


[Home](#) | [Shopping](#) | [Find a job](#) | [Newsletter](#) | [Feedback](#) | [Advertise - Online](#) | [Help](#)



 Search

Web dqindia.com

[Search by issue](#) | [Sitemap](#)

CIOL Network Sites

ADVERTISEMENT



Action canceled

Internet Explorer was unable to link to the Web page you requested.
The page might be temporarily unavailable.

To print: [Click Here](#) **Best Printed on HP LaserJet's**

This story was printed from Dataquest at <http://dqindia.ciol.com>

Do you want to receive FREE weekly Information Technology updates by email?

Sign up for our newsletters at <http://www.ciol.com/content/newsletters>

Article Title: Cyber Crimes @ Web 2.0

URL: <http://dqindia.ciol.com/makesections.asp/07051005.asp>

Section: Focus

Author Name:

Author Email:

December 2006: The Economic Offences Wing (EOW), Crime Branch, Delhi Police, unearthed a major phishing scam involving fake emails and websites of UTI Bank. An analysis of the accounts of the four arrested Nigerian nationals indicated financial transactions of over Rs 1 crore in an eight-month period till December 2006. This indicates the estimated amounts involved. Investigations revealed that the scam is multi-layered with pan-India and international characteristics.

This is the direction in which cyber crimes are increasingly moving, a marked shift from the unorganized and casual cyber crimes of two years back, driven more by vindiction or some casual fun. As cyber crime graduates to the Web 2.0 level, it's sophisticated and lethal.



Crime Statistics

As per the National Crime Records Bureau statistics, during the year 2005, 179 cases were registered under the IT Act as compared to 68 cases during the previous year, thereby reporting a significant increase of 163.2% in 2005 over 2004. During 2005, a total of 302 cases were registered under IPC sections as compared to 279 such cases during 2004, thereby reporting an increase of 8.2% in 2005 over 2004. NCRB is yet to release the statistics for 2006. In 2006, 206 complaints were received in comparison with only 58 in 2005, a 255% increase in the total number of complaints received in the Cyber Cell/EOW over the last year. In terms of cases registered and investigated in 2006 (upto 22.12.06), a total of 17 cases, where the computer was the victim, a tool or a repository of evidence, have been registered in the Cyber Cell/EOW as compared to 12 cases registered in 2005. And mind you, these are just the reported cases.

While the number of cyber crime instances has been constantly growing over the last few years, the past year and a half, in particular, has seen a rapid spurt in the pace of cyber crime activities. Cyber lawyers, Pavan Duggal, advocate with the Supreme Court of India and Karnika Seth, partner, Seth Associates, Advocates and Legal Consultants, testify to this, pointing out that they have seen a jump in the number of cyber crime cases that they've been handling in the last one year. One also should remember that the term 'Cyber Crime' should be applied to all offences committed with the use of 'Electronic Documents'. Hence, cyber crimes must grow at the same rate as the use of the Internet, mobile phone, ATM, credit cards or perhaps even faster.



"With the little offences came the larger ones involving huge money, and one has seen this sudden jump from smaller crimes to financial crimes in the last one year"

-Karnika Seth,
partner, Seth
Associates,
Advocates and Legal
Consultants

According to Captain Raghu Raman, CEO, Mahindra Special Services Group (SSG), the contributing factors are high volume of data processing, rapid growth and major migration into the online space, especially of financial institutions and their customer transactions.

However, actual numbers continue to elude, considering the fact that a majority of the cases go unreported. Most victims, especially the corporates, continue to downplay on account of the fear of negative publicity thereby failing to give a correct picture of the cyber crime scene in the country. According to Cyber law expert Na Vijayashankar (popularly known as Naavi), it is difficult to measure the growth of Cyber Crimes by any statistics, the reason being that a majority of cyber crimes don't get reported. "If we, therefore, focus on the number of cases registered or

number of convictions achieved, we only get diverted from real facts," he adds. Duggal points out to the results of a survey he conducted in early 2006 on the extent of under-reporting. For every 500 instances of cyber crimes that take place in India, only fifty are reported and out of that fifty, only one is registered as an FIR or criminal case. So, the ratio effectively is 1:500 and this, he points out, are conservative estimates. Giving an insight into the reasons for low reporting, Nandkumar Sarvade, director, Cyber Security and Compliance at Nasscom, points out that very often, people are not aware whether an incident is a cyber crime; there is also lack of awareness on where to lodge a complaint or whether the police will be able to understand. "Added to this is the fear of losing business and hence, many cases don't come to light," he adds.

Changing Face of Crime

The last year has seen a quantum jump not only in the quantity and quality but also the very nature of cyber crime activities. According to Naavi, a perceptible trend being observed is that cyber crimes are moving from 'Personal Victimization' to 'Economic Offences'. SD Mishra, ACP, IPR and Cyber Cell, Economic Offences Wing, Delhi Police concurs that the cases that are now coming up are more related to financial frauds. As opposed to obscenity, pornography, malicious emails that were more prevalent in the past, now credit card frauds, phishing attacks, online share trading, etc. are becoming more widespread. As Seth points out, initially, when the Internet boom began, certain crimes were noticeable and cyber stalking was one of the first ones. "However, with the little offences came the larger ones involving huge money and one has seen this sudden jump from smaller crimes to financial crimes in the last one year," she adds.

As per the statistics of the Economic Offences Wing of Delhi Police, 21 complaints were received for phishing as compared to none in 2005. The number of complaints received for online share trading increased from three in 2005 to 22 in 2006 and those that were received for credit card fraud increased from one in 2005 to 17 in 2006. Complaints for job scam also emerged for the first time in 2006 with altogether five complaints received by the EOW during the year.

