Our Take

August 2022

pwc

Navigating the Cyber pass

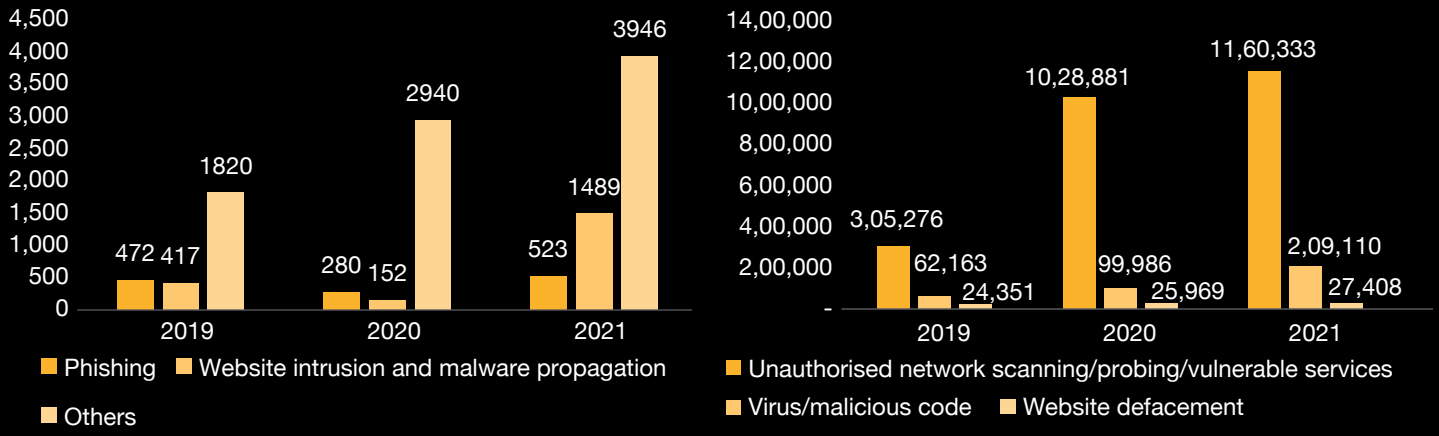
With cyber war becoming the asymmetric weapon of choice for all threat actors, India needs to significantly up its cyber investments to create bespoke solutions to safeguard its interests.

The accelerated pace of cyberattacks the world over is a cause for grave concern. Vigilance is the need of the hour as the cyberthreat landscape witnesses an exponential increase in threat actors with different motivations and varied skill levels.

According to our June 2022 Global Risk Survey - India highlights, nearly 80% of India leaders agree that keeping up with digital and other transformations is a major risk management challenge.[1] Data from the Indian Computer Emergency Response Team (CERT-IN) corroborates this as it underlines that in CY 2021, CERT-IN handled about 14 lakh attacks on various Indian entities.[2]

The rise in the cases of unauthorised network scanning/probing over the past three years has been exponential, with a 280% increase in the number of reported incidents in CY21 over the CY19 numbers. CY 2021 also shows a near doubling of website intrusion and malware propagation/phishing incidents compared to CY 2019.

