Science and Technology Trends
Governance Systems for Cybersecurity

Cybersecurity in India: Regulations, Governance, Institutional Capacity and Market Mechanisms

Nir Kshetri

1. Introduction

The meteoric rise in cybercrime has been an issue of pressing concern to businesses and consumers in India. Among the Indian organizations, which responded to KPMG's (2014) Cybercrime Survey report 2014, 89% considered cybercrime as a "major threat" (p, 3). One estimate suggested that 42 million Indians were victimized online in 2011 (indolink.com, 2012).

As early as in 2009, it was reported in some Indian cities such as Mumbai in India, there had been more cybercrime cases were registered with the police than conventional crimes (Hindustan Times, 2009). According to a 2016 report of the National Crime Records Bureau (NCRB) 11,592 cases of cybercrime cases were registered in India in 2015 (Das, 2017). This is more than 300% increase of the 2009 level when there were 2,866 reported cybercrime incidents (Economictimes, 2012).

India also generates cybercrimes that affect Internet users worldwide. For instance, according to the U.S.-based Internet Crime Control Centre, India ranked fifth in the number of complaints received by the agency (Internet Crime Complaint Center, 2011). As an example, in 2012, the U.S. Federal Trade Commission (FTC) sued the California-based American Credit Crunchers. According to the FTC, an Indian company associated with American Credit Crunchers made threatening calls to U.S. consumers with histories of applying for payday loans, which are short-term, high-interest loans that are typically applied online. Agents in India with massive amount of personal data allegedly called potential victims and threatened dire consequences if the fictitious loans of up to US$2,000 were not repaid. U.S. consumers had lost over US$5 million to the scam, which had been in operation for two years (Shaftel and Narayan, 2012). Likewise, India was the top origin country for spam in 2011 and 2012. Similarly, a phishing survey released by the Anti-Phishing Working Group (APWG) in April 2012 found that India had the highest phishing top-level domain (TLD) by domain score (calculated as phish per 10,000 domains) in the second half (H2) of 2011 (Kshetri, 2015b).

Factors such as cybercrime's relative newness in the country and resource constraints have led to a poor cybersecurity orientation and weak defense measures among consumers, businesses and government agencies (Kshetri, 2013). According to a study of the Security

Bryan School of Business and Economics, The University of North Carolina at Greensboro
Bryan Building, Room: 368, P. O. Box 26165, Greensboro, NC 27402-6165, USA
E-mail: nbkshetr@uncg.edu

and Defense Agenda, a Brussels-based think-tank, India is among countries most vulnerable to cyberattacks due to a lack of systems and procedures to defend among the public and private sector (Blitz, 2011).

Due partly to the above trends, many initiatives and efforts of the government and private sector actors have emerged to strengthen cybersecurity in the country. Table 1 presents some of the key initiatives on the cybersecurity front. As a major recent regulatory initiative, in July 2013, the government of India (GOI) released the National Cyber Security Policy (NCSP), which had 14 objectives that included enhancing the protection of critical infrastructure and developing 500,000 skilled cybersecurity professionals in the next five years. The NCSP was formulated in response to domestic and international pressure to enhance cybersecurity measures.

Private sector actors such as the National Association of Software and Services Companies (NASSCOM) have also taken measures to strengthen India's cybersecurity standards. For example, the Data Security Council of India—a self-regulatory member organization set up by NASSCOM—imposes a fine of up to US$1 million for member companies that fail to secure data (Kshetri, 2016b).

Public–private partnerships (PPPs) are probably the most notable feature of the Indian cybersecurity landscape and an appropriate institutional means of dealing with underdeveloped cybersecurity-related institutions. For instance, a key component of NCSP is the development of PPP efforts to enhance the cybersecurity landscape. Note that PPPs are especially well-suited for areas that require diverse types of expertise and knowledge to address complex problems, including cybersecurity (Yu and Qu, 2012).

In light of the above observations, our goal in this paper is aimed at providing an overview of current cybersecurity landscape in India. We examine regulations and enforcement, governance mechanisms, functions of relevant actors as well as challenges and opportunities facing India on the cybersecurity front.

The paper is structured as follows. We proceed by first examining the regulatory environment related to cybersecurity in India. Next, we discuss private sector initiatives and market mechanisms in India in this evolving phenomenon. Then, we look at the public–private partnership in cybersecurity. It is followed by a section on discussion and implications. The final section provides concluding comments

Table 1. The evolution of cybersecurity-related initiatives in India: Major events

Time	Event
October 2000	Information Technology Act, 2000 came into force.
2006	Cyber Appellate Tribunal (CAT) started functioning.
2008	NASSCOM established the DSCI.
December 2008	Information Technology (Amendment) Bill 2008 passed by Indian Parliament
February 2009	The IT (Amendment) Act 2008 received the assent of the President
October 2009	The IT (Amendment) Act 2008 came into force.
2011	The central bank, RBI introduced a set of recommendations, which include the formation of separate information security groups within banks and maintenance of adequate cybersecurity resources based on their size and scope of operation.
October 2012	Cybersecurity joint working group (JWG) released its "Engagement with Private Sector on Cyber Security" report.
July 2013	The government released the NCSP, 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.
April 2017	The IRDAI issued guideline, which require all insurance companies to appoint a CISO.

