India's Cybersecurity Landscape: The Roles of the Private Sector and Public-Private Partnership

By: Nir Kshetri

Kshetri, Nir (2015). "India's Cybersecurity Landscape: The Roles of the Private Sector and Public-Private Partnership" *IEEE Security & Privacy* 13(3), 16-23.

Made available courtesy of IEEE: http://dx.doi.org/10.1109/MSP.2015.61

Abstract:

Are public–private partnerships an appropriate means of dealing with underdeveloped cybersecurity-related institutions in India? Whereas the government lacks the resources and expertise to develop new templates, monitor industry behaviors, and enforce laws, trade associations are likely to have more experience and well-focused priorities in these areas.

Keywords: public-private partnerships | India | cybersecurity | NASSCOM | DSCI

Article:

In July 2013, in response to domestic and international pressure to enhance cybersecurity measures, the government of India released the National Cyber Security Policy (NCSP; http://deity.gov.in/content/national-cyber-security-policy-2013-1), which set forth 14 objectives that included enhancing the protection of critical infrastructure and developing 500,000 skilled cybersecurity professionals in the next five years. A key component of NCSP is the development of public–private partnership (PPP) efforts to enhance the cybersecurity landscape. PPPs are especially well-suited for areas that require diverse types of expertise and knowledge to address complex problems, including cybersecurity.(1)

In this article, I provide insight into various constraints the Indian government faces in strengthening cybersecurity and examine the private sector's role in this area.

Background

India's economy and the government's limited resources have given rise to self-regulatory bodies in the private sector.

Economic Issues

Two key features of the Indian economy affect its cybersecurity posture. First, owing to the rapidly growing IT and business process management (IT&BPM) sector and its various data breaches, the country is facing unprecedented pressure from foreign offshoring clients and Western governments to strengthen cybersecurity. In 2011, the US and India signed a memorandum of understanding to promote cybersecurity-related cooperation and exchange information. In bilateral talks, the US emphasized India's need for capacity building in cybersecurity, especially in cybercrime detection and investigation. Because India is a major offshoring destination for back offices and other high-value business functions, cybersecurity orientation of Indian businesses has been an issue of pressing concern to US and other Western businesses.

Second, the Indian government severely lacks the resources to develop and enforce criminal cybersecurity-related regulations, standards, and guidelines. For instance, in 2011, the police cybercrime cell of Delhi had only two inspectors. In 2012, the Delhi High Court noted the Delhi police website's lack of functionality, calling it "completely useless" and "obsolete."(2) Until 2010, there wasn't a single cybercrime-related conviction in Bangalore, the country's biggest offshoring hub. One law enforcement officer attributed the low conviction rates to the police's lack of technical skills, knowledge, and training in collecting evidence.(3) For instance, when a police officer was asked to seize a hacker's computer, he brought in the monitor. In another case, the police seized the CD-ROM drive from a hacker's computer instead of the hard disk.

Government Constraints

Nascent and formative areas such as cybersecurity are often characterized by underdeveloped regulatory structures. There's no template for policy development, assessment, and analysis. Developing templates, monitoring the behaviors of individuals and organizations, and enforcing regulations require extensive resources and expertise in such areas. However, most governments in developing countries are characterized by weak public administration, inadequate technical competence, and lack of political will in the implementation of economic and social policies.(4)

Another factor is perhaps more important. The way the Indian government is positioned doesn't allow it to spend state resources to support a new area at the cost of competing sectors. If policymakers allocate disproportionately more resources to develop modern sectors such as IT&BPM, they face stiff opposition from the mass of population that depends on the traditional economy. For instance, in India's Andhra Pradesh state in the late 1990s and the early 2000s, political opponents attacked then–Chief Minister Chandrababu Naidu's decision to raise rice and electricity prices by cutting subsidies, which would worsen the welfare of most people. They also labeled his promotion of offshoring-related sectors and foreign capital as elitist. Naidu was voted

out of office in 2004. For the majority of the Indian population, data privacy and security are largely irrelevant.