Consequent to this trend is the emergence of organized cyber crime in the country. According to Mishra, "There is evidence abroad of organized crime moving into the cyber space abroad. And, it's started to show here in India as well. Another trend is the emergence of organized gangs for credit card theft, usage and organized gangs for money laundering," he adds.

The convergence of cyber crime, money laundering, contraband trade and terrorism is a logical play out of the scenario.

Considering that cyber crimes are becoming more of financial frauds, they are increasingly targeted toward corporates as opposed to earlier focus on individuals. Duggal feels that over 77% of the cyber crimes today are targeted at corporates. The sophisticated crimes that can be expected in the banking and financial sector involve tampering of software to siphon off money from "Expenses Account" in the form of "Salaami Attacks". In the e-Governance sector where tax collections could be misappropriated. In fact, web threats are more pervasive and one of the fastest growing threat vectors.

Turning Professional

As the face of cyber crime is changing, so is the hand behind it. Findings from the McAfee Virtual Criminology Report 2006 reveal how organized crime is grooming a new generation of high-flying cyber criminals using tactics akin to those employed by the KGB to recruit operatives at the height of the cold war. The second annual McAfee report into organized crime and the Internet, with input from Europe's leading hi-tech crime units and the FBI, suggests crime gangs are targeting top students from leading academic institutions to provide them with the skills they need to commit hi-tech crime on a mass scale.



Kartik Shahani, director, Sales, India and Saarc, McAfee points out the trend of the emergence of cyber crime activities by internal employees and ex-employees. "We have been seeing external entities hacking into the system, namely intrusion and stealing critical data. However, now a lot of the cyber crime activities are happening from inside, namely extrusion," he explains.

Riding on Web 2.0

Web 2.0 is bringing in more interactivity and collaboration on the Internet and it's the users who are increasingly driving the content. Social networking sites and blogging have been some of the key fall-outs of that.

With the quantum of exposure and reach that it can provide, Web 2.0 is becoming a fertile ground for cyber crimes, which are slowly graduating to the Web 2.0 era and beginning to pervade its applications. "The Web 2.0 cyber crimes are a notch above the existing cyber crimes and further refined," explains Duggal.

Gearing Up Legally

Indian law for cyber crimes is embodied in ITA-2000 (Information Technology Act-2000). The Act is weak in the sense that it does not cover the entire gamut of cyber crimes. However, its flexible enough to make any offence in any other statute such as IPC to be also recognized if the offence is committed with the use of electronic documents. The law is therefore as strong as any other law in India.



"It's the implementation and not the law which is the major issue"

-Captain Raghu Raman CEO, Mahindra Special Services Group

"One perceptible trend that can be observed is that cyber crimes are moving from 'Personal Victimization' to 'Economic Offences'"

-Na Vijayashankar, Delving on her experience with the cases that she's been handling, Seth points out that for crimes which can't be covered under the IT Cyber law expert Act, cyber lawyers can resort to the IPC, CrPC, Evidence Act and can find some provision to resort to as most of the cyber crimes are online and electronic manifestations, and counterparts of crimes in the offline word.

While there have been amendments proposed and is currently pending before the parliament, experts are not much satisfied with them. According to Naavi, "What we need to take note of is that even where the IT Act-2000 was strong, the proposed amendments will make it weaker. It is unfortunate that MCIT is trying to create a false impression that the amendments are meant to strengthen the law while it is in fact having an opposite effect," he adds.

For instance, Section 66 of ITA 2000 is a comprehensive clause which makes "Diminishing of value of information residing inside a comp uter" by any means, by any person is an offence, with three years imprisonment. The offence is recognized even when the offender is having no "intention" but is "negligent". The section, therefore, had the potential of goading IT workers into being more "responsible".

However, now the proposed amendments besides reducing the imprisonment to two years and making it "Non Cognizable" and "Compoundable" also introduce the condition that the offence will be recognized only if it is committed "dishonestly" and "fraudulently". This will give a huge escape route for any criminal who can plan his cyber attacks with some finesse.

Similarly, the ITA-2000 recognized the importance of intermediaries to act responsibly if cyber crimes are to be controlled. Hence, it had made "intermediaries" liable unless they exercise due diligence". "Due Diligence" would be a concept, which would again promote voluntary cyber law compliance and adoption of information security practices. The proposed amendments however state that "Intermediaries shall not be liable under any law (including IPC), unless they have conspired and abetted or fails to remove an offending information after receiving a notice from an appropriate government agency.

According to Seth, the proposed amendments were prepared at a time when the MMS scandal, etc were ripe and hence they've been prepared in the context of the scenario at that time. Duggal suggests that the IT Act needs to incorporate some very general terms and provisions so that new instances can be easily covered under the broad umbrella.

While the legal framework will take its own time to strengthen, the focus should be currently on strengthening the enforcement of the law. According to Captain Raman, it's the implementation and not the law, which is the major issue. This becomes even more critical as cyber crime threatens to assume huge economic proportions.

Shipra Malhotra
shipram@cybermedia.co.in



"Almost over 77% of the cyber crimes today are targeted at the corporates"
-Pavan Duggal,
 advocate, Supreme Court of India

 Copyright (c) 1999 [CMIL](#) All rights reserved. Additional reproduction in whole or in part or in any form or medium without express written permission of CMIL is prohibited.

Send your questions to webmaster@ciol.com

[Close this window](#)