Source: Kshetri (2010, 2015a)

2. The Regulatory Environment

India is strengthening cybersecurity-related regulatory and enforcement capacity (Kshetri, 2016a). India is among the first developing countries to criminalize cybercrimes by enacting the IT Act in 2000. India's IT Act 2000, however, did not cover offenses such as phishing, cyberstalking, and cyber-harassment (Hindustan Times, 2006). To address these drawbacks, the IT (Amendment) Act 2008, added specific provisions to deal with and punish cyber-offenses such as publication of sexually explicit material, cyber-terrorism, Wi-Fi hacking, child pornography, identity theft, and spam (Deshpande, 2009).

Privacy is also becoming an increasingly important issue. Recently legal institutions have recognized that citizens have a fundamental right to protect privacy. In September 2013, India's Supreme Court issued an interim order, which ruled that people cannot be required to have the Aadhaar identification in order to collect state subsidies (Ribeiro, 2014). Note that the government of India (GoI) led by the Bharatiya Janata Party (BJP) indicated that it would require residents to have biometric IDs in order to collect government benefits. The project had set a target of 1 billion enrolments by 2015 (cio.de, 2014). The biometric ID assigns a person a 12-digit number, which is called the Aadhaar number. It requires the collection of 10 fingerprints, iris scans and other information such as the name, date of birth and address and will be hosted in the eGovernance cloud platform.

The country's regulatory bodies overseeing various markets have also issued guidelines, best practices and regulations to monitor and control cybersecurity activities. For instance, India does not have data breach disclosure laws. However, the central bank, RBI has asked banks and financial institutions in the country to share information on data breach. The idea is to provide opportunities to learn about cyber-threats. For instance, a database of banking malware "signatures" would allow banks to set up firewalls against known malware types. For instance, the knowledge about breach in a bank would help other banks to look for the signatures of the same type of breach. Likewise, in April 2017, the Insurance Regulatory and Development Authority of India (IRDAI) has issued guideline, which require all insurance companies in the country to appoint a Chief Information Security Officer (CISO) (DNA, 2017).

Despite some enforcement activities, however, there is an enormous gap between laws on the books and the government's capability to enforce laws. India's most daunting challenge lies in overcoming the severe shortage of cybersecurity manpower. For instance, in 2004, of the 4,400 police officers in India's Mumbai city, only five worked in the cybercrime division (Duggal, 2004). Likewise, in 2011, the police cybercrime cell of Delhi had only two inspectors (Nolen, 2012). In 2012, the Delhi High Court noted the Delhi police website's lack of functionality, calling it "completely useless" and "obsolete" (Nolen, 2012).

In the same vein, consider India's only Cyber Appellate Tribunal (CAT), which started functioning since 2006 (catindia.gov.in, 2014). It was reported in June 2014 that the tribunal had not adjudicated a single case during the previous three years due to the non-availability of the chairperson and judicial members (Singh, 2014).

Cybercrime awareness level is very low among the law-enforcement community.

For instance, it was reported that when a police officer was asked to seize the hacker's computer in an investigation of a cybercrime in India, he brought the hacker's monitor. In another cybercrime case, the police seized the CD-ROM drive from a hacker's computer instead of the hard disk (Aggarwal, 2009).

Overall, India is facing a severe shortage of

cybersecurity professionals which hampers the country's ability to fight rapidly rising cybercrime (Kshetri, 2016c). For instance, a large number of IT security auditors are needed to evaluate the adequacy of controls in the management of project and business processes and validate whether the controls are effective (Hettigei 2005). An estimate suggested that in 2013, India had only 60 auditors (Doval 2013). Regarding the requirement of government agencies to conduct security auditing of IT infrastructures, websites and applications, it is important to note that most Indian government agencies' websites are hosted by the National Informatics Centre (NIC), which was established by the GoI to promote IT culture among government organizations. It is argued that NIC-hosted websites are vulnerable to cyberattacks due to a shortage of manpower, especially IT security auditors. NIC outsources security audit works due to the lack of manpower. Likewise, in 2011, India's central bank, Reserve Bank of India (RBI) introduced a set of recommendations, which include the formation of separate information security groups within banks and maintenance of adequate cybersecurity resources based on their size and scope of operation. The country is finding it difficult to enforce the RBI guidelines due to the lack of IT security auditors to validate banks' cybersecurity practices (Bradbury 2013).

In India about 10% cybercrimes are reported. Of the reported crimes, about 2% are registered. The conviction rate is as low as 2% (Hindustan Times, 2006). For instance, while most BPOs in Gurgaon had been cybercrime victims about 70% of the respondents did not report to the police (indiatimes.com, 2011). Most organizations reported doubt about competence, professionalism and integrity of the police in handling cybercrime cases. About 50% of the respondents not reporting thought that the cases are not dealt with professionally and 30% noted that they had "no faith" in Gurgaon police (indiatimes.com, 2011).