Self-Regulatory Bodies

Because of these factors, India's IT&BPM sector manages cybersecurity risk through effective industry self-regulation. A highly visible private-sector actor is the National Association of Software and Services Companies (NASSCOM), established in 1988 as an industry-funded not-for-profit organization to contribute to the software industry's development. NASSCOM aims to help the IT&BPM sector to be a "trustworthy, respected, innovative and society friendly industry in the world" and to "[e]stablish India as a hub for innovation and professional services" (www.nasscom.in/vision-and-mission).

Owing primarily to the uptick in data incidents, addressing data security and privacy issues has become increasingly important for the Indian IT&BPM sector's success and vitality. In 2008, realizing the importance of an organization with an exclusive focus on data protection, NASSCOM established the Data Security Council of India (DSCI), a self-regulatory member organization. DSCI's mission is to create trust in Indian companies as global outsourcing service providers. Its focus on cybersecurity is to "[h]arness data protection as a lever for economic development of India through global integration of practices and standards conforming to various legal regimes" (https://www.dsci.in/taxonomypage/1). DSCI took over most of NASSCOM's data protection–related activities.

NASSCOM and DSCI have been exemplary self-regulatory bodies, playing key roles in strengthening the IT&BPM sector's cybersecurity orientation. They've played an equally important role in the PPP cybersecurity initiatives and worked with government and law enforcement agencies to formulate and enforce cybersecurity-related legislation. Table 1 shows major events associated with NASSCOM and DSCI's evolution and their roles in enhancing cybersecurity.

The Roles of NASSCOM and DSCI

As of 2015, NASSCOM had more than 1,800 members, compared to 485 corporate members of DSCI. Although any company operating in India's IT&BPM sector might have incentive to join NASSCOM, DSCI membership is especially important for companies for which cybersecurity is a key priority. NASSCOM membership fees vary from approximately US$450 to $100,000, depending on organization size. Many of NASSCOM's members are also global firms from the US, Europe, Japan, China, and other countries. NASSCOM thus has a fairly high level of expertise and the financial resources to take various cybersecurity measures.

DSCI monitors member companies to ensure they adhere to cybersecurity standards. For instance, it requires members to self-police and provide additional layers of security at the infrastructure, applications and other levels. The maximum fine for companies that fail to secure data is $1 million. Noncompliant companies might also lose their NASSCOM and DSCI memberships.

Trade associations influence industry behaviors directly as well as through causal chains. Indirect effects entail mimicking behaviors of other actors that are perceived to be exemplary and have a higher degree of effectiveness.(5) Exemplary firms serve as models for smaller firms to imitate. In such cases, knowledge flow takes place by externalities mainly due to interactions among firms or their employees. Trade associations are likely to accelerate this process by stimulating interaction among member companies.

A trade association's enforcement strategy becomes efficient and powerful if a large number of firms join the association. NASSCOM ex-president Kiran Karnik addressed the importance of DSCI membership: "While it would be voluntary for the members to be part of the body, it would ensure at the same time that market forces make it mandatory for companies to register themselves."(6)

Table 1. NASSCOM and DSCI's evolution and roles in enhancing India's cybersecurity profile.

