Sovereign Data

THESIGERS

India’s cybersecurity challenge

India’s sluggish cybersecurity policy needs timely intervention to preserve its market leadership in global information technology services.

Citation: “India’s cybersecurity challenge,” *Sovereign Data* Vol. 2, No. 4 (April 2016).

Keywords: CYBERSECURITY, DIGITAL INDIA, INDIA, NATIONAL CYBER SECURITY POLICY, NATIONAL E-GOVERNANCE PLAN
--
Explanation of dates:
Drafted: 2016-04-05
Information cut-off: 2016-04-05
Published: 2016-04-14

On 1 July 2015, Indian Prime Minister Narendra Modi launched the national ‘Digital India’ programme, giving Indian citizens and businesses the ‘power to empower’ themselves and the country in the new global knowledge economy.[1] This would build on the National e-Governance Plan (2006) to promote growth in the digital sector and deliver connectivity benefits across Indian society and government. In his inaugural remarks, Modi identified the need to secure India from the ‘bloodless war’ of cyberwarfare and cybercrime threatening the integrity of online commerce and social exchange.[2] The appeal to cybersecurity rang slightly hollow to some experienced ears. Melissa Hathaway, the former director of the US Joint Interagency Cyber Task Force and a sitting Commissioner for the Global Commission on Internet Governance, suggested that the rhetoric accompanying the Digital India initiative did not reflect the reality of Indian cybersecurity efforts.[3] It is a conclusion that aligns with persistent criticisms of India’s undercooked approach to cybersecurity.

Sovereign Data explores Indian national cybersecurity and reports on the challenges and prospects of providing cybersecurity to 1.3 billion citizens and the world’s seventh-largest economy.

Governance: a stuttering start

In July 2013, India published its first National Cyber Security Policy (NCSP).[4] The NCSP aimed ‘to build a secure and resilient cyberspace for citizens, businesses and Government.’ Its 14 objectives stressed a conventional range of cybersecurity, information assurance and regulatory goals and incentives, plus ambitions to boost the indigenous cybersecurity industry through innovation and recruitment. Opinions differ as to the reasons for the specific timing of the NCSP. The 2013 Snowden disclosures, particularly regarding a National Security Agency program called Boundless Informant, may have played a part.[5] Adverse Indian reactions to US mass surveillance of Indian internet traffic undercut progress made under a 2011 US-India Memorandum of Understanding on cyber cooperation and information exchange.[6] It is equally likely that India’s status as a global provider of IT services and business process outsourcing (BPO) had attracted growing domestic and international pressure to address outstanding cybersecurity issues. In particular, new legislation might be necessary to supersede elements of the creaking and controversial Information Technology Act (2000, amended 2008), not least its inability to meet global information security and data protection standards.[7]

The NCSP was a statement of first principles, rather than a blueprint for progress, but its implementation has been uneven at best. Lack of political will, an under-resourced public sector, and an over-reliance on industry self-regulation have combined to complicate further the challenges facing government in securing India’s enormous information infrastructure. Further policy and legislative moves have proven difficult too. A draft National Encryption Policy was withdrawn in September 2015 in the face of public concern it would criminalise ordinary users of social media applications like Facebook and WhatsApp.[8] The NCSP has yet to be integrated with

Sovereign Data is a journal of data, politics, and risk in emerging markets.

Editor: Michael A. Innes
Author: Tim Stevens

ISSN: 2059-075X

For more information on the subject of this report, or to subscribe to our services, contact us at:

Office: 37 Great Russell Street,
London, WC1B 3PP, England.

Phone (UK): +44 (0)134 430 6541
Email: enquiries@thesigers.com
Web: thesigers.com

“Thesigers” is a trading name of Thesiger & Company Limited.

Company registered in England and Wales. Registration number: 7234402. VAT number: 135658985.

National Security Policy. A promised Cyber Crisis Management Plan has not materialised to coordinate multiple-agency responses to major cyber incidents. There have been minor successes, such as the March 2015 appointment of a new National Cyber Security Coordinator.[9] Soon after, government green-lit the 'nodal agency' for cybersecurity identified in the NCSP, although this National Cyber Coordination Centre (NCCC) is not yet operational.[10]

Infrastructure: an uneven landscape

Since 2004, the Indian Computer Emergency Response Team (CERT-In) has provided monitoring, analysis and guidance on cybersecurity incidents to the Indian ICT community.[11] CERT-In has no remit to prosecute counter-measures against cyber attackers, however, and it was not until 2015 that the National Critical Information Infrastructure Protection Centre (NCIIPC) was created to cooperate with security agencies and the private sector in this field.[12] The NCIIPC sits within the National Technical Research Organisation (NTRO), a technical intelligence agency that reports directly to the National Security Adviser, and which has been accused of hacking Indian citizens' phones and the networks of sister agencies.[13]

Government regulation is weak and much regulatory activity is conducted by industry bodies such as the National Association of Software and Services Companies (NASSCOM), founded in 1988 to promote trust and innovation in the Indian software industry.[14] In 2008, NASSCOM bolstered its activities by creating the Data Security Council of India (DSCI) to further encourage compliance with standards and best practice in data protection. Together, NASSCOM and DSCI are considered effective self-regulatory entities and have improved Indian cybersecurity significantly. They have also been instrumental in developing one of the pillars of cybersecurity, constructive public-private partnerships (PPPs) between the private sector, law enforcement and government agencies.[15] Absent higher-level institutional buy-in to PPPs – highlighted by the NCSP but so far under-developed – NASSCOM and other industry bodies continue to be influential brokers of improved cybersecurity concepts and practice.

