cyberattacks, systematically planned and executed by non-state as well as state actors, to the target CII sectors causing more substantial or kinetic impact, demand concerted and smart strategies.

- The focus of the efforts for CII protection should be to ensure the delivery of essential services even in the time of the attack, assuring the economic growth, and promising safety of the citizens
- Empowering security leadership, ensuring adequate resources with it, and making it independent from routine ICT and business operations. Moreover, by devising specific responsibility for the SCADA/OT security and integrating with enterprise security.
- Developing regulatory capabilities, wherever possible, that would further development of more contextual and objective norms and guidance
- Augmenting the due diligence to draw technology profile of the CII sectors by closely monitoring the digitization and technology adoption, evaluating devices and solutions planned to deploy for the security, and maintaining a repository of vulnerabilities and exploits likely to affect them
- Harmonizing national security efforts to make the compliance more productive and effective for the organizations falling in the CII
- Adopting differentiated approaches that cater to specific requirements of the plant, transport, distribution, and retail deployment of SCADA/OT solutions to ensure risk-based treatment, specific solutions, and ensure proportionate actions at the desired level
- Mandating a security-by-design culture in the technical transformation, however, facilitating that with investing in the aggregate level efforts of security evaluation and testing devices, issuing guidance and directives, and by notifying reference architectures
- Promotion of innovation and co-creation for the development of SCADA/OT security solutions by incentivizing user enterprises, providing funding support to the start-ups and incubators working in the area, and creating a conducive environment for commercialization of the research work

- Preparing an aggregate level security baseline of the sector and monitor the progress in the collective improvement of the baseline by closely tracking of security controls, capabilities, solutions deployed, and security management practices
- Promoting the efforts in developing advanced skills and expertise in SCADA/OT security, ensuring skilled resource deployment in the security function, and mandating that audit and assessment work to be carried by skilled resources only
- Devising areas, depth, norms, frequency, and methods for the audit and assessment to ascertain the level of preparedness against the prevailing and evolving threats
- Ensuring an advanced level of Product Security and Incident Response [PSRT] set up by the OEMs, and the solution providers of the sector to provide timely and speedier resolutions of vulnerabilities and incidents
- Promoting the development of cyber insurance products that cater to the security risks of SCADA/OT environment

Digital Payment: digitization of payment and financial transaction processing would be the prime driver of the digital economy. Careful and concerted efforts would be needed for securing high paced but innovative and experimental transformation of transaction processing.

- Promoting exercise for mapping and modeling of:
    - the supply chain of transaction processing,
    - architectural ideas under experimentations
    - devices and platform deployed
    - type of entities participating in the processing of transactions
    - enabling technologies and stacks
    - payment flows and paths
    - types of interfaces
    - exchange of data and information
- Advocating extensive and routine threat modeling exercises that factor the possible and disclosed vulnerabilities, weaknesses, exposures
- Ensuring better coordination and harmonization in regulatory initiatives to enhance the level of preparedness in predictable ways
- Promoting the adoption of the framework, architectures, and capabilities emerged in the technology ecosystem for improving the security posture
- Promoting threat research and sharing of threat intelligence in a very productive and timely manner. Also, by enabling the sharing of data to make security decisions risk-based
- Mandating advanced cybersecurity operations by the primary owners in the chain of transaction processing

- Advocating a sound, agile, and efficient third-party security assurance mechanism
- Promote the adoption of standards while selecting, evaluating, deploying, configuring, and operating devices, solutions, and platforms. Leveraging India's leadership position for shaping global standards impacting payment industry
- Developing competent incident and emergency response capabilities for the financial sector
- Promote responsible and timely disclosure of vulnerability and incident reporting for the devices, solutions, and platforms deployed for transaction processing
- Overhauling assurance system, making it more agile, threat aligned, and intelligence-driven

Promoting efforts and collaborations for making people aware of payment security in a targeted, entrenched, and scalable manner

Sectoral preparedness: Digitization is increasingly leading to the verticalization of IT, where every sector is evolving to verticalize technology stack for their requirements. Their digital footprint is increasing, spreading the threat exposures. The sectors may not be ready or fall short of handling security affairs impacting their prospects.