Cyber issues handled by CERT-IN



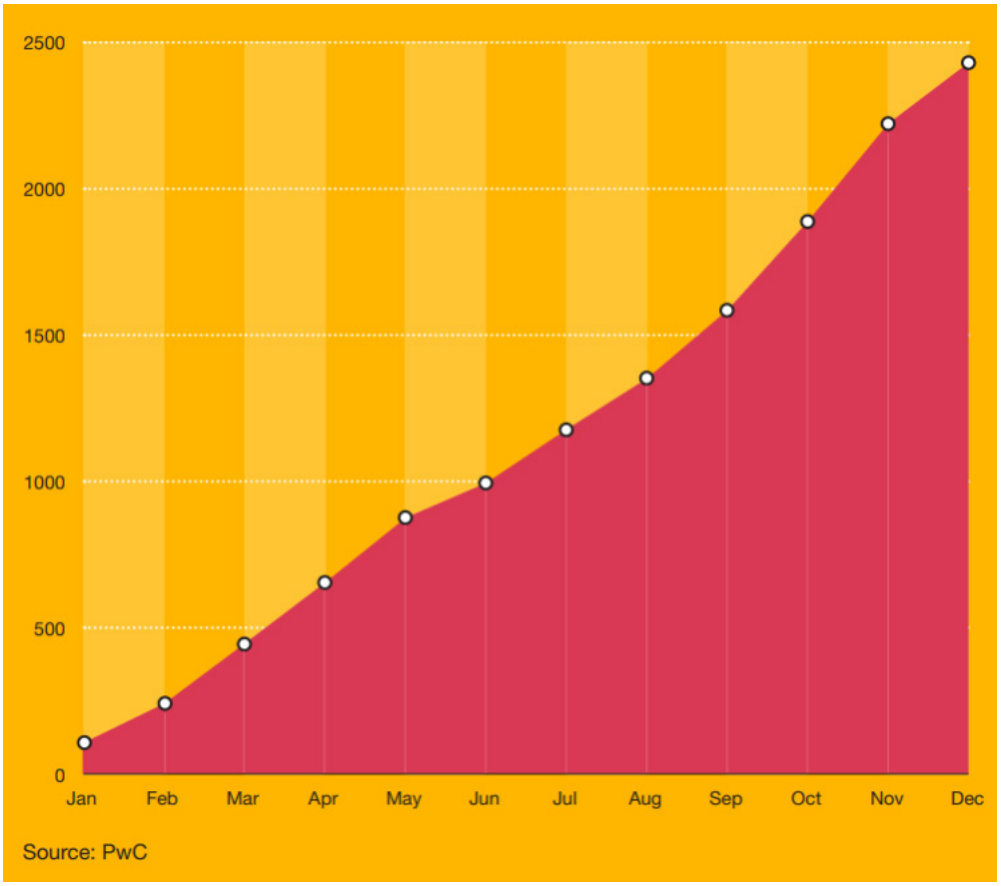
Source: CERT-IN Annual Report 2021

1 PwC | 2022 Global Risk Survey - India highlights

2 CERT-In | Annual Report 2021

Ransomware too continues to be a potent threat. PwC's report Cyber Threats 2021: A Year in Retrospect[3] indicates that ransomware will continue to be the most potent threat for organisations across the world, with attacks on supply chains becoming the new normal. The emergence of commercial digital quartermasters – who could be both state sponsored or those driven by pure monetary considerations – compounds the menace, by equipping cyberattackers with high-end tools and capabilities. All these developments have resulted in an increased focus on zero-day vulnerabilities. As the figure below indicates, 2,435 ransomware victims were exposed on leaked sites in CY 2021, about double the number for the previous year.

Running total of ransomware leaks in 2021



Concerns around cybersecurity prompted a joint press conference by the heads of the Federal Bureau of Investigation (FBI), USA, and Military Intelligence, Section 5 (MI5),[4] on 6 July 2022. The joint press conference served to underscore the potency of cyberthreats to which nations are exposed. It brought to the fore the issue of a state actor undertaking a coordinated campaign on a grand scale to attain significant advantage over its enemies. The steps that a state actor can take, include:

- covert theft of technology
- technology transfer
- exploiting research and
- acquiring information through the 'thousand grains of sand' strategy.

Cyberattacks, it emphasised, are also a key element of the strategy to inflict damage on other countries.

3 *PwC | Cyber Threats 2021: A Year in Retrospect*

4 *BBC News - MI5 and FBI heads warn of 'immense' cyber threat*

With geopolitical conflicts and subtle changes in the Power Blocs, India too needs to contend with increasing cyberthreats from various quarters, as cyberwar is now the asymmetric weapon of choice for all threat actors. It is a low-cost-high-yield vector capable of inflicting targeted damage across sectors while enabling easy deniability.