In one way, there is a vicious circle: a) law enforcement agencies' unwillingness to put efforts for investigating cybercrimes and their technological illiteracy indicate that they lack the skills and capability to address cybercrime related offenses; b) the survey conducted among Gurgaon-based BPOs indicates that there are low cybercrime reporting rates because of the victims' lack of confidence in law enforcement agencies; and c) cybercriminals may become more confident, resourceful and powerful because their offenses are not reported.

As of 2006, no one charged for data fraud in India was convicted (Ribeiro, 2006). As of August 2009, only four people were convicted for cybercrime (Aggarwal, 2009). Until 2010, there was not a single cybercrime related conviction in Bengaluru, the biggest offshoring hub. The total number of convicted cases by 2010 was estimated at less than 10 (Narayan, 2010).

One reason behind the low rate of registration of cybercrime cases concerns the barriers, hurdles and hassles that confront the victims. In some cases, the police show unwillingness to take the extra work needed for the investigations (Narayan, 2010). There are reports that the police do not support the victim when they want to report a cybercrime case. Cybercrime victims have also complained that the police follow a long and inefficient process to build a criminal case (Anand, 2011).

3. Private Sector Initiatives and Market Mechanisms

Due to escalating cyber-threats, cybersecurity has become an area of increasing priority among enterprises in India. Cybersecurity is reported to account for 30-40% of most overall IT budgets in some Indian companies (Goswami, 2017).

Nonetheless, cybersecurity initiatives among

Indian firms have been hampered by insufficient investments. According to Gartner, Indian organizations spent US$882 million in 2013 in cybersecurity, which was expected to increase to US$953 million in 2014 and US$1.06 billion in 2015. Over half of the cybersecurity spending goes to consulting, implementation, support and managed services (TechTarget, 2014). As a point of comparison, China's cybersecurity spending is much higher, which is estimated to amount US$4.9 billion by 2015 (Kshetri, 2016b).

3.1. Hollow Internet Diffusion and Weak Cybersecurity Measures

The concept of "hollow diffusion" of the Internet among firms may help understand weak defense mechanisms (Otis and Evans 2003, p. 49). The basic idea behind "hollow diffusion" is simple: Many organizations digitizing their activities lack organizational, technological and human resources, and other fundamental ingredients needed to secure their system, which is the key for the long-term success of online businesses.

As to organizational resources, on the cybersecurity front, one key global trend in organizational structure involves the tendency to create the position of Chief Information Security Officer (CISO). For instance, a 2014 PwC survey found that only 28% of over 500 companies surveyed had a CISO or Chief Security Officer (Damouni 2014). CEOs and board often consult CISOs to understand cyber risk, implement appropriate security controls and promote a culture of defense. One study suggested that 90% of CISOs are connected directly to their organizations' top leadership team, and half of them were on the leadership team (Sweeney 2016). For instance, in India, except for few firms in banking, financial services and insurance, telecom, and business process outsourcing (BPO) it is rare to have a CISO in organizations (Pandya 2009).

On the human resources front, demand of cybersecurity professionals greatly exceeds supply. According to international data corporation (IDC), only 22,000 security professionals were available in the country by early 2012 whereas the country needed 188,000 (Saraswathy, 2012). An adviser to the Information Systems Audit and Control Association noted that India needs 300,000 cybersecurity professionals but there are about 30,000 such professionals (Gent, 2016). Citing a study by the Indian CERT, an indiatimes.com article reported that Indian organizations faced a shortage of about 400,000 trained cybersecurity professionals in 2013 (PTI, 2014).

On the technological front, unlike some developing countries, India lacks major anti-virus companies. For instance, Moscow-based Kaspersky Labs is among the world's biggest cybersecurity companies. Some other former second world economies also have top cybersecurity companies such as the Czech Republic's AVG Technologies, Romania's BitDefender and the Slovak Republic's ESET (Kshetri, 2011). Likewise, the Belarusian firm VirusBlokAda was the first company to identify the Stuxnet code in June 2010 (Borland, 2010). India's lack of high profile cybersecurity firms is related to the broader problems of the country's low R&D profile. Due to India's poor R&D and innovation performance, some liken economic activities in the Indian IT and offshoring industry to a "hollow ring." An Economist article notes: "India makes drugs, but copies almost all of the compounds; it writes software, but rarely owns the result. … [it has] flourished, but mostly on the back of other countries' technology" (Economist, 2007).

India's R&D profile is relatively lower compared to other BRIC economies. According to the World Bank, India had 100 researchers in R&D per million people in 2000 (the numbers for other BRIC economies were Brazil, 424; China, 548; and Russia,

3,451). Looking at more recent data, according to a report presented by Science and Technology Minister Kapil Sibal to the Rajya Sabha, the Upper House of the Indian Parliament, India had 156 researchers in R&D per million people in 2008. As a point of comparison, according to the World Bank, the corresponding numbers for other BRIC economies for 2008 were Brazil, 696; China, 1,199; and Russia, 3,152. Sibal suggested that universities in India were characterized by inferior R&D quality and capabilities (rediff.com, 2008). A related point is that much of the R&D in India is geared towards smaller projects that complement other innovation centres in Silicon Valley and other parts of the world (Economictimes, 2005). Moscow-based Kaspersky Lab's CEO and Chairman Eugene Kaspersky put the issue this way: " [Engineers in] China or India …are good if you just want something programmed, but if it's about research, then it has to be Russia" (Robinson, 1998).