- Profiling sectors, their digitization plan, architectural developments, technology adoption, possible exposures, and likely ramifications, which can be used for ascertaining the priorities for the interventions
- Ensuring evaluation of sectors and specific companies in them, for their role in the critical supply chain to identify possible ramifications to national cybersecurity from a security breach
- Providing special attention to the sectors that rely on the operating environment for enhancing SCADA/OT/IoT security, and integrating that with organizational security function
- Keeping watch on sectoral cybersecurity preparedness through developing and maintaining index and setting up a mechanism for continually monitoring exposures of members of the sectors
- Developing regulatory capabilities wherever possible to create and drive the agenda of cybersecurity in the sectors and making them more contextual and objective to the sectoral challenges
- Promoting the development of frameworks, policies, guidance, and technical standards in the sensitive sectors
- Ensuring the development of security function and leadership in the companies, empowering them, and by making the security function independent from routine IT and business operations
- Developing an audit, assurance, and assessment ecosystem in the sectors that measure the level of preparedness and help to build risk management culture

- Promoting aggregate level efforts that evaluate, test, and rate security capabilities of devices, solutions, and architectures deployed by industry sectors
- Incentivizing contributions of the industry for developing cybersecurity technology, their initiatives to work with start-ups, academia, and incubators, and the investment they are making critical areas of cybersecurity
- Promoting information sharing, vulnerability reporting, and incident reporting in the industry sectors, and calling for cybersecurity drills in high priority sectors

State Level Cyber Security: States would be the key to realizing India's goal of USD 5 trillion economy. Many states in the country are taking concerted efforts for digitizing levers of the economy and delivering public services on digital channels. The strategy exercise for national cybersecurity wouldn't be complete without factoring efforts required at the states.

- Ensuring that states take cybersecurity on their agenda in their efforts of industrialization and digitization
- Promoting, acknowledging, and driving the states for proportionate attention and investment in cybersecurity by calling for measures like:
    - Promoting the development of state-level cybersecurity policies
    - Mandating roles and responsibilities of cybersecurity functions
    - Allocation of dedicated funds
    - Incentivizing enhancement in the security preparedness
    - Creation of the infrastructure and development of capabilities
    - Subjecting the digitization plans for critical scrutiny, validation, and authorization
    - Issuing guidelines for enhancing security architecture, operations, and governance
    - Advocating the sharing of threat information/intelligence to address target attacks from state/non-state actors
    - Promoting responsible use of cyberspace and data
- Developing capabilities of the state machinery to address cybersecurity challenges
- Developing a mechanism for overseeing and monitoring cybersecurity preparedness and performance of the states
- Promoting the programs of developing skills and talent at the state level
- Partnering for developing India as a global hub for cybersecurity products and services by orchestrating the state-level efforts
- Bootstrap the Cyber Security Capability building program in states through central funding on lines of eGov

Security of Small and Medium Businesses (SMB): The sector is seeing an increasing move to online and digital. There is a thrust on ERP implementation, urge to leverage e-commerce wave, and transition to GST. Moreover, it is going through digitization of payments, cloudification, and industrialization 4.0 at a rapid pace. Without focusing on security, it would hamper digitization, weaken supply-chain, disrupt the objective of promotion of SMB and associated Make-in-India possibilities.

- Ensuring evaluation of SMB sectors and their role in the supply chain in the technologies is important for economic and strategic interests to ascertain priority sectors and type of work
- Keeping watch on the digitization of SMB sectors, levers and vehicles working for it, adoption of technology and devices by them, and their exposures to threats
- Promoting cybersecurity and privacy awareness in targeted campaign with SMB using relevant levers and vehicles
- Policy intervention to bring attention to cybersecurity in the sector, such as below:
    - Procurement incentives for a higher level of cybersecurity preparedness
    - Grant/subsidy for investment in the cybersecurity
    - Development of cyber insurance products
    - Driving line ministries, MSME development initiatives (state and central level), and industry bodies to take cybersecurity on the agenda
    - Reporting of cybersecurity preparedness and breaches
- Promoting technical standards, frameworks, and reference architectures for the adoption of IoT and industrialization 4.0 for enhanced cybersecurity, privacy, and safety
- Developing assurance framework that relies on self-certification and third-party certification depending on the sensitivity level
- Promotion of development of cybersecurity technologies targeted at the SMB sector