Given this context, it is important to revisit the broad spectrum of cyberthreats, the reasons behind these threats, and the strategies that India needs to adopt in the near and long term to safeguard its interests and those of its citizens. The country's sheer diversity and complexity demand that a bespoke approach be adopted instead of a one-size-fits-all approach while devising solutions for the Indian ecosystem.

The changing dynamics of the cyberthreat landscape in India

In the Indian context, the broad spectrum of cyberthreats may be classified into those impacting critical infrastructure, businesses and citizens.

1. **Threats impacting critical infrastructure**

   Past cyberattacks on critical Indian infrastructure have included attempts on India's ports, nuclear facilities and power utilities. These attacks have a severe impact given that the critical infrastructure serves large populations. In a recent attack in April 2022, cybersecurity researchers observed hackers penetrating the networks of at least seven Indian State Load Dispatch Centres (SLDCs)[5] which are critical for maintaining grid frequency and stability, and access to supervisory control and data acquisition (SCADA) systems across the respective states for grid control and electricity dispatch.

   While these attacks were countered, they had the potential to severely disrupt the power system. In the same month, hackers also attacked the headquarters of a large state-owned Indian hydrocarbon company and compromised some of its servers. Similarly, in July 2022, a prominent Indian regulator reported that e-mail accounts of its officials were hacked, and mails were sent from them; however, no loss of data was reported. As regulators possess extremely sensitive data, a data breach can prove very costly.

2. **Threats impacting businesses and the corporate sector**

   The Indian corporate sector has faced a slew of cyberattacks. The bulk of the attacks on corporate houses have been related primarily to ransomware and data theft. Some of the recent attacks include those on Indian companies in varied sectors, including pharmaceuticals, heavy engineering, online groceries, quick service restaurants, diagnostic labs, start-ups and finance portals. The ambit of the cyberattacks includes various types of incidents such as denial of service attacks, lost and stolen assets, basic web application attacks, privilege misuse, system intrusion, social engineering.

   Data from the International Data Corporation's (IDC's) India Ransomware Survey 2021 indicates that ransomware attacks can have a debilitating impact on companies and a third of the victims take a week or more to recover from such an attack.

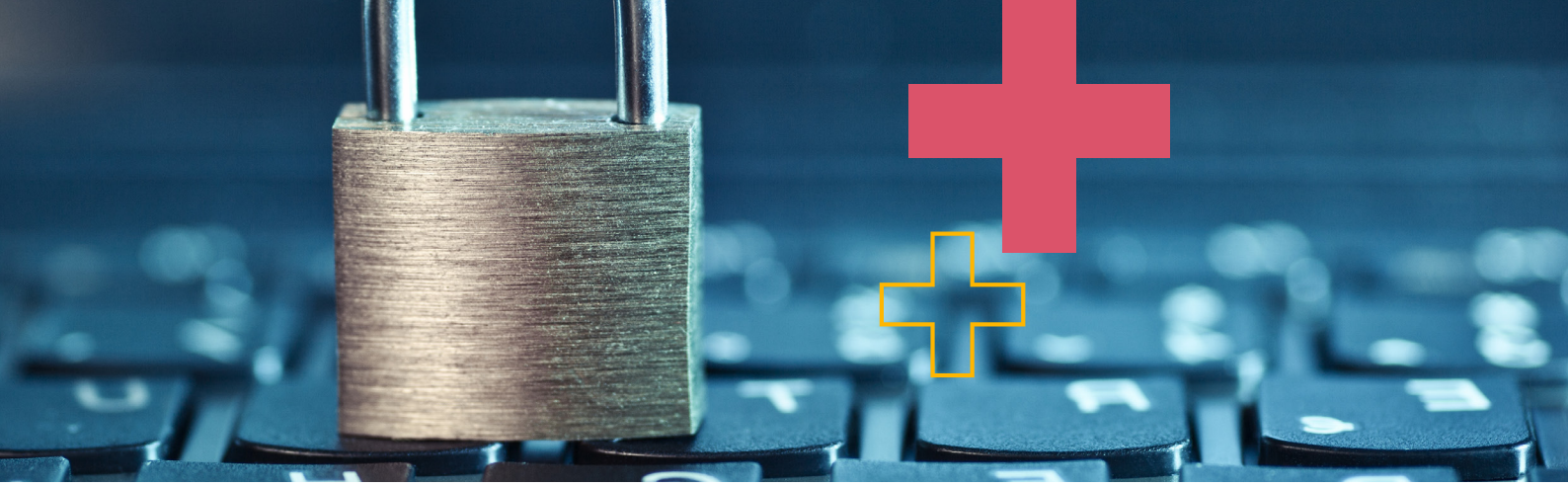
The number of days that the business remained disrupted because of a ransomware attack