Lack of political will, an under-resourced public sector, and an over-reliance on industry self-regulation have combined to complicate further the challenges facing government in securing India's enormous information infrastructure.

Another challenge to Indian cybersecurity capacity consists in attracting sufficient numbers of qualified individuals to public- and private-sector cybersecurity careers, a problem shared with countries further along in cybersecurity development, including the US and UK. In 2013, a leaked report by the National Security Council Secretariat (NSCS) recorded that India could call on only 556 government cybersecurity experts.[16] In stark contrast to the many thousands employed by the US, Russia and China, the NSCS considered this 'grossly inadequate'. The government responded by announcing a drive to recruit over 4000 experts across six government agencies with principal cybersecurity responsibilities.[17] The private sector is struggling similarly. The 2013 NCSP identified the need to recruit an additional half a million cybersecurity professionals by 2018, but NASSCOM projects the 2019 shortfall to be some 1.5 million.[18]

Stakeholders: interconnection and interdependency

The NSCP was correct to identify a wide range of government, civil, military and commercial stakeholders, all of whom rely on cybersecurity to provide and consume goods and services safely and efficiently. The NCSP was also correct to note the absence of clear boundaries around these groups, making the task of cybersecurity ever more complex as these interconnections and interdependencies grow and intensify. This requires robust solutions to inter-agency and multiple-stakeholder operations that the National Cyber Coordination Centre (NCCC) will help to encourage once established. Also of concern is India's military cyber posture, which is currently poorly defined and inhibits clarity of communications between India and its allies, not to mention potential adversaries like Pakistan.[19] India has taken part in a number of bilateral initiatives aimed at information-sharing, confidence-building and training, including, in the last year alone, with UK, Australia, China, Malaysia and Singapore. Importantly, it is repairing relations with the US, notably through the ongoing US-India Cyber Dialogue series.[20]

Perhaps India's biggest challenge is to enact cybersecurity policy and legislation that preserves its international standing as a trustworthy location for ICT outsourcing and services. India's long domination of offshore business processing and software development has been predicated on plentiful supplies of cheap labour. Automation threatens to erode this market advantage and, in order to keep attracting enterprise-level clients, India needs more than ever to demonstrate its ICT infrastructure and operations meet global cybersecurity standards and expectations. The many ICT multinationals working in India, and Indian companies themselves – all of whose business depends on effective cybersecurity – have worked closely with groups like NASSCOM to promote better practice and cybersecurity investment. However, the Indian government must also find ways to further enable the domestic and international partnerships this situation demands.

Another challenge to Indian cybersecurity capacity consists in attracting sufficient numbers of qualified individuals to public- and private-sector cybersecurity careers, a problem shared with countries further along in cybersecurity development, including the US and UK.

Conclusion

Many of the challenges facing Indian cybersecurity will resonate with the south Asian nation's international partners, particularly the torpor that afflicts all large bureaucracies, compounded by serious skills shortages. Initiatives announced in countries like the UK – the forthcoming National Cyber Security Centre in London, for instance – have taken some time to stand up. The specific criticism made of India is that it is taking too long to align practice and policy with stated aspirations. This will not be news to the Indian government and it is probably better aware than most of an additional cybersecurity challenge: the sheer scale of effective national-level policy change for a country of 1.3 billion people.

Allocating finite public resources always requires difficult decisions and not all constituencies will be satisfied with all policy outcomes. As befits an environment that touches so many aspects of society and economy, the security of cyberspace is similarly the need and responsibility of a bewildering array of technologies and organisations, all of which need to pull together towards common goals. This is as true in Uruguay or the United States as it is in India but no less difficult or daunting for it.

Most governments recognise that cybersecurity is a double-edged proposition. Get it right and cybersecurity can protect state and society, as well as being a driver of economic growth. Get it wrong and poor cybersecurity threatens prosperity and well-being. India has a unique opportunity to draft detailed and appropriate cybersecurity policy to propel it forwards as a world-leading economy. Which path will India take?

HOW TO SUBSCRIBE

Sovereign Data is published monthly and distributed direct to subscribers via email as a PDF attachment. Subscribers to the Reporting Service benefit from daily, weekly and monthly reporting and analysis.

Thesigers defines “sovereign” and “data” broadly, in order to more fully understand the risks and opportunities associated with knowledge in all its tributary forms – “information”, “data”, “evidence”, “intelligence”, and so on.

Thesigers’ view of sovereign data is that it contains essential elements of substance and form, of context and meaning – original, often perishable artefacts about people, places, events, issues and things.

Monthly Journal

Thesigers’ monthly journal, *Sovereign Data*, provides short, digestible analysis of the state of the information environment. Each monthly issue focuses on a single, current topic selected by Thesigers staff, given additional context and assessed for relevance and impact.