The above said, there have been recent initiatives to accelerate startups in cybersecurity related areas. According NASSCOM, as of 2016, there were about 150 cybersecurity companies. A challenge has been limited access to funding for such startups. NASSCOM suggested that only 40% of cybersecurity companies had received funding from investors (Srivastava, 2016).

3.2. Underdeveloped Market for Cyber Insurance.

Market forces and mechanisms are evolving that may enhance firms' cybersecurity performances. For instance, the cyber liability insurance (data breach insurance) industry and market are are growing fast in industrialized economies (Kshetri, 2016b). A company is required to strengthen cybersecurity in order to buy coverage at a lower rate. A system that requires cybersecurity insurance thus raises cybersecurity S standards. That is, such insurance could help companies improve their cybersecurity S systems and put efforts to help secure policies (Business Insurance, 2014). Cyber liability insurance provides coverage for the theft or loss of first-party and third-party data. For the loss or theft of first-party data, an insurer may cover expenses related to notifying clients regarding the data breach, purchasing credit monitoring services for affected customers and launching a public relations campaign to restore the company's reputation. Third-party coverage includes claims related to unlawful disclosure of a third-party's information and infringement of intellectual property rights (IPR) (McGrayer, McGinnis, Leslie, and Kirkland, 2014).

India is regarded as an underdeveloped market for cyber liability insurance. Until as late as 2008, there was no insurance company in India that offered an anti-cybercrime policy for a company (Syed and D'monte, 2008). In the early 2017, insurers such as New India, National, ICICI Lombard, Tata AIG, HDFC Ergo and Bajaj Allianz offered cyber liability insurance (PTI, 2017). One estimate put the size of the Indian cyber liability insurance market in the range of US$14-19 million (PTI, 2016). The cyber-Insurance market is thus relatively small and immature.

3.3. The Information Technology-Business Process Management (IT&BPM) Sector

A key characteristic that distinguishes India from other developing countries is the well developing information technology-business process management (IT&BPM) sector. The sector is expected to exceed $155 billion by FY17 (Venkatesh, 2017). The IT&BPM sector is arguably an enclave economy in India. Call centers in India have already spread from big cities to intermediate towns, and even to small towns in rural areas. In this sense, this sector deserves special attention and should be a prominent subject of discussions in the context of cybersecurity.

Before proceeding further, it is important to stress that most high-profile and widely publicized cybercrimes in India are concentrated in the offshoring sector (Kshetri, 2010). The British Tabloid, Sun, reported that an Indian call center employee sold confidential information of 1,000 bank accounts to its reporter working as an undercover (tribuneindia.com, 2005; Hindustan Times, 2006). In another case, call center workers at Pune, India, subsidiary of Mphasis, a provider of outsourcing services, transferred about US $500,000 from four Citibank customers' accounts to their personal accounts (Schwartz, 2005; Fest, 2005). It was reported that in first- and second-tier cities, there are data brokers and data merchants, who buy data from people working in offshoring companies (Aggarwal, 2009). For instance, data frauds have been reported in call centers in Pune, Hyderabad, Bangalore, and Gurgaon. In a more recent case reported in March 2012, two "consultants", who claimed to be workers in Indian offshoring firms, met undercover reporters of The Sunday Times. They came with a laptop full of data and bragged that they had 45 different sets of personal information on about 500,000 UK consumers. The information included credit card holders' names, addresses, phone numbers, start and expiry dates and security verification codes. Data for sale also included information about mortgages, loans, insurance, phone contracts and television subscriptions (Gardner, 2012).

Unsurprisingly firms in the Indian IT&BPM sector are taking strong cybersecurity measures to prevent attacks on computers by current and former employees (Kshetri, 2013). This is due primarily to address their clients' fear that customer data will be stolen and even sold to criminals. For instance, call centre employees are required to undergo security checks which are considered to be "undignified" according to the Indian culture (The Economist, 2005). Firms have established biometric authentication controls for workers and banned cell phones, pens, paper and Internet/email access for employees for a long time (Fest, 2005). Computer terminals of firms in the IT&BPM sector (e.g., Mphasis) lack hard drives, email, CD-ROM drives, or other ways to store, copy or forward data (Engardio et al., 2004). Indian outsourcing firms also extensively monitor and analyze employee logs (Fest, 2005).

India's IT&BPM sector thus manages cybersecurity risk through effective industry self-regulation. A highly visible private-sector actor on this front is the National Association of Software and Services Companies (NASSCOM). NASSCOM was 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" (NASSCOM, 2017).

Owing to the rapid rise in data incidents, addressing cybersecurity issues has become increasingly important for the Indian IT&BPM sector's success and vitality. NASSCOM launched a registry of IT employees, which allows employers to perform background checks on existing or prospective employees (Hindustan Times, 2006). Creation of criminal and public records databases has been a part of the program (Fest, 2005).