13%	33%	20%	27%	7%
less than one day	one day	a few days	one week	a few weeks

Source: *IDC India Ransomware Survey*

5 *Center for Strategic and International Studies | Significant Cyber Incidents*

6 *IDC India Ransomware Survey-November, 2021*



3. Threats impacting citizens

A personal data breach can be broadly defined as a security incident that compromises the confidentiality, integrity or availability of personal data. The hackers deploy a range of techniques and tools to extract data from unsuspecting victims. These techniques include use of a fake website, phishing, collection of username and passwords, subscriber identity module (SIM) cloning, extraction of one-time-password (OTP), capturing of biometric data through fake apps, and collection of fake donations.

The data being targeted by hackers is primarily of two types:

- financial data and
- personally identifiable information (PII).

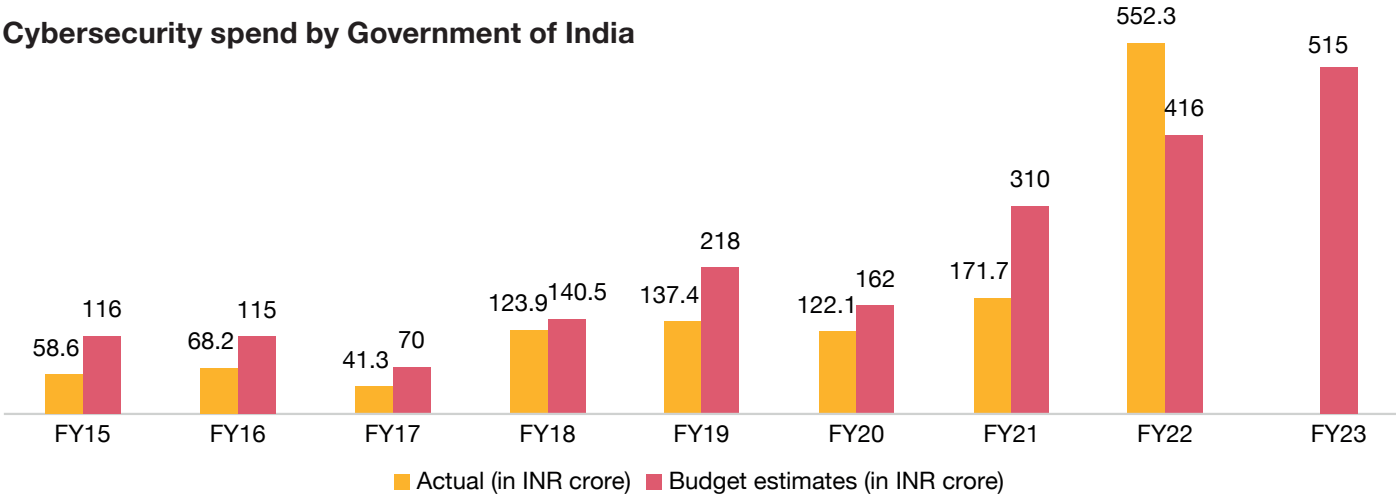
While users have some awareness of financial fraud, PII-related data and its potential for misuse is not fully understood by the masses, as there is limited awareness of data privacy as a concept. This results in a fair amount of PII, including biometric information such as fingerprints, iris scans and facial images, being shared without adequate precautions. This information, if compromised, can impede the privacy of citizens all through their lifetime. This serves to underscore the point that while significant investments are being made in Digital India initiatives, proportionate investments are needed to create user awareness and educate the masses.