Date	**Milestones and major events**
1988	The National Association of Software and Services Companies (NASSCOM) was established as a not-for-profit organization with 38 members, which accounted for 65 percent of the software industry's revenue.
1990	NASSCOM began a public-awareness campaign to educate software users and encourage lawful use.
Early 1990s	NASSCOM teamed up with the Manufacturers Association for Information Technology to launch the Indian Federation against Software Theft.
1994	NASSCOM and *Business Software Alliance* set up the toll-free Anti-Piracy Hotline in New Delhi.
2003	NASSCOM started working with Mumbai police on cybercrime-related matters.
2004	NASSCOM announced a plan to have its members' security practices audited by international accounting firms.
2004	NASSCOM started the Cyber Labs program with support from the government's Department of Electronics and Information Technology.
2005	NASSCOM announced a training initiative for Pune's cybercrime unit.
April 2005	Three former employees of Mphasis were arrested for allegedly stealing more than US$350,000 from Citibank customers.
2006	NASSCOM drafted plans for new legal measures to safeguard intellectual property and prevent data theft.
January 2006	The National Skill Registry (NSR) launched, allowing employers to perform background checks on existing or prospective employees.
April 2007	The number of individuals registered in the NSR database reached 100,000, and the number of participating companies reached 36.
2008	NASSCOM announced the establishment of the Data Security Council of India (DSCI) as a self-regulatory body.
February 2008	The number of technology employees signed up for the NSR reached 220,000.
2009	Cloud computing security was reviewed by the NASSCOM–DSCI Information Security Summit. It has been the focus of every annual summit since.
2011	DSCI announced a plan to set up a cloud security advisory group that would develop a policy framework. The group advises the government on security and privacy issues in a cloud environment.

June 2011	In the DSCI Best Practices meeting, issues related to data protection in cloud computing and compliance were discussed.
December 2012	A seminar organized by DSCI focused on preventing data theft and cyberattacks and securing critical infrastructure.
March 2013	The DSCI had 654 organizations as corporate members, and more than 1,350 security and privacy professionals and practitioners as chapter members.
August 2013	The number of individuals registered in the NSR database reached 1.3 million, and the number of participating companies reached 118. It's supported by 17 employee background-checking companies and 126 point-of-service vendors in various locations.
December 2013	NASSCOM had more than 1,504 members, representing 95 percent of industry revenue.

NASSCOM collaborates with other entities. For instance, in the 1990s, it teamed up with the Manufacturers Association for Information Technology to launch the Indian Federation against Software Theft. Similarly, it announced a plan to have its members' security practices audited by international accounting firms. Industry leaders also advocated the adoption of certification under the British Standards Institution's information security management systems, which covers network security, data sanctity, and data utilization terms.

Partnerships between the government and the private sector are viewed as a promising way of generating new opportunities to leverage financial, human, and technological resources that aren't likely to be available if the government attempts to do it alone.(7) This is especially pertinent for cybersecurity in developing economies owing to their resource-poor environments.

The Need for PPP

Prior research suggests that the public and private sectors' different strengths, expertise, and experience could lead to complementary roles in meeting developmental and social needs.(8) A unique strength of the state government is its ability to impose harsh sanctions and penalties on violators of laws and regulations. Trade associations such as NASSCOM often have this level of technical expertise and resources and don't face some of the constraints that limit the state's ability to monitor and control cybercrime activities.

Private and public sectors engaged in PPPs have different objectives, agendas, and interests. For example, one goal of the public sector is to employ private sector's capital and technology and share risks with the latter to provide the delivery of public services or goods. By winning the public sector's support, the private sector can increase profitability.

The Indian government and the private-sector actors' motivation and objectives partly overlap in strengthening cybersecurity. The IT&BPM sector plays a strategic role in the national economy, and most high-profile and widely publicized cybercrimes occur in this sector. In another case, call center workers at outsourcing services provider Mphasis transferred more than $350,000 from four Citibank customers' accounts to their personal accounts.(9) In major Indian cities, "data brokers" obtained data illegally from people working in offshoring companies. For instance, two people who claimed to be workers in Indian offshoring firms met *Sunday Times* undercover reporters with a laptop full of data and bragged that they had 45 different sets of personal information on approximately 500,000 UK consumers.(10) The information included

credit card holders' names, addresses, phone numbers, start and expiry dates, and security verification codes as well as information about mortgages, loans, insurance, phone contracts, and television subscriptions. NASSCOM initiated its crime-fighting efforts in response to these events in the Indian IT&BPM sector.