Advanced Technology [5G, wireless, cloud, mobility, IoT, AI/ML, robotics, AR/VR, hardware/semiconductor, HPC and Quantum Computing, DLT, UAV, SDI & material science]: Technology transformations and breakthroughs poised to bring an entirely new paradigm for cybersecurity. Many listed here would bring immediate challenges, while some would start shaping cybersecurity discussion in the long term. The national cybersecurity strategy 2020, envisioned for the five years, should lay down options to deal with the technology transformations.

- [Future Casting 1] Investing in the work of forecasting technology, their likely role in shaping society, industry, businesses, and economy. Evaluating ramification to cybersecurity, considering the impact on:
    - Personal transaction processing

    - Social exchanges
    - Business and financial transaction processing
    - National economic transformation
    - Cross border exchanges: exchanges, data flows, trade, etc.
- [Future Casting 2] Promoting the efforts and research for:
    - Developing a comprehensive & structural understanding of the current state. Relating, mapping & categorizing the elements of future and assess threats
    - Assessing contemporary evolutions & ongoing fundamental researches that would determine future technology roadmap by
    - Evaluating paradigms that bring structural change, for example, speech-to-text AI would be making most aspects of infrastructures voice-enabled
  - Understanding ingredients and conditions lead to transformational changes and thresholds that bring these changes
  - Studying the cybersecurity ramifications of these evolutions
- [Future Casting 3] Identifying the areas of strategic interests or the ones that would be bringing transformational changes
  - Mapping of current technologies and capabilities that would be vital for it. Maintaining the repository of the work of start-ups, private sector, public sector, academia, and research institutes in them
  - Evaluating the role of technology capabilities' role in the supply chains of the key product lines. Assess India's contribution to them
  - Identifying the areas essential from the perspective supply-chain security
- Ensuring institutional and infrastructural development for security evaluations of the technologies, devices, solutions, and platforms
- Ensuring active participation in the standard making initiatives shaping new technology developments
- Promoting investment in the start-ups and institutional research in the critical technology areas, with a specific focus on cybersecurity
- Advocating the development of sandboxes for identifying and evaluating cybersecurity issues and the type of interventions required
- Providing the risk capital for the development of core cybersecurity capabilities focused on solving the problems in the technology transformations
- Making the conducive environment for attracting investment in the areas leading to new paradigms for cybersecurity
- Promoting the development of niche skills and expertise that can address complex cybersecurity issues in new technology areas

- Incentivizing the efforts and contributions in developing security technologies against the new use cases emerged out of new technologies

Part 2: Strengthen

Structure, Institutions, and Governance: The challenges of technology transformation, widespread digitization, and advancing threat landscape demand a fresh look at the Governance and Institutional Structures in India factoring the learnings from India and evolving models from across the world. Current Challenges and anticipated future threats call for evolving the institutions for national cybersecurity and governance that is commensurate with the complexities and cyber risks for a country of India's scale.

To orchestrate the country's cyber strategy and execution roadmap, elevate the function from Coordination to crafting the country's cyber strategy and planning and directing its execution through identified institutions, both central and state. They key priorities for this central agency could be:

- Minimize the headwinds from cyber risks for the USD 1Trillion Digital economy aspirations.
- National level initiatives and programs for enhancing preparedness, strengthening defense, and ensuring a swift response
- Synergize role and functions of various agencies and restructure them with role and functional responsibility aligned to the national strategy and execution blueprint.
- Guiding and Coordinating efforts of the agencies including critical sectors agencies
- Assess readiness at National, State and Sectoral Level and structure all efforts to drive outcomes to further country's cyber preparedness
- Securing strategic and critical assets in line with geo political and economic interests and growth agenda of country and make India a role model in a forward leaning cyber defense and response.
- Evolve the Cyber Security Innovation Agenda and R&D Strategy for the country, fostering Government-Academia-Industry partnership to achieve outcomes aligned to the strategy.
- Enable Policy and Legal Research to address future Technology Developments and impact on Society and Economy and potential cyber risks in truly harnessing next gen technologies for Public good.