Need for investments in the cybersecurity space

The cyber vulnerabilities in the Indian context primarily arise from inadequate investments in cybersecurity, be it in terms of investments in technology, building cybersecurity awareness or investing in strategic initiatives. As per the graph showing the trajectory of the Government of India's (GoI's) budget for cybersecurity, it is evident that there is an increasing trend in the budgeted amount. Incidentally, FY22 has been the first year when the actual amount exceeded the budgeted amount.[7]

This earmarked amount also needs to be viewed in relation to the spending by larger economies like the US, where the Government's budget for civilian cybersecurity for FY22 was about USD 9.8 billion.

Cybersecurity spend by Government of India



Source: *Business Standard*

7 *Business Standard article on cyber spend*

For many Indian businesses cybersecurity remains a non-productive cost centre as investments in cyber defence become rapidly obsolete, as cyberattacks improve in complexity and sophistication. Moreover, many organisations still follow a compliance-oriented approach to cybersecurity that is more of a tick in the box, rather than a risk-based approach. Coupled with the direct and indirect impact of a cyberattack, organisations often hesitate to divulge information related to cyberattacks and share the same with regulators and other institutions or even organisations in the same sector for fear of backlash and negative publicity.

Inadequate investments in cybersecurity and the above approach of businesses to this imminent threat serve to amplify the existing fault lines in the Indian cybersecurity landscape. The following are a few factors that need to be considered:

- **Gap between the pace of digital adoption and that of increase in cybersecurity awareness**

  While India's literacy rate currently stands at 77.7%,[8] the worldwide numbers are several notches higher at 87%.[9] Within India too, there are disparities pertaining to literacy that centre around the states, age group and gender. In states which have low literacy levels, cybersecurity awareness levels are correspondingly low. This lack of awareness and alertness regarding cyberthreats makes a large section of the Indian population vulnerable to cyberthreats.

- **Increasing threat surface area**

  The threat surface area in India is substantial owing to certain peculiarities of the Indian market. These include:

  a. **Increasing digitisation:** Increasing digitisation along with the 5G roll-out, while aligned with the nation's progress goals, also opens the door to increased cyberattacks with more connected devices, greater interconnectivity, and increased usage of the internet of things (IoT). All these factors expand the threat surface area and hence also result in increased potential for, as well as payoffs from, cybercrime. IoT devices pose risks of misuse, both in terms of malicious use of data and user profiling, resulting in violation of user privacy.

  b. **Extensive use of pirated software:** A substantial proportion of the operating systems[10] in use in India are pirated. Due to the lack of stringent enforcement of IP rules, and on account of the high price differential, users prefer to adopt pirated software. The pirated software leaves users vulnerable to malware and cyberattacks.

  c. **Extensive mobile usage for internet access:** India is one of the world's most dynamic mobile markets, adding 2.5 crore new smartphone users every quarter, with a monthly mobile data consumption rate of 12 gigabytes per user.[11] More complex threats are now coming into play as cybercriminals continue to evolve as well as adapt their techniques to exploit the growing reliance on mobiles. India's extensive mobile usage poses specific vulnerabilities, as 40% of the world's mobile devices are inherently vulnerable to cyberattacks.

  d. **Use of hardware/software created and manufactured outside India:** As various Indian installations and networks utilise hardware and software that has been created and manufactured outside India, there exists the risk of data leakage, remote surveillance or intentional introduction of a system malfunction through a remote connection. This risk is especially pronounced in sensitive industries such as telecom, power generation and distribution, and internet data centres where any such Trojan horse can have serious consequences. This risk is exacerbated by the fact that most cybersecurity-related hardware/software is also of foreign origin.

