The PoliceChief
The Professional Voice of Law Enforcement

send to a friend

Broken Windows in Cyberspace

By Pradnya Saravade, Indian Police Service, Additional Commissioner of Police, Anticorruption Bureau, and Nandkumar Saravade, Indian Police Service, Director, Cybersecurity and Compliance, NASSCOM, Mumbai, India

Cyberspace has been found to be less law-abiding than the real world. In India, there is a need to help police investigators acquire the skills to detect and prosecute computer crimes. This is in tune with the approach of mending broken windows in real-world policing.[1] The collaboration of different stakeholders will facilitate this process and prevent larger cybercrimes by attending to smaller ones.

Quick Facts
Republic of India

Size:
Slightly more than one-third the size of the United States

Population:
1,095,352,995 (July 2006 estimate)

Median age:
24.9 years

Gross domestic product:
U.S.$4.042 trillion (2006 estimate)

Government administrative divisions:
28 states and seven union territories

India is capitalizing on its large number of well-educated people skilled in the English language to become a major exporter of software services and software workers.

Source: https://www.cia.gov/cia/publications/factbook

The phenomenon of globalization has been one of the remarkable developments in the last few decades. The International Monetary Fund (IMF) defines globalization as "a historical process, the result of human innovation and technological progress . . . the increasing integration of economies around the world, particularly through trade and financial flows . . . [and] the movement of people (labor) and knowledge (technology) across international borders."[2]

The process of informational globalization has flattened the world.[3] India, like other countries in the world, has profited from this mutually beneficial trend of globalization, with its information technology (IT) sector growing rapidly. In India this sector continues to chart remarkable double-digit growth and is expected to exceed U.S. $36 billion in annual revenue in fiscal year 2005–2006, an increase of nearly 28 percent over the previous fiscal year.[4] The bulk of this revenue is expected to come from software and services export and has the potential of reaching U.S.$60 billion by 2010.[5]

One of the key concerns arising from the use of information technology is the perception of the security and privacy of the information. This is especially true of outsourced data processing. A survey done by Booz Allen Hamilton[6] concluded that companies perceive a significantly higher security risk in working with offshore providers over those in the United States, due to a lack of trust in legal and regulatory environments in developing countries, and that providers with operations in Asia and South America are particularly challenged by the perception gap. The study also revealed that just 5 percent of respondents believed that China has a strong regulatory and legal infrastructure, followed by South America (6 percent) and Southeast Asia (11 percent). India fared slightly better, in that 27 percent of respondents believed that India has a robust legal infrastructure.

The domestic use of IT in India is exploding. The trading of securities in the stock market is entirely in dematerialized form now, through online bidding and negotiations. Most banks have switched over to computerized core operations. Banks are pushing credit cards at customers at a furious pace. The booming air transport sector is using IT aggressively to drive down costs. The changing technological scenario is most spectacularly seen in the growth of telephony in India. The total number of phone lines stood at 183.46 million at the end of November 2006, of which 78 percent were mobile phone lines. The growth is expected to continue; it could reach 250 million users this year[7] and 500 million by 2010.[8]

The Four-E Initiative for Data Security

Engagement—with the key stakeholders

Enactment—of laws and regulations to provide essential legal framework

Education—by companies, industries, and consumer groups

Enforcement—best practices in security, focusing on people, processes, and technologies

The Logic of Cybersecurity

NASSCOM (the National Association of Software and Service Companies) is a premier trade body of IT companies in India. Its roughly 1,050 members account for an estimated 95 percent of Indian software revenue. NASSCOM has been working closely with the business process outsourcing (BPO) industry to create an information security culture in these segments, with the realization that the export-driven growth of the Indian IT industry is critically dependent on India's reputation as a safe place for data processing.

NASSCOM has also been interacting with the Indian government on the issue of creating a relevant regulatory environment that will further strengthen information security initiatives being rolled out in ITESBPO[9] organizations. NASSCOM seeks to deal with the problem of data security in India through its Trusted Sourcing Initiative, encompassing the four-E framework: engagement (with the key stakeholders nationally and internationally to understand and work on the key concerns); enactment (of the right laws and regulations to provide the essential legal framework); education (projects for the member companies, the user industry, and the consumer groups within the country); and enforcement (of best practices in security using the risk management approach focusing on people, processes, and technologies).

One of the important aspects of improving the information security infrastructure in India is strengthening the capacity of Indian law enforcement to understand the new economic environment and the emerging crimes and deal with the crime effectively. Any serious information security incident will become a concern of the local police organization first.