In 2008, realizing the importance of an organization with an exclusive focus on data protection, NASSCOM established the Data Security Council of India (DSCI). The DSCI is 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.

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. Companies failing to secure their data may be fined as much as US $1 million. Noncompliant companies might also lose NASSCOM and DSCI membership.

NASSCOM and DSCI also help create awareness of the latest trends in cybercrime and cybersecurity. Security in cloud computing was one of the topics reviewed by the NASSCOM–DSCI Information Security Summit 2009 (http://www.dsci.in/events/about/225) and every annual summit since then. In the DSCI Best Practices meeting held in June 2011, issues related to data protection in cloud computing and compliance were discussed (Haran, 2011). In 2011, the 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 security and privacy issues in a cloud environment (Das, 2011).

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 U.S., Europe, Japan, China, South Korea and other countries. NASSCOM thus has a fairly high level of expertise and the financial resources to take various cybersecurity measures.

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." (thehindubusinessline.com 2007).

We noted above that India lacks major anti-virus companies. Recently NASSCOM and DSCI have taken various initiatives on this arena. During 2015-2016, the DSCI incubated 80 cybersecurity startups (Goswami, 2017).

4. Public–Private Partnership in Cybersecurity

In the context of developing countries such as India, cybersecurity is in a nascent stage. Like other economic sectors characterized by nascentness, cybersecurity exhibits an underdeveloped regulatory structure. There is 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 (Pughm, 1999).

But there is another point that is perhaps even more important. The way the Indian government is positioned does not 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 most the Indian population, data privacy and security are largely irrelevant.

Due to the above limitations, the resulting regulatory vacuum needs to be addressed by collaborative actions of the public and the private sector actors. A number of such efforts stand out in the context of India.

NASSCOM has engaged in advocacy and lobbying activities. In the mid-2000s, NASSCOM asked the Indian government to create a special court to try people accused of cybercrimes and other violations of the country's Information Technology Act (Ribeiro, 2006). NASSCOM has also established a CyberCop committee and a member of the committee serves as a technical advisor to the Indian CyberCrime Investigation Cell. NASSCOM works with police officers, lawyers, and industry bodies to ensure the enforcement of cybersecurity regulations. NASSCOM meets with bar councils in different cities to educate legal communities. It also educates police officers about cybersecurity and trains them to recognize and prosecute cybercrimes.

NASSCOM started working with Mumbai police since 2003 (Saravade & Saravade, 2007). NASSCOM helped police departments of cities such as Mumbai and Thane in establishing cybercrime units and providing training to officers. In 2005, NASSCOM announced a training initiative for Pune's cybercrime unit, which caught data crime perpetrators from Mphasis (Cone, 2005). A third cybercrime unit established in Bangalore in January 2007 has resources to train more than 1,000 police officers and other law-enforcement personnel annually. NASSCOM also offered to work with authorities in the U.K. and India to investigate cases involving identity theft (tribuneindia.com, 2005).

DSCI helped to establish cyberforensic labs in Mumbai, Bengaluru, Pune and Kolkata. As of the early 2012, DSCI had organized 112 training programmes on cybercrime investigation and awareness, which benefited about 3,700 police officials, judiciary and public prosecutors (Kshetri, 2013). As of 2014, there were eight Cyber Labs in various Indian cities, which provided training to over 28,000 police officers (DSCI, 2014).

Some PPP activities have been initiated by the government. Due to the country's lack of indigenous technology and patents related to cybersecurity, the GoI has announced that it would provide financial incentives to Indian firms to acquire foreign firms with high-end cybersecurity technology (Thomas, 2012). The Ministry of External Affairs would explore possible targets worldwide through Indian embassies and missions. The fact that Indian government agencies have been under cyber-attacks, suspected from foreign governments, has provided a major motivation for such an approach. An Indian company which owns the technology gained through the acquisitions is required to give the government agencies an access to the intellectual property rights (IPR).

5. Discussion and Implications

The Indian government severely lacks the resources to develop and enforce cybersecurity-related regulations, standards, and guidelines. Some have rightly labeled India's cybersecurity policy as "incomplete" and "all words and no action" (Desai, 2013) due to a lack of national cybersecurity action plan document or any guidelines regarding how the policy will be implemented. For instance, there is no clear action plan as to how the various goals proposed by the NCSP are going to be achieved. Overall, the NCSP lacks details of tangible actions and specific guidance, direction and procedures in

order to achieve the vision of a secure cyberspace. The director of Israel's Military and Strategic Affairs Program and director of the cyber-warfare program at the Tel Aviv University's Institute for National Security Studies (INSS) noted: "India has published its strategy .., but it is far away from what I call strategy ... It does not have the substance ... (and is) a very generic, high-level paper" (Alawadhi, 2014).

NASSCOM and DSCI have been exemplary self-regulatory bodies, playing key roles in strengthening the IT&BPM sector's cybersecurity orientation. They have 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.

Trade associations such as NASSCOM and DSCI 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 ((Dickson et al. 2004; Lawrence et al., 2001). 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.