8 *Women and Men in India, 2021*

9 *World Bank | Literacy rate 2020*

10 *The Economic Times: News article on Microsoft Tests*

11 *The Economic Times: Interview of CEO of the National Health Authority of India*

e. **Third-party vendors who are especially vulnerable and can compromise the overall supply chain:** India has a very large base of micro and small and medium enterprises (MSMEs). MSMEs play a critical role in the Indian economy and contribute to about 30% of the GDP and 40% of exports, and provide employment to over 11 crore people.[12] Many MSME vendors may have IT systems that are not very robust but form a part of the overall supply chain of larger enterprises. These systems could inject vulnerabilities into the larger ecosystem, as any chain is as strong as its weakest link.

- **State actors working against India**

  On account of its geography and its political stance, India also faces threats from various state-sponsored actors who have direct or tacit support from their respective governments. These attacks are especially powerful given the extensive machinery of the state and the fact that these hackers have far greater capabilities than rogue hackers.

  The motives may be varied and can include espionage, sabotaging critical infrastructure or spreading disinformation. The asymmetry and economic and social disparities in India lead to powerful amplification of any such disinformation campaign. In incident after incident, security agencies have observed that the spread of disinformation in an increasingly interconnected world with real-time digital linkages can hurt sentiments and vitiate the economic landscape through its explosive non-linear spread. Using such actors is especially useful for enemy nation states as, on detection, they can distance themselves from such actors.

- **Inadequate investor attention**

  Cybersecurity-related disclosures in annual reports are few and far between, indicative of the fact that this aspect may not be receiving appropriate attention from investors and other stakeholders. Currently, the disclosures in annual reports are primarily focused on mentioning cybersecurity risks as a key risk in the Management Discussion and Analysis (MD&A) section, and indicate that these aspects are being discussed by the Risk Management Committee. Even among Nifty 50 Companies, there are a few in which there is no mention of cyber risks. Providing increased disclosures regarding cybersecurity in annual reports and other investor communication can help investors make an informed decision.

12 Report of Committee on MSMEs

Our take

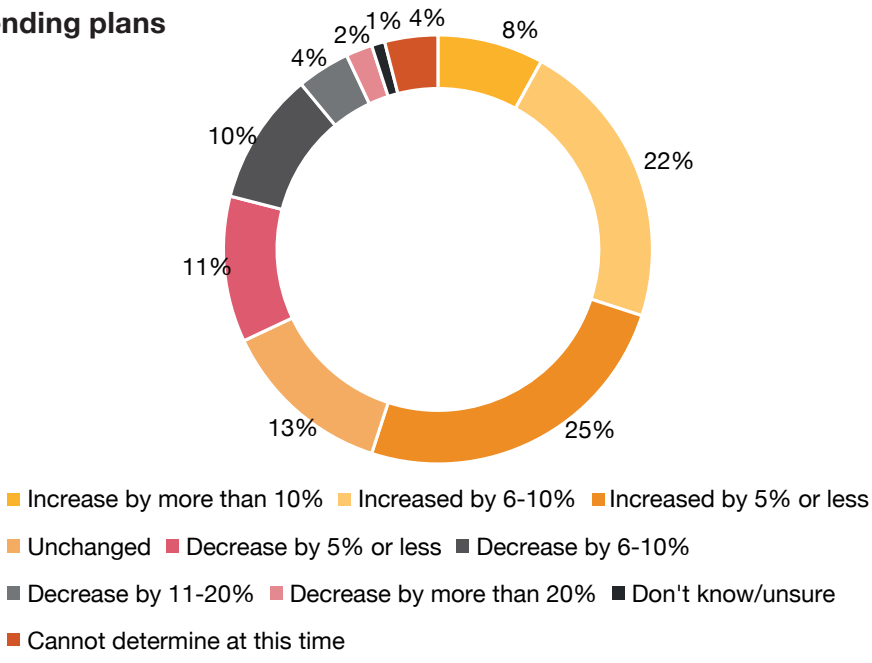
The need for increased investments in cybersecurity