With this understanding, NASSCOM started working with Mumbai police in 2003 through a mass awareness campaign called the Cyber Safety Week. This awareness campaign informs computer users about the inherent risks with the technology, especially the Internet infrastructure, and how they could protect themselves against the risks. The important assumption in stressing prevention as the main approach is that cybercrime investigation is an expensive and reactive response and, although one cannot replace the other, the resources are more effectively used in educating the end-users.

Cyber Safety Week

The first Cyber Safety Week (CSW), held August 18–23, 2003, had the following salient features:

- Leading technology authorities participating in public meetings and speaking about better security

- Personalities from India's thriving and popular movie industry visiting colleges to generate interest in cybersecurity among young people and the media
- Ethical hackers conducting technology demonstrations about the risks of uninformed use of information technology
- Senior police officers visiting colleges to tell young people about the support police can provide to the victims of cybercrime

The second Cyber Safety Week, celebrated August 23–28, 2004, saw a shift in focus to make it more relevant to online commerce and financial activities.[10] A digital videoconference on cyberterrorism with an expert from the U.S. Federal Bureau of Investigation, under the auspices of the local U.S. consulate, added an international dimension to Cyber Safety Week, which also featured special events for parents, senior government officials, and prosecutors. An all-India seminar brought together chiefs of investigation of different states in India to discuss trends in technology crime.

The third Cyber Safety Week, November 21–26, 2005, like the 2003 and 2004 events, featured innovative ways of reaching out to the target audience, such as banners on bus shelters, newspaper advertisements, posters and handbills, IRC[11] for ethical hackers, technology demonstrations, television programs featuring the city police chief, and radio phone-in programs. Partner organizations included the Computer Society of India, All India Association of Industries, Federation of Indian Chambers of Commerce, Bombay Stock Exchange, Indian Merchants' Chamber, Mumbai University, and Indian Banks' Association.

An important feature of the third Cyber Safety Week was the introduction of the India Cyber Cop Award 2005 for the best-investigated cybercrime case in the country. The objective was to stimulate interest among investigators in this new field of expertise, recognize good work, and promote excellence. In all, 16 entries arrived from different police departments and a panel of judges picked the winners. Subsequently, all these cases were published as a compendium[12] for the benefit of investigators, lawyers, security professionals, and consultants. The next version of the award will see more categories and a more elaborate presentation format, culminating in a workshop for the participants.

NASSCOM has taken this model of involving the common Internet users in improving cybersecurity to other major IT centers in India, and the first such exercise took place in Hyderabad, capital of the state of Andhra Pradesh in July 2006. Chennai, in the state of Tamil Nadu, is scheduled to host a similar exercise early in 2007.

The Genesis and Progress of India Cyber Lab

The support extended by the IT industry during the first CSW saw a surplus of unspent financial sponsorship support that was then available for other activities. This resource helped provide training on technology crime investigations for the police field investigators. Because the use of computers by police in India is comparatively uncommon, the curriculum included training in the basics of computer systems.

The training facility, called the Mumbai Cyber Lab, was set up in World Police Station in Mumbai, which is home to more than 2,000 police investigators, and started training in March 2004. NASSCOM engaged a project manager and two instructors as technical staff. Mumbai police assigned an officer with experience in investigating technology crime as the project administrator. The technical staff, assisted by several volunteers, covers topics on the technology behind computers and the Internet. The project administrator instructs on the legal and procedural aspects of investigation. The duration of the program is six days. The syllabus covers the basics of computers and the Internet, digital media, the legal framework, introduction to mobile phone forensics, and online frauds.

Inspired by the success of Mumbai Cyber Lab, another lab was set up in August 2005 in suburban Thane, about 19 miles from Mumbai. The trainers from the two labs have conducted outstation programs in other states of India. As of November 2006, these two labs have trained 2,077 investigators. The concept has now been tried and tested and has evolved into a viable model known as India Cyber Lab. The new lab at Bangalore, inaugurated January 3, 2007, has been underwritten by a sponsor, the Canara Bank, on a request made by NASSCOM through the Indian Banks' Association. It is an exceptional example of different stakeholders working together. Another lab, in Pune, will be commissioned soon.

The infrastructure lends itself to alternative uses. The labs carry out occasional outreach programs for students of nearby schools, by making presentations about the dos and don'ts of online activities. Training programs on computer familiarization have also been held for children of police officers during school holidays.

India Cyber Lab Portal

It was clear after the first two Cyber Safety Weeks that computer users needed help, and this is being accomplished now through an Internet portal at www.indiacyberlab.in . Educational material is contained on this site and future plans include a discussion forum, where visitors to the site can post their queries and get replies from a panel of experts.