Since the early 2000s, NASSCOM partnered with the Ministry of Information Technology to draft data protection and privacy laws in response to offshore clients' privacy concerns. The goal was to bring Indian data protection laws to the same level as European and US standards. In 2011, DSCI announced a plan to set up a cloud security advisory group that would develop a policy framework. The group would also advise the government on cloud security and privacy issues.

PPP Achievements

PPPs involve arrangements and cooperative relationships between public and private sectors, under which the latter undertakes actions that have been traditionally performed by the former.(11) NASSCOM has played a lead role in developing and implementing vital cybercrime-fighting programs that are normally initiated and led by the government agencies in the US and other industrialized countries. Consider the Cyber Labs program (www.dsci.in/cyber-labs), which is modeled after the National Cyber-Forensics & Training Alliance (NCFTA) in the US. Whereas NCFTA is a US federal government effort established by the Federal Bureau of Investigation, India's Cyber Labs program is a private-sector initiative started by NASSCOM in 2004 with support from the government's Department of Electronics and Information Technology. Cyber Labs provide training and other support to police officers, prosecutors, bank officials, and others. As of April 2015, there were eight Cyber Labs in various Indian cities, which provided cybercrime training to more than 28,000 police officers. The Bangalore Cyber Lab alone has resources to train more than 1,000 law enforcement personnel annually. To educate legal communities, NASSCOM and DSCI also meet with bar councils in different cities.

DSCI presents public- and private-sector employees and organizations with special awards and recognitions. For instance, the DSCI Excellence Awards began in 2011 in two areas: corporate (based on the preparedness level and cybersecurity response) and law enforcement (given to police and investigation agencies for capacity building in investigating and solving cybercrime cases).

NASSCOM and DSCI have helped increase consumers' cybersecurity awareness. In the early 1990s, NASSCOM began a public-awareness campaign to educate software users and encourage lawful use. Other efforts include dissemination measures, such as CyberSafety Week, organized by the NASSCOM and government agencies in major cities. For instance, in 2010, NASSCOM, DSCI, and Mumbai police, with support from Ministry of Information Technology, organized CyberSafety Week—Mumbai to educate users on cyber safety and IT security.

In recent years, NASSCOM has realized the need to focus on security issues associated with new technologies such as cloud computing and social media. NASSCOM–DSCI Information Security Summits address cloud security every year. In the 2011 DSCI Best Practices meeting, issues related to data protection and compliance in cloud computing were discussed. Likewise, a

December 2012 DSCI seminar focused on preventing data theft and cyberattacks and securing critical infrastructure.

Various State Roles and PPP Conditions

It's important to understand the enabling and constraining conditions that influence the success of PPP projects. Among the most important is the conduciveness of institutional environments to PPP. A government that's friendly with the private sector, willing to involve players in key national economic policies, and interested to see this sector flourish is likely to be supportive of PPP initiatives.

Broadly speaking, these conditions exist in India's IT&BPM sector, which has facilitated cybersecurity-related PPP in the country. Major emphasis must be placed on enactment and enforcement of necessary laws. These conditions can be captured by the state's regulatory, participatory, and supportive roles. The regulatory roles entail establishing and enforcing the rule of law. The participatory roles are about ensuring that businesses and citizens contribute to national policymaking. The supportive roles involve creating conditions that foster the growth of businesses in certain sectors.

Regulatory Role

In a regulatory state, a set of factors influences the enforcement of contracts: sound political institutions and the rule of law, a government free from corruption, bureaucratic quality, a strong and effective court system, and citizens' willingness to accept the established institutions.(12) Again, the Indian government faces several challenges in performing regulatory state functions, which is its most glaring shortcoming. Indian states have faced budget problems and failed to comply with federal directives to hire judges and upgrade legal infrastructures and court facilities.

Factors such as ineffective national legal systems, ambiguous laws on the books, a lack of resources, or a state's unwillingness to allocate resources often severely hinder a state's ability to control criminal activities. This is especially relevant for new types of crimes such as cybercrimes. India's greatest barrier to cybersecurity is its unavailability and ineffectiveness of law enforcement owing primarily to its lack of resources and unwillingness to invest in such resources.