- Take accountability for National Cyber Emergencies and its response and orchestrating all associated agencies during such responses
- Orchestrate all efforts of Government in bilateral, multilateral, regional cyber cooperation, and participation in Global forums and influence and drive the agenda aligned to India's interests in Cyber Space and Security.

Budgetary Provisions: As cyber security is critically important to national security and the digital economy, it is recommended to have a separately carved budget head.

- The union budget should have a sperate head for cybersecurity by consolidating thoroughly prepared budget by different ministries and institutions. It is recommended that minimum 0.25% of total Government of India annual budget should be invested in cyber security, which subsequently can be raised to 1% as India approaches to USD 5 Trillion economy, 20% of which would be Digital Economy
- Apart from the budgetary requirements of operational expenses, new investment for security baseline improvement, investment in R&D and technology development, incentivization, enhancement in the infrastructure, and all other developmental initiatives should be factored in the exercise.
- Given current state of preparedness and rapidly evolving threats, we recommend a 15-20% of overall IT/Technology spend across all ministries and agencies to be earmarked for cyber security
- The budgetary allocation should be linked to outcomes, and a mechanism should be devised to measure them

Research, Innovation, and Technology Development: Concerted efforts for research, innovation, development of technology, and more importantly, their commercialization would be critical for both the strategic and commercial interests of the country.

- Ensuring that substantial investments in ICT, modernization, and digitization should trigger cyber security technology development work through appropriate norms and incentives
- Promoting the efforts of identifying the new use cases and supporting technology development against them
- Emphasizing productization and commercialization of the investment in cyber security R&D by notifying associated performance criteria, calling for industry linkages, and supporting the focused efforts and programs for it
- Devising research agenda, short-term and long-term, for cyber security through a focused outcome-based programs. Supporting forecasting research to identify research priorities.

- Ensuring proportionate but outcome-driven investment in the development of technology for long-term requirements
- Allocating a budget for research in the priority areas for timely and sufficient support
- Incentivizing industry for contributions to cyber security technology development, working with academia and start-ups, and providing opportunities to industry for productization and commercialization of public funded R&D
- Developing a conducive environment for cyber security product entrepreneurship by supporting incubators, providing risk capital required for deep tech cyber security innovation, and by creating an investment ecosystem that supports growth stages
- A Fund of Funds for Cyber Security to be established
- Ensuring a sound and vibrant market for innovative cyber security technology products by reducing the risks and liabilities working with start-ups
- Reforming public procurement process for proportionate investment in cyber security and enabling the public institutions to work with the start-ups
- Attracting investment in cyber security research and product development, identifying and recognizing the areas and zones for such investment, and by positioning the country in the global market for the purpose
- Investing in the efforts of developing niche skills required for core research and product development. Promote security technology thinking through specialized programs and initiatives
- Arranging challenges at regional and national levels for attracting the attention of technologists to cyber security

Attracting the attention of security researchers, start-ups, and companies to the nationally critical areas

Capability and Skill Building: India is a leading provider of cyber security skills. A well-rounded skills strategy would not only help to maintain India's global leadership but also exploit its potential to the fullest. Moreover, it will help in serving the rising needs of India's USD 1 trillion digital economy.

- Setting up an overarching national framework that leverages the market offered programs, global professional certifications, institutional interventions like NOS (under NSDC) and ISEA (Information Security Education and Awareness), and academic contributions
- The intense process of developing cybersecurity skills demands competent infrastructure, which can be achieved by providing proper incentives to the players, working in both formal and informal segments
- Promoting and recognizing the center of excellence for cyber security capability building