Given India's aspirations towards becoming a USD 5 trillion economy and the increased emphasis on Digital India, it is essential that investments in cybersecurity are suitably ramped up. Accordingly, there is a need for promoting indigenous cybersecurity solutions. The Indian corporate sector too should focus on shifting from a consumption mindset to an innovative one that results in the in-house production of India-centric solutions.

India, as the software powerhouse of the world that is noted for its talent and expert base, can create a multitude of solutions in the cybersecurity sector. The current push by the Government to promote cyber risk management, digital forensics, cyber product ecosystem needs further consolidation. Start-ups dealing with cybersecurity need to be incubated, preferably along sectoral lines, and the seed capital should be made available by the Government and/or industry bodies. In-Q-Tel, which uses funds from the Central Intelligence Agency (CIA) to invest in start-ups that develop technologies for the agency's use, is a case in point.

The need for additional investments in cybersecurity is also borne out by the findings of PwC's Global Digital Trust Insights Survey 2021.[13] As per the survey, 55% of the respondents intend to increase their cyber spend compared to the prior year.

Cybersecurity spending plans



Source: *PwC | Global Digital Trust Insights 2021*

The following cybersecurity areas demand both Government and corporate investments:

- **Adoption of a participative framework for building trust**

  Given the specific constraints, India needs to craft its own bespoke strategy to counter cyberthreats. Towards this end, building trust in the computing environment is a key imperative. The strategy could take a leaf out of the Aadhaar development playbook. Aadhaar's quick development and rapid scale-up was accomplished by combining tech-sector skills and public policy.

13 *PwC | Global Digital Trust Insights 2021*

This imbued the development and implementation of Aadhaar with a sense of urgency and enabled the Government to use the private sector as a catalyst for execution purposes. The Aadhaar project involved contributions by tech volunteers who created a combination of technological projects that is collectively known as the India Stack.[13] This accelerated financial inclusion, enabling the country to leapfrog about three decades.

The Indian cyber stack for trusted computing could be developed by applying the same principles and drawing on participation from the private sector. A consultative mechanism between all stakeholders could be used, adopting a public-private partnership (PPP) model. As expertise in the cyber tech arena is not age driven, and the private sector is known for its project implementation abilities, public-private participation in cyber tech can offer considerable benefits. Indian tech companies often serve as tech providers for the world, and thus can play a significant role in improving the nation's cybersecurity ecosystem.

The broad contours for the Indian cyber stack have been articulated in the India Enterprise Architecture (IndEA) framework and need to be further advanced. The Indian cyber stack could cater to Government and corporate sector requirements and should address the following areas:

- national cybersecurity response
- national cybersecurity situation awareness
- national cybersecurity process and guidelines
- systems and data protection
- products and technologies.

- **Clinical examination of supply chains to identify and fix vulnerabilities**

  The supply chain of any organisation includes an array of diverse actors with varying levels of cybersecurity readiness. It is critical that the cybersecurity robustness of all the elements of the supply chain be suitably enhanced. Towards this end, having a standardised framework for cybersecurity readiness could be very useful and may include the development of a single rating scale for evaluating cyber readiness. This will not only enable relative benchmarking of corporates, but also serve to establish a baseline to help track incremental progress. Moreover, it will help companies to make informed decisions about their supply chain networks.

- **Assurance and certification programmes**

  The 'Make in India' initiative, along with assurance programmes which proactively check for any embedded software, should provide a solution to the threat from software/hardware originating from countries with whom there is some friction. This is especially relevant for the defence sector, which has traditionally been heavily reliant on imports.

