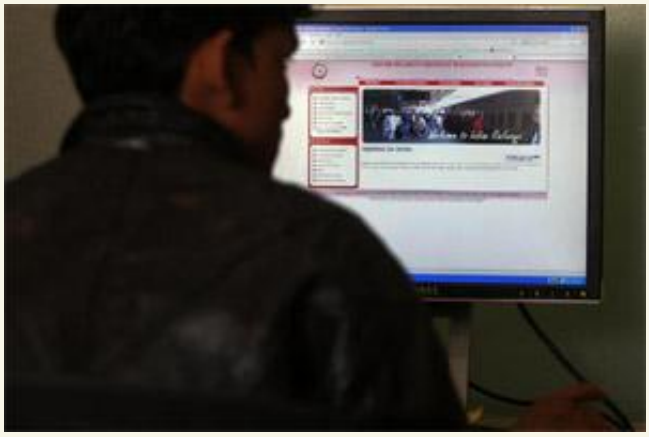
CYBERCRIME NCRB SYMANTEC IT ACT CERT-IN

Cybercrime on the rise, but not all cases getting reported

Cybercrime on the rise, but not all cases getting reported

Leslie D'Monte

First Published: Mon, Dec 19 2011. 12 53 AM IST



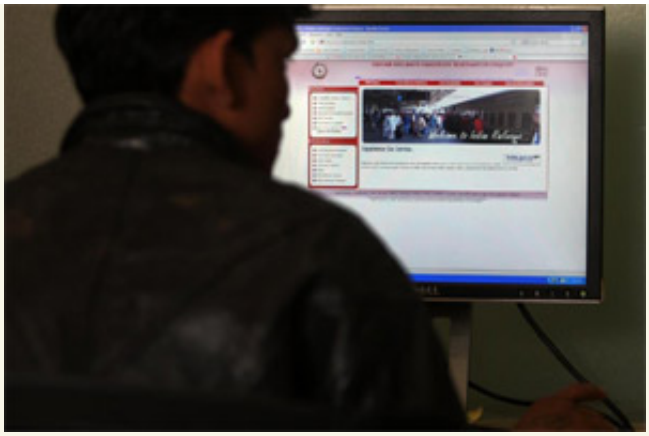
Updated: *Mon, Dec 19 2011. 12 53 AM IST*

Mumbai: Cybercrime is a big threat to India's online population, which loses billions to Internet fraud every year, but when it comes to reporting such cases, very few seem to come forward, if government records are anything to go by.

The police have recorded only 3,038 cases and made fewer arrests (2,700) between 2007 and 2010, under both the Information Technology (IT) Act as well as the Indian Penal Code (IPC).

And only three convictions have taken place, according to lawyers.

Going by the latest available figures from the National Crime Records Bureau (NCRB), 966 cybercrime cases were filed under the IT Act, 2000, in 2010 and 420 in 2009. Of



these, 153 cases were reported from Karnataka, followed by Kerala (148), Maharashtra (142), Andhra Pradesh (105), Rajasthan and Punjab (52 each).

About one-third of the cases registered were related to hacking and 233 persons were arrested in 2010.

Under the IPC, 356 cybercrime cases were registered in 2010 and 276 cases in 2009. Maharashtra reported the maximum number of such cases (104), followed by Andhra Pradesh (66) and Chhattisgarh (46).

A majority of these crimes were either forgery or fraud cases. Although such offences fall under traditional IPC crimes, they had "cyber-overtones", according to NCRB.

"These numbers give us a false sense of security," said cyber law expert and Supreme Court lawyer Pavan Duggal. "They fall way short of the reality. For every 500 cybercrimes that take place, only 50 are reported to the police and just one gets registered as an FIR (first information report)," Duggal said.

Another cyber law expert Na Vijayashankar, who runs cyber law information portal Naavi, also said the number of registered cases appears to be very low. "There's no organized method of collecting information from states, because of which these numbers do not reflect reality," he pointed out.