Regarding the active and influential roles played by NASSCOM and DSCI, it is worth noting that the Indian economy and society are less centralized with more room for trade associations to flourish and to have a strong voice (Frankel, 2006). Since the 1990s, there has been a shift from a state-dominated economic policy framework towards 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 (Frankel, 2006). A strong mutual interdependence between the state and the private economic actors, particularly organized business groups, has developed very quickly.

The initiatives and responses of NASSCOM and DSCI can be considered to be the results of a hollow state and the thin institutions that hamper legislative and law enforcement efforts. For instance, India lacks standard identifiers like the U.S. Social security number making it difficult to check potential employees' backgrounds. It was reported that a thorough background check cost up to $1,000 per employee to (Schwartz, 2005). In response to the lack of such databases, in 2005, 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. Subsequently it was developed into the National Skill Registry (NSR), which allows employers to perform background checks on existing or prospective employees. It is a voluntary registry for call center employees.

6. Concluding Comments

Like other developing economies, India faces problems such as ineffective regulation, a lack of poorly trained law enforcement manpower and up-to-date technology. These factors have led to under-resourced and underdeveloped institutional capacity on the cyber front. As is the case of the rest of the world, India faces a severe shortage of cybersecurity professionals. This is among the key obstacle in addressing the growing cybercrimes in the country. A strong civil society has been recognized as a crucial feature of India's political development. This phenomenon has also allowed private-sector participants such as NASSCOM to play an important role in strengthening cybersecurity. Indeed, Indian offshoring industry provides a remarkable example of industry government collaboration in combating cybercrimes.

References

Aggarwal, V. (2009). Lead: Cyber crime's rampant, Express Computer, 03 August 2009. <http://www.expresscomputeronline. com/20090803/market01.shtml. Accessed 1 October 2009>

Alawadhi, N. (2014). Cyber security policy must be practical: Experts. <http://articles.economictimes.indiatimes.com/2014-10-22/news/55318902_1_cybersecurity-digital-india-national-cyber-security-policy>

Anand, J. (2011). Cybercrime up by 700% in Capital. http://www.hindustantimes.com/India-news/NewDelhi/Cyber-crime-up-by-700-in-Capital/Article1-766172.aspx

Blitz, J. (2011). Security: A Huge Challenge from China, Russia and Organised Crime. <http://www.ft.com/intl/cms/s/0/b43488b0-fe2a-11e0-a1eb-00144feabdc0.html#axzz1dnezI1eF>

Borland, J. (2010). A Four-Day Dive Into Stuxnet's Heart. <http://www.wired.com/threatlevel/2010/12/a-four-day-dive-into-stuxnets-heart/>

Bradbury, D. (2013). India's Cybersecurity challenge. <http://www.infosecurity-magazine.com/view/34549/indias-cybersecurity-challenge/>

Business Insurance. (2014). N.Y. state financial regulator will focus on cyber security. <http://www.businessinsurance.com/article/20140923/NEWS07/140929962?tags=|338|299|69|80|83|302|303>

catindia.gov.in (2014). History, September 22, <http://catindia.gov.in/History.aspx, Cyber Appellate Tribunal, Government of India>

cio.de (2014). India's biometric ID project is back on track, <http://www.cio.de/index.cfm?pid=156&pk=2970283&p=1>

Damouni, N. (2014). Exclusive: U.S. companies seek cyber experts for top jobs, board seats, May 30. Reuters. <http://www.reuters.com/article/us-usa-companies-cybersecurity-exclusive-idUSKBN0EA0BX20140530>

Das, G. (2011). Panel to Advise Govt, IT cos on Cloud Security on the Cards. <http://www.financialexpress.com/news/Panel-to-advise-govt—IT-cos-on-cloud-security-on-the-cards/809960/>

Das, S. (2017). 11,592 cases of cyber crime registered in India in 2015: NCRB. <http://www.livemint.com/Politics/ayV9OMPCiNs60cRD0Jv75I/11592-cases-of-cyber-crime-registered-in-India-in-2015-NCR.html>

Desai, V.V. (2013). Is India's cyber policy all words and no action? <http://searchsecurity.techtarget.in/news/ 2240 207148/Is-Indias-cyber-policy-all-words-and-no-action>

Deshpande, S. (2009, October 28) New cyber law casts its net wide. The Economic Times. <http://economictimes.indiatimes.com/infotech/internet/New-cyber-law-casts-its-net-wide-/articleshow/5170897.cms>

Dickson, M., BeShers, R., Gupta, V. (2004). 'The impact of societal culture and industry on organizational culture: Theoretical explanations', Culture, leadership, and organizations: the GLOBE study of 62 societies, Robert J. House, Paul J. Hanges, Mansour Javidan, Peter W. Dorfman, and Vipin Gupta (eds) Thousand Oaks, Calif. : Sage Publications.