14 Nandan Nilekani's presentation on Financial Inclusion

Here too, private sector participation can be useful, as companies could play a key role in equipment accreditation and threat identification. Any IoT device provides an opportunity for misuse – both in terms of malicious use as well as user profiling – resulting in the violation of user privacy and data misuse. Indigenous certification can help in this regard, with private players being entrusted with the responsibility of certifying that IoT devices are not malicious. The assurance programmes also need to be accompanied by rigorous enforcement of intellectual property (IP) to ensure that only original software is used.

- **Playbooks tailored to different players**

  An integral component of an organisation's cybersecurity journey is the creation of a cybersecurity framework and having a standard operating procedure (SOP) in place, in the event of cyberattacks. This can be driven by the security operations centre (SOC) within an organisation, which can help with threat discovery, preliminary investigations and a security triage. Thereafter, it could conduct a detailed investigation and take effective steps to contain and respond to the threat. Having an SOC in place is a prerequisite that helps in the timely identification of vulnerabilities and a swift response in the event of a cyberattack.

- **Streamlining the operations of various Government agencies and policy dynamism**

  Clear demarcation of responsibilities among various Government agencies will help in ensuring greater ownership and gathering of the required expertise. This will also ensure that different event-reporting timelines are properly thought out and that a materiality threshold against which cybersecurity events are tested is clearly defined, before the reporting obligation kicks in. Annual revisions to the National Cybersecurity Policy, 2013, will help keep the policy framework current and relevant to the rapidly changing threat landscape, and will impart dynamism to policy articulation. Also, given the rapidly changing threat landscape, it is important that coverage under the National Critical Information Infrastructure Protection Centre also keeps evolving. Adoption of the National Cybersecurity Strategy, 2020, will provide policy cohesion in terms of approach. It will ensure that fragmentation of the cybersecurity mandate across agencies is avoided, and that consolidation of the national cybersecurity apparatus takes place along similar lines of development in the USA and China.

- **Capacity building and certification**

  The need for cybersecurity experts is evident. However, most experts are differentiated based on industry-recognised certifications promoted by foreign bodies. Therefore, there is a requirement for cybersecurity education at the grassroots level and indigenous low-cost certification programmes in regional languages.

- **Integrated risk strategy**

  According to our 2022 Global Risk Survey - India highlights,[14] it is important to engage early and obtain risk insights at the time of decision making. A panoramic view of risk needs to be taken in order to understand the risk appetite and take advantage of underlying opportunities. For example, in a typical risk management framework, cybersecurity risks are handled by the information security team or the chief technology officer of a company, whereas geopolitical risks are handled by the business teams. In the case of cyberthreats emerging due to geopolitical issues – such as a stand-off between two countries, or due to the stance of an enemy state – an intersection of these two elements is required, thereby reinforcing the need for a comprehensive and integrated risk strategy.

In this digital age, a nation's IT infrastructure and the associated cybersecurity measures are of critical importance. While India faces a unique set of challenges on the cybersecurity front, it also has the intellectual wherewithal to devise creative solutions to address these problems. A PPP model can foster the development of solutions that cater to the whole of society, paving the way for a stronger and more secure India.

15 2022 Global Risk Survey - India highlights

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 155 countries with over 327,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

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

Contact us

Sivarama Krishnan
APAC Cyber Security and Privacy Leader
sivarama.krishnan@pwc.com

Sangram Gayal
Partner, Cyber Security
sangram.gayal@pwc.com

Core team

Bhoomi Yagnik
Dheeraj Kaushal
Manish Ballabh
Raju Gupta
Sangram Gayal
Vishnupriya Sengupta

Editorial team

Dion D'Souza

Design

Kirtika Saxena

pwc.in

Data Classification: DC0 (Public)

KS/August 2022-M&C 21295