- Emphasizing incorporation of cyber security in the larger public reskilling efforts for widening pool of the workforce
- Concerted efforts of building niche skills by promoting hosting of hackathons and challenges, conducting hands-on workshops, focusing on technology development aspects, and setting up simulations and cyber ranges
- Special programs for capacity building of government and public sector enterprises concentrating on technology, operations, governance, and leadership aspects
- Creation of 'cyber security services' leveraging Indian Engineering Services to create a pool of security leaders for government and public enterprises
- Attracting bright young minds to the field of cyber security through awareness, targeted campaigns, and providing enticing career opportunities. Run national programs for transitioning non-computer science graduates/ post-graduates to cyber security, especially from the areas like electronics and mathematics
- Close monitoring of demand-supply gaps through continual research, study, and tracking

Supporting the efforts for closing diversity gaps in cyber security field

Audit and assurance: The security threat landscape is continuously evolving for more targeted, advanced, and persistent attacks. On the other hand, digitization momentum is increasingly increasing the digital footprint and hence exposures. The audit and assurance function need to be overhauled to address scale, pace, and complexity.

- Advocating a more nuanced approach for developing audit and assurance ecosystem for the country Increasing robustness of auditor/ assessor empanelment process
    - Making the assessment standards or references more specific, granular, and relevant to factor all key possible scenarios of compromises
    - Ensuring deployment of skilled resources on the audit, assessment, and assurance projects
    - Making the assessment, audit and assurance process intelligent driven to measure preparedness against the newly identified vulnerabilities and threats
    - Calling for continual monitoring and evaluation instead of one-off exercises
    - Advocating the use of technology for monitoring readiness, baseline improvement, and risk quantification
    - Calling for regular training and skilling of audit professionals
    - Keeping a close watch on the new devices, solutions, and architectures deployed. Notifying standards, practices, and guidelines for auditing them
- Advocating the development of intelligence on assessment and audits for benchmarking and security baseline monitoring

- Calling for well-thought governance process for timely resolution of identified issues and non-conformances
- Develop regulatory capabilities, wherever possible, to broaden the reach of audit and assurance to sectors and targets emerging as a target for cyberattacks

Incident/Crisis Management: The best-invested security program would not be spared from the possibility of an incident that could lead to significant crises. Science, process innovation, and technology contributing a lot in identifying and managing the incidents and handles resultant crises more predictably and productively.

- Promoting the efforts for continuous identification and inventorization of the scenarios. Prioritizing them to ascertain which one leads to the significant ramification
- Advocating scenarios planning of incident and crisis management plan devising roles and responsibilities for its execution
- Conducting scenario planning and simulation exercises:
    - Scaling up the effort of cybersecurity drill to extend its reach and include real-life scenarios
    - Advocating the enterprise-level exercises for clarity on what incident cause the more significant ramification and requiring national attention
    - Calling for simulation exercises for critical sectors: at the levels of enterprise, industry sector, and national, within and cross-sections
    - Inter-country simulation exercises for cross-border scenarios
- Ensuring the knowledge gained from the incidents and crises maintained for its productively managing future incidents
- Promoting the use of state-of-art threat information sharing mechanisms, threat intel gathering, threat hunting operations, and security research to identify the possible weakness and exploitations
- Promoting the use of contemporary technology for identifying incident, timely notifications, ensuring desired actions, dissemination of actionable intelligence, and managing the process in an effective way
- Promoting participation in the global work and communities that engaged in incident categorization, finding IOC and IOAs of new attacks, and suggesting procedural steps

Data Security and Governance: Foundations of the digitization are based on data-centric products and services. There is a significant rise in digitizing records, collecting data, enriching decisions with data, finding new ways and ideas of making use of data, and sharing it to serve other purposes. National cybersecurity strategy, hence, should emphasize enhancing the data governance in the country to systematize the security of data.

- Promoting the adoption of data governance practices that rely on ideas such as discovery, visibility, classification, and risk-based
- Ensuring the adoption of data governance practices by the government bodies and public sectors
- Emphasizing on data-centric approach to security in planning, design, deployment, and operations phases

Part 3: Synergize

Internet Infrastructure: India's IT industry is worth USD 181 billion in FY19; more than 76.3% of revenue comes from the export. It is poised to reach USD 350 billion by 2025. India's approach to the Internet Infrastructure should be shaped on this economic reality. On the backdrop of geopolitics dynamics associated with technology, cross-border data flow, supply-chain of the products, governing affairs of the infrastructure, espionage, and militarization of cyberspace, India should chart its strategy carefully to advance its interest.