DNA (2017). Irdai asks insurers to appoint data security officer by April 30. DNA Daily News & Analysis. <http://www.dnaindia.com/money/report-irdai-asks-insurers-to-appoint-data-security-officer-by-apr-30-2391043>

Doval, P. (2013). Govt orders security audit of IT infrastructure. <http://timesofindia.indiatimes.com/tech/tech-news/Govt-orders-security-audit-of-IT-infrastructure/articleshow/38398644.cms>

DSCI. (2014). Cyber Labs, <http://www.dsci.in/cyber-labs>

Duggal, P. (2004). What's wrong with our cyber laws? <http://www.expresscomputeronline.com/20040705/newsanalysis01.shtml>

Economictimes. (2005). R&D in India: The Curtain Rises, the Play Has Begun. <http://economictimes.indiatimes.com/rd-in-india-the-curtain-rises-the-play-has-begun/articleshow/1207024.cms>

Economictimes. (2012). Cyber Crime Increasing in India at Fast Clip: P. Chidambaram.<http://economictimes.indiatimes. com/tech/internet/cyber-crime-increasing-in-india-at-fast-clip-p-chidambaram/articleshow/11891033.cms>

Economist. (2007). Imitate or Die; Technology in China and India, 385(8554): 9.

Engardio, P., Puliyenthuruthel, J., & Kripalani, M. (2004). Fortress India? Business Week, 3896, 42–43.

Fest, G. (2005). Offshoring: Feds take fresh look at India BPOs; Major theft has raised more than a few eyebrows. Bank Technology News, 18(9), 1.

Frankel, R. (2006). Associations in China and India: An Overview, European Society of Association Executives. <http://www.esae.org/articles/2006_07_004.pdf>

Gardner, T. (2012). Indian Call Centres Selling Your Credit Card Details and Medical Records for Just 2p. <http://www.dailymail.co.uk/news/article-2116649/Indian-centres-selling-YOUR-credit-card-details-medical-records-just-2p.html>

Gent, E. (2016). Lack of cybersecurity expertise could derail 'Digital India' initiative, Tech Wire Asia <http://techwireasia.com/2016/08/lack-cybersecurity-expertise-digital-india/#iyi6YSKdmJ4eeotO.97>

Goswami, S. (2017). India's Cyber Security Startups Are Gaining Traction, Thanks To Demonetization, Forbes. <https://www.forbes.com/sites/suparnagoswami/2017/02/02/indias-cyber-security-startups-are-gaining-traction-thanks-to-demonetization/#e9dc12e58261>

Haran, V. (2011). Insider Threats a Major Concern for India Inc: DSCI–PwC Study.<http://searchsecurity.techtarget. in/news /2240037365/Insider-threats-a-major-concern-for-India-Inc-DSCI-PwC-study>

Hettigei, N.T. (2005). The Auditor's role in IT development projects. <http://www.isaca.org/Journal/Past-Issues/2005/Volume-4/Pages/The-Auditors-Role-in-IT-Development-Projects1.aspx>

Hindustan Times. (2006). Securing the web.

Hindustan Times. (2009). Wired for trouble. <http://www.tmcnet.com/usubmit/2009/10/24/4442635.htm>

indiatimes.com. (2011). Most Gurgaon IT, BPO companies victims of cybercrime: Survey, November 6, <http://timesofindia.indiatimes.com/city/gurgaon/Most-Gurgaon-IT-BPO-companies-victims-of-cybercrime-Survey/articleshow/10626059.cms>

indolink.com. (2012). India Battles Against Cyber Crime. <http://www.indolink.com/displayArticleS.php?id=102112083833>

Internet Crime Complaint Center (2011). 2010 Internet Crime Report. <http://www.ic3.gov/media/annualreport/2010_ic3report.pdf>

KPMG. (2014).Cybercrime survey report 2014, Retrieve from www.kpmg.com/in

Kshetri, N. (2010). The Global Cyber-crime Industry: Economic, Institutional and Strategic Perspectives, Springer-Verlag: New York, Berlin and Heidelberg.

Kshetri, N. (2011). Kaspersky Lab: From Russia with Anti-virus, Emerald Emerging Markets Case Studies, 1(3): 1–10.

Kshetri, N. (2013). Cybercrime and Cybersecurity in the Global South, Palgrave Macmillan: Houndmills, Basingstoke, U.K.,

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

Kshetri, N. (2015b). Cybercrime and Cybersecurity Issues in the BRICS Economies. Editorial, Journal of Global Information Technology Management, JGITM, 18(4), 1-5.

Kshetri, N. (2016c). Cybersecurity and Development. Markets, Globalization & Development Review, 1(2), Article 3: <http://digitalcommons.uri.edu/mgdr/vol1/iss2/3>

Kshetri, N. (2016d). Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future. Crime, Law and Social Change, 66 (3), 313–338.

Kshetri, N. (2016a). Big Data's Big Potential in Developing Economies: Impact on Agriculture, Health and Environmental Security. Centre for Agriculture and Biosciences International (CABI) Publishing, Wallingford, Oxon, the U.K.

Kshetri, N. (2016b). The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies, Springer-Verlag: New York, Berlin and Heidelberg.

Lawrence, T. B., Winn, M. I., Jennings, P. D. (2001). 'The Temporal Dynamics of Institutionalization', The Academy of Management Review, 26(4): 624-644.