A related problem is the low reporting rate of cybercrimes. Approximately 10 percent of cybercrimes are reported, and of those reported, about 2 percent are registered.(13) The conviction rate is estimated at 2 percent. The barriers, hurdles, and hassles that victims confront contribute to the low registration rates. Police often don't support victims who want to file a cybercrime case and show unwillingness to investigate such crimes. For instance, a survey conducted by research firm BPO News indicated that although most Gurgaon business process outsourcing firms had been cybercrime victims, approximately 70 percent didn't report to the police; many expressed doubt about competence, professionalism, and integrity of the police handling cybercrime cases.(14) Approximately 50 percent of these respondents believed cases aren't dealt with professionally, and 30 percent noted that they had "no faith" in Gurgaon police.

Cybercrime victims have also complained that the police's process to build a case is long and inefficient.

Thus, there is a vicious cycle: law enforcement agencies lack the skills, orientation, and capability to address cybercrime-related offenses; there are low cybercrime reporting rates because of victims' lack of confidence in law enforcement agencies; and cybercriminals become more resourceful and powerful because their offenses aren't reported and law enforcement agencies lack motivation or justification to improve their skills.

Although NASSCOM and DSCI's measures have been quite successful in boosting firms' cybersecurity in the IT&BPM sector, many critical factors are beyond their control. The state's weak regulatory role has negatively impacted key ingredients of cybersecurity. For instance, one estimate suggested that approximately 20 percent of resumes submitted for IT&BPM positions in India are fake.(15) The maximum punishment for faking a resume is termination of employment. Due to India's highly inefficient legal system, fraudsters are rarely caught and punished. The rule of law is weakly developed and often ignored with impunity. Getting an outsourcing job on the basis of a fake resume is a high-reward, low-risk activity because such jobs pay better than those in other economic sectors.(15)

Many of NASSCOM's and DSCI's responses are the result of a hollow state and institutions that are highly ineffective in dealing with India's cybersecurity challenges. For instance, India lacks standard identifiers like the US Social Security number, making it difficult to check potential employees' backgrounds. It costs up to $1,000 per employee to check backgrounds thoroughly.

In 2005, in response to the lack of such databases, the NASSCOM announced a plan to launch a pilot employee-screening program called Fortress India, which would allow employers to screen out potential workers who have criminal records. This became the National Skill Registry (NSR), which allows employers to perform background checks on existing or prospective employees. It's a voluntary registry for call center employees. Although the NSR doesn't include the profiles of most potential job seekers, it's a step in the right direction.

Participatory Role

A participatory state captures the extent to which policies and institutions represent the wishes of the members of society.(4) To protect their independence and autonomy, businesses might participate in national policymaking and work closely with state agencies.

India's PPP cybersecurity initiatives are largely a product of a participatory state. The country's 1991 economic liberalization was a major driving force behind the increased importance of groups such as trade associations; the state-dominated economic policy framework shifted to a decentralized one. Religious, social, economic, and political associations have offered a viable set of examples encouraging the development of many new trade and professional associations. A strong mutual interdependence between the state and the private sector—particularly organized business groups—has developed quickly. The liberalization thus resulted in more room for associations to flourish and have a strong voice as well as increased their participation in national policy development and planning processes.(16)

The Indian government's relationship with the private sector has involved a high level of trust and partnership in cybersecurity-related matters. In the early 2000s, the NASSCOM established a CyberCop Committee to provide cybersecurity services to the government and the private sector in an advisory capacity. In 2006, the NASSCOM drafted plans for new legal measures to safeguard intellectual property and prevent data theft.