- Active participation in the initiatives shaping cyber norms, governing the cyberspace, and regulating data flows
- Proportionate investment in study and research for advancing India's cause in various diplomatic efforts shaping global cyberspace
- Facilitating the participation of stakeholders and taking efforts for factoring all critical dimensions and views in developing the national positions
- With multidimensional initiatives like building internal capacity, the enhanced trust of multiple stakeholders within and across the borders, and active persuasion, bring the critical infrastructure, root server, with power to control and govern to the country

Standards Development: Until now, with a few exceptions, the country's role had been in adopting standards or contributing to administrative or managerial standards. The management of affairs of security is increasingly becoming a matter of technology, as the volume of information required to process for taking a decision has risen beyond human intervention. The pace of technology innovation, and their adoption, for example, in the case of IoT, is brining unprecedented scale and complexity in managing security. Investment of time and efforts in the development of technical standards would be becoming vital at an unprecedented scale

- Creating awareness about contribution to the development of technology standards and attract the best talent
- Promoting capability and skill building efforts in core technology and security standards
- Incentivizing the individuals, institutions, and companies for their contribution to standards

- Recognizing and acknowledging the efforts in technical standard making
- Promoting campaigns of attracting the attention of the product and deep tech companies to the standard making initiatives
- Keeping a close watch on the global efforts of developing standards and bodies and institutions involved to identify the essential standards that are vital strategic and commercial interests
- Developing capability in the existing bodies or create a new institutional mechanism for raising India's participation in the standard making initiative

Cyber insurance: Cyber insurance is evolving as one of the key instruments of cyber risk management. The global cyber insurance market would be reaching USD 22.4 billion by 2024 from USD 4.2 billion in 2017. The cyber insurance market in India is its early stage, although it's catching up the pace. There is a need for a concerted national effort to develop a market for cyber insurance in the country.

- Spreading awareness of cyber insurance among industry, public sector, and SMB sector
- Prompting development of actuarial science for addressing complex cybersecurity risks that factor nuances of industry sectors, specific business and technology scenarios, threat exposures, and types of coverage
- Driving consultation with stakeholders such as infrastructure owners and operators, insurers, chief information security officers (CISOs), and risk managers
- Promoting measures for developing repositories of cyber incidents and sharing information to support actuarial decision making
- Promoting the development of skills and expertise in risk management, cyber actuarial science, assessments, and forensic investigations
- Advocating development of cyber insurance products for critical information infrastructure especially for SCADA/OT environments
- Promoting the science of risk quantification and measurement. Incentivizing enhancement in the risk management rating/measures
- Advocating the development of cyber insurance products for the SMB sector
- Ensuring the development and growth of the cyber insurance market and closely monitoring the adoption

Brand India: A long experience of global delivery of IT and business services, aggressive efforts for the digital economy hence growing domestic market, rising export of cybersecurity services, emerging security start-ups, and preferred destination for moving global security engineering operation are making India a global force in the domain of cybersecurity. India has been playing a constructive role in shaping the discussions of governance of cyberspace to make it open, equitable, and inclusive. For strategic and commercial interests, there is a need for specific efforts for positioning and branding India's value proposition at both domestic and global platforms.

- Devising the objectives of branding and positioning exercise
    - Attracting and developing talent and skills in the niche and cognitively intense cybersecurity field
    - Promoting research, innovation, product entrepreneurship, and investment in cybersecurity
    - Promoting India as a destination of cybersecurity product and research and for attracting investment
    - Demonstrating India's capabilities and experiments in the space of cybersecurity
    - Promoting India as a responsible nation, leader in proactive efforts of shaping global matters, and contributor in developing the global capability
- Keeping a close watch on the strengths, capabilities, value deliveries, success stories, innovation and experimentations in the domain of cybersecurity
- Undertaking a concerted branding exercise in the space of cybersecurity
- Creating an agenda of cybersecurity in the existing brand India initiatives, programs and campaigns
- Devising marketing and communication campaigns for continual outreach
- Promoting campaigns nationally and internationally leveraging the existing vehicles and channels and identifying new ways
- Incentivizing the efforts of demonstration of India's capabilities in the global market for export and attracting investment
- Creating an agenda of cybersecurity in India's missions in countries and multilateral institutes
- Supporting the efforts of attracting the global market forces, leaders, and industry to India