McGrayer, McGinnis, Leslie, and Kirkland (2014). What is Cyber Liability Insurance? The National Law Review. <http://www.natlawreview.com/article/what-cyber-liability-insurance>

Narayan, V. (2010). Cyber Criminals Hit Esc Key for 10 yrs. <http://timesofindia.indiatimes.com/city/mumbai/Cyber-criminals-hit-Esc-key-for-10-yrs/articleshow/6587847.cms>

NASSCOM (2017). Vision and Mission. <http://www.nasscom .in/vision-and-mission>

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

Otis, C. and Evans, P. (2003). The Internet and Asia-Pacific Security: Old Conflicts And New Behavior. Pacific Review, 16 (4), 549–550.

Pandya, D. (2009). CISO reporting to board of directors: Myth or for real? <http://www.computerweekly.com/news/1375176/CISO-reporting-to-board-of-directors-Myth-or-for-real>

PTI (2014). Shortage of over a million cyber security experts globally, The Economic Times.<http://economictimes.indiatimes.com/tech/internet/shortage-of-over-a-million-cyber-security-experts-globally/articleshow/29110114.cms?intenttarget=no>

PTI (2016). Cyber insurance premium rates increase after debit cards hack, BGR. <http://www.bgr.in/news/cyber-insurance-premium-rates-increase-after-debit-cards-hack/>

PTI (2017). Banks rush to buy cyber security cover as digital payments rise, The Times of India. <http://timesofindia.

indiatimes.com/business/india-business/banks-rush-to-buy-cyber-security-cover-as-digital-payments-rise/articleshow/57109647.cms>

Pughm, C. (1999) Getting Good Government: Capacity Building in the Public Sectors of Developing Countries," Urban Studies, 36, 2, pp. 400–402.

rediff.com (2008). Researchers? Only 156 per Million in India. <http://www.rediff.com/money/2008/mar/12rnd.htm>

Ribeiro, J. (2006). India's Nasscom calls for special cybercrimes court. Network World. <http://www.networkworld.com/news/2006/090706-indias-nasscom-calls-forspecial.html>

Ribeiro, V. J. (2014). India's biometric ID project is back on track. CIO. <http://www.cio.de/index.cfm?pid=156&pk=2970283&p=1>

Robinson, G.E. (1998), Elite cohesion, regime succession and political instability. Syria Middle East Policy, 5 (4), 159-79.

Saraswathy, M. (2012). Wanted: Ethical Hackers. <http://www.wsiltv.com/news/three-states/Protect-Yourself-from-Cyber-Crime-139126239.html>

Saravade, P., & Saravade, N. (2007). A public-private partnership in India: Broken windows in cyberspace. The Police Chief, 74(3), 16.

Shaftel, D. and Narayan, K. (2012). Call Centre Fraud Opens New Frontier in Cybercrime. <http://www.livemint.com/2012/02/26225530/Call-centre-fraud-opens-new-fr.html>

Singh, S.R. (2014). India's only cyber appellate tribunal defunct since 2011, Retrieve from <http://www.hindustantimes.com/india-news/india-s-only-cyber-appellate-tribunal-defunct-since-2011/article1-1235073.aspx>

Srivastava, M. (2016). India to promote indigenous expertise in cyber security, to fund start-ups, Business Standard. <http://www.business-standard.com/article/companies/india-to-promote-indigenous-expertise-in-cyber-security-to-fund-start-ups-116101300028_1.html>

Sweeney, B. (2016). Cybersecurity Is Every Executive's Job. Harvard Business Review. September 13. <https://hbr.org/2016/09/cybersecurity-is-every-executives-job>

Syed, F., & D'monte, L. (2008). India lags in cybercrime insurance. <http://www.rediff.com/money/2008/apr/07cyber.htm>

Schwartz, K. D. (2005). The background-check challenge. InformationWeek, 59–61.

TechTarget (2014). Indian businesses wake up to IT security risks, Computer Weekly. <http://www.computerweekly.com/news/2240225781/Indian-businesses-wake-up-to-IT-security-risks>

The Economist. (2005). Business: Busy Signals; Indian Call Centres, The Economist, 376(8443): 66.

thehindubusinessline.com. (2007). Regulator Soon for Monitoring Data Security Standards. 24 Apr. 2007. <www.thehindubusinessline.com/todays-paper/regulator-soon-for-monitoring-data-security-standards/article1656182.ece>

Thomas, T.K. (2012). Govt will help fund buys of foreign firms with high-end cyber security tech, <http://www.thehindubusinessline.com/industry-and-economy/info-tech/article3273658.ece?homepage=true&ref=wl_home>

tribuneindia.com. (2005). Outsourcing crime Call centre expose can wreak havoc. <http://www.tribuneindia.com/2005/20050625/edit.htm>

Venkatesh, S. (2017). Indian IT-BPM industry clocks growth rate of 8.6 percent in FY2017: NASSCOM. Forbes India. <http://www.forbesindia.com/article/special/indian-itbpm-industry-clocks-growth-rate-of-8.6-percent-in-fy2017-nasscom/45951/1>

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