Reporting Service

Thesigers’ reporting service tracks current developments in sovereign data. Intended for clients who need more frequent, detailed updates, the service features summary reports and briefings based on locally-sourced news, data analytics, risk indexes and regular assessment.

Research and Development

Thesigers’ conducts ongoing research and development through a sense-making program of workshops, system design and technology innovation. Workshops investigate problems covered in our reporting and analysis. Our systems and technology work creates working solutions to them.

For more information on the subject of this report, or to subscribe to our services, contact us directly at:

Email: subscriptions@thesigers.com
Phone (UK): +44 (0)134 430 6541

Notes

1. http://www.digitalindia.gov.in/. [Accessed 5 April 2016.]
2. ‘Digital India: PM Modi says India can play a big role in cyber security globally’, NDTV, 2 July 2015, http://www.ndtv.com/india-news/digital-india-pm-modi-says-india-can-play-a-big-role-in-cyber-security-globally-777319. [Accessed 5 April 2016.]
3. ‘Digital India must focus more on cyber-security’, The Times of India, 1 October 2015, http://timesofindia.indiatimes.com/city/bengaluru/Digital-India-must-focus-more-on-cyber-security/articleshow/49179988.cms. [Accessed 5 April 2016.]
4. Ministry of Communications and Information Technology, National Cyber Security Policy-2013, July 2013.
5. ‘Boundless Informant: the NSA’s secret tool to track global surveillance data’, The Guardian, 11 June 2013, http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining. [Accessed 5 April 2016.]
6. US Department of Homeland Security, ‘United States and India sign cybersecurity agreement’, 19 July 2011, https://www.dhs.gov/news/2011/07/19/united-states-and-india-sign-cybersecurity-agreement. [Accessed 5 April 2016.]
7. Pavan Duggal, ‘Why 2015 was a landmark year for Indian cyberlaw’, Huffington Post, 4 January 2016, http://www.huffingtonpost.in/pavan-duggal-/2015-a-landmark-year-for-_b_8898122.html. [Accessed 5 April 2016.]
8. ‘National Encryption Policy draft withdrawn: 13 things to know’, The Times of India, 22 September 2015, http://timesofindia.indiatimes.com/tech/tech-news/National-Encryption-Policy-draft-withdrawn-13-things-to-know/articleshow/49056912.cms. [Accessed 5 April 2016.]
9. ‘Gulshan Rai becomes first chief of cyber security’, The Economic Times, 4 March 2015, http://economictimes.indiatimes.com/news/politics-and-nation/gulshan-rai-becomes-first-chief-of-cyber-security-post-created-to-tackle-growing-e-threats/articleshow/46449780.cms. [Accessed 5 April 2016.]
10. ‘Government clears setting up of National Cyber Coordination Centre’, The Economic Times, 9 April 2015, http://economictimes.indiatimes.com/news/defence/government-clears-setting-up-of-national-cyber-coordination-centre/articleshow/46864939.cms. [Accessed 5 April 2016.]
11. http://www.cert-in.org.in/. [Accessed 5 April 2016.]
12. ‘The deadly new age war’, The Hindu, 23 June 2015, http://www.thehindu.com/opinion/op-ed/the-deadly-new-age-war/article7342982.ece. [Accessed 5 April 2016.]
13. ‘NTRO hacking email IDs of officials, says govt’s IT dept’, The Indian Express, 22 April 2013, http://archive.indianexpress.com/news/ntro-hacking-email-ids-of-officials-says-govts-it-dept/1105875/. [Accessed 5 April 2016.]
14. Nir Kshetri, ‘India’s cybersecurity landscape: the roles of the private sector and public-private partnership’, IEEE Security & Privacy 13, no. 3 (2015): 16-23.
15. Kshetri, ‘India’s cybersecurity landscape’.
16. ‘An IT superpower, India has just 556 cyber security experts’, The Hindu, 19 June 2013, http://www.thehindu.com/news/national/an-it-superpower-india-has-just-556-cyber-security-experts/article4827644.ece. [Accessed 5 April 2016.]
17. Ministry of Defence; NTRO; Department of Electronics and Information Technology (DeitY); Intelligence Bureau (IB); Dept of Telecommunications (DoT); Defence Research and Development Organisation (DRDO).
18. ‘IT industry faces shortage of 1.5 million IT security pros: Nasscom’, The Times of India, 18 June 2015, http://timesofindia.indiatimes.com/tech/tech-news/IT-industry-faces-shortage-of-1-5-million-IT-security-pros-Nasscom/articleshow/47721984.cms. [Accessed 5 April 2016.]
19. Muhammad Baqir Malik, ‘Pakistan and India cyber security strategy: a comparative analysis’, Defence Journal 17, no. 11 (2014): 59.
20. Jonathan Reiber and Eli Sugarman, ‘Opinion: Deeper India, US ties should include cybersecurity, too’, The Christian Science Monitor, 9 March 2016, http://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/0309/Opinion-Deeper-India-US-ties-should-include-cybersecurity-too./ [Accessed 5 April 2016.]