In recent years, the government has made efforts to create a favorable climate for a higher participatory involvement in cybersecurity. For instance, a cybersecurity joint working group (JWG) was established with representatives from government agencies and the private sector and mandated to come up with PPP recommendations in capacity building and policymaking for government consideration. The JWG released its "Engagement with Private Sector on Cyber Security" report in October 2012 (https://www.dsci.in/node/1211). NCSP incorporated many of the recommendations of this report as well as that of the NASSCOM–DSCI report "Securing Our Cyber Frontiers" (https://www.dsci.in/node/1092). Both reports placed high level of emphasis on the formulation of PPP to address cybersecurity issues—a key element of NCSP.

Another sign of the improving climate for participatory involvement of the private sector occurred in October 2012, when India's National Security Advisor announced a plan to establish a permanent working group on cybersecurity, with representatives from the government and the private sector, would implement the country's cyberdefense framework. This marked the first time the Indian government allowed the private sector to participate in national security matters.

Supportive Role

A government can support cybersecurity development via legal and nonlegal influence. One way to do so is to address barriers related to skills, information, market, technology, and infrastructures. Nations that have achieved innovation-led growth also directly support these innovations. For instance, the US government invested heavily in several mission-oriented innovations, such as the microchip, the Internet, biotechnology, and nanotechnology.

In general, the Indian government offers a low level of support to private businesses. The state's supportive role is found to be less favorable to private businesses in India than in China. Nonetheless, the Indian government has shown a higher level of support and commitment to cybersecurity. For instance, the NASSCOM asked the government to create a special court to try people accused of cybercrimes. In response, the first cyber-regulation court was established in Delhi in 2009.

Likewise, in view of the country's lack of indigenous technology and patents in this area, the Indian government announced the possibility of providing financial assistance to Indian firms for acquiring foreign firms with high-end cybersecurity technology. The Ministry of External Affairs explored possible targets worldwide through Indian embassies and missions.(17) The Indian company that owns the technology gained through the acquisitions is required to give government agencies access to the intellectual property rights.

Discussion and Implications

Although sectoral business organizations such as trade associations are generally numerous and exist in almost every country, their level of development and influence on national policymaking and implementation vary greatly. NASSCOM is probably among the most influential and effective trade associations and has been successful in strategically solving collective cybersecurity problems of organizations in India's IT&BPM sector.

NASSCOM's measures have paid off brilliantly. In regard to the Indian IT&BPM sector's data security measures, a UK Banking Code Standards Board (BCSB) report noted: "Customer data is subject to the same level of security as in the UK. High risk and more complex processes are subject to higher levels of scrutiny than similar activities onshore" (http://www.rediff.com/money/2006/oct/07bpo.htm).

Citing the findings of the BCSB and Forrester Research, NASSCOM's then-president Karnik asserted that security standards in Indian call centers were among the best in the world, and there were more security breaches in the UK and the US in 2005 than in India.(18) DSCI's principal consultant Rahul Jain attributed the Indian IT&BPM sector's rapid growth to the adoption of best practices and global standards related to cybersecurity, investments in the latest cybersecurity technologies and processes, staff training, creation of high levels of employee awareness of cybersecurity, focus on IT governance, and internal cybersecurity auditing mechanisms.(19)

Some have rightly labeled India's cybersecurity policy as incomplete and "all words and no action" owing to the lack of a national cybersecurity action plan document or any guidelines regarding how the policy will be implemented.(20) Likewise, no clear action plan explains how NCSP's various goals can be achieved. Nonetheless, if we look at the track record of the roles of the collaborations between public and private sectors, which have been mainly initiated by the NASSCOM, we have a wealth of detailed evidence about PPP's role in strengthening cybersecurity.

PPP has resulted in the enactment of regulations and rules related to cybersecurity. However, there are also major weaknesses and shortcomings in the enforcement of the existing laws. In this regard, NASSCOM's efforts represent a limited but important part of India's overall cybersecurity posture.