Communities of Practice

An important concept in fostering specialized knowledge is that of communities of practice.[13] Police in India are using mailing lists and discussion groups to disseminate the latest information about cybercrime trends and modus operandi and the latest articles on technology to concerned computer users. People who come from different backgrounds but have common concerns about a safe online experience can meet at the labs to ask questions, provide answers, and share experiences about computer safety. Another effort was forming eSecurity Clubs in engineering colleges to bring together students, faculty members, and outside experts in a structured environment to talk about how to protect information systems and stimulate interest in the area of security, which is seldom an engineering student's first choice as a career. These clubs are functioning in a few colleges in Mumbai.

A three-day workshop on best practices in technology crime investigation was held March 21–23, 2006, when a four-member team from the Technology Crime Division of the Hong Kong Police visited Mumbai and conducted the workshop attended by over 40 investigators from all over India. There are plans to continue this advanced training activity in the future.

The attempt to reach out to the law enforcement community has been structured at two levels. Top decision makers attend half-day seminars designed to provide an executive overview of the issues in cybersecurity. Investigators receive in-depth training during longer, six-day programs that are more hands-on in nature. Police leadership in most of the larger states in India has now been exposed to the issues of an effective response to cybercrime.

What began as an experiment in public-private partnership between law enforcement and the Indian IT industry has evolved and matured in a movement with great potential for transforming the way the Indian police perceive and use technology and how disparate stakeholders can work together to foster the atmosphere of trust. The plan now is to create an ecosystem where mutually complementary groups work together to deal with cybercrime and keep

it under acceptable limits. The partnership will continue to promote capacity building in law enforcement as well as specialization and community building in the IT industry in major IT centers and metropolitan areas. ■

Top

1 George L. Kelling and James Q. Wilson, "Broken Windows: The Police and Neighborhood Safety," *The Atlantic Monthly* (March 1982), www.theatlantic.com/doc/prem/198203/broken-windows , December 26, 2006.

2 International Monetary Fund, "Globalization: Threat or Opportunity," IMF Issues Brief, April 12, 2001, www.imf.org/external/np/exr/ib/2000/041200.htm#II , December 24, 2006.

3 Thomas Friedman, *The World Is Flat: A Brief History of the Twenty-first Century* (New York: Farrar, Straus and Giroux, 2005).

4 NASSCOM, *Strategic Review 2006: The IT Industry in India*, www.nasscom.in/upload/34530/Exe_summry_feb_07.pdf , December 24, 2006.

5 McKinsey, *NASSCOM-McKinsey Report 2005: Extending India's Leadership of the Global IT and BPO Industries*, www.mckinsey.com/locations/india/mckinseyonindia/pdf/NASSCOM_McKinsey_Report_2005.pdf , December 24, 2006.

6 Booz Allen Hamilton, "Information Security Risk a Top Concern among Outsourcing Executives," March 23, 2006, www.boozallen.com/services/services_article/1876648? , December 25, 2006.

7 "Indian Telecom Sec Poised for Further Growth in '07," *Economic Times* (December 25, 2006), http://economictimes.indiatimes.com/News/News_By_Industry/Telecom/Indian_telecom_sec_poised_for_further_growth_in_07/articleshow/925061.cms , December 27, 2006.

8 John Ribeiro, "India Targets 500 Million Telephones by 2010," *InfoWorld* (May 25, 2006), www.infoworld.com/article/06/05/25/78665_HNindiatelephones_1.html?TELEPHONY , December 26, 2006.

9 BPO (business process outsourcing) firms are companies in less-developed countries such as India and China that handle information technology-enabled services (ITES) for companies in developed countries. Medical transcribing and credit card processing are among the more commonly outsourced ITES.

10 Mumbai Cyber Lab, *Be-Secure Newsline*, no. 1, www.nasscom.in/upload/48563/be_secure.pdf , December 26, 2006; and *Be-Secure Newsline*, no. 1, www.nasscom.in/Nasscom/Templates/NS-NewsLineLanding. aspx?id=49514 , December 26, 2006.

11 IRC (Internet Relay Chat) is a popular interactive service on the Internet that allows users to participate in real-time conversations.

12 NASSCOM, "India Cyber Cop Award 2005 Compilation of Cases," www.nasscom.in/Nasscom/templates/NormalPage.aspx?id=50576 , December 26, 2006.

13 Etienne Wenger, "Communities of Practice: Learning as a Social System," *Systems Thinker*, vol. 9, no. 5 (1998), www.co-i-l.com/coil/knowledge-garden/cop/lss.shtml , December 26, 2006.

Top

Return to Article