

A BUNCH OF LIES

DSCI DEBUNKS THE UNIVERSITY OF BRIGHTON'S 'CRIME ONLINE - CYBER CRIME AND ILLEGAL INNOVATION' STUDY

BY KAMLESH BAJAJ, CEO, DATA SECURITY COUNCIL OF INDIA

The University of Brighton's 'Crime Online - Cyber Crime and Illegal Innovation' report is not factual and is steeped in incorrect assumptions. A team of researchers, including professors of University of Brighton, published this report in July 2009 and since then, it has been a cause of outrage and concern for India. The study was picked up by online news channels and quoted in news items to propagate lies about cyber crimes in the BPO services industry of the country. The report tries to present data from the annual reports of the Indian Computer Emergency Team and Symantec, in a way that it projects India as a centre of cyber crimes. It also attempts to attack the outsourcing industry.

In this article, I would like to set the record

straight as far as some of the key charges are concerned.

To begin with, I would like to comment on the section titled 'Global Distribution of Cyber Crime'. The report notes that, "Cyber crime is a global industry, but the combination of poor economic opportunities and high skills is driving many developing regions to surface as major players in cyber crime." It states that most cyber attacks are directed at the US and the UK, even though the origin of phishing activities is also concentrated in a few international locations such as the US, Southern Asia and Eastern Europe.

According to the university's study and another report by Symantec, the US is still a major generator of malware, the country with the

most underground servers. It says that China is the focus of attention, when considering the future of cyber crimes. Russia, it adds is the original home of cyber crime, where high-tech skills are combining with a stumbling economy and a long tradition of organised crime. The report quotes the 'Sophos Security Threats Report of 2007-08', identifying the Top 10 countries hosting web-based malware. This report states that China is at the top, followed by the US, Russia, Ukraine, Germany, Netherlands, France, Poland, the UK and Canada. India does not figure in this list.

Where the country does figure, is the part that claims that the reported cases of spam, hacking and frauds in India have multiplied 50-fold during 2004-07. A close examination of CERT-In reports, however, reveals that the number of spam cases and phishing websites hosted in India is very small. Of the 2,565 security incidents reported in 2008, there were 604 phishing incidents. In 2007, these were 1,237 and 392, respectively. What do these numbers indicate? Even the growth in the incidents from 2007-08 is only four times, while the absolute numbers are insignificant on global scale of incidents.

It is instructive to examine the Microsoft Security Intelligence Report H2, 2008. It provides information about the worldwide distribution of phishing sites in percentages. India has 0.125-0.25 per cent – the same as Australia, with the US at 10 per cent, Russia between 5-10 per cent, and China at 2-5 per cent. In the case of malware hosting sites too, India is at the bottom, with 0.0001-0.16 per cent – even lower than Australia, with the US at 5-10 per cent, and China hosting malware in excess of 10 per cent.

Clearly, the facts tell a different story. India is neither a malware hosting country, nor does it figure anywhere as a phishing sites hosting country.

Elsewhere, the university study observes that "Brazil, Turkey, Poland, India and Russia are expected to increase their share of malicious activity, because they have a rapidly growing internet infrastructure. Countries that have a relatively new and growing internet infrastructure, tend to experience increasing levels of malicious activity, unless security protocols and measures are improved to control". This is a strange logic. What makes the researchers presume that India will not put in place 'security protocols and measures'?

Facts show, that Indian companies employ highly qualified manpower; put it through intensive training in data security; and

implement robust privacy and security policies, which are constantly monitored for compliance. The delivery centres are physically secured, and appropriate technology solutions are deployed to isolate customer networks. Employees are put through stringent background checks at the time of hiring, while the operational area is kept under electronic surveillance.

Finally, the report states that Russia, Brazil and China are world leaders in cyber crimes. It also observes that, "India, Russia and Brazil share a light regulatory regime, an acceptable IT infrastructure and a relatively weak state". This statement is unwarranted and needs to be strongly condemned. India has a strong data protection regime under the Information Technology (Amendment) Act, 2008, along with several other enactments such as the Indian Penal Code. There are specific clauses like Section 43A and 72A in the IT Act, 2008, that mandate implementation of reasonable security practices, while processing personal information, and any disclosure of personal information without consent of the data subject, constitutes a breach that attracts penal and civil liability, including compensation and imprisonment. India is certainly not a banana republic.

NASSCOM has set up the Data Security Council of India (DSCI) as a self-regulatory organisation to promote best practices in data security and privacy through the development of appropriate standards; training IT-BPO companies, helping them implement best practices and go for data protection certifications. NASSCOM has also set up the National Skills Registry (NSR), to enroll manpower deployed in the IT-BPO industry, conduct background checks on professionals, and store their biometric information. These initiatives by the industry along with the implementation of the amended IT Act strengthens the data protection regime ensure that India remains a trusted destination of choice for global sourcing.

The mischievous statements made by the authors in the report are totally unfounded, and deserve to be strongly rejected.

NASSCOM has set up the Data Security Council of India (DSCI) as a self-regulatory organisation to promote best practices in data security and privacy, through the development of appropriate standards; training IT-BPO companies, helping them implement best practices and go for data protection certifications.

"Cyber crime is a global industry, but the combination of poor economic opportunities and high skills is driving many developing regions to surface as major players in cyber crime."

'Crime Online - Cyber Crime and Illegal Innovation', University of Brighton