Regarding the role of domestic spillover of cybersecurity-related knowledge and technology, it's important to look at learning processes. Researchers have suggested that such processes generally take place through intra-IT&BPM and inter-industry externalities. The diffusion of information and expertise, interfirm labor mobility, and development of specialized services would facilitate such externalities. Research has also suggested that inter-industry spillover effects associated with export activities are positively related to industrial linkages. In this regard, to increase the effects associated with spillover and externalities, policy measures are needed to strengthen the linkages between the IT&BPM industry and other economic sectors.

Especially when the state's regulatory roles are weak, trade associations can fill the regulatory vacuum. Interfirm linkages, such as trade associations in emerging economies, can establish the

industry's moral legitimacy in Western economies. For instance, developed world–based offshoring clients might rely more on trade associations such as NASSCOM than on a weak, ineffective state.

Trade associations can influence industry behaviors in several ways. These associations' norms, informal rules, and codes of behavior can create order—without the law's coercive power—by relying on a decentralized enforcement process in which noncompliance is penalized with social and economic sanctions.(21) In some situations, the state finds it beneficial to collaborate with such associations to rationalize an arena of activity. Associations can provide the state with expertise in developing new regulatory frameworks and strengthening enforcement.

Although DSCI's measures in strengthening data protection in the IT&BPM sector have been largely successful and can serve as a model for other developing economies, their effects aren't noticed outside this sector. For instance, DSCI increases its members' cybersecurity compliance by monitoring their security practices and providing training and education. Although DSCI's codes of behavior are irrelevant outside the IT&BPM sector, training and educating law enforcement personnel is key to strengthening the national cybersecurity profile. One reason behind the extremely low conviction rate could be that DSCI's training programs are insufficient to develop measurable competence in cybercrime investigation among law enforcement officers. A majority of its initiatives are special lectures or three- to five-day programs. More comprehensive training programs would allow trainees to master the cybercrime investigation techniques and feel confident about their ability to deal with cybercrimes. Although most current programs focus mainly on police officers, DSCI and the government need to educate prosecutors, judges, and lawyers using practical and layman's language.

PPPs are probably the most notable feature of the Indian cybersecurity landscape and an appropriate institutional means of dealing with underdeveloped cybersecurity-related institutions. Although the government has expressed a high degree of willingness to participate in PPP, resource constraints are a significant barrier to the legislation's effective enforcement. And it's fair to say that the government's initiatives to enhance IT&BPM cybersecurity are more symbolic than substantive.

In 2015, cybersecurity experts pointed out a number of challenges facing India's cybersecurity initiatives, such as inadequate budget, lack of coordination of different states' cybersecurity strategies, and lack of audits in software used in government agencies for security loopholes.(22) For instance, the Department of IT's cybersecurity budget for the 2015 fiscal year was less than $20 million. In addition, attacks on Indian websites increased by about 500 percent between 2010 and 2014.

India's digital economy has benefited greatly from NASSCOM's and DSCI's expertise in the interpretation, implementation, and application of data protection principles and their role as a repository of experience and source of cybersecurity best practices and cutting-edge knowledge. In this way, these agencies have been a driving force that has a major effect on India's cybersecurity posture. In sum, whereas the government lacks resources, expertise, and legitimacy to develop new templates, monitor the behaviors of industries, and enforce laws, trade associations' influences are likely to be more readily apparent. With well-focused priorities,

trade associations will likely be better, more effective, and more efficient institutions to effect change in this area.

References

1. J.X. Yu and Z.Y. Qu, "PPPs: Inter-Actor Relationships Two Cases of Home-Based Care Services in China," *Public Administration Q.*, vol. 36, no. 2, 2012, pp. 238–264.

2. S. Nolen, "India's IT Revolution Doesn't Touch a Government That Runs on Paper," *The Globe and Mail (Canada)*, 13 June 2012, p. A1.

3. "Cyber Crime: 1,600 Arrested, Only 7 Convicted," 11 Dec. 2012; www.rediff.com/business/report/tech-cyber-crime-1600-arrested-only-7-convicted/20121211.htm.