Cyber diplomacy: Sustained and scaled efforts for fostering India's leadership in the global governance of cyberspace

- Approaching from the position of strength of world's second-largest Internet user base, the global technology hub, third-largest start-up ecosystem, a destination of global R&D, rapid transitioning to the product economy, leading provider of skills, successful architectural experiments towards inclusive and vibrant digitization, and an active market for digital product & services

- Promoting India as a destination of cyber security products and investment, attracting inward investment in cybersecurity, and cautiously developing market for India delivered products and services. Leveraging inclusion of India in dual-use technology export control regime, like Wassenaar agreement, for attracting core cyber security research and product development
- Driving cyber security preparedness of key regional blocks important to the strategic goals of the country, such as BIMSTEC and SCO, through concerted programs, exchanges, and by providing support with the help of industry
- Fostering partnerships at multiple levels, academia, industry, and government, to draw strategic and commercial interests
- Promoting and incentivizing active participation in global standard making initiatives, especially in the technical standards
- Taking cautious efforts to promote brand India as a responsible player in cyber security, and the global destination of innovation, research, products, services, and skills
- Create role of Cyber envoys for the key countries/regions

Cybercrime investigation: Investigation of cybercrimes and traditional crimes using advanced technological tools & solutions including digital forensics technologies, methods, and legal procedures would be an essential area of national cybersecurity strategy due to the ubiquitous role of technology in commission and detection of crimes.

- Legislative reform: Investing resources and efforts to ensure concerted actions on the legislative agenda
    - Identifying and resolving areas for immediate attention such as spamming and fake news.
    - Evaluating technology transformation, business adoption, platformization of both technology and business, and evolutions of new roles from the perspective of law enforcement
    - Creating a roadmap for legislative agenda for the next five years factoring possible technology transformation
- Advocating compilation and effective and timely dissemination of information, data, and reports on cybercrime cases, modus operandi, and patterns
- Setting up exclusive courts across the country to deal with cybercrime cases for speedy trails.
- Removing backlog of investigation and resolution of cybercrimes by more centers for providing opinion related to digital evidence under section 79A of Information Technology Act, 2000.

- Promoting efforts for developing the capability of law enforcement officials, prosecutors, and judiciary in a targeted and scalable manner
- Incentivizing the efforts of building advanced forensics training and investigation capabilities required in the age of AI/ML, Blockchain, IoT, Cloud, Automation, etc.
- Promoting the efforts of developing new technologies for forensics investigation
- Calling for development of an index of preparedness of states in cybercrime investigations that would factor investment made, reach and scale of the effort, undertaken experimentations, timeliness in the resolution of the cases, and improvement in the conviction rate
- Encourage Govt. organizations to setup their own cybercrime/cyber security breach incident response team for effective first incident response.
- Ensuring the monitoring of specific categories of cybercrime that undermine public order, hamper economic interest, and disrupt the health of cyberspace. Advocating a particular action plan for improving status in each of them
- Calling for effective mechanisms for coordination and cooperation for solving inter-state cybercrime cases
- Promoting partnership with law enforcement and other agencies abroad for seeking information from service providers overseas
- Advocating proactive participation of the country in the international efforts and institutions working to solve the problems of cross-border cybercrime investigations
- Propose strongly on international platforms for developing an electronic system for submitting, managing and responding to seeking assistance under MLAT (Mutual Legal Assistance Treaty) signed by Govt. of India.
- Creation of separate/special cadre of Cybercrime investigators within the Law Enforcement
- Promoting the programs and initiatives for enhancing exchanges and cooperation at bilateral, regional, and multilateral levels

DATA SECURITY COUNCIL OF INDIA