According to Duggal, the police continue to register some cybercrime cases under the IPC Act (and not the IT Act) since they're more familiar with the IPC. "There have been only three reported cybercrime convictions till date—two under the IT Act in Chennai and one under IPC in Delhi," he added.

"It is laughable that in 2010, India registered only 1,350 cases under the IT Act and IPC. It either shows that we are the most secure country in cyberspace, which is not true, or we do not take virtual crime seriously and thus do not file cases. We are sitting on a time bomb waiting to explode," said Vijay Mukhi, a Mumbai-based freelance consultant

who writes on Internet security.

The official cybercrime numbers also do not match the findings of security reports. For instance, the *Norton Cybercrime Report 2011*, released in September by research firm Symantec Corp., estimated that nearly 30 million people were victims of cybercrime in 2010, suffering $4 billion in direct financial losses and an additional $3.6 billion in time spent resolving the crime.

In India, four in five online adults have been a victim of cybercrime, according to the report.

RSA, the security division of EMC Corp., which released its findings on phishing attacks this month, estimated that Indian corporations lost $27.8 million in the first half of 2011. Phishing refers to attempts made to acquire information such as user names, passwords and credit card details by pretending to be a trustworthy entity.

The RSA report also ranked India as the third-most targeted country for phishing attacks after the US and the UK.

The NCRB statistics not only fly in the face of numbers from security vendors, but also from those retrieved from the Cert-In (Indian Computer Emergency Response Team) 2010 annual report. Under the IT (Amendment) Act, 2008, Cert-In is designated to serve as the national agency in the area of cyber security.

Statistics retrieved from Cert-In reveal that it tracked around 6.9 million bot-infected systems and 14,348 website defacements in India in 2010. It reported that around 6,850 .in and 4,150 .com domains were defaced during January-September 2011.

On 9 December, hackers broke into the official website of India's ruling Congress party and defaced the profile page of party president Sonia Gandhi with a pornographic message, according to an *AFP* report.

Experts such as Mukhi, Duggal and Vijayashankar, however, admit they have no way of corroborating how groups such as Norton publish the statistics as India has no "reliable" published data on cybercrime.

Symantec researchers maintain that credit cards and bank account credentials continue to be the top two advertised items on the black market. In the underground economy, bidding for credit card information starts at Rs 13 and that for bank account information at Rs 450, according to Symantec.And the average cost to resolve a data breach in 2010 was $7.2 million, according to Symantec researchers.

Cybercrime cover

The threat is set to increase. Research firm KPMG's *e-Crime Report 2011* cautions that the "the future of targeted malware delivery is also inextricably linked to social networking". Yet, just one company, Tata AIG General Insurance Co. Ltd, offers cybercrime insurance in India. It has been doing so for more than a year and has a portfolio of at least Rs 10 crore.

HDFC ERGO General Insurance Co. Ltd is hopeful of getting its product approved in a few months.

Tata AIG has around 50 policies in their portfolio and expects to add more customers. "With the pervasive and increasing use of networked computers to run business, cyber risks are growing exponentially. As businesses take to this insurance, either proactively or reactively, the market is expect to grow in line with the risk," Gaurav D. Garg, chief executive officer (CEO) and managing director of Tata AIG, said in an email response.

The claims have been "far and few", but Garg would not put a number to it, pleading confidentiality.

Cyber liability insurance addresses first- and third-party risks associated with e-business, the Internet, networks and informational assets. "The market is at a very nascent stage and we believe a right product will find takers as awareness of cybercrime insurance grows," said Ritesh Kumar, managing director and CEO of HDFC ERGO.

According to him, the product that the company has filed with the regulator will cover first-party losses and third-party legal liabilities.

Experts say it will take a while for Indian firms to freely register cybercrime cases for fear of their image suffering.

Sneha Shah contributed to this story.

leslie.d@livemint.com

First Published: Mon, Dec 19 2011. 12 53 AM IST