4. C. Pughm, "Getting Good Government: Capacity Building in the Public Sectors of Developing Countries," *Urban Studies*, vol. 36, no. 2, 1999, pp. 400–402.

5. M. Dickson, R. BeShers, and V. Gupta, "The Impact of Societal Culture and Industry on Organizational Culture: Theoretical Explanations," *Culture, Leadership, and Organizations: The GLOBE Study of 62 Societies*, R.J. House et al., eds., Sage, 2004.

6. "Regulator Soon for Monitoring Data Security Standards," 24 Apr. 2007; www.thehindubusinessline.com/todays-paper/regulator-soon-for-monitoring-data-security-standards/article1656182.ece.

7. P.V. Rosenau, *Public-Private Policy Partnerships*, MIT Press, 2000.

8. S.H. Linder, "Coming to Terms with the Public–Private Partnership: A Grammar of Multiple Meanings," *American Behavioral Scientist*, vol. 43, no. 1, 1999, pp. 35–51.

9. N. Kshetri, *Cybercrime and Cybersecurity in the Global South*, Palgrave Macmillan, 2013.

10. T. Gardner, "Indian Call Centres Selling Your Credit Card Details and Medical Records for Just 2p," 18 Mar. 2012; www.dailymail.co.uk/news/article-2116649/Indian-centres-selling-YOUR-credit-card-details-medical-records-just-2p.html.

11. E.S. Savas, Privatization and Public-Private Partnerships, University Press, 2002.

12. A.C. Sobel, State *Institutions, Private Incentives, Global Capital*, Univ. Michigan Press, 1999.

13. "Securing the Web," *Hindustan Times*, 22 Oct. 2006.

14. “Most Gurgaon IT, BPO Companies Victims of Cybercrime: Survey,” 6 Nov. 2011; http://timesofindia.indiatimes.com/city/gurgaon/Most-Gurgaon-IT-BPO-companies-victims-of-cybercrime-Survey/articleshow/10626059.cms.

15. S. Rai, “How Bogus Resumes Raise Questions about Indian Outsourcing Skills,” *TechRepublic,* 10 Sept. 2012; www.techrepublic.com/blog/cio-insights/how-bogus-resumes-raise-questions-about-indian-outsourcing-skills.

16. R. Frankel, “Associations in China and India: An Overview,” European Society of Association Executives, 15 June 2006, pp. 32–33.

17. T.K. Thomas, “Govt Will Help Fund Buys of Foreign Firms with High-End Cyber Security Tech,” *BusinessLine* 2012; www.thehindubusinessline.com/industry-and-economy/info-tech/article3273658.ece?homepage=true&ref=wl_home.

18. “India Could Process 30 Pct of US Bank Transactions by 2010—Report,” AFX News, 27 Sept. 2006; www.finanznachrichten.de/nachrichten-2006-09/7050839-india-could-process-30-pct-of-us-bank-transactions-by-2010-report-020.htm.

19. R. Jain, “Cyber Security: Imperatives for India,” Information Week, 7 Aug. 2012.

20. V.V. Desai, “Is India’s Cyber Policy All Words and No Action?,” TechTarget, 14 Oct. 2013; http://searchsecurity.techtarget.in/news/2240207148/Is-Indias-cyber-policy-all-words-and-no-action.

21. D.C. North, Institutions, Institutional Change and Economic Performance, Cambridge Univ. Press, 1990.

22. P.K. Jayadevan and N. Alawadhi, “India’s Cyber-Security Budget ‘woefully inadequate’: Experts,” 28 Jan. 2015; http://articles.economictimes.indiatimes.com/2015-01-28/news/58546771_1_cyber-security-cert-in-national-cyber-coordination-centre.

Nir Kshetri is a professor at the University of North Carolina at Greensboro and a research fellow at the Research Institute for Economics and Business Administration at Kobe University, Japan. His research focuses on global cybersecurity. Contact him at nbkshetr@